The Technology Adoption Model for Cloud Computing, Storytelling Artificial Intelligence, and the Federal Risk and Authorization Management Program

A Dissertation Presented in Partial Fulfillment of the

Requirements for the Degree of

Doctor of Computer Science

by

Freeman Augustus Jackson

School of Business and Technology, Aspen University

February 2024

Committee Members

Daniel Schilling Weiss Nguyen, Ph.D., DTM, Chair

Ebony Mason, Ph.D., Committee Member

Tony Robinson, DBA-MIS, Committee Member

APPROVED BY:

Committee Chair: Dr. Daniel Schilling Nguyen, PhD, Faculty Mentor

Committee Members:

Ebony Mason, Ph.D., Committee Member

Tony Robinson, DBA-MIS, Committee Member

ACCEPTED AND SIGNED:

X DocuSigned by: Daniel Nguyen 86B54FEF6FD749A...

Dr. Daniel Schilling Weiss Nguyen, PhD Dissertation Chair

2/9/2024 DocuSigned by: Daniel Nguyen 86B54FEF6FD749A... 2/22/2024

Dr. Daniel Schilling Weiss Nguyen, PhD Date

DocuSigned by: Daniel Zimmerman 07B85FF43D4C4E1... 2/22/2024

Dr. Daniel Zimmerman Date

Dean - School of Business and Technology

Abstract

This dissertation examines challenges and opportunities in federal government Conversational AI and Machine Learning (CAIML) integration. It emphasizes Conversational AI (CAI)'s impact on decision-making across sectors and its improvement of human-technology interactions, particularly in IoT and cloud computing. The study reviews AI storytelling, including NLP, character generation, VR/AR, deep learning, leadership, and FedRAMP compliance.

Qualitative research follows PRISMA and uses NVivo for data analysis. A comprehensive literature review, qualitative analysis, and expert interviews reveal CAIML adoption challenges and opportunities. Leadership, economic and legal factors, privacy, data protection, and national security are studied.

The dissertation concludes with a summary of its findings and research questions on federal agency CAI and ML adoption barriers, operational improvements, legal/regulatory issues, privacy, data protection, security threats, and effective leadership strategies. CAI and ML integration into federal infrastructure and national security and intelligence implications are also discussed.

The dissertation recommends federal agencies prioritize personnel training, migration planning, and solution sustainability to advance CAIML adoption. It helps federal policymakers and practitioners adopt CAIML technologies by highlighting their transformative potential and challenges.

KEYWORDS: CAIML Integration, Federal Government, Cloud Computing, Data Privacy and Protection, Leadership Practices.

Acknowledgments

I want to take this opportunity to thank everyone who has contributed to completing this dissertation.

First, I would like to thank Chair Daniel Nguyen, Ph.D., DTM, for his/her guidance, support, and feedback throughout the course of this research. His support and knowledge were instrumental in shaping my ideas and bringing my research to fruition.

In addition, I would like to extend my deepest gratitude to my family and friends for their unwavering support, understanding, and encouragement throughout this challenging and rewarding process. Their words of encouragement, knowledge, and support have been crucial in assisting me to maintain concentration and motivation.

Without the participants' participation in this research study, this dissertation would not be possible. I greatly appreciate their time and contribution to my research.

Lastly, I am grateful to the academic community and all the researchers who have contributed to my understanding and knowledge of the topic. Their research and publications have proven to be an indispensable resource for this dissertation.

Again, I would like to extend my deepest gratitude to everyone who has contributed to completing this dissertation.

Table of Contents

LIST OF TABLES

CHAPTER 1: INTRODUCTION

Background

Conversational artificial intelligence (CAI) has assumed the reins of decision-making in many business areas and innovative knowledge-oriented platforms in the current technological landscape. Despite CAI's long history, it continues to present difficulties. This field of technological progress has benefited notably from this innovative technology. Moreover, advancements in the disciplines of science and engineering, where the impact of this improvement may be seen, are more common when innovation is managed correctly. New machine learning (ML) methods and approaches are attracting interest for similar reasons as CAI. Although conversational artificial intelligence has been around for a while, only recently has it reached a level of reliability that allows us to label it as CAI confidently. Recent breakthroughs in CAI and ML have enormously contributed to developing new, more secure systems based on the Internet of Things (IoT) and cloud computing, Rath et al., (2021). This study shows an in-depth analytical analysis of the difficulties associated with using ML and CAI in IoT and Federal Cloud Computing environments. This study introduces a process called CAIML, which merges CAI & ML with Innovation Diamonds (Reunanen et al., 2020; Ferguson, n/d; Hawryszkiewycz,2020; Ojeda, 2023; Schleith, 2022; Ojeda, 2021).

The US National Security Agency and other intelligence groups face the necessity of policy and acquisition agility, as outlined by Haney (2020), Schmidt et al. (2021), Hoadley et al. (2018), Krebs (2020), Stone (2021), and Talent, (2021). This requirement arises from the need to effectively respond to customer demands and navigate the intensifying pressures of the market. By strategically reallocating funds and leveraging technologies like Conversational AI and Machine Learning, as highlighted by Novak (2021), intelligence groups can bring about fundamental shifts

much-needed agility underscored by Allen et al. (2017), allowing for adaptive decision-making and improved responsiveness. The integration of Conversational AI and Machine Learning (CAIML) empowers intelligence groups to effectively meet evolving customer demands and address the complexities of the intelligence landscape.

Federal agencies can only realize the benefits of CAIML if they cultivate a culture of innovation and constant learning. For modernization to be successful, improvements must be made more frequently than once every decade. Instead, modernization is in flux and is critical to any organization's normal technical infrastructure operations. To foster a culture of continuous improvement, agency leadership must prioritize personnel training and education, rigorous migration planning, and finding a balance between solution sustainability and the acquisition of new skills. Government agencies will have to revise their policies and technical guidance, and business continuously needs to react to new requirements, drive acceptable outcomes, and prevent the inevitable obsolescence of their IT portfolio (Medaglia et al., 2023; Kent, 2019).

The field of artificial intelligence, particularly the relationship between humans and technology, is undergoing significant transformations. The advancement in natural language acquisition, interpretation, and utilization has paved the way for various technologies and applications. Conversational Artificial Intelligence (CAI) has emerged as a groundbreaking development in human-computer interaction (HCI) through the integration of machine learning, deep learning for graphs, and natural language processing (Sundar & Liao, 2023; Grigera et al., 2023; Rangapur & Wang, 2023; Ray, 2023; Kusal et al., 2022). These studies highlight conversational agents as a prime example of AI systems that mimic natural language. Their comprehensive review delves into various aspects of conversational agents, including implementation options such as XML/DOM and Deep Learning for Graphs, as well as the diverse information security responsibilities associated with story agents. The study also explores how

storytelling agents can replicate human behavior by incorporating emotions, sentiments, and affect. Additionally, the authors investigate deep learning approaches and public datasets utilized by storytelling agents while also identifying research gaps and forecasting the future of this field.

The cited studies collectively contribute to the understanding of the transformative impact of CAI and its implications for human-computer interaction, user interface design, information security, and storytelling capabilities. These advancements in AI have opened new possibilities for conversational agents and have significant implications for various domains and future directions in the field of artificial intelligence.

Even though large language models are advantageous for agency leadership, the industry typically only considers the corpus of pre-trained flat text data (Veres, 2022; Li et al., 2021; Carenini, n/d). This misalignment may cause management to have erroneous expectations regarding the organization's realized benefits, the timeline for a CAI and ML transformation, and the agency's federal cloud presence structure. As the rate of CAI and ML adoption increases, indicating that technology diffusion is racing to catch up and meet information diffusion (Novak, 2021) parity, the true capability of an organization for cloud adoption and digital transformation lies with leaders who leverage CAIML to their advantage. CAIML facilitates the negotiation of organizational inertia and unanticipated market obstacles, which are frequently addressed too late in the CAI ML implementation process (Jackson, 2021).

Due to organizational, political, and geographical complexities, the transfer to the cloud for federal cloud computing (FedRAMP) presents problems. There was a lack of study on the steps FedRAMP officials should take to ensure the success of cloud adoption. Due to the ongoing evolution of cloud adoption methods, cloud products, and migration technologies, a leader must take informed action to maximize the cloud's benefits. Due to best leadership practices, FedRAMP

can adopt CAI & ML in a sustainable manner that produces actual business benefits by employing storytelling AI technologies.

Statement of the Problem

The problem statement revolves around the challenges and opportunities in cloud computing adoption within the federal government, with a particular emphasis on the economic, legal, and categorization aspects (Ash & Hansen, 2022; Park & Kim, 2022; Mukhamediev et al., Federal). The federal government's IT infrastructure is plagued by inefficiencies stemming from disjointed resource needs, redundant systems, challenging management settings, and extended procurement lead times, leading to inadequate public service delivery (Kundra, 2011). The exponential growth of cloud computing has resulted in increased data consumption and generation, necessitating cloud computing enterprises to embrace new intellectual property to keep up with the demands of the evolving landscape (Ash & Hansen, 2022; Park & Kim, 2022; Mukhamediev et al., Federal).

In addition to these challenges, security concerns related to Large Language Models (LLMs) must be addressed, requiring informed decision-making and effective leadership. LLMs, while offering immense potential, raise privacy and data protection issues that require careful consideration (Henderson et al., 2023; Lukas et al., 2023; Belgodere et al., 2023; Huang et al., 2023). Leaders, including CEOs and decision-makers, play a critical role in understanding the internal and external factors that impact their firms and industries, enabling them to make informed and effective cloud-related decisions (Aarestrup et al., 2020; Blau, 2020). Federal government leadership should proactively address the complexity of regulatory frameworks such as FedRAMP, which poses challenges to cloud conversion, and leverage automation advancements to streamline the process (Panda et al., 2023).

The problem statement seeks an efficient solution that addresses the economic, legal, and categorization aspects while ensuring data protection, privacy, and regulatory compliance within the cloud computing infrastructure. Effective leadership and decision-making are critical to navigating the complexities associated with cloud adoption and LLM security concerns (Henderson et al., 2023; Li, Qi, et al., 2023; Li, Tan, et al., 2023; Lukas et al., 2023; Belgodere et al., 2023; Huang et al., 2023; Carranza et al., 2023; Yu et al., 2023; Gupta et al., 2023; Ding et al., 2023; Kabra & Elenberg, 2023; Hewage & Madusanka, 2022). Additionally, the research approach involves qualitative analysis utilizing PRISMA guidelines for systematic review and NVivo Version 14, a software developed by QSR International (2023), ensuring a rigorous and comprehensive investigation of the challenges and opportunities in CAIML adoption within the federal government. The problem statement asserts the critical imperative for leaders within the federal government to proactively adopt privacy-preserving techniques and innovative approaches to address the security concerns associated with Large Language Models (LLMs) in the context of cloud computing adoption. By utilizing the rigorous PRISMA and NVivo methodologies, this research guarantees the generation of reliable and insightful findings, empowering leaders with the knowledge needed to make informed decisions that prioritize data protection and ensure regulatory compliance.

Statement of the Purpose

This dissertation aims to delve into the intricacies of adopting Cloud Computing, storytelling AI, and FedRAMP within the federal government. It focuses on evaluating the Technology Adoption Model in this context, offering a comprehensive analysis of various facets, including leadership strategies, economic and legal considerations, data privacy, and protection. The study utilizes qualitative analysis methodologies, including PRISMA guidelines for systematic review and NVivo (Version 14) software for data analysis, to ensure a rigorous and

comprehensive examination of the challenges and opportunities associated with Conversational AI and Machine Learning (CAIML) adoption. By exploring the integration of Conversational AI and Machine Learning into federal infrastructure, it aims to contribute significantly to national security and intelligence, highlighting the importance of continuous learning and innovation in government agencies.

Significance of the Problem

The problem holds significant importance and has implications in multiple domains, encompassing national security, ethics, cybersecurity, geopolitics, and communication. The incorporation of artificial intelligence (AI), particularly Large Language Models (LLMs), into national security strategies and intelligence analysis, is acknowledged as a crucial necessity (Mikhailov, 2023). Nevertheless, the utilization of AI in intelligence analysis and counterterrorism gives rise to ethical concerns (Blanchard & Taddeo, 2023; Esmailzadeh, 2023).

Furthermore, LLMs and generative AI pose substantial security hazards, as indicated by Derner and Batistiÿ (2023) and Grinbaum and Adomaitis (2023). Implementing advanced technologies, such as AI, requires improved cybersecurity protocols (Oxford Analytica, 2023).

Moreover, the geopolitical aspects of artificial intelligence, specifically in Central Asia and in addressing Chinese aggression, enhance the importance of this issue (KÜÇÜKSOLAK & FIRAT, 2023; Pathak & Jindal, 2023). The utilization of artificial intelligence (AI) in hybrid and information warfare presents novel obstacles.

The examination of AI-powered manipulation and its capacity to generate influential propaganda highlights the significance of comprehending and tackling synthetic influence (Burtell & Woodside, 2023; Goldstein et al., 2023). These citations highlight the importance of the problem, emphasizing the requirement for thorough research and knowledgeable decision-making

to tackle the ethical, security, geopolitical, and communicative consequences linked to conversational AI and machine learning in the cloud.

Research Question

The primary objective of this dissertation is to investigate the adoption of CAIML in the cloud within the federal government, focusing on the challenges and opportunities associated with this integration. To address this objective, the following research questions have been formulated:

1. What are the key challenges faced by federal government agencies in the adoption of Conversational AI and Machine Learning in the cloud?
2. How can the integration of Conversational AI and Machine Learning enhance the efficiency and effectiveness of federal government agencies' operations and decision-making processes?
3. What are the economic implications of adopting Conversational AI and Machine Learning in the cloud for federal government agencies?
4. What are the legal and regulatory considerations that need to be addressed in the adoption of Conversational AI and Machine Learning in the cloud within the federal government?
5. What are the privacy and data protection concerns associated with the use of Large Language Models (LLMs) in Conversational AI and Machine Learning applications?
6. How can federal government agencies effectively address the security risks and vulnerabilities related to the use of LLMs in Conversational AI and Machine Learning?
7. What leadership practices and strategies are required to successfully implement Conversational AI and Machine Learning initiatives in the federal government?

8. How can federal government agencies ensure a smooth migration and integration of Conversational AI and Machine Learning technologies into their existing infrastructure?
9. What are the implications of adopting CAIML for national security and intelligence analysis within the federal government?
10. How can federal government agencies cultivate a culture of innovation and continuous learning to support the successful adoption of Conversational AI and Machine Learning in the cloud?

These research questions will guide the investigation and analysis of various aspects related to the adoption of CAIML in the federal government. They encompass the economic, legal, regulatory, security, leadership, and national security dimensions of the research topic, providing a comprehensive understanding of the challenges and opportunities associated with this integration.

By addressing these research questions, this dissertation aims to contribute to the existing knowledge base, provide insights into the effective adoption of CAIML in the federal government, and offer recommendations for policymakers, leaders, and practitioners in leveraging Conversational AI and Machine Learning to enhance operational efficiency and decision-making processes within the federal government agencies.

Scope

The scope of this dissertation is focused on examining the challenges and opportunities associated with the adoption of Conversational AI and Machine Learning (CAIML) in the cloud within the federal government context. The research will utilize a qualitative approach, employing the PRISMA guidelines for systematic review and NVivo (Version 14) software for data analysis.

The study will primarily concentrate on federal government agencies and their adoption of CAIML technologies. It will consider agencies at various levels and across different domains within the federal government, aiming to provide a comprehensive understanding of the adoption landscape. The research will encompass a range of perspectives, including policymakers, leaders, and practitioners involved in the decision-making, implementation, and management of CAIML initiatives.

The geographical scope of the research will focus on the United States federal government, considering the unique regulatory and policy environment in which these agencies operate. The study will explore the specific challenges and opportunities that arise within this context, providing insights that are relevant to the federal government's adoption of CAIML technologies.

The timeframe for the research will encompass the most recent developments in CAIML adoption within the federal government, with a focus on the past decade. By examining recent advancements, the study aims to provide up-to-date insights into the current state of CAIML adoption and its implications for federal government operations.

It is important to note that the research will not delve into the technical intricacies of specific CAIML algorithms or models. Instead, it will take a broader perspective, focusing on the challenges and opportunities associated with the adoption and integration of CAIML technologies within the federal government.

The research methodology, based on PRISMA and NVivo (Version 14), will enable a systematic review and qualitative analysis of relevant literature and data. By utilizing PRISMA guidelines, the study ensures a rigorous and comprehensive examination of the existing body of knowledge. NVivo software will facilitate data analysis, allowing for in-depth exploration and interpretation of qualitative data.

This dissertation's scope is to analyze the adoption challenges and opportunities of Conversational AI and Machine Learning (CAIML) in cloud environments within the U.S. federal government. Emphasizing a qualitative approach, it employs PRISMA guidelines for systematic review and NVivo (Version 14) for data analysis. The study focuses on various federal agencies, gathering diverse perspectives from policymakers, leaders, and practitioners. It contextualizes these insights within the specific regulatory framework of the U.S. federal government. The timeframe of the research encompasses the latest decade, capturing recent CAIML advancements without delving into the technical details of specific algorithms. By utilizing PRISMA and NVivo, the research ensures a thorough and systematic exploration of CAIML adoption, aiming to inform and guide federal decision-makers and implementers in this technological domain.

Limitations

While conducting research on the adoption of CAIML in the federal government, it is important to acknowledge potential limitations that may impact the study. These limitations include those presented in the subsections that follow.

Limitation 1: Availability and Selection of Studies

Availability and Selection of Studies: The limitations of the study may arise from the availability and selection of relevant studies. Despite conducting a comprehensive literature search, some relevant studies may be missed or inaccessible, which could potentially limit the scope and generalizability of the findings.

Limitation 2: Bias and Quality of Included Studies

Bias and Quality of Included Studies: The quality and bias of the included studies can impact the validity and reliability of the findings. Despite adhering to PRISMA guidelines, variations in study quality, design, and reporting may introduce potential limitations in terms of data quality and the overall strength of evidence.

Limitation 3: Limited Data Types

Limited Data Types: NVivo (Version 14) software primarily focuses on qualitative data analysis. While it offers robust tools for analyzing text-based documents and qualitative data sources, it may have limitations in handling other types of data, such as quantitative data or data from specific formats that are not compatible with NVivo.

Limitation 4: Interpretation and Subjectivity

Interpretation and Subjectivity: The process of coding and categorization in NVivo (Version 14) involves subjective interpretation by the researcher. This subjectivity could introduce biases and impact the consistency of coding and analysis, potentially influencing the outcomes and interpretations of the study.

Limitation 5: Generalizability

Generalizability: The findings and conclusions drawn from the systematic review and qualitative analysis may have limitations in terms of generalizability. The studies included in the analysis might have been conducted in specific contexts or settings, which may limit the generalizability of the findings to broader populations or different contexts.

Limitation 6: Time and Resource Constraints

Time and Resource Constraints: Conducting a systematic review and qualitative analysis using PRISMA and NVivo (Version 14) can be time-consuming and resource-intensive. The availability of time, resources, and access to relevant literature and software tools could impact the depth and breadth of the analysis.

Discussion of Limitations

It is essential to acknowledge these limitations and discuss their potential impact on the study's outcomes and conclusions. Providing a transparent and honest assessment of the

limitations demonstrates the researcher's awareness of the potential constraints and enhances the overall credibility of the study.

Delimitations

The delimitations of this dissertation outline the specific boundaries and constraints within which the research will be conducted. These delimitations help to define the scope of the study and provide clarity on what will not be included or addressed. The delimitations for this research are as discussed in the subsections that follow.

Delimitation 1: Federal Government Context

The study will specifically focus on the adoption of CAIML in the cloud within the federal government. It will not include other sectors or organizations outside the federal government context.

Delimitation 2: Qualitative Research Approach

The research methodology will be based on qualitative analysis, utilizing the PRISMA guidelines for systematic review and NVivo (Version 14) software for data analysis. Quantitative methods or other research approaches will not be employed in this study.

Delimitation 3: Time Frame

The research will primarily focus on the most recent developments in CAIML adoption within the federal government, mainly in the past decade. Historical perspectives beyond this time frame will not be extensively explored.

Delimitation 4: Geographical Scope

The study will mainly examine the adoption of CAIML within the U.S. federal government. While insights from international contexts may be utilized for comparative analysis, the primary focus will be on the U.S. federal government.

Delimitation 5: Strategic and Leadership Perspective

The research will primarily investigate the challenges and opportunities associated with CAIML adoption from a strategic and leadership perspective. Technical aspects of CAIML algorithms or models will not be extensively explored.

Delimitation 6: Data Sources

The study will primarily rely on published literature, reports, case studies, and other relevant sources available in the public domain. It may not include proprietary or classified information that is not publicly accessible.

Delimitation 7: Generalizability

The findings and conclusions of this research may not be generalizable to all federal government agencies or other contexts beyond the specific scope of this study. The results should be interpreted within the context of the federal government's unique requirements, policies, and challenges.

Discussion of Delimitations

By setting these delimitations, the study aims to maintain focus, provide a clear scope, and ensure that the research is conducted within manageable boundaries. These delimitations also help to define the specific contribution and relevance of the research to the field of CAIML adoption within the federal government context.

Assumptions

This section outlines the underlying beliefs and premises upon which the research is based. These assumptions provide a foundation for the study and shape the researcher's perspective. The assumptions for this research are discussed in the subsections that follow.

Assumption 1: Availability of Sufficient and Relevant Data

It is assumed that there will be a reasonable quantity of existing literature, reports, case studies, and other relevant sources available in the public domain that address the adoption of CAIML in the cloud within the federal government context. The research will rely on these sources to gather insights and information for analysis.

Assumption 2: Accuracy and Reliability of Data

It is assumed that the information obtained from the selected sources will be accurate and reliable. The research will critically evaluate the credibility and validity of the data sources to ensure the integrity of the findings and conclusions.

Assumption 3: Compliance With Research Ethics

The research assumes that all necessary ethical considerations will be followed throughout the study. This includes obtaining appropriate permissions, ensuring the protection of personal information, and adhering to ethical guidelines for data collection, analysis, and reporting.

Assumption 4: Generalizability of Findings

The research assumes that the findings and conclusions derived from the study will provide insights and recommendations applicable and valuable to federal government agencies within the defined scope. However, it is acknowledged that the specific contexts, policies, and challenges of individual agencies may vary, and therefore the generalizability of the findings may be limited.

Assumption 5: Openness and Cooperation of Participants

The research assumes that federal government agencies and their stakeholders will be open and willing to provide information and insights relevant to the study. It is anticipated that key individuals—including policymakers, leaders, and practitioners—will be cooperative and forthcoming in sharing their experiences and perspectives.

Assumption 6: Technological Advancements

The research assumes that the existing technological infrastructure and advancements regarding CAIML within the federal government will provide a suitable foundation for the analysis. It is anticipated that the technology landscape will support the integration and adoption of CAIML, allowing meaningful insights and recommendations to be generated.

Assumption 7: Continuity of Policies and Regulations

The research assumes that the policies, regulations, and frameworks relevant to CAIML adoption within the federal government will remain relatively stable during the research period. Any significant changes or shifts in policies may impact the findings and conclusions of the study.

Discussion of Assumptions

These assumptions guide the research process and shape the researcher's perspective. They are acknowledged as inherent in the study and provide a framework for conducting the research within reasonable boundaries and expectations.

Summary

CAI has become prevalent in various industries and platforms, driving advancements in technology (Rath et al., 2021). The combination of CAI and ML has led to the development of more secure IoT and cloud computing systems (Rath et al., 2021). These technological advancements have enabled businesses to make more informed decisions and improve their operations.

The adoption of CAIML in the federal sector has gained popularity due to the need for policy and acquisition agility in intelligence agencies (Haney, 2020; Schmidt et al., 2021). The ability to respond to customer needs and navigate market pressures has become crucial for these agencies (Haney, 2020). Strategic allocation of funds and the utilization of technologies like CAIML can significantly impact spending and growth in intelligence groups (Novak, 2021).

CAIML offers agility, improved decision making, and enhanced responsiveness in the intelligence landscape (Allen et al., 2017).

To benefit from CAIML, federal agencies must prioritize personnel training, migration planning, and solution sustainability while fostering a culture of continuous improvement (Medaglia et al., 2023). Constant updates to policies, technical guidance, and business needs are necessary to meet new requirements and achieve desired results (Kent, 2019).

The evolution of human–technology relationships has been influenced by AI, particularly in the context of natural language acquisition, interpretation, and use (Sundar & Liao, 2023). CAI combines ML, deep learning for graphs, and NLP to revolutionize human–computer interaction (Sundar & Liao, 2023). Storytelling agents, which mimic human behavior by incorporating emotions and sentiments, have been developed using deep learning methods and public data sets (Grigera et al., 2023).

The advancements in CAIML have opened new possibilities for conversational agents and have significant implications across various domains (Sundar & Liao, 2023). However, the adoption of LLMs in the industry typically focuses on pretrained flat text data, leading to misalignment in understanding of the benefits and transformation timeline (Veres, 2022). Effective leadership that utilizes CAIML can help organizations successfully adopt cloud computing and drive digital transformation (Novak, 2021).

The adoption of cloud computing in the federal government faces economic, legal, and categorization challenges, along with concerns about data privacy and protection (Ash & Hansen, 2022; Park & Kim, 2022). The integration of CAIML in the federal government's cloud infrastructure requires informed decision making and effective leadership to address these challenges (Henderson et al., 2023).

Research questions have been formulated to guide the study of federal government CAIML adoption, covering various aspects such as barriers, economic implications, legal issues, privacy concerns, leadership, and national security (Belgodere et al., 2023; Henderson et al., 2023; Huang et al., 2023; Li, Tan, et al., 2023; Li, Qi, et al., 2023; Lukas et al., 2023). The study aims to contribute to the existing knowledge base, provide insights into effective adoption strategies, and offer recommendations for policymakers and leaders in federal government agencies.

This dissertation focuses on the challenges and opportunities of cloud based CAIML adoption in the federal government, using qualitative research methods such as systematic review and data analysis with PRISMA guidelines and NVivo (Version 14) software. The study specifically examines federal agencies' adoption of CAIML, primarily within the context of the U.S. federal government. The study covers the past decade of federal CAIML adoption and does not extensively explore the technical details of CAIML algorithms or models. The research findings aim to aid federal government policymakers and practitioners in decision making and implementation associated with CAIML technologies.

Cloud computing adoption, particularly the integration of CAIML, presents both challenges and opportunities for the federal government. The adoption of CAIML can drive improvements in operational efficiency and decision making in federal agencies. However, economic, legal, regulatory, security, and leadership aspects must be considered for successful adoption. The research aims to address these issues and provide insights and recommendations for federal government agencies. The study's scope is limited to the U.S. federal government's adoption of CAIML, and qualitative research methods will be employed to ensure comprehensive and rigorous analysis.

CHAPTER 2: LITERATURE REVIEW

Literature Review

A review of the literature was conducted, which involved searching more than 1,300 online sources for information and documentation on the use of storytelling AI by FedRAMP. These sources included academic journals, conference proceedings, and various reports, accessed through extensive searches in databases such as Google Scholar, IEEE Xplore, and the ACM Digital Library. The specific methodologies employed in this literature review are detailed in the document, including the NVivo (Version 14) software coding themes for cloud computing adoption, storytelling AI integration, and FedRAMP compliance (Appendices D, F, G) and the PRISMA flowchart diagram and checklist (Appendices H, I).

Storytelling AI

Introduction

The field of AI has opened new possibilities for storytelling, and researchers have explored various applications and implications of AI in this domain. Several studies have examined the integration of AI in storytelling, highlighting its potential to revolutionize the creation and narration of stories (Fotedar et al., 2020; Riedl et al., 2011). The use of AI in virtual reality environments and its impact on inducing emotions through AI characters have also been explored (Pyjas et al., 2022; Santiago et al., 2023). Large generative AI models like OpenAI's ChatGPT have significantly advanced AI-driven storytelling (Gartner, n.d.). However, it is essential to recognize the limitations of these models and explore alternative solutions (Gozalo-Brizuela & Garrido-Merchan, 2023). The ethical implications of AI in storytelling have also been a subject of discussion, emphasizing the need for responsible and ethical practices (Blanchard & Taddeo, 2023).

Furthermore, the collaboration between humans and AI in data storytelling has been investigated (Li, Wang, Liao, & Qu, 2023). Li, Wang, Liao, & Qu (2023) conducted interviews to gain insights into human–AI collaboration in data storytelling, shedding light on the challenges and complexities of this partnership. In addition to AI's impact on storytelling, integration of AI into national security strategies has also been explored.

(Mikhailov, 2023, "Artificial Intelligence Integration") and (Mikhailov, 2023, "Optimizing National Security Strategies") highlighted the strategic importance of AI integration to national security, emphasizing the need to optimize national security strategies through AI-driven approaches. The ethical considerations of AI in intelligence analysis and counterterrorism have also been examined (Esmailzadeh, 2023; Grinbaum & Adomaitis, 2023).

Adopting AI in various sectors, including government organizations, presents challenges. Cloud adoption in the government sector is a complex area that requires careful consideration of factors such as organizational culture, change management, and management support (Carney, 2019; Diaz, 2022; Hall, 2019). Understanding the barriers to cloud adoption and exploring strategies for successful migration can facilitate the effective adoption of cloud technologies in government contexts (Griffith, 2020; Hall, 2019).

Furthermore, AI integration's potential risks and implications in storytelling, national security, and other domains have been examined. Researchers have investigated privacy concerns, legal frameworks, cybersecurity threats, and the dual-use nature of AI (Belgodere et al., 2023; Fotedar et al., 2020; Pizzo et al., n.d.). Understanding and addressing these risks and challenges are essential to harnessing the benefits of AI while mitigating potential negative consequences.

In conclusion, integrating AI in storytelling, national security, and government sectors presents opportunities and challenges. Researchers have explored various aspects of AI integration, including generative models, human–AI collaboration, ethical considerations, risk

management, and legal frameworks. Further research is needed to advance the understanding of these areas and develop responsible and practical approaches to AI integration in diverse domains.

Technological Components

The field of storytelling AI has rapidly evolved in recent years, with technology playing a crucial role in creation of engaging and interactive story experiences for audiences. To understand the structure of technology for storytelling AI, it is vital to examine the various components that work together to create a seamless and personalized story experience. This section provides an overview of the various components that make up the technology structure of storytelling AI.

Data Collection and Analysis.

Data collection and analysis are essential components of storytelling AI, as they provide the foundation for personalizing each user's story experience. Storyboarding AI systems can tailor a story experience to each user's specific needs and preferences by collecting data on user behavior, preferences, and emotions. This makes the story more engaging and personalized, making the experience more memorable. Data collection and analysis are crucial in developing and applying storytelling AI. Data collection and analysis have been used in gaming to develop a story-generation suspense system (Cheong & Young, 2014).

Similarly, in the field of phenomics, the application of AI has been informed by data collection and analysis (Nabwire et al., 2021). In infectious disease big data analytics, AI has been used to analyze copious quantities of data collected from various sources (Wong et al., 2019). In the study of AI models such as GPT-3, data collection and analysis have been used to analyze a model's ability to inform better than humans (Spitale et al., 2023) and its potential as a general-purpose technology (Guidetti, 2023). The feasibility of using AI in public health has also been explored through data collection and analysis (Jungwirth & Haluza, 2023). Data collection and analysis have also been used to study AI governance and the law of AI for good (Lobel, 2023;

Simonÿiÿ & Jerele, 2023). Data collection and analysis have also informed the principles and practices of trustworthy AI (Li, Yang, Islam, & Ren, 2023). In the field of extensive web archive collections, data collection and analysis have been used to inform the development of infrastructure and services (Wang, 2023). In the field of NLP, data collection and analysis have been used to develop deep learning techniques for abstractive text summarization of low-resourced languages (Shafiq et al., 2023) and end-to-end transformer-based models in textual-based NLP (Rahali & Akhloufi, 2023). In conclusion, data collection and analysis play a crucial role in developing and applying storytelling AI, informing the development of AI models and techniques, and shaping the future of this field.

The NLP Engine.

The NLP engine is a crucial component of storytelling AI, as it processes and understands the language used in storytelling. This includes text to speech, speech recognition, and sentiment analysis, which allow AI systems to generate and understand speech, text, and emotions. This is a crucial component of storytelling AI, as it enables the creation of interactive and engaging stories. NLP is a crucial component of storytelling AI, as it allows an AI system to understand, interpret, and generate human language. The NLP engine is responsible for processing and analyzing copious amounts of text data, which forms the basis for the AI system's ability to generate stories. Numerous studies and research efforts have been aimed at improving the NLP engines used in storytelling AI. For example, Onyalo (2022) conducted a study to improve the efficiency of student query handling using an AI chatbot. Singh and Singh (2022) analyzed the RASA and Dialogflow Chatbot frameworks. Dale (2022) discussed the importance of investing in NLP technology, while Fan et al. (2023) examined the psychometric properties of machine-inferred personality scores in AI chatbots. Papadopoulou (2022) conducted a study on developing and evaluating a chatbot, while Imperial (2022) built a knowledge-based chatbot for customer support. Laudy et al. (2022)

explored the use of collective intelligence in building probabilistic causal models. These studies demonstrate the ongoing efforts to improve the NLP engines in storytelling AI to enable AI systems to generate stories that are more humanlike and capable of engaging their audiences.

Character Generation and Animation.

Character generation and animation play a vital role in storytelling AI, as they bring the story to life by creating digital characters that can interact with the audience. This adds realism and engagement to the story, making it feel like it is taking place in a living, breathing world. By generating animations for the characters, storytelling AI systems can make a story more immersive and interactive, allowing the audience to feel like they are part of it. Character generation and animation are essential components of storytelling AI. In recent years, researchers have been exploring ways to use AI to generate characters and animations that can be used in different storytelling contexts. For example, Pataranutaporn et al. (2021) explored the use of AI-generated characters to support personalized learning and well-being. They found that AI-generated characters can be used to personalize learning experiences, positively impacting well-being. Latif et al. (2022) evaluated various procedural content generation approaches for digital twins and found that AI can create unique and diverse characters for storytelling. Chen et al. (2022) used visual planning and token alignment to create character-centric story visualizations. They found that this approach can help to make stories more engaging and interactive. Amato et al. (2019) discussed the use of AI in the media and creative industries, including character generation and animation.

Short and Adams (2019) also discussed procedural storytelling in game design, which includes character generation. Cavazza et al. (2002) and Charles et al. (2001) explored character-based interactive storytelling. They found that AI-generated characters can play a significant role in interactive storytelling, helping to create engaging and dynamic stories. Cheng et al. (2020)

performed a review of literature on generative adversarial networks, which can be used to generate characters and animations. Freiknecht and Effelsberg (2017) surveyed the procedural generation of virtual worlds. They found that AI can be used to create diverse and dynamic characters and animations for storytelling. These studies show that character generation and animation are essential components of storytelling AI, and that AI can create unique, diverse, and engaging characters for use in different storytelling contexts.

Dialogue Generation.

Dialogue generation is another critical component of storytelling AI, as its focus is on generating conversations and interactions between characters in response to user inputs. This makes a story more immersive and interactive, allowing the audience to feel part of it. By generating dynamic and personalized dialogue, storytelling AI systems can create a more engaging and personalized story experience for each user. In storytelling AI, dialogue generation is crucial to character-based interactive storytelling. Generating believable and engaging dialogues requires the consideration of numerous factors such as character personality, style, and context. Cavazza and Charles (2005) explore dialogue generation in character-based interactive storytelling, examining the challenges of generating meaningful and coherent dialogues in this context. Akoury et al. (2023) focus on grounded dialogue generation in video game environments, where the context and environment play a critical role in determining the content of dialogue. Xu (2022) explores stylistic dialogue generation based on character personality in narrative films, highlighting the importance of considering character personality in dialogue generation. Biermann et al. (2022) discuss the relationship between AI writers and human story writers in dialogue generation, emphasizing the need for AI writers to respect personal values and writing strategies. Lee et al. (2022) examines the empathy in dialogues generated by the GPT-3 model, proposing a novel in-context example selection method and automatic evaluation metric for empathetic

dialogue generation. Amjad et al. (2023) present EMP-EVAL, a framework for measuring empathy in open-domain dialogues, which is crucial for generating engaging and emotionally resonant dialogues. Zhu and Luo (2023) explore the use of generative transformers for design concept generation, another application of dialogue generation in storytelling AI. Finally, Safovich (2019) presents a study of abstractive narrative generation, which involves generating a narrative from a set of given input data, highlighting the challenges and opportunities in this area. In conclusion, generating engaging and meaningful dialogue is a crucial aspect of storytelling AI, and myriad studies have been conducted to address the challenges and opportunities in this area.

Virtual and Augmented Reality Technologies.

Virtual and augmented reality technologies play a crucial role in storytelling AI, as they create immersive and interactive environments for stories to take place in. This adds realism and engagement to a story, making it feel like it is taking place in a living, breathing world. By using virtual and augmented reality technology, storytelling AI systems can create more immersive and interactive story experiences for audiences, allowing them to feel like they are part of the stories. Virtual and augmented reality are increasingly being utilized in storytelling, providing an immersive experience for users. Virtual and augmented reality technologies allow users to enter a digital world and interact with artificial environments and objects, making them ideal for storytelling. For example, Noh and Shin (2022) studied virtual and augmented reality in libraries, using these technologies to activate a library and improve user engagement. Qian (2022) investigated the use of virtual reality technology in digital media art creation, focusing on its application in teaching methods. In service-experience research, Kozinets (2023) proposed using “immersive netnography,” which involves using virtual and augmented reality technologies to study service experiences in virtual, augmented, and metaverse contexts. Alshammari et al. (2022) conducted a systematic review of robotics and AI in automatic vision-based assessment systems,

exploring the potential of these technologies for shaping the future of virtual and augmented reality. Anand and Kumar (2022) discussed the rise of AI in video games and the potential for these technologies to create new and innovative gaming experiences. Mystakidis (2022) defined the metaverse as a shared virtual space where users can interact and experience a new reality. Trichopoulos et al. (2023) surveyed computational and emergent digital storytelling, exploring recent technologies such as virtual and augmented reality to enhance the storytelling experience. Finally, Koohang et al. (2023) discussed the opportunities, challenges, and future research relating to shaping the metaverse into reality, highlighting the role of virtual and augmented reality technologies in shaping the future of storytelling.

Emotion Recognition and Simulation.

Emotion recognition and simulation are critical components of storytelling AI, as they use AI and ML to recognize and respond to the emotional state of an audience, as well as to generate and simulate emotions for the characters in the story. This makes the story more engaging and emotional, making the audience feel more connected to the characters and the story itself. Emotion recognition and simulation allow storytelling AI systems to create a more personalized and engaging story experience for each user. Emotion recognition is an essential aspect of storytelling, as it allows the creation of more personalized and engaging narratives. Wang et al. (2023) discuss the use of social robots in personalized storytelling, where the robots use emotion recognition to adapt a story to a listener's emotions. De Lope and Graña (2023) provide an ongoing review of speech emotion recognition, highlighting the advances in the field and the challenges that still need to be addressed. Jarrahi et al. (2023) examine the role of AI in the workplace, including its potential for emotion recognition and its implications for workers. Semeraro et al. (2023) present EmoAtlas, a tool that combines psychological lexica, AI, and network science to create an emotional profile of individuals. Lavi (2023) discusses the ethical implications of manipulating emotions using AI,

highlighting the need for regulation. In conclusion, the use of emotion recognition in storytelling has the potential to enhance the narrative experience, but it also raises important ethical considerations that need to be addressed.

Personalization and Adaptation.

Personalization and adaptation are vital components of storytelling AI, as their focus is on the use of data and algorithms to personalize each user's story experience, adapting to their preferences, behavior, and emotions. Personalization and adaptation in storytelling AI is a growing field of research that aims to create more engaging and effective storytelling experiences. The goal is to provide users with personalized narratives that adapt to their preferences, moods, and contexts. Personalization and adaptation can be achieved using data science, ML, and AI technologies. Göbel and Wendel (2016) have studied the concept of personalization and adaptation in serious games and provide an overview of the critical challenges and opportunities in this field. Göbel and Mehm (2013) have also explored the use of personalized, adaptive digital educational games that use narrative game-based learning objects to enhance learning experience. In recent years, the development of AI technologies has led to significant advances in personalization and adaptation in storytelling. For example, De Benedictis et al. (2023) proposed a transformer-based approach for choosing actions in social robotics that can personalize and adapt to individual users. Anoir et al. (2022) studied personalization in adaptive e-learning and explored how data science can be used to design user interfaces that are more personalized and adaptive. Wen et al. (2021) investigated the use of electronic science games to enhance cognitive ability through personalization and adaptation. Baraka et al. (2020) have developed an extended framework for characterizing social robots that can be used for personalization and adaptation in storytelling. Axelsson et al. (2022) explored the use of robots as mental well-being coaches and provided ethical recommendations for their design and use. Alves-Oliveira et al. (2019) conducted a field study of

an empathic robot for group learning and found that personalization and adaptation can enhance the learning experience. In conclusion, personalization and adaptation in storytelling AI is a rapidly evolving field that offers new opportunities for the creation of more engaging and effective storytelling experiences. AI technologies like ML and data science provide new ways to personalize and adapt narratives to individual users, leading to more meaningful and memorable storytelling experiences.

Deep Learning with Graphs.

Deep learning with graphs has emerged as a prominent area of research, offering new opportunities for modeling, and analyzing complex relational data. Jiang (2022) provides a comprehensive survey of the application of graph-based deep learning in communication networks. The survey explores various graph neural network architectures and their applications in network optimization, anomaly detection, and traffic prediction tasks. It also discusses this domain's challenges and open research questions, including those relating to scalability, interpretability, and handling of dynamic networks.

Text representation and classification using graph-based deep learning techniques have gained significant attention in NLP. Pham et al. (2022) present a survey that explores the utilization of deep learning and graph-based approaches for text representation and classification. The survey discusses different graph construction methods, graph-based representation learning algorithms, and their integration with deep learning models. It highlights the advantages of graph-based representations for capturing semantic relationships between words and documents, improving performance in tasks such as sentiment analysis, document classification, and text summarization. The survey also identifies challenges, including the scalability of graph-based models and the need for interpretability in text classification.

Roshanfekr et al. (2023) propose an approach for learning graphs from graph signals using sensitivity analysis over a deep learning framework. The approach focuses on inferring the underlying graph structure based on the observed signals. By exploiting graph sensitivity, the method aims to capture the relationships between graph nodes and their influence on the signals. The proposed framework combines deep learning techniques with graph-based analysis to enable efficient learning of graph structures from data. The study demonstrates the approach's effectiveness for reconstructing graph structures from various signals. It highlights potential applications in domains such as social network analysis, recommendation systems, and biological networks.

Combining ML with the semantic web has gained significant interest recently. Breit et al. (2023) conducted a systematic mapping study to explore integration of ML techniques with the semantic web. The study surveys the existing literature, identifying different approaches and applications where ML and the semantic web intersect. It highlights the potential benefits of combining these two areas, such as enhancing knowledge representation, improving information retrieval, and supporting intelligent decision making. The mapping study also discusses challenges, including data integration, ontology learning, and explainability, providing insights into future research directions in this interdisciplinary field.

In summary, deep learning with graphs has shown great promise in various domains, including communication networks, text representation and classification, learning of graph structures, and combining ML with the semantic web. These studies provide valuable insights into the state of the art, challenges, and potential applications of graph-based deep learning approaches. As researchers continue to explore and innovate in this field, deep learning with graphs is expected to advance the ability to analyze and understand complex relational data, paving the way for AI and data-driven decision-making breakthroughs.

Risk Management

Risk management in the context of storytelling is an important aspect to consider when incorporating AI technology. Several studies and frameworks have been proposed to manage the risk associated with AI technology in storytelling. Tabassi (2023) proposed the AI risk management framework to provide guidelines for managing the risk associated with AI technology. This framework offers a structured approach with which to identify, assess, and mitigate risks specific to AI in storytelling, promoting responsible and ethical use of AI systems.

To operationalize responsible AI, Lu et al. (2023) introduced a pattern-oriented approach that emphasizes the incorporation of responsible practices throughout the AI development lifecycle. By integrating responsible AI principles and patterns into the development process, this approach aims to address ethical considerations systematically. Xia et al. (2023a) conducted a systematic mapping study of responsible AI risk assessment, highlighting the importance of evaluating potential risks and implementing safeguards to mitigate adverse consequences. Further, Xia et al. (2023b) explored AI risk assessment frameworks, underscoring the need for comprehensive methods to assess and manage AI-related risks.

In enterprise risk management, McGrath (2022) proposed an enterprise risk management framework tailored to designing proethical AI solutions. This framework takes a holistic approach by considering the organizational, legal, and ethical dimensions of AI risk management in storytelling. Rassolov and Chubukova (2022) discussed the legal framework for AI and effective governance, stressing the significance of establishing regulatory frameworks to protect stakeholders while fostering innovation in AI-driven storytelling.

CAI also improves local environmental risk management, as Clímaco et al. (2022) demonstrated. They showcased the application of CAI to providing real-time information and assisting decision-making processes related to environmental risks. Lütge et al. (2022) proposed a

risk-based assessment approach to AI ethics governance, offering a structured methodology for identifying, analyzing, and mitigating ethical risks associated with AI technologies. Barta and Görcsi (2021) highlighted the importance of risk management considerations for AI business applications, emphasizing the need for a proactive approach to identify and address potential risks early in the development cycle.

Considering the challenges associated with AI, privacy and security are critical concerns. Recent studies have focused on privacy-preserving techniques and the implications of AI models. Panda et al. (2023) explored differentially private in-context learning, addressing the privacy challenges in AI applications. Researchers such as Lukas et al. (2023) and Huang et al. (2023) investigated the leakage of personally identifiable information and the privacy implications of retrieval-based language models. These studies highlight the need for privacy-preserving approaches to protection of sensitive data when leveraging AI capabilities.

Ethical considerations and risks associated with AI technology have also been examined in the context of national security and intelligence analysis. Mikhailov (2023) emphasized the strategic imperative of AI integration for national security. Blanchard and Taddeo (2023) reviewed the ethics of AI for intelligence analysis, providing recommendations for addressing key challenges. Esmailzadeh (2023) explored the potential risks of ChatGPT in counterterrorism and international security, while Derner and Batistiÿ (2023) delved into the security risks of ChatGPT. Grinbaum and Adomaitis (2023) discussed the dual-use concerns relating to generative AI and LLMs.

Adopting and integrating AI technology requires collaboration, strategic planning, and geopolitical considerations. Pathak and Jindal (2023) highlighted the importance of collaboration for countering Chinese aggression in the AI race. Geer and Gaffney (2023) emphasized the need to establish conditions of engagement with machines to navigate the challenges and opportunities

presented by AI. Küçüksolak and Firat (2023) explored the geopolitics of AI in Central Asia, specifically examining the Russian and Chinese cases. Moy and Gradon (2023) discussed the role of AI in hybrid and information warfare, highlighting its dual-edged-sword nature.

AI's influence and persuasion capabilities have also been the subject of investigation. Burtell and Woodside (2023) analyzed AI-driven persuasion, shedding light on the potential impact of AI on influencing behavior. Goldstein et al. (2023) examined whether AI can write persuasive propaganda, exploring the implications and ethical considerations associated with AI-generated persuasive content.

In conclusion, managing the risks associated with AI in storytelling requires a multifaceted approach encompassing technical, ethical, legal, organizational, and geopolitical considerations. The frameworks, studies, and discussions highlighted in this synthesis provide insights and guidelines valuable for addressing risks and ensuring AI technology's responsible and ethical use in storytelling. Continued research and collaboration are crucial to further understanding of the implications and challenges of AI integration in various domains, such as national security, privacy, and ethical decision making.

Technical Insights

Technical insights into storytelling AI have been explored by several researchers and authors in recent years. The integration of AI into storytelling has been seen as the future of storytelling in the age of AI and post humanity, as stated by Tuncer (2020). Baiheng and Wen (2020) proposed rethinking AI storytelling in digital media, while Pierosara (2022) explored the concept of narrative autonomy and artificial storytelling in AI and society. Hermann (2021) examined the role of AI in fiction and its impact on narratives and metaphors. The integration of AI technology has also been studied in other fields, such as cloud security and supply-chain risk management (Ghaffar et al., 2019; Schroeder & Lodemann, 2021).

The adoption of AI technology has been studied in various industries and organizations, including business-to-business sales, small- and medium-sized enterprises, higher education institutions, and corporate social responsibility initiatives (Bettoni et al., 2021; Boukhari, 2021; Mohd Rahim et al., 2022; Pai & Chandra, 2022; Pillai et al., 2023). The use of AI in conversational web services has also been explored, focusing on run-time verification of behavioral conformance (Dranidis et al., 2009). Barros and Dumas (2006) also studied the rise of web service ecosystems. These studies provide valuable insights into the technical aspects of AI and its application in storytelling.

Why Artificial General Intelligence Fails

Artificial general intelligence (AGI) has long been a subject of interest and debate among researchers and experts in AI. Despite significant advancements in the development of AI technology, AGI remains a major challenge, and there are several reasons why it has yet to be achieved. One reason for the failure of AGI is the lack of quality criteria for the continuous evaluation and improvement of conversational agents, as highlighted by Lewandowski et al. (2023). They argue that establishing quality criteria is crucial for leveraging the potential of conversational agents and achieving AGI. Another reason is the challenge of integrating blockchains and intelligent agents, as Fluharty (2022) discussed. Integrating these two technologies is crucial for achieving AGI, but it is also challenging due to the complex nature of both technologies.

The safety issue in AI is also a significant concern, and Morales-Forero et al. (2022) argue that this is a principal factor in the failure of AGI. The development of safe AI is crucial for ensuring that AGI systems are not used for harmful purposes. The limitations of machine intelligence and the difficulty of achieving AGI are also recognized by Shevlin et al. (2019), who argue that despite progress in machine intelligence, AGI remains a significant challenge.

Landgrebe and Smith (2019) similarly argue that there is no AGI, and McPherson (2020) highlights the importance of psychometric AGI. Finally, the rule of algorithm and the rule of law are also critical factors in the failure of AGI, as discussed by Tasioulas (2023). Integrating these two concepts is crucial to ensuring that AGI systems are used ethically and responsibly. In conclusion, the failure of AGI is due to a combination of factors, including the lack of quality criteria, the challenge of integrating blockchains and intelligent agents, the importance of safety in AI, the limitations of machine intelligence, and the integration of the rule of algorithm and rule of law.

Research Gap

Research into storytelling AI has revealed a gap in understanding regarding how to create conversational agents that are both humanlike and effective at narrating stories. This gap is evident in studies such as those of Fotedar et al. (2020), who focus on the generative approach to story narration in AI, and Bringsjord and Ferrucci (1999), who explore the relationship between AI and literary creativity. Abdulmajeed and Fahmy (2022) conducted a meta-analysis of AI research in journalism. They found challenges and opportunities for future research in the field, while Dvorak et al. (2022) questioned the concept of explainable AI and its impact on AI adoption.

Fox (2022) highlights the importance of human survival principles in the shaping of ML world models, while Guenduez and Mettler (2023) analyze the narratives constructed in governmental AI policies. Kristensen and Andersen (2023) examine the role of leadership by principal officers in digital government, while Ganguly (2022) explores the future of investigative journalism in the age of automation and AI. Wang et al. (2022) focus on the role of human-centered AI systems in assisting with data-science code documentation, while Ahmad et al. (2022) proposes a framework for personality cues in conversational agents. Gkinko and Elbanna (2022a) analyzed AI chatbots' sociotechnical aspects and future directions, and in a separate study, Gkinko and

Elbanna (2022b) explored the appropriation of conversational AI in the workplace, developing a taxonomy of AI chatbot users.

These studies highlight the need for further research in the field of storytelling AI, specifically in the areas of humanlike conversational agents, explainable AI, and the impact of AI on various fields such as journalism, government, and data science.

Leadership

The burgeoning field of storytelling AI underscores the pivotal role of leadership as technology continues to advance and gain widespread adoption. In this context, Jajee et al. (2023) shed light on how leadership styles and strategies profoundly influence the strategic implementation of AI technology within organizations. Their study delves into the nuances of leadership dynamics in AI environments, emphasizing the necessity for leaders to adeptly navigate the myriad challenges and opportunities presented by AI in the workplace.

Complementing this perspective, Frangos (2022) conducted an integrative literature review, underscoring the critical role of leadership in fostering organizational readiness for AI. This review illuminates the significance of visionary leadership in promoting the adoption and effective implementation of AI technologies across various sectors. For instance, Harisanty et al. (2022) highlight the pivotal role of informed leadership in various industries, including libraries, in the successful deployment and utilization of AI. Their research underscores the need for a comprehensive understanding of AI, alongside strategic planning, to leverage AI for organizational advancement effectively.

The integration of AI into leadership roles also raises questions about the acceptance of AI-driven leadership solutions. Petrat et al. (2022) explore this phenomenon, focusing on individual perceptions such as trust in technology and sense of control. Their findings reveal the

considerable impact these personal attitudes have on willingness to embrace AI leadership within organizational contexts.

Amidst the growing prevalence of AI in organizational settings, De Cremer (2022) raises concerns about the potential risks to responsible leadership. The paper argues for a reevaluation of ethical standards and leadership practices considering AI's growing role in decision-making processes. This call for ethical vigilance is further echoed by Audibert et al. (2022), who delve into the evolution of AI and ML in the context of leadership, underscoring the need for a comprehensive understanding of AI's impact to guide its ethical integration into leadership roles.

The concept of E-leadership 2.0, which encapsulates the integration of AI in leadership, is gaining traction, as discussed by Song and Ford (2022). Their exploration of how AI is reshaping leadership landscapes highlights the emerging challenges and opportunities related to melding AI with traditional leadership practices. Similarly, Rüth and Netzer (2022) investigate the development of strategies for effective human–machine cooperation, providing a road map for synergistically integrating AI into leadership practices.

The exploration of AI in the context of data management and skill development is intricately tied to the evolution of leadership in this field. The work of Reddy et al. (2023) highlights the critical elements that bind leadership with AI, emphasizing strategic decision making and innovation management beyond mere technological expertise. Complementing this view, White and Bruton (2011) stress the importance of leaders strategically managing technology and innovation, including AI, to foster organizational growth. Whitlock and Strickland (2022) further emphasize the growing importance of data science skills for AI leaders, underscoring informed decision making based on robust data analysis, essential for steering organizations through AI complexities.

Wong (2021) expands on this by examining the research methodologies in AI and data governance, advocating flexible, responsive methods that align with the dynamic nature of AI governance. Similarly, Huygh (2021) explores the integration of data and AI governance, highlighting their interdependence and the need for a comprehensive management approach. Micheli et al. (2022) delve into AI ethics and data governance, particularly in the geospatial domain, emphasizing inclusive and ethical approaches in AI implementation.

Kroll (2018) addresses the gaps in governance and oversight in AI and data science, focusing on the need for accountability and ethical considerations in AI-driven systems. This is crucial for AI leaders' understanding of the ramifications of software-driven decision making. Ethan (2023) discusses the evolution of data governance in the banking sector, analyzing AI/ML technologies' integration and emphasizing the importance of ethical and responsible AI/ML use.

Furthering this discourse, Kanying et al. (2023) emphasize the significance of standard data analytics governance, advocating for concrete frameworks in organizations. Braga et al. (2022) propose a research approach for improvement of AI algorithm and data governance, while Giron (2023) presents a comparative analysis of public data governance and AI policies in key technological regions, offering diverse insights.

Lee and Darbellay (2022) advocate for standardized data governance in the financial sector, exploring the regulatory aspects of data governance in AI, fintech, and legal tech. AI (2019) underlines the importance of data quality in AI, highlighting data governance's role in effective AI use in organizations.

In conclusion, the effective implementation and adoption of AI, particularly storytelling AI, are fundamentally linked to leadership and governance. The collective insights from these studies underscore the need for continued research to understand AI leadership's impact on organizations and to identify best practices for responsible and effective leadership. As AI

continues to permeate various sectors, the need for leadership and governance in AI to evolve and adapt becomes increasingly apparent. These studies provide a comprehensive understanding of the challenges and opportunities in AI leadership and governance, highlighting the strategic and ethical approaches necessary for responsibly harnessing AI's potential.

Innovation

The field of storytelling AI is rapidly evolving, and numerous factors shape the innovation trajectory in this field. Research has explored the factors that influence the adoption of AI in organizations and how they affect the implementation of AI technology. Technology readiness and the organizational journey toward AI adoption are crucial for determining the success of AI implementation in storytelling (Uren & Edwards, 2023). Studies have investigated the impact of AI adoption on organizations, including the factors that determine AI adoption, such as complementary investments and research and development strategies (DeStefano et al., 2022; Lee et al., 2022). The effective adoption of AI principles is also influenced by employee perceptions (Kelley, 2022).

Geopolitical implications of AI and digital surveillance adoption have also been studied (Peterson & Hoffman, 2022), as has the role of procurement officials in leading AI adoption in the federal sector (Cooke, 2022). Additionally, the key enablers of and barriers to adoption of AI-based conversational agents have been modeled using interpretive structural modeling and MICMAC approaches (Choudhary et al., 2023). The impact of responsible AI adoption through private-sector governance has been investigated (Wiesmüller et al., 2023), and AI adoption in organizations has been linked to several factors, such as the key enablers of and barriers to AI adoption (Kurup & Gupta, 2022).

In conclusion, the innovation trajectory of storytelling AI is influenced by several factors, including technology readiness, organizational journey toward AI adoption, employee perceptions,

geopolitical implications, procurement, and responsible AI adoption through private-sector governance.

Adopting Innovation

The adoption of storytelling AI in organizations is a complex endeavor influenced by various factors including technological readiness, organizational culture, competitive dynamics, legal compliance, and public perception. The subsections that follow delve deeper into these aspects.

Technological and Organizational Readiness.

According to Uren and Edwards (2023), successful AI integration demands that organizations possess not only necessary technological infrastructure but also the appropriate organizational frameworks. This includes availability of hardware and software resources, data management systems, and network capabilities needed to support AI functionalities. Organizational readiness also involves having personnel skilled in AI and related technologies, along with processes and structures that support innovation and technological adoption. It is about creating an ecosystem within an organization that is conducive to exploring and implementing AI solutions.

Supportive Organizational Culture.

According to Rizk (2020), the culture of an organization significantly impacts its ability to adopt new technologies like AI. A culture that values innovation, encourages risk taking, and supports continuous learning is more likely to succeed at integrating AI. This means fostering an environment where experimentation with AI is encouraged, failures are seen as learning opportunities, and employees are motivated to develop new skills. The leadership's role in championing AI initiatives and driving a culture shift toward embracing technology is crucial.

Understanding the Competitive Landscape.

According to Alsheibani et al. (2020) and Gans (2022), an organization's approach to AI adoption is greatly influenced by its competitive environment. In a monopoly setting, the organization might face fewer competitive pressures but also fewer stimuli of innovation. Conversely, in a competitive market, the need to stay ahead might drive faster and more aggressive AI adoption strategies. Understanding these dynamics helps organizations tailor their AI strategies to their specific market conditions, ensuring they remain competitive and relevant.

Navigating Legal Liability and Compliance.

According to Stern (2022), legal issues pose significant challenges to AI implementation. Organizations need to consider the legal implications of AI, particularly regarding data privacy, intellectual property rights, and ethical considerations. This includes understanding and adhering to relevant laws and regulations, establishing clear policies on data use and AI ethics, and ensuring transparency in AI operations. Addressing these legal aspects not only aids risk mitigation but also builds trust among users and stakeholders.

Structured Innovation Frameworks.

Medaglia et al. (2023) argue that utilizing organized frameworks such as the diamond of innovation offers a methodical approach to navigating the process of adopting AI. These frameworks facilitate the progression of organizations through the stages of problem definition, idea generation, prototyping, and implementation, guaranteeing that the adoption process is systematic and in line with organizational objectives. By incorporating these frameworks with AI-specific procedures such as cloud computing, artificial intelligence, and machine learning, it guarantees that the distinct needs of AI technologies are effectively met.

Impact of Public Perception on AI.

According to Von Walter et al. (2022), public perception and lay beliefs about AI significantly influence its adoption. Organizations need to be aware of how their employees, customers, and the broader public perceive AI. Addressing misconceptions, building awareness about the benefits and limitations of AI, and fostering trust are key to successful AI integration. This might involve educational initiatives, transparent communication about AI projects, and efforts to showcase the tangible benefits of AI.

Summary of Adopting Innovation.

In sum, the adoption of storytelling AI in organizations is a complex endeavor that requires a holistic approach that takes into consideration technological capabilities, cultural readiness, market dynamics, legal compliance, structured approaches to innovation, and public perception. By carefully addressing these factors, organizations can navigate the complexities of AI adoption, leading to successful implementation and integration of AI into their operations.

FedRAMP

Introduction

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring of cloud products and services used by the U.S. federal government. The program was introduced in 2011 and has since been adopted by numerous agencies within the U.S. federal government (Taylor, 2014). FedRAMP aims to improve the security and privacy of the federal government's cloud computing services and provide a streamlined process for agencies to adopt cloud services (McLaughlin, 2020).

The program is based on the National Institute of Standards and Technology risk management framework. It includes security controls, authorization processes, and continuous monitoring requirements for cloud service providers (Risk, 2020). The FedRAMP program uses a

“do once, use many times” approach, meaning that once a cloud service provider has been authorized, other federal agencies can use their authorization (Warren & Sabetto, 2018, p. 8). The program also includes the use of third-party assessment organizations to assess and validate the security controls of cloud service providers (Alliance & Bureau, n.d.).

The FedRAMP program has been widely discussed in the academic and technology communities. Several studies have compared the program to other cloud security certification systems in different countries (Seo, 2012), analyzed its impact on the U.S. federal government’s move to cloud computing (McGillivray, 2016), and explored its potential for improvement (McLaughlin, 2020; Utin, 2015). Additionally, McGillivray (2021) provided an in-depth look into government cloud procurement. Various articles have also provided practical guides for FedRAMP compliance (Graf, n.d.; Walsh, 2018) and discussed the authorization of major cloud service providers under the program (Doubleday, 2019; Weber, 2019).

In conclusion, FedRAMP is essential for the U.S. federal government’s adoption of cloud computing services. The program provides a standardized approach to security assessment, authorization, and continuous monitoring, ensuring the security and privacy of cloud services used by the federal government. The program has been widely discussed and analyzed, and various resources are available to help organizations comply with FedRAMP requirements.

Leadership

Leadership is crucial to successful implementation of FedRAMP and to ensuring that AI technologies are developed, adopted, and utilized ethically and responsibly. According to Schwartz et al. (2022), leaders must prioritize identification and management of bias in AI. The public sector can also serve as a model for deployment of AI technologies, as noted by Nili et al. (2022). Kennedy (2022) highlights the importance of prioritizing technology leadership and innovation.

Governance and leadership in innovation are crucial aspects of deploying AI technologies and are discussed by Shark (2023). The implementation challenges of the three pillars of America's AI strategy is also explored by Lawrence et al. (2022). Omar (2022) highlights the importance of leadership to ensuring that America remains a leader in AI technology.

Naqvi and Janakiram (2022) discuss the importance of regaining America's leadership position in AI technology. Pierre (2022) explores the leadership of human–machine teams in military environments. These studies emphasize the importance of leadership to ensuring the successful implementation of FedRAMP and the responsible deployment of AI technologies.

The Mental Model

The use of mental models has become increasingly relevant in the context of FedRAMP, a framework for the security assessment and authorization of cloud computing services used by the U.S. federal government. Mental models refer to individuals' cognitive representations of phenomena and can significantly impact their perceptions and decision-making processes. In the context of FedRAMP, mental models can play a significant role in determining the success of implementation and organizations' adoption of AI technologies. Studies have shown that a managerial mental model is crucial to driving innovation in digital transformation (de Paula et al., 2023). A predictive algorithm for team mental model convergence can also help ensure effective collaboration and alignment within a team (Poozhithara et al., 2022). Stakeholder mental model alignment can also impact the performance of new product engineering teams (Krehbiel, 2022).

A mental-model-centric landscape of human–AI symbiosis can provide insights into the influence of human perceptions and beliefs on integration of AI technologies (Zahedi et al., 2022). A mental model-based trust theory can also be used to understand the trust dynamics between humans and AI systems (Zahedi et al., 2023). The influence of leadership and communication on

organizational learning can also be analyzed using an adaptive network modeling approach (Bouma et al., 2023).

Leadership is also a crucial aspect of ensuring the success of FedRAMP implementation. Extreme crisis leadership can help organizations navigate unpredictable situations and drive change (Casto, 2023). AI policy can also significantly shape the trajectory of AI adoption and implementation (Calo, 2018). In conclusion, mental models significantly shape the perception and decision-making processes related to implementation of FedRAMP and adoption of AI technologies. Understanding the mental models of stakeholders and leaders is crucial to ensuring the success of FedRAMP implementation.

Process

The processes of FedRAMP are an essential aspect of program. The program provides a standardized approach for the assessment, authorization, and continuous monitoring of cloud services utilized by the federal government. Accountability in the federal acquisition process is a crucial factor of ensuring the success of FedRAMP, as highlighted by Fox and Morris (2015). The federal government's budget reform process is critical for driving innovation and effectively implementing AI technologies. Phaup (2022) highlights the need for decision-makers to have an economic perspective in the budget reform process. Procurement officials play a vital role in leading the federal government's adoption of AI technologies, as outlined by Cooke (2022).

A risk-management model for the federal acquisition process is crucial to implementing FedRAMP. Ross (1999) provides a comprehensive model for the same. Preventing racial bias in AI is a crucial aspect of the FedRAMP process, as highlighted by Livingston (2020). The integration of AI agents in federal agencies is a significant aspect of the process, as Walker (2020) outlined. Ensuring trustworthiness of AI is an essential aspect of the FedRAMP process, as

discussed by Weaver (n.d.). The recognition of AI systems as inventors by federal courts is an essential aspect of the process, as outlined by Stoianoff (2021).

Federal data science is transforming government and agricultural policy through the use AI technologies, as highlighted by Batarseh and Yang (2017). The federal government's spending on AI is expected to top $6,000,000,000, as Harper (2021) outlined. The enhancement of information needed for contractor workplace safety is crucial for the FedRAMP process's success, as Woods (2019) discussed. Analyzing perceived and reported outcomes in federal contracting is a crucial aspect of the process, as discussed by Snyder (2021). Small business leaders' strategies for obtaining U.S. government subcontracts are a critical aspect of the FedRAMP process, as discussed by Dunbar (2019).

People

The burgeoning integration of AI into the workplace heralds a transformative era, presenting a complex interplay of challenges and opportunities that significantly affect employee dynamics. This transition underscores the need for a nuanced understanding and strategic approach to workforce management and development in the AI-infused industrial landscape.

Hur's (2022) research poignantly illustrates the need for improved job satisfaction among racial and ethnic minorities, a critical factor of retaining a diverse and inclusive federal workforce. This emphasis on diversity aligns with Malik et al.'s (2022) examination of the impact of AI within organizations governed by the principles of Industry 4.0, revealing the profound influence of AI on employee engagement and operational dynamics.

The evolving AI landscape necessitates a strategic focus on development of advanced skills and knowledge. Paÿko et al. (2022) advocate for a concerted effort to equip future industrial workers with proficiency in AI, the IoT, and edge computing. Echoing this sentiment, Jaiswal et al. (2022) emphasize the importance of upskilling employees, particularly in multinational

corporations, to adapt and thrive in an AI-driven environment. The federal government context, as explored by Engstrom et al. (2020) and Diaz (2022), further underscores the role of AI in workforce shaping and highlights the inherent challenges to cloud adoption. Carter (2022) contributes to this discourse by exploring the correlation between federal employees' work–life balance and their intention to leave, thereby underlining the broader human resource implications of AI deployment.

Chetty (2023) offers an innovative perspective by advocating for AI literacy among aging workers, positing that late-career employees can significantly contribute to the digital economy through AI training. This approach seeks to harmonize the rich experience of seasoned workers with the exigencies of modern digital work environments. Concurrently, Farrow (2022) presents a forward-thinking analysis of potential organizational scenarios shaped by varying human-to-AI workforce ratios, providing a framework for anticipatory workforce planning in an increasingly AI-centric world.

The potential for AI to redefine traditional job roles is a theme explored by Haran and Gangadharan (2022), who probe into the future landscape where AI might supplant human roles, raising questions about the extent of this technological ascendancy and its ramifications for human adaptability. Gehlhaus and Mutis (2021) offer a comprehensive view of the U.S. AI workforce, highlighting the critical balance between technical and nontechnical roles and the importance of fostering a diverse talent pool. Vogel (2021) adds depth to this conversation by emphasizing the need to consider the broader social, political, and economic contexts that shape technology workers, especially within the U.S. intelligence workforce.

Addressing policy implications, Heston and Arnold (2019) propose targeted immigration reforms and educational initiatives to bolster the U.S. AI workforce, recognizing the pivotal role of human capital in maintaining a competitive edge in AI. In a similar vein, Papadopulos and

Christiansen (2023) delve into the transformative effects of conversational AI platforms like ChatGPT on work roles and organizational structures within the IT industry, highlighting a dynamic shift in required skills and competencies.

Azah (2021) adopts a human-resource-management lens to examine the integration of AI and robotics in the workplace, exploring the implications for manpower and the reshaping of job roles. Walkowiak and MacDonald (2023) offer an evidence-based analysis of the risks associated with generative AI in the Australian labor market, quantifying worker exposure to AI and its associated risks. AbuMusab (2023) discusses the disruptive potential of generative AI technologies such as ChatGPT, which could render certain human labor roles obsolete. Eglash et al. (2019) propose an alternative economic model that leverages AI to sustain unalienated labor and environmental harmony. Huang et al. (2023) challenge the prevailing narrative of job losses due to AI by introducing AI augmentation as a metric with which to assess AI's influence across job roles, suggesting a more nuanced understanding of AI's impact on the labor market.

In summation, these studies collectively provide a comprehensive and multifaceted view of AI's impact on the workplace. They underscore the importance of strategic planning, skill enhancement, and informed policy development to navigate the challenges and harness the opportunities presented by AI across various sectors. This body of work serves as a foundational reference for stakeholders shaping a future in which AI is integrated into the workforce in a manner that is ethical, efficient, and enhances human potential.

Leaders

To excel as a leader in FedRAMP, one must possess a profound comprehension of technology leadership, governance of innovation, and the execution of AI strategy. Kennedy (2022) asserts that prioritizing offensive strategies in the pursuit of technological leadership is a key focus of the final competitiveness bill. Shark (2023) emphasizes the significance of

governance and leadership in driving innovation, underscoring the necessity for leaders to determine who is responsible for making crucial decisions in the realm of artificial intelligence and its societal impact. Leaders in FedRAMP must also effectively manage their dedication to innovation while addressing the ethical and societal consequences of AI. Lawrence, Cui, & Ho (2022) analyze the difficulties encountered in implementing the three fundamental aspects of America's AI strategy. This highlights the significance of leaders in FedRAMP in surmounting these obstacles. Furthermore, Lawrence, Cui, & Ho (2023) delve into the bureaucratic challenges to AI governance, particularly the empirical assessment of implementation at US federal agencies. Leaders must possess a comprehensive understanding of the potential risks and advantages linked to artificial intelligence (AI) and adeptly oversee the intricate process of AI integration. Somers (2022) examines the mutual exchange of leader and follower conduct within the context of federal employees and the influence of leadership on employee welfare. Leaders in FedRAMP must cultivate a workplace culture that is positive and inclusive, prioritizing the well-being and support of their employees.

Oates (2021) and Hylton (2021) investigate the correlation between leader empathy, emotional intelligence, and employee well-being within the context of federal employment. Leaders in FedRAMP must possess a deep understanding of their employees and demonstrate high levels of emotional intelligence to effectively lead and manage their teams. To summarize, being a leader in FedRAMP necessitates possessing a distinct combination of skills and qualities, such as a profound comprehension of technology leadership, innovation governance, and AI implementation. Additionally, it requires the capacity to cultivate a favorable workplace culture and proficiently oversee and guide employees.

Opportunities and Obstacles

The integration of AI within FedRAMP unfolds as a complex journey filled with both promising opportunities and formidable challenges. This multifaceted landscape necessitates a nuanced and strategic approach in governance and policymaking. Bachner (2022) emphasizes the crucial role of optimized analytics in enhancing AI's utility within FedRAMP, while Schwartz et al. (2022) identify management of bias as a significant challenge in AI implementation, particularly in high-stakes domains. Adding to this complexity, K. Walsh (2018) provides a practical checklist for FedRAMP requirements, underscoring the importance of rigorous compliance standards. Meanwhile, M. A. Walsh (n.d.) brings forth the ethical considerations required in AI usage, especially in sensitive military operations, highlighting the need for responsible AI practices.

The research by Al Batayneh et al. (2021) on integrating AI and big data in smart city development, exemplified by Dubai's case, parallels the governance challenges in federal AI settings. Selten and Klievink (2024) explore the strategic management of AI adoption in public organizations, identifying a critical balance between structural rigidity and the need for innovation and agility in AI integration, a concept crucial for federal agencies on their AI adoption paths.

In customer relationship management, Ledro et al. (2023) navigate AI integration challenges and offer guidelines vital for federal agencies. Complementing this, Wen et al. (2023) examines a multidevice edge AI system that integrates sensing, computation, and communication, providing strategic insights for AI deployment in federal network systems.

The human dimension of AI integration, highlighted by Fox et al. (2023), reveals the essential human labor involved in AI system implementation. This aspect is crucial for federal agencies to incorporate into their AI strategies. The legal and ethical discourse is further expanded by Novelli (2023), who proposes the concept of legal personhood for AI systems, a notion with

significant implications for AI governance and policy in federal agencies (Verma, 2020; Verma, 2022).

Mohanty et al. (2023) offers insights into the integration of IoT and AI in education, providing valuable guidance for federal training and development programs. Rosenthal and Simmons (2023) emphasize the importance of autonomous agents in AI integration across diverse applications, proposing adaptable strategies for federal agencies. Shorey (2023) advocates for organizational and communication-based solutions to AI challenges in federal settings.

Bodemer's (2023) comprehensive analysis of AI integration in the German government provides a comparative perspective, offering a model U.S. federal agency could use to enhance efficiency and innovation while upholding transparency and accountability.

The deployment of AI across various sectors—particularly in the military, public sector operations, and cybersecurity—presents a landscape rich in complexity and strategic depth. Mattila and Parkinson (2019) advocate use of a nuanced and multifaceted approach by enterprise architects analyzing the potential and limitations of AI within military contexts. This perspective is pivotal to comprehending AI's transformative impact on military strategies and operational paradigms.

Complementing this military focus, Nili et al. (2022) explore the interplay between public sector AI deployments and military applications. Their analysis reveals a synergistic relationship, in which innovations in public sector AI inform and enhance military technological advancements. Similarly, Krebs (2020) scrutinizes the Department of Defense's integration of commercial-style AI in procurement processes, underscoring the importance of developing robust and effective strategies for assimilating AI within military frameworks.

Stone (2021) outlines essential steps to augment AI initiatives within the intelligence community, concentrating on leveraging AI to bolster intelligence operations. In parallel, Talent

(2021) uncovers the hidden AI workforce within the Department of Defense, emphasizing the significance of recognizing and utilizing the existing pool of talent skilled in AI and related fields.

The intersection of AI and cybersecurity introduces unique challenges and opportunities. Sangwan et al. (2023) conduct an exhaustive study of AI systems' cybersecurity, creating a taxonomy of cyberattacks targeting these systems and proposing early-stage defense strategies for safeguarding AI applications. Their research is particularly relevant for enhancement of the security of AI implementations in both military and intelligence spheres.

Mohamed (2023) extends this discussion by surveying the latest advancements in AI and ML within cybersecurity. The paper highlights the effectiveness of AI and ML for anomaly detection and predictive analytics, while also acknowledging the challenges, such as the need for extensive and diverse data sets and susceptibility to manipulation by adversarial actors.

In the realm of network security, Ali and Alqaraghuli (2023) investigate the role of advanced AI technologies in bolstering cybersecurity defenses. Their study focuses on the application of ML and deep learning algorithms to detection of cyber threats, an aspect critically relevant to securing military and intelligence network infrastructures.

Chan et al. (2019) delves into the emerging challenges of applying AI to cybersecurity for business information management. Their research provides valuable insights into AI's role in this domain, offering guidance beneficial for military sectors with respect to management of their information and technology assets.

Pooyandeh et al. (2022) explore the cybersecurity challenges within AI-based metaverse environments. Their research, which covers AI's protective role and the complex architecture of the metaverse, has direct implications for military and intelligence applications, in which AI and virtual environments are increasingly integral.

The integration of AI in FedRAMP requires addressing the political imaginary of national AI strategies, as Paltieli (2022) discussed. It also necessitates effective leadership, as highlighted by Pierre (2022). Hujran et al. (2023) examine the antecedents and outcomes of intelligent government usage, providing insights into the broader context of AI adoption. Turobov (2022) delves into the transformation and consistency of AI and security, shedding light on considerations critical to the adoption of AI within the FedRAMP framework. Biersmith and Laplante (2022) introduce AI assurance for policymakers, emphasizing the need for robust mechanisms to ensure responsible and ethical AI practices. Bruno et al. (n.d.) discuss the national employment system, emphasizing the potential impact of AI on workforce dynamics.

Despite the potential benefits of AI in FedRAMP, there are also obstacles to overcome. McLaughlin (2020) provides a guide to improving federal procurement and risk management of cloud services, offering insights into enhancement of the adoption and utilization of AI technologies. Metheny (2017) and Kent (2019) discuss federal cloud computing strategies, which are crucial to shaping the overall AI landscape within FedRAMP. Egan (2022) suggests fixing the Technology Modernization Fund to overcome obstacles to funding critical IT initiatives, ensuring adequate resources for AI implementation.

In conclusion, the use of AI in FedRAMP offers numerous opportunities. It presents several obstacles, including management of bias, balancing of information needs, effective leadership, and securing of sufficient funding for critical IT initiatives. Addressing these challenges requires technical expertise, active citizen engagement, and integration of insights from different sectors and domains, as Clarke et al. (2022) discussed. By navigating these complexities, FedRAMP can harness the transformative power of AI to enhance its operations and deliver more efficient and effective services to the government and the public.

CHAPTER 3: METHODOLOGY

Introduction

The research methodology and design for the dissertation incorporates a systematic literature review using the PRISMA framework as well as qualitative analysis using NVivo (Version 14) software and expert studies/interviews.

The initial step in the research methodology will involve conducting a systematic literature review to gather existing knowledge of and insights on cloud computing, storytelling AI, and FedRAMP adoption. The researcher can follow the guidelines outlined by PRISMA to ensure a systematic and comprehensive review of the relevant literature (Bhushan et al., 2018; Fatima et al., 2020; Fatima 2022; Maroc & Zhang, 2019; Palanivinayagam et al., 2023; Sohail et al., 2023; Syafrizal et al., 2020; Taboada Puente et al., 2023; Waseem et al., nd; Yan et al., 2023).

Next, qualitative analysis using NVivo (Version 14) software can be employed to analyze the data extracted from the systematic literature review. NVivo is a widely used qualitative analysis tool that allows researchers to organize, code, and analyze qualitative data efficiently. The researcher can use NVivo to identify patterns, themes, and relationships within the literature, providing a deeper understanding of the technology adoption model for cloud computing, storytelling AI, and FedRAMP.

Rationales

The choice of a qualitative case study design is based on several rationales. The subsections that follow present the rationales for choosing a qualitative case study design instead of a quantitative or mixed methods design.

In-Depth Exploration.

A qualitative case study design allows for a detailed and holistic exploration of the research topic. It enables the researcher to delve deeply into the technology adoption model, storytelling

AI, and FedRAMP, gaining a rich understanding of the complexities and nuances involved. The qualitative approach is well-suited to capturing the subjective experiences, perspectives, and meanings that individuals attribute to their adoption decisions (Yin, 2018).

Contextual Understanding.

The qualitative case study design provides an opportunity to examine the research topic within its real-life context. By studying real-world cases and their specific contextual factors, the researcher can uncover the unique dynamics and challenges associated with the adoption of cloud computing, storytelling AI, and FedRAMP. This approach helps to capture the contextualized knowledge and insights necessary for understanding the phenomena under investigation (Creswell & Poth, 2017).

Complexity and Process Orientation.

Technology adoption in organizations is a multifaceted and dynamic process. A qualitative case study design allows for the exploration of this complexity and the identification of causal mechanisms and contextual factors that influence adoption outcomes. It enables the researcher to trace the evolution of the adoption process, examine interrelationships between different variables, and capture dynamics over time (Yin, 2018).

Participant Perspectives and Experiences.

By employing a qualitative case study design, the researcher can give voice to the perspectives and experiences of individuals involved in the adoption of cloud computing, storytelling AI, and FedRAMP. Through interviews, observations, and document analysis, the researcher can gather rich, detailed data that provides insights into participants' decision-making processes, challenges faced, and outcomes achieved. This approach facilitates a deeper understanding of the human aspects of adoption (Creswell & Poth, 2017).

Exploratory Nature and Emergent Design.

The dissertation aims to explore the potential role of storytelling AI in enhancement of the adoption of cloud computing, storytelling AI, and FedRAMP. A qualitative case study design allows for flexibility and adaptability to emerging themes and ideas. It enables the researcher to explore novel insights and unexpected findings that may arise during data collection and analysis, contributing to the generation of new knowledge (Yin, 2018).

Methodology

In addition to the systematic literature review and qualitative analysis, the research methodology will incorporate expert studies and interviews. Expert interviews can be conducted to gather insights, perspectives, and experiences from professionals and practitioners working in relevant fields. The researcher can utilize interviews with experts to gain a comprehensive understanding of the potential role of storytelling AI in enhancement of the adoption of cloud computing and FedRAMP in organizations.

To enhance the research design, the researcher can draw on the methodologies employed in previous qualitative studies related to cloud computing adoption (Carney, 2019; Diaz, 2022; Greer, 2015; Griffith, 2020; Hall, 2019; Steele, 2018; Yigitbasioglu, 2015).

These studies utilized qualitative approaches, such as interviews and case studies, to investigate various aspects of cloud computing adoption, risk acceptance criteria, and barriers to adoption in the federal sector. The researcher can adapt and refine these methodologies to suit the specific objectives of the dissertation.

Overview of Chapter Structure

Section 1: Population, Sample, and Participant Recruitment

In this section, the population of interest for the study will be defined, and the process of selecting a representative sample will be described. Additionally, the recruitment procedures for participants, including experts and professionals in the field, will be outlined.

Section 2: Data Collection Instrumentation and Procedures

This section will detail the data collection instruments used in the research, such as interview guides or questionnaires. The procedures for administering these instruments and collecting data from participants will be explained.

Section 3: Data Analysis Procedures

The data analysis procedures employed in the study will be described in this section. It will include an overview of how the data collected from the systematic literature review, interviews, and expert studies will be analyzed using qualitative analysis techniques, such as coding, categorization, and thematic analysis. The use of NVivo (Version 14) software for organizing and analyzing qualitative data will be highlighted.

Section 4: Trustworthiness

In this section, the measures taken to ensure the trustworthiness of the research findings will be discussed. This may include the use of strategies such as member checking, triangulation of data sources, and peer debriefing to enhance the validity and reliability of the study.

Section 5: Ethical Assurances

The ethical considerations and assurances associated with the research will be addressed in this section. It will outline the steps taken to protect the rights and confidentiality of participants, obtain informed consent, and adhere to ethical guidelines and regulations.

Discussion of Structure

This chapter structure will provide a comprehensive understanding of the population, sample, and participant recruitment process; the data collection instruments and procedures employed; the data analysis techniques utilized; the measures taken to ensure trustworthiness; and the ethical considerations of the study.

The aforementioned publications (Anderson, 2021; Bhushan et al., 2018; Fatima 2022; Fatima et al., 2020; Hall, 2019; Maroc & Zhang, 2019; Moore, 2022; Norman, 2020; Palanivinayagam et al., 2023; Rana, 2023; Sohail et al., 2023; Syafrizal et al., 2020; Let's say Puente et al., 2023; Tekic & Fuller, 2023; Waseem et al., nd; Yan et al., 2023) will serve as valuable references and resources for conduct of the systematic literature review, qualitative analysis, and expert studies/interviews, informing the research methodology and design of the dissertation.

In summary, the research methodology and design for the dissertation will incorporate a systematic literature review using the PRISMA framework, qualitative analysis using NVivo (Version 14) software, and expert studies/interviews. The systematic literature review will provide a foundation of existing knowledge, while qualitative analysis will aid identification of patterns and themes within the literature. Expert studies and interviews will offer insights from professionals and practitioners in the field. By utilizing these methods, the research aims to explore the technology adoption model for cloud computing, storytelling AI, and FedRAMP and understand the potential role of storytelling AI in enhancement of the adoption of these technologies in organizations.

Research Methodology and Design

Due to its capacity to provide in-depth insights into the adoption of CAIML in FedRAMP enterprises, qualitative methodology was selected as the primary methodology for this dissertation

(Creswell & Poth, 2017). Qualitative research permits a thorough examination of complex phenomena and captures the richness and contextual nuances of the research topic. By conducting in-depth case studies, researchers can collect rich and detailed data through interviews, observations, and document analysis, thereby gaining a comprehensive understanding of the adoption process, its obstacles, and its strategies (Yin, 2018).

Qualitative research also allows for a more nuanced exploration of the variables and factors influencing adoption. It enables researchers to uncover underlying meanings, motivations, and perceptions of individuals and organizations involved in the adoption process (Merriam, 2015). In the context of CAIML adoption, factors such as perceived usefulness, ease of use, top-management support, organizational culture, and user feedback can be explored in depth through qualitative case studies (Marr, 2019; Nguyen et al., 2022).

Furthermore, qualitative case studies allow for examination of specific cases, providing rich and detailed descriptions of real-world adoption scenarios in FedRAMP enterprises. This approach offers valuable insights into the complexities, challenges, and successes of adopting CAIML in a specific organizational context (Yin, 2018). It enables researchers to identify and categorize successful leadership strategies specific to CAIML systems (Chen, Jiang, et al., 2022; Gkinko & Elbanna, 2022a; Gkinko & Elbanna, 2022b).

Regarding citations supporting the rationale for qualitative case studies, the works of Yin (2018), Creswell (2017), Merriam (2015), Nguyen et al. (2022), Marr (2019), Gkinko & Elbanna, 2022, Gkinko & Elbanna, 2022b, and Chen, Jiang, et al., 2022 can be referenced. These authors have provided valuable insights into the advantages of qualitative research methods and their application to exploration of adoption processes, factors influencing adoption, and successful strategies.

Population, Sample, and Participant Recruitment

The study target population for this research consists of professionals, practitioners, and experts in organizations that have adopted or are considering the adoption of cloud computing, storytelling AI, and FedRAMP. The estimated size of the population is approximately 500 individuals based on the number of organizations known to have implemented these technologies or expressed interest in doing so.

The sample for this study will be selected using a purposive sampling method. Purposive sampling is appropriate in this context because it allows for the deliberate selection of individuals who possess relevant knowledge and experience of the adoption of cloud computing, storytelling AI, and FedRAMP. The sample will include individuals from diverse backgrounds, including IT professionals, managers, executives, and other key stakeholders involved in technology adoption decisions.

The minimum sample size proposed for this study is 15 participants. This sample size is determined based on the principle of saturation, with the aim of reaching a point where new insights and themes emerge less frequently, indicating that sufficient data have been collected to address the research objectives (Daniël, 2022; Hennink, 2022).

To recruit participants for the study, a strategic approach will be employed, primarily utilizing purposive sampling through the LinkedIn professional networking platform, supplemented by industry conferences and relevant online communities. This method is chosen to ensure access to a diverse range of professionals across various organizations and industries, particularly those with direct involvement in cloud computing, storytelling AI, or FedRAMP initiatives. Participants will be selected based on their expertise and experience in these areas, aiming to achieve diversity in organization size, industry sector, and job roles for a comprehensive perspective. The recruitment process will involve compiling a preliminary list of potential

participants from these platforms, followed by sending personalized invitations to explain the research's purpose and significance. Additionally, snowball sampling will be incorporated, encouraging participants to refer other suitable professionals, thereby expanding the pool of potential respondents, and enriching the study with varied insights.

Upon receiving consent from participants, arrangements for semistructured interviews will be made. These interviews will be conducted either in person or through online communication platforms, depending on the geographical locations and preferences of the participants. The interviews will follow a predetermined interview guide that includes open-ended questions designed to explore participants' experiences, perceptions, and challenges related to the technology adoption model for cloud computing, storytelling AI, and FedRAMP.

Throughout the recruitment and data collection process, ethical considerations will be upheld. Participants will be informed about the voluntary nature of their participation and their right to withdraw from the study at any time without consequences. The confidentiality and anonymity of the participants will be ensured by assigning unique identifiers instead of using real names in research materials. Informed consent will be obtained from each participant prior to the interviews, and data will be securely stored and used only for research purposes.

In conclusion, the study's target population consists of LinkedIn professionals involved in cloud computing, storytelling AI, and FedRAMP. The recruitment process will involve compiling a list of potential participants, sending personalized invitations, and employing snowball sampling techniques. Semistructured interviews will be conducted to gather rich qualitative data. Ethical considerations will be prioritized throughout the process to protect the participants' rights and ensure confidentiality.

Data Collection Instrumentation and Procedures

In this dissertation, a combination of data collection instruments and procedures will be employed to gather and analyze data related to the technology adoption model for cloud computing, storytelling AI, and FedRAMP and the potential role of storytelling AI in enhancement of the adoption of these technologies in organizations. The following sections describe the data collection instrumentation and procedures.

Semistructured Interviews

Semistructured interviews will be conducted with participants to explore their perspectives, experiences, and insights. The interview protocol will be developed based on the initial research questions and objectives, providing flexibility to probe deeper into participants' responses and to explore emerging themes and ideas. Adams (2015) and Ramsden (2016) provide guidance on conducting semistructured interviews and determining an appropriate number of interviews. A purposeful sampling strategy (Palinkas et al., 2015) will guide the selection of participants who possess relevant knowledge and experiences of cloud computing, storytelling AI, and FedRAMP.

Observations

On-site observations will be conducted to gain firsthand insights into the use of cloud computing, storytelling AI, and FedRAMP technologies within organizations. Field notes will be taken to record observations, capturing relevant contextual information and any emerging patterns or themes. The data collected through observations will complement the interview data, providing a deeper understanding of participants' actions and behaviors (Lawson, 2016).

Document Analysis

Documents such as organizational policies, reports, guidelines, and relevant literature will be analyzed to gain additional insights into the technology adoption model and the role of

storytelling AI. The content analysis approach outlined by Saldaña (2021) will guide the systematic analysis of documents, allowing identification of key themes and patterns.

NVivo Software

Qualitative data analysis software, such as NVivo (Version 14), will be used to support the organization and analysis of the collected data (Paulus, 2023). NVivo provides a platform for efficient coding, categorization, and identification of relationships within data. It will aid identification of emerging themes and patterns across different data sources, facilitating the analysis and interpretation of the findings (Tang, 2023).

Discussion of Procedures

The data collection procedures will involve an iterative process, aligning with the action research design. Each cycle/spiral will inform subsequent data collection by activating additional questions and areas of exploration. The dissertation will follow ethical guidelines for research (Rana et al., 2021), ensuring the protection of participants' rights and privacy.

Overall, this data collection approach will provide a comprehensive and multifaceted understanding of the technology adoption model for cloud computing, storytelling AI, and FedRAMP, as well as the potential role of storytelling AI in organizations. The selected data collection instruments and procedures are well-suited to an action research study design, allowing for flexibility, adaptability, and rigorous analysis of qualitative data.

Data Analysis Procedures

In this dissertation on Storytelling AI and FedRAMP, data analysis procedures will be crucial to deriving meaningful insights from the collected data. The chosen data analysis method aligns with the action research design, which is situated within the qualitative tradition. The procedures for data analysis will be discussed for each action cycle/spiral in a detailed manner to enable replication by other researchers. It is important to note that the preferences and

collaboration of participants at the research site will be considered when determining the data analysis approach, as it may involve both qualitative data analysis software and traditional hands-on methods.

The following subsections outline the steps of the proposed data analysis procedures for the action cycles/spirals.

Step 1: Data Preparation

Before analysis, the collected data, which may include interviews, observations, documents, and possibly video or audio recordings, will be carefully transcribed. This transcription process is crucial for converting spoken words or observed phenomena into a written format that can be systematically analyzed. Following transcription, the data will be meticulously organized, categorizing it according to different types and sources. Each piece of data will then be coded, assigning labels or tags that will assist in identifying key concepts and patterns. This initial organization and coding, as outlined by Rana et al. (2021), are essential steps to prepare the data for in-depth analysis.

Step 2: Initial Coding

During the initial coding stage, each piece of data will be examined thoroughly. Open coding will be applied to different segments, where specific codes representing concepts, themes, or patterns observed in the data will be assigned. This process, guided by the methodology of Saldaña (2021), involves an exploratory approach, where the data is openly interpreted without preconceived categories. The objective of this stage is to remain as unbiased and open-minded as possible, allowing the data to reveal its inherent meanings and relationship.

Step 3: Theme Development

Following the initial coding, the next step involves grouping the open codes to develop broader, more encompassing themes. This stage is critical in identifying connections and

relationships between different codes, leading to the formation of overarching themes. As new insights emerge during the analysis, these themes will be continually refined and revised, a process highlighted by Saldaña (2021). This iterative approach ensures that the themes accurately represent the complexities and nuances of the data.

Step 4: Data Comparison

In this step, as more data is collected through multiple iterations, comparisons will be made across different cycles or spirals of data. This comparison is aimed at identifying similarities, differences, and emerging patterns across various data sets. This iterative process, as noted by Palinkas et al. (2015), is crucial for refining the emerging themes and deepening the overall analysis. It allows for a more robust and comprehensive understanding of the data, ensuring that the analysis captures all relevant aspects and dimensions.

Step 5: Member Checking

To enhance the credibility and confirmability of the findings, member checking will be conducted as per Saldaña (2021). This involves sharing the analyzed data and the developed themes with the participants for their review. The purpose of this step is to validate the accuracy and relevance of the interpretations made by the researchers. Participants will have the opportunity to confirm, correct, or elaborate on the findings, ensuring that the results are a true reflection of their experiences and perspectives.

Step 6: Reflection and Action Planning

Throughout the data analysis process, there will be continuous reflection and discussion with both participants and research collaborators. These reflective discussions, as emphasized by Lawson (2016), are aimed at gaining additional insights into the data. They will also be crucial in refining the action plan for the study, ensuring that it remains aligned with the overarching research

objectives. This reflective phase is not only about analyzing the data but also about considering the implications of the findings and planning subsequent steps in the research process.

Discussion of Analysis Procedure

For the data analysis process, qualitative data analysis software, such as NVivo, may be employed to facilitate the management, organization, and analysis of qualitative data (Paulus, 2023). However, the preferences of the research participants and collaborators will be considered. If a more traditional approach is preferred, manual coding and analysis methods will be used in close collaboration with the research team.

Following these data analysis procedures allows the research findings to be thoroughly examined, interpreted, and validated, thereby contributing to the trustworthiness and rigor of the study. The iterative nature of the action research design allows for continuous refinement and enrichment of the analysis, leading to a comprehensive understanding of the technology adoption model for cloud computing, storytelling AI, and FedRAMP.

Trustworthiness

In the qualitative tradition, particularly within an action research design as used in this study on storytelling AI and FedRAMP, the trustworthiness of the research is a critical factor. To ensure robust trustworthiness, this research adheres to four key criteria: credibility, transferability, dependability, and confirmability. The following subsections meticulously detail how each of these criteria is effectively met in the context of this dissertation.

Credibility

Credibility is a measure of how believable and trustworthy the research findings are. In this study, credibility is enhanced through the employment of multiple data collection methods, including interviews, observations, and document analysis, as recommended by Adams, 2015. These varied methods facilitate the gathering of comprehensive and nuanced perspectives from

participants, thereby enriching the study's findings. Further reinforcing credibility, member checking is integrated into the research process, allowing participants to review and affirm the accuracy and relevance of the findings (Saldaña, 2021).

Transferability

Transferability refers to the extent to which the research findings are applicable in other contexts or settings. This dissertation provides in-depth descriptions of the research context, the characteristics of the participants, and the methodologies implemented (Ante & Ante, 2016). Such detailed documentation enables readers to assess the relevance and potential applicability of the findings to different contexts. The study also employs purposeful sampling techniques to select participants whose experiences and insights are representative of a broader population, thus enhancing the generalizability of the findings (Palinkas et al., 2015).

Dependability

Dependability concerns the stability and consistency of the research process and its outcomes. To ensure dependability, a comprehensive audit trail detailing the research procedures, decisions, and revisions throughout the study will be maintained (Rana et al., 2021). This meticulous documentation allows for the research process to be replicated and its reliability assessed. Peer debriefing and consultation with field experts are also incorporated, providing an additional layer of scrutiny to ensure the research's consistency and methodological rigor (Lexis & Julien, 2022).

Confirmability

Confirmability pertains to the neutrality and objectivity of the research findings. To support confirmability, qualitative data analysis software, such as NVivo (Version 14), will be utilized (Paulus et al., 2023). This software facilitates a systematic and transparent analysis, helping in the identification of patterns, themes, and relationships in the data, thereby reducing subjective

interpretation. Additionally, reflexive practices are employed throughout the research process, allowing the researcher to acknowledge and address any personal biases, ensuring that the findings are a true reflection of the data and not influenced by the researcher's predispositions (Saldaña, 2021).

Discussion of Trustworthiness

By addressing these four criteria—credibility, transferability, dependability, and confirmability—the trustworthiness of this action research study of the technology adoption model for cloud computing, storytelling AI, and FedRAMP will be established. The use of multiple data collection methods, purposeful sampling, member checking, and detailed documentation will contribute to the credibility and dependability of the findings. Furthermore, the provision of detailed contextual information and use of reflexive practices will support the transferability and confirmability of the research.

Ethical Assurances

Protection of Human Participants and Participant Rights

The rights and welfare of human participants in this study were carefully protected throughout the research process. Participants were informed of the voluntary nature of their participation and the purpose of the study. They were assured of their right to withdraw at any time without consequences. Written informed consent was obtained from each participant; the instrument for obtaining consent from participants clearly stated the purpose of the study, the nature of their involvement, and the confidentiality and anonymity of their responses (Rana et al., 2021). The informed consent form was included in the proposal but removed from the final manuscript to ensure participant confidentiality.

Confidentiality and Privacy

Confidentiality was strictly maintained to protect the privacy of participants. All data collected were deidentified and stored securely. Participant identifiers were replaced with unique codes to ensure anonymity during data analysis and reporting. The data were limited to the research team and any external data sharing. Access was mediated in an aggregated and anonymized manner to prevent identification of individual participants (Rana et al., 2021).

Preventing Coercion and Conflicts of Interest

Efforts were made to ensure that participants were not coerced into participation. They were provided with clear and unbiased information about the study's objectives and potential benefits and risks. Each participant was informed that their decision to participate or withdraw would not affect their relationship with the researchers or any organization involved (Rana et al., 2021). To address potential conflicts of interest, the researcher-maintained objectivity and transparency throughout the study, refraining from any actions that might compromise the integrity of the research.

Treatment/Intervention Groups and Control Group

In this study, there were no specific treatment or intervention groups. The focus was on understanding the technology adoption model and the potential role of storytelling AI in the enhancement of the adoption of cloud computing, storytelling AI, and FedRAMP. Therefore, no specific protocols or interventions were administered to participants.

Concealment, Deception, and Debriefing

There was no concealment or deception involved in this study. Participants were provided with accurate and transparent information about the study's purpose, procedures, and potential implications. Debriefing was not necessary, as no deceptive practices were employed.

Data Management and Security

All data collected, whether in paper-based or electronic form, were stored securely. Electronic data were encrypted and stored on password-protected devices, and physical records were kept in locked cabinets accessible only to the research team. The duration of data retention met ethical guidelines (Rana et al., 2021).

Institutional Review Board Approval

Before recruiting participants, the research protocol was subjected to evaluation and endorsement by the institutional review board (IRB). This guaranteed that the study complied with ethical principles and safeguarded the rights and well-being of human participants. The proposal included a statement affirming the intention to obtain IRB approval before initiating the research (see Appendix A).

Discussion of Ethical Assurances

This action research study, delving into the technology adoption model for cloud computing, storytelling AI, and FedRAMP, establishes its trustworthiness by meticulously addressing four pivotal criteria: credibility, transferability, dependability, and confirmability.

Credibility and Dependability are fortified through the employment of diverse data collection methods. These methods include detailed interviews, comprehensive observations, and thorough document analysis, ensuring a multifaceted and robust collection of data. Purposeful sampling is strategically utilized to encompass a broad spectrum of perspectives, further enhancing the representativeness and reliability of the findings. Additionally, the integration of member checking acts as a vital step, enabling participants to verify the findings, thereby adding to their authenticity and reliability. Detailed and systematic documentation of every stage of the research process serves to solidify the dependability of the study, ensuring that each methodological decision is transparent and reproducible.

The Transferability of the research is significantly augmented by providing rich, contextual descriptions of the settings, participants, and scenarios involved in the study. This comprehensive detailing allows for a deeper understanding of the environment in which the research is conducted, facilitating the application of the findings to similar contexts by other researchers or practitioners.

Confirmability is rigorously addressed through the implementation of reflexive practices. These practices involve consistent self-evaluation by the researcher to identify and mitigate any personal biases, ensuring that the findings are a true and unbiased reflection of the data. The use of qualitative data analysis tools further supports this objectivity, allowing for a systematic, transparent, and verifiable analysis of the data.

Overall, by conscientiously adhering to these criteria, this research not only upholds the integrity of its findings but also contributes valuable insights into the field of technology adoption, specifically in the domains of cloud computing, storytelling AI, and FedRAMP.

Chapter Summary

This dissertation adopts an action research methodology, synergizing a systematic literature review, qualitative analysis through NVivo (Version 14) software, and expert interviews/studies. This approach is inherently qualitative, facilitating a thorough exploration of the technology adoption model for cloud computing, storytelling AI, and FedRAMP, including the influential role of storytelling AI in their organizational adoption.

The action research framework commences with a systematic literature review, guided by the PRISMA framework, to collate and assess pertinent research articles. This review aims to construct a comprehensive landscape of the existing knowledge base in this field. The subsequent phase involves qualitative analysis using NVivo (Version 14), which is instrumental in coding, categorizing, and distilling insights from data derived from expert interviews/studies. These expert

engagements, conducted through semi-structured interviews, are designed to delve into the experiences and perspectives of professionals in the field, offering rich, qualitative insights.

Data collection is tailored through purposive sampling, targeting a diverse group of about 500 professionals, practitioners, and experts. Recruitment leverages professional networks, industry events, and online platforms. Ethical considerations are paramount; informed consent will be obtained, and data collection will encompass interviews, observations, and document analysis, ensuring respect for participant rights and data integrity.

The analysis framework is comprehensive, encompassing data preparation, initial coding, theme development, data comparison, member checking, and reflective action planning. NVivo (Version 14) plays a pivotal role in this process, providing a structured and efficient means for managing and analyzing qualitative data. The iterative nature of action research is a key advantage, allowing for ongoing refinement and enhancement of the analysis.

Trustworthiness is a cornerstone of this research and is addressed by adhering to the criteria of credibility, transferability, dependability, and confirmability. These are achieved through diverse data collection methods, purposeful sampling, member checking, and meticulous documentation. Ethical assurances are rigorously maintained, including participant protection, confidentiality, and data security, complemented by seeking IRB approval before participant recruitment.

In summary, the selected methodology and design of this study—encompassing ethical considerations, data collection and analysis strategies, and trustworthiness measures—constitute a holistic and rigorous framework. This framework is adeptly suited for investigating the technology adoption model for cloud computing, storytelling AI, and FedRAMP, as well as evaluating the role of storytelling AI in augmenting their organizational adoption.

CHAPTER 4: FINDINGS AND RESULTS

Introduction

Chapter 4 stands as a testament to the extensive exploration of the outcomes achieved through this research, firmly rooted in the principles of thematic analysis. This chapter is pivotal, serving as the cornerstone for the presentation and critical discussion of the key findings that have emerged from a meticulous systematic literature review, an in-depth qualitative analysis, and the valuable insights gleaned from expert interviews and studies. The overarching aim of this chapter is to meticulously delve into and elucidate the data collected and analyzed throughout the research journey, thereby illuminating the multifaceted dimensions and intricate dynamics of cloud computing, storytelling AI, and FedRAMP adoption within organizational contexts.

The structure of Chapter 4 is meticulously crafted to seamlessly navigate readers through the integral components and findings of the research, systematically organized in the following subsections.

Systematic Literature Review Findings Section

This segment provides a distilled summary of the extensive findings from the systematic literature review, adhering to the methodological guidelines set forth by Page (2022) and Moher (2010). It furnishes readers with a lucid comprehension of the prevailing body of knowledge surrounding cloud computing, storytelling AI, and FedRAMP adoption, thereby framing the stage for the novel contributions of this research.

Qualitative Analysis Findings Section

Employing the nuanced techniques of thematic analysis, as championed by Clarke (2015) and Braun (2006), this section delves into the rich data amassed from various documents identified in the systematic literature review. This methodical approach has unraveled intricate themes and

patterns, providing a profound understanding of the practical implications and complex intricacies associated with the adoption of cloud computing, storytelling AI, and the FedRAMP framework.

Expert Studies/Interviews Findings Section

This section, adopting a thematic approach, serves as a conduit for encapsulating invaluable insights and opinions offered by field experts. Thematic analysis has been widely employed in diverse studies, ranging from understanding risk management practices in microgreen growing operations (Hamilton, 2023) to exploring technology use within dating relationships (Basting et al., 2023). By conducting thematic analysis of expert interviews and studies, I draw out significant themes and firsthand experiences concerning cloud computing, storytelling AI, and FedRAMP adoption.

Integration of Findings Section

Through thematic analysis, I integrate findings from different data sources—systematic literature review, qualitative analysis, and expert interviews/studies. This approach enables identification of areas of consensus and divergence, fostering a holistic view of the research findings and the emergent themes that bridge these sources (Colville et al., 2009).

Discussion of Findings Section

In this segment, I engage in a thorough interpretation of the findings within the context of this dissertation's research questions and objectives. The thematic analysis of these findings allows the researcher to uncover the deeper implications, insights, and relevance of the data to the technology adoption model for cloud computing, storytelling AI, and FedRAMP.

Validation and Trustworthiness of Findings Section

Returning to the trustworthiness criteria outlined in Chapter 3—including credibility, transferability, dependability, and confirmability—I revisit how these criteria were maintained throughout the research process (O'Kane et al., 2021). I discuss the role of validation mechanisms

such as member checking and peer debriefing in upholding the rigor of thematic analysis, emphasizing the importance of building transparency and trustworthiness in inductive research (O'Kane et al., 2021).

Limitations Section

Thematic analysis also plays a role in the acknowledgment of limitations encountered during the research. By examining these constraints thematically, the researcher can better understand how they may have influenced the findings and their applicability across various contexts (Alam, 2021).

Summary

In summary, Chapter 4 employs thematic analysis as a powerful tool for organizing and presenting research findings. This analysis method allows researchers to delve deep into the nuances of data, uncovering the essential themes and patterns that underpin this study. Through this structured exploration, I aim to provide a comprehensive understanding of cloud computing, storytelling AI, and FedRAMP adoption, laying the groundwork for Chapter 5, where I will draw conclusions and offer recommendations based on the findings elucidated in this chapter.

Research Methodology and Data Collection Methods

Fundamental Pillars

The fundamental pillars of the research design and data collection methods are summarized in the subsections that follow.

Systematic Literature Review.

I embarked on an exhaustive journey through existing literature, adopting the PRISMA framework for systematic literature reviews (Moher, 2010). The systematic literature review served as a bedrock of knowledge, offering a panoramic view of prior research, and setting the stage for a more profound exploration (Page, 2022).

Qualitative Analysis Using NVivo Software.

Employing the power of NVivo (Version 14) software, I meticulously analyzed the data derived from the systematic literature review (Hilal, 2013; Maene, 2022). This qualitative analysis approach allowed us to identify, code, and categorize patterns and themes that had emerged from the literature, emphasizing the utility of software-driven methods for enhancing the rigor and depth of the analysis (Sutopo, 2022).

Expert Studies/ Interviews.

I engaged in enlightening conversations with professionals and experts steeped in the realms of cloud computing, storytelling AI, and FedRAMP. These interviews opened a window into the practical experiences and perspectives of individuals actively engaged with these technologies. While the narrative captures the essence of these dialogues, the use of NVivo (Version 14) for qualitative analysis further strengthened the systematic approach to deciphering and interpreting the rich data these conversations offered (Hilal & Alabri, 2013; Maene, 2022; Sutopo, 2022).

Data Collection Methods

Moreover, the dissertation's data collection methods were strategically designed to provide a 360° view of the research topics.

Semistructured Interviews.

The interviews, conducted with precision, offered participants opportunities to delve into their experiences and share nuanced insights (Adams, 2015; Magaldi & Berler, 2020). The approach, grounded in the methodology of semistructured interviews, allowed the researcher to probe deeply into responses, enriching the qualitative data sought (Pin, 2023).

Document Analysis.

Following the recommendations of Morgan (2022) and Sankofa (2022), the analysis of organizational documents, guidelines, and relevant literature acted as a supplementary source of insight, further elucidating the dynamics surrounding the research topics.

NVivo Software.

The systematic organization and analysis of qualitative data were made possible through the utilization of NVivo (Version 14) software, which facilitated efficient coding, categorization, and identification of meaningful relationships within the data (Hilal, 2013; Maene, 2022; Sutopo, 2022).

Discussion of Research Design and Methods

Throughout this journey, ethical considerations have been the researcher's lodestar, guiding actions and decisions. The rights and privacy of human participants have been safeguarded through transparent processes, including informed consent (Lunt et al., 2019; Nijhawan et al., 2013; Whelan, 2007; Yusof et al., 2022), and IRB approval (Dutka & Astroth, 2022; Lapid et al., 2023).

With this recapitulation of the methodology and data collection methods, the researcher stands poised to unveil the rich tapestry of results and findings that have emerged from this arduous but rewarding exploration. In Chapter 4, I delve into the heart of the research, presenting the fruits of my labor, the insights garnered, and the implications for the fields of cloud computing, storytelling AI, and FedRAMP adoption within organizational contexts.

Systematic Literature Review Findings

The systematic literature review conducted in this research, following the PRISMA framework (Moher, 2010; Page, 2022), unearthed a wealth of insights and knowledge. The

objective of this section is to provide a concise, yet comprehensive summary of the key findings derived from the extensive body of literature examined.

Inclusion and Exclusion of Studies

- A total of 1,344 research articles, reports, and scholarly publications were identified during the initial search process.

- Following the application of predefined inclusion and exclusion criteria, 35 studies were retained for detailed analysis (Dekkers, 2022; Meline, 2006; Patino, 2018).

- The rationale for study exclusions primarily revolved around irrelevance to the research objectives, lack of empirical data, or publication outside the specified timeframe (Hornberger, 2020).

Thematic Analysis

Thematic analysis, a qualitative research method, surfaced as the cornerstone of the researcher's review of the selected studies. This method allows for an intricate, layered exploration of data, facilitating the identification and interpretation of prominent patterns, or themes, within a data set. The process of thematic analysis is iterative and reflexive, often commencing with a phase of familiarization wherein researchers immerse themselves in the data. This is followed by systematic coding, theme development, and final theme refinement (Braun & Clarke, 2006). In the researcher's analysis, the power of this method became evident as it enabled us to discern nuanced insights and converge them into coherent, overarching themes (Clarke et al., 2015). Such analysis goes beyond mere data description, offering a deeper interpretative lens. By applying thematic analysis to topics like cloud computing and storytelling AI, I could delve deeper into the essence of the subjects, understanding not just the "what" but also the "why" behind prevailing trends and patterns (Gupta & Sharma, 2022; Rashid et al., 2019).

Key Findings

Cloud Computing Adoption.

Through an extensive analysis of cloud computing adoption, several key findings have emerged that resonate with the challenges and considerations highlighted in Table 1. Just as cloud security concerns and cloud compliance issues underscore the significance of security and compliance in cloud adoption, the key findings emphasize the multifaceted challenges organizations face, including data migration complexities and the imperative for visionary leadership and change management. Additionally, cloud data privacy risks and cloud ethical use of data parallel the critical balance between data privacy and ethical data use in the cloud, which is an integral part of cloud computing adoption. Furthermore, the profound implications of cloud adoption for national security and intelligence analysis align with the implications mentioned in Table 1. These key findings underscore that cloud computing adoption is not solely an IT endeavor but is also a strategic imperative, emphasizing the importance of holistic strategies, visionary leadership, and continuous learning and innovation, echoing the themes found in Table 1.

Table 1

Cloud Computing Adoption Coding Matrix

Code	*f*	Description/excerpt
Cloud data migration challenges	1,342	Challenges associated with data migration in the cloud
Cloud data privacy risks	1,342	Risks related to data privacy in the cloud
Cloud ethical use of data	1,342	Ethical considerations in using data in the cloud
Cloud continuous learning	1,351	Emphasizing continuous learning in cloud technology
Cloud integration challenges	912	Challenges related to integration in cloud environments

Code	*f*	Description/excerpt
Cloud change management	897	Managing change in cloud adoption
Cloud improved customer service	926	Enhancing customer service through cloud technologies
Cloud cybersecurity measures	827	Implementing cybersecurity measures in the cloud
Cloud visionary leadership	676	Leadership with a visionary approach to cloud adoption
Cloud compliance issues	804	Issues related to compliance in cloud computing

Note. This table provides an overview of the top 10 codes and their prevalence in the data.

Table 1 functions as a concise yet comprehensive guide to the core themes and issues uncovered during the analysis of cloud computing adoption data. In this table, the top 10 codes are meticulously distilled, offering readers a clear glimpse into the most salient aspects of cloud adoption. Each code encapsulates a crucial dimension of this transformative technology, from addressing data migration challenges to grappling with ethical considerations and security imperatives. The purpose of Table 1 is to serve as a navigational beacon within the vast sea of cloud computing adoption, allowing researchers, practitioners, and decision-makers to identify the major focal points and concerns swiftly. It underscores the multifaceted nature of cloud adoption while highlighting the central themes that shape the strategic, economic, and ethical dimensions of this critical technological shift. Table 1 is a foundational reference, illuminating the path to informed decision-making and innovation in the ever-evolving world of cloud computing adoption.

Table 2 serves as a comprehensive summary of the key themes that have emerged from the analysis of data related to cloud computing adoption. It provides a structured overview of these themes, which encompass various aspects of cloud adoption, ranging from challenges and security considerations to economic implications and the impact on national security.

Storytelling AI Integration.

The findings relating to storytelling AI integration share common threads with the challenges and considerations outlined in Table 3. Just as AI data security concerns and AI data privacy risks highlight the importance of safeguarding data in AI applications, AI integration underscores the need to seamlessly integrate AI technologies while addressing potential security and privacy risks. Similarly, AI's ethical use of data resonates with the ethical considerations relating to AI data usage, emphasizing the importance of responsible integration of storytelling AI. Moreover, AI continuous learning mirrors the imperative for ongoing learning and adaptation when incorporating AI into storytelling practices. As AI plays a crucial role in intelligence analysis, the integration challenges outlined in Table 3 align with the complexities of weaving AI-driven insights into narrative experiences.

Table 2

Cloud Computing Adoption Emerging Themes

Theme	Key subtopics and insights
Challenges in cloud adoption	Data migration challenges Compliance issues Lack of expertise Cost concerns
Security and compliance	Security concerns Data privacy regulations Federal regulations Cybersecurity measures
Economic implications	Cost savings Return on investment Budget allocation
Data privacy and ethics	Data privacy risks Ethical use of data Compliance versus privacy Data handling policies

Theme	Key subtopics and insights
Efficiency and automation	Cloud process automation Data-driven decision making Predictive analytics
Leadership and change	Visionary leadership Change management Innovation culture Continuous learning
Integration and migration	Migration strategy Integration challenges Legacy system impact
National security impact	Implications for national security Intelligence analysis Data sharing concerns
Customer service	Improved customer service Competitive advantage
Interdisciplinary collaboration	Collaboration Interdisciplinary teams

Note. This table summarizes the key themes that emerged from the analysis.

Therefore, these key findings underscore the critical balance between harnessing AI's storytelling potential and addressing the ethical, security, and integration aspects inherent to AI adoption, with implications not only for narrative experiences but also for broader applications in national security and compliance.

Table 3

Storytelling Artificial Intelligence (AI) Coding Matrix

Code	*f*	Description/Excerpt
AI data security concerns	1,342	Concerns about data security in AI applications
AI data privacy risks	1,342	Risks related to data privacy in AI
AI ethical use of data	1,342	Ethical considerations in AI data usage

Code	*f*	Description/Excerpt
AI data security measures	1,342	Measures to ensure data security in AI
AI national security impact	351	Impact of AI on national security
AI continuous learning	342	Emphasis on continuous learning in AI
AI legacy system impact	311	Impact on legacy systems due to AI adoption
AI intelligence analysis	317	Use of AI for intelligence analysis
AI integration challenges	267	Challenges related to AI integration
AI compliance challenges	264	Challenges in complying with AI regulations

Note. This table provides an overview of the top 10 codes and their prevalence in storytelling AI data.

Table 3 serves as a vital analytical tool, distilling the complex landscape of storytelling AI into its essential components. Through a careful examination of the data, Table 3 captures the essence of storytelling AI by pinpointing the recurring themes and concerns that dominate discussions and initiatives within this field. These codes are not merely statistical representations but also key indicators of the narrative that storytelling AI weaves in today's technological landscape. It reflects the fusion of narrative creativity and technological innovation, emphasizing the ever-present considerations of data security, ethical conduct, national security implications, continuous learning, and the challenges associated with AI integration and compliance. As organizations and storytellers embrace AI as a storytelling companion, Table 3 illuminates the path forward, reminding us that the art of storytelling is evolving in tandem with the capabilities and responsibilities of AI-driven narratives.

Table 4 succinctly summarizes the core thematic elements that have arisen from the analysis of storytelling AI data. These themes are systematically organized into key categories, offering a clear and concise overview of the essential insights within the storytelling AI domain.

Table 4 acts as a navigational aid, providing a streamlined understanding of significant focus areas, including security and privacy concerns, compliance and regulation, the impact on legacy systems, intelligence, and analysis, as well as the importance of continuous learning and addressing integration challenges in the context of AI-powered storytelling.

Table 4

Storytelling Artificial Intelligence (AI) Emerging Themes

Theme	Key subtopics and insights
Security and privacy	AI data security concerns AI data privacy risks Ethical use of data Data security measures National security impact
Compliance and regulation	AI compliance challenges AI federal regulations
Impact on legacy systems	Legacy system impact
Intelligence and analysis	Intelligence analysis
Continuous learning	Continuous learning Integration challenges
Integration challenges	AI integration challenges

Note. This table summarizes the key themes that emerged from the analysis.

FedRAMP Compliance.

The key findings regarding FedRAMP compliance underscore the multifaceted nature of this crucial framework in the context of federal government agencies. FedRAMP, while providing a standardized approach to cloud security, faces several challenges. These include resource constraints and evolving requirements, which demand careful management. Enhanced security measures are paramount but must be balanced with concerns about the cost of compliance. The

study highlights the need for visionary leadership and change management strategies to effectively navigate the complex landscape of FedRAMP. Moreover, it sheds light on the intricate interplay between compliance, privacy, and cybersecurity. The implications for national security and intelligence analysis are significant, emphasizing the critical role FedRAMP plays in safeguarding sensitive government data. This analysis ultimately reveals that achieving FedRAMP compliance is not only a regulatory necessity but also a strategic imperative, requiring careful consideration of resource allocation, security measures, and leadership practices.

Table 5 serves as a comprehensive summary of codes and their prevalence within the data set, providing a condensed view of critical aspects related to FedRAMP compliance. Table 5 allows for quick and informative reference, highlighting the frequency and essence of each code. The codes encompass various dimensions of FedRAMP, from threat mitigation to compliance challenges, shedding light on the intricacies of complying with FedRAMP regulations. Additionally, Table 5 underscores the role of FedRAMP in intelligence analysis, addresses data privacy risks and handling policies, delves into its impact on national security, and emphasizes continuous learning and change management. Table 5 also acknowledges the challenges associated with integrating FedRAMP into existing systems. In essence, Table 5 offers a concise snapshot of key aspects essential for understanding the FedRAMP compliance landscape within the federal government.

Table 6 offers a condensed and organized perspective of the central themes that have emerged from the analysis of FedRAMP compliance within federal government agencies. Table 6 categorizes these themes into distinct domains, making it a navigational aid for understanding the multifaceted landscape of FedRAMP. The themes range from the challenges organizations face in complying with FedRAMP requirements, encompassing resource constraints and evolving

regulations, to the critical considerations of security, privacy, and the intricate balance between data privacy and compliance.

Table 5

Federal Risk and Authorization Management Program (FedRAMP) Coding Matrix

Code	*f*	Description/excerpt
FedRAMP threat mitigation	4,261	Mitigating threats in FedRAMP compliance
FedRAMP compliance challenges	4,205	Challenges in complying with FedRAMP regulations
FedRAMP intelligence analysis	4,228	Use of FedRAMP for intelligence analysis
FedRAMP data privacy risks	2,327	Risks related to data privacy in FedRAMP
FedRAMP data handling policies	2,212	Policies related to data handling in FedRAMP
FedRAMP national security impact	829	Impact on national security due to FedRAMP compliance
FedRAMP continuous learning	698	Emphasizing continuous learning in FedRAMP
FedRAMP legacy systems impact	462	Impact on legacy systems due to FedRAMP adoption
FedRAMP change management	257	Managing change in FedRAMP adoption
FedRAMP integration challenges	272	Challenges related to integration in FedRAMP

Note. This table provides an overview of the codes and their prevalence in the data.

Table 6 also explores the economic implications, regulatory aspects, and profound impact of FedRAMP on national security. Moreover, Table 6 underscores the pivotal role of leadership, innovation culture, continuous learning, and the potential for gaining a competitive edge through trust and credibility. In essence, Table 6 is a structured guide that enables a comprehensive grasp of the strategic dimensions and complexities inherent in achieving and maintaining FedRAMP compliance within the federal government landscape.

Table 6

Federal Risk and Authorization Management Program (FedRAMP) Emerging Themes

Theme	Key subtopics and insights
Challenges in FedRAMP compliance	Compliance challenges Resource constraints Evolving requirements Change management Integration challenges Legacy systems impact
Security and privacy	Threat mitigation Data privacy risks Data handling policies Data privacy versus compliance Cybersecurity measures
Economic implications	Cost of compliance Cost savings Return on investment Budget allocation
Regulation and legal compliance	Federal regulations Legal compliance Regulatory landscape
National security impact	National security impact Intelligence analysis Data sharing concerns
Leadership and change	Leadership vision Innovation culture Continuous learning
Competitive advantage	Competitive advantage Trust and credibility
Continuous learning and adaptation	Continuous learning Integration challenges Evolving requirements
Legacy systems impact	Legacy systems impact

Note. This table summarizes the key themes that emerged from the analysis.

Qualitative Analysis Findings

Cloud Computing Adoption

The qualitative analysis findings for cloud computing adoption, as presented in Table 7, offer a comprehensive and structured link between the research questions and the key insights derived from the data analysis. These findings provide a contextual backdrop for understanding the intricate dynamics of cloud computing adoption within federal government agencies. The challenges associated with data migration complexities and data privacy risks emerge as prominent concerns, echoing the need for a robust strategy to overcome these obstacles. Furthermore, insights into the potential efficiency gains possible through cloud-based automation and data-driven decision-making underline the transformative power of cloud technologies. The role of visionary leadership in ensuring effective integration and addressing compliance issues is underscored, emphasizing the pivotal role of leadership practices. Additionally, considerations related to costs, regulations, security, and ethical data use in the cloud resonate throughout the analysis, providing a holistic perspective on the multifaceted aspects of cloud adoption. This interplay between research questions and findings encapsulates the intricate landscape of cloud computing adoption in the federal government domain.

Table 7 serves as a valuable tool for synthesizing the core research inquiries with the pivotal insights drawn from the comprehensive analysis of cloud computing adoption. Table 7 establishes a clear and organized connection between each research question and the corresponding discoveries uncovered during the investigation.

Table 7

Research Questions and Cloud Computing Key Findings

Research question	Key findings/insights from data analysis
1. What are the critical challenges faced by federal government agencies in the adoption of CAIML in the cloud?	High number of references related to “cloud data migration challenges” and “cloud data privacy risks” indicate significant challenges. Topics such as “cloud compliance issues” and “cloud federal regulations” suggest regulatory challenges.
2. How can the integration of CAIML enhance the efficiency and effectiveness of federal government agencies’ operations and decision-making processes?	Topics such as “cloud process automation” and “cloud data-driven decision making” highlight potential efficiency gains. “Cloud visionary leadership” suggests leadership is key for effectiveness.
3. What are the economic implications of adopting CAIML in the cloud for federal government agencies?	“Cloud cost concerns” and “cloud cost savings” topics indicate cost considerations. “Cloud ROI” suggests agencies are interested in measuring ROIs.
4. What are the legal and regulatory considerations that need to be addressed in the adoption of CAIML in the cloud within the federal government?	High number of references in “cloud data privacy regulations” and “cloud data sovereignty” highlight legal and data sovereignty concerns. “Cloud federal regulations” emphasizes the importance of federal regulations.
5. What are the privacy and data protection concerns associated with the use of LLMs in CAIML applications?	“Cloud data privacy risks” and “cloud ethical use of data” topics are directly related to privacy and ethical concerns.
6. How can federal government agencies effectively address the security risks and vulnerabilities related to the use of LLMs in CAIML?	“Cloud security concerns” and “cloud cybersecurity measures” highlight security as a critical concern. “Cloud vulnerability assessment” indicates the need for risk assessment.
7. What leadership practices and strategies are required to successfully implement CAIML initiatives in the federal government?	“Cloud visionary leadership” suggests visionary leadership is crucial. “Cloud change management” indicates the importance of change management strategies.

Research question	Key findings/insights from data analysis
8. How can federal government agencies ensure a smooth migration and integration of CAIML technologies into their existing infrastructure?	"Cloud migration strategy" and "cloud integration challenges" topics related to migration and integration challenges.
9. What are the implications of adopting CAIML for national security and intelligence analysis within the federal government?	This question may require further analysis and data specifically related to national security and intelligence topics.
10. How can federal government agencies cultivate a culture of innovation and continuous learning to support the successful adoption of CAIML in the cloud?	"Cloud innovation culture" and "cloud continuous learning" suggest the importance of fostering an innovative and learning-oriented culture.

Note. This table links the research questions to key findings or insights from the cloud computing adoption data analysis. CAIML = conversational artificial intelligence and machine learning; ROI = return on investment; LLM = large language model.

It provides a concise road map with which to navigate the complex terrain of cloud adoption within federal government agencies. For instance, the link between Research Question 1 and the prevalence of cloud data migration challenges highlights the formidable obstacles to data migration. Similarly, the connection between Research Question 3 and topics like cloud cost concerns and cloud return on investment (ROI) emphasizes the economic considerations that underpin cloud adoption strategies. With each research question paired with pertinent findings, Table 7 elucidates the intricate interplay between research inquiry and empirical evidence, offering a structured perspective of the multifaceted landscape of cloud computing adoption.

Relationships and Connections.

The following relationships and connections relate to cloud computing adoption:

1. Challenges in adoption (Component 1) may necessitate addressing legal and regulatory considerations (Component 4) and security risks and vulnerabilities (Component 6) to mitigate associated risks.

2. Benefits and efficiency (Component 2) can be realized through leadership practices and strategies (Component 7) that promote innovation (Component 9).

3. Economic implications (Component 3) are influenced by budget allocation (Component 3) and can be measured through ROI (Component 3).

4. Privacy and data protection concerns (Component 5) are intertwined with the ethical use of data (Component 5) and may involve compliance issues (Component 1).

5. Migration and integration challenges (Component 8) can be guided by a migration strategy (Component 8) and align with cloud innovation culture (Component 9).

This theoretical framework provides a structured way to conceptualize the various components related to cloud computing adoption and their interrelationships, offering a foundation for further research and analysis in this area.

Table 8 offers a structured representation of the theoretical underpinnings derived from the researcher's thematic analysis of cloud computing adoption. This framework delves into the multifaceted facets of cloud adoption, categorizing them into 10 conceptual components. It delineates how challenges in adoption, benefits and efficiency, economic implications, legal and regulatory considerations, privacy concerns, security risks, leadership practices, migration challenges, culture, and national security intertwine within the context of cloud computing. Table 8 highlights the connections between these components, illustrating how handling challenges may require addressing legal and regulatory considerations and security risks. Table 8 also elucidates how leadership practices can drive innovation and how economic implications are influenced by budget allocation. This theoretical framework serves as a foundational structure for comprehending the complex landscape of cloud computing adoption and informs future research and analysis in this domain.

Table 8

Theoretical Framework for Cloud Computing Adoption

Conceptual component	Facets
1. Challenges in adoption	Cloud data migration challenges Cloud compliance issues Cloud lack of expertise Cloud cost concerns Cloud federal regulations
2. Benefits and efficiency	Cloud process automation Cloud data-driven decision making Cloud improved customer service Cloud visionary leadership
3. Economic implications	Cloud cost savings Cloud return on investment Cloud budget allocation
4. Legal and regulatory considerations	Cloud data privacy regulations Cloud data sovereignty
5. Privacy and data protection concerns	Cloud data privacy risks Cloud ethical use of data
6. Security risks and vulnerabilities	Cloud security concerns Cloud cybersecurity measures Cloud vulnerability assessment
7. Leadership practices and strategies	Cloud visionary leadership Cloud change management
8. Migration and integration challenges	Cloud migration strategy Cloud integration challenges
9. Culture of innovation and learning	Cloud innovation culture Cloud continuous learning
10. National security and intelligence implications	

Note. This table outlines the development of a theoretical framework related to cloud computing adoption based on the thematic analysis. Component 10 may require further data and analysis specific to national security and intelligence.

Storytelling AI Integration

The qualitative analysis findings for storytelling AI integration offer a profound exploration of the intricate tapestry of integration of AI-driven storytelling into various contexts. This journey unveils vital insights derived from qualitative data analysis, shedding light on the multifaceted challenges, opportunities, and strategies associated with the incorporation of AI-powered narrative technologies. These findings form a rich tapestry of knowledge that illuminates how organizations, individuals, and industries are leveraging AI to craft compelling stories, thereby reshaping engagement and communication paradigms in the digital era. As I navigate through this exploration, I unearth critical themes, emerging trends, and noteworthy patterns that underscore the transformative potential of storytelling AI integration. The qualitative analysis serves as a compass, directing the researcher's attention to key areas of interest in the realm of AI-driven narrative and its far-reaching implications.

Table 9 serves as a concise bridge between the research inquiries and the invaluable insights gleaned from the analysis of storytelling AI data. Table 9 effectively encapsulates the essential facets of exploration, mapping each research question to its corresponding key findings and insights. This structured presentation differs from a navigational tool to allow comprehension of the multifaceted landscape of CAIML adoption within federal government agencies. The findings encompass critical aspects, such as challenges, efficiency enhancements, economic implications, legal considerations, privacy concerns, security risks, leadership strategies, migration complexities, national security implications, and the fostering of innovation and continuous learning. Table 9 provides a clear and organized entry point for readers to delve into the nuanced world of storytelling AI integration, highlighting both the questions that drive the exploration and the discoveries that illuminate the researcher's path.

Table 9

Research Questions and Storytelling Artificial Intelligence (AI) Key Findings

Research question	Key findings/insights from data analysis
1. What are the key challenges faced by federal government agencies in the adoption of CAIML in the cloud?	The high number of references related to "AI data security concerns" and "AI compliance challenges" indicate significant challenges. "AI resistance to change" suggests organizational barriers.
2. How can the integration of CAIML enhance the efficiency and effectiveness of federal government agencies' operations and decision-making processes?	Topics like "AI automation" and "AI streamlined operations" highlight potential efficiency gains. "AI informed decision making" indicates the impact on decision processes.
3. What are the economic implications of adopting CAIML in the cloud for federal government agencies?	"AI cost savings" and "AI return on investment" topics indicate cost considerations. "AI budget allocation" suggests budget planning is essential.
4. What are the legal and regulatory considerations that need to be addressed in the adoption of CAIML in the cloud within the federal government?	High number of references in "AI data privacy regulations" and "AI federal regulations" highlight legal concerns. "AI compliance challenges" emphasizes the need for adherence to regulations.
5. What are the privacy and data protection concerns associated with the use of LLMs in CAIML?	"AI data privacy risks" and "AI ethical use of data" topics are directly related to privacy and ethical concerns.
6. How can federal government agencies effectively address the security risks and vulnerabilities related to the use of LLMs in CAIML?	"AI data security concerns" and "AI data security measures" highlight security as a critical concern. "AI vulnerability assessment" indicates the need for risk assessment.
7. What leadership practices and strategies are required to successfully implement CAIML initiatives in the federal government?	"AI visionary leadership" suggests visionary leadership is crucial. "AI change management" indicates the importance of change management strategies.
8. How can federal government agencies ensure a smooth migration and integration of CAIML	"AI migration strategy" and "AI integration challenges" topics related to migration and integration challenges.

Research question	Key findings/insights from data analysis
technologies into their existing infrastructure?	"AI legacy system impact" highlights the effect on existing systems.
9. What are the implications of adopting "AI national security impact" and "AI intelligence CAIML for national security and analysis" topics directly address the implications intelligence analysis within the for national security and intelligence. federal government?	
10. How can federal government agencies cultivate a culture of innovation and continuous learning to support the successful adoption of CAIML in the cloud?	"AI innovation culture" and "AI continuous learning" suggest the importance of fostering an innovative and learning-oriented culture. "AI interdisciplinary teams" indicates collaboration across disciplines.

Note. This table links the research questions to key findings or insights from the storytelling AI data analysis. CAIML = conversational AI and machine learning; LLM = large language model.

Relationships and Connections. The following relationships and connections relate to storytelling AI integration:

- Challenges in integration (Component 1) may require addressing efficiency and effectiveness (Component 2) and economic implications (Component 3) to overcome barriers.

- Legal and regulatory considerations (Component 4) are crucial for addressing privacy and data protection concerns (Component 5) and may involve compliance challenges (Component 4).

- Privacy and data protection concerns (Component 5) intersect with security risks and vulnerabilities (Component 6) and ethical use of data (Component 5).

- Leadership practices and strategies (Component 7) can drive cultural transformation (Component 10) and support migration and integration (Component 8).

This theoretical framework provides a structured way to conceptualize the various components related to AI integration and their interrelationships, offering a foundation for further research and analysis in this area.

Table 10 is a comprehensive guide to the conceptual landscape of storytelling AI integration. It elucidates the development of a structured theoretical framework based on an in-depth analysis of the subject. This framework dissects storytelling AI integration into 10 key conceptual components, ranging from challenges in integration to cultural aspects such as innovation and continuous learning. Each component represents a vital facet of AI integration, forming a cohesive map with which to understand the intricate relationships between these elements. The framework highlights connections, dependencies, and interplay among these components, providing a systematic foundation for further exploration and research in the realm of storytelling AI integration. It serves as an indispensable tool for comprehending the multifaceted dimensions of this field, offering clarity and structure to both researchers and practitioners seeking to navigate the challenges and opportunities presented by AI in storytelling.

FedRAMP Compliance

The qualitative analysis findings for FedRAMP compliance provide an illuminating exploration of the intricate terrain surrounding the adoption and implementation of FedRAMP within federal government agencies. This research delves into the multifaceted aspects of FedRAMP compliance, uncovering key challenges, implications, and strategies associated with its integration. The analysis unveils insights into how government agencies navigate the complex regulatory landscape, manage resource constraints, and address the evolving requirements of FedRAMP.

Table 10

Storytelling Artificial Intelligence (AI) Theoretical Framework

Conceptual component	Aspects
1. Challenges in integration	AI integration challenges AI legacy system impact
2. Efficiency and effectiveness	AI automation AI streamlined operations AI informed decision making AI automation
3. Economic implications	AI cost savings AI return on investment AI budget allocation
4. Legal and regulatory considerations	AI federal regulations AI compliance challenges
5. Privacy and data protection concerns	AI data privacy risks AI ethical use of data
6. Security risks and vulnerabilities	AI data security concerns AI data security measures AI vulnerability assessment
7. Leadership practices and strategies	AI visionary leadership AI change management
8. Migration and integration challenges	AI migration strategy AI integration challenges
9. National security and intelligence implications	AI national security impact AI intelligence analysis
10. Culture of innovation and learning	AI innovation culture AI continuous learning AI interdisciplinary teams

Note. This table outlines the development of a theoretical framework related to storytelling AI based on the analysis.

It also highlights the economic implications, legal and regulatory considerations, and security risks associated with the adoption of CAIML in the cloud within the federal government context.

Furthermore, this study sheds light on the leadership practices required for successful implementation, the importance of addressing legacy systems' impact, and the cultivation of a culture of innovation and continuous learning to support the adoption of advanced technologies. These findings offer a comprehensive understanding of the FedRAMP compliance landscape, aiding policymakers, government officials, and researchers in their pursuit of secure and compliant cloud technology adoption.

Table 11 serves as a valuable bridge between the research questions and key findings derived from an in-depth analysis of federal government agencies' adoption of CAIML in the cloud, with a specific focus on FedRAMP compliance. Table 11 distills the multifaceted research inquiries into concise insights and discoveries. Table 11 reveals that FedRAMP compliance challenges are at the forefront, underscored by the complexity of the regulatory landscape and resource constraints faced by these agencies. Additionally, Table 11 sheds light on the potential for enhanced efficiency through adaptability and change management while emphasizing the significance of improved security and cybersecurity measures as economic implications. Legal and regulatory considerations, privacy and data protection concerns, and leadership practices are also highlighted, offering a comprehensive overview of the key dimensions involved in this adoption process. Lastly, the table addresses migration and integration challenges, the impact on legacy systems, and the cultivation of an innovative and interdisciplinary culture, presenting a structured framework for understanding this intricate landscape.

Table 11

Research Questions and Federal Risk and Authorization Management Program (FedRAMP) Compliance Key Findings

Research question	Key findings/insights from data analysis
1. What are the key challenges faced by federal government agencies in the adoption of CAIML in the cloud?	"FedRAMP compliance challenges" is a prominent challenge with a high number of references. "FedRAMP regulatory landscape" suggests the complex regulatory environment. "FedRAMP resource constraints" indicate limitations in resources.
2. How can the integration of CAIML enhance the efficiency and effectiveness of federal government agencies' operations and decision-making processes?	"FedRAMP resource constraints" highlight resource limitations. "FedRAMP evolving requirements" points to the need for adaptability. "FedRAMP change management" indicates the importance of managing change effectively.
3. What are the economic implications of adopting CAIML in the cloud for federal government agencies?	"FedRAMP enhanced security" emphasizes improved security as a benefit. "FedRAMP cybersecurity measures" indicates the importance of cybersecurity. "FedRAMP threat mitigation" suggests efforts to mitigate threats.
4. What are the legal and regulatory considerations that need to be addressed in the adoption of CAIML in the cloud within the federal government?	"FedRAMP trust and credibility" relates to trust and credibility. "FedRAMP competitive advantage" suggests potential advantages.
5. What are the privacy and data protection concerns associated with the use of LLMs in CAIML?	"FedRAMP cost of compliance" and "FedRAMP cost savings" highlight cost considerations. "FedRAMP ROI" touches on the ROI aspect.
6. How can federal government agencies effectively address the security risks and vulnerabilities related to the use of LLMs in CAIML?	"FedRAMP regulatory landscape" and "FedRAMP legal compliance" emphasize the legal and regulatory aspects.
7. What leadership practices and strategies are required to successfully implement CAIML initiatives in the federal government?	"FedRAMP data privacy risks" and "FedRAMP data handling policies" are directly related to data privacy.

Research question	Key findings/insights from data analysis
	"FedRAMP compliance versus privacy" suggests a potential trade-off.
8. How can federal government agencies ensure a smooth migration and integration of CAIML technologies into their existing infrastructure?	"FedRAMP migration strategies" and "FedRAMP integration challenges" relate to migration and integration challenges.
9. What are the implications of adopting CAIML for national security and intelligence analysis within the federal government?	"FedRAMP legacy systems impact" suggests an impact on legacy systems. "FedRAMP national security impact" and "FedRAMP intelligence analysis" relate to national security and intelligence.
10. How can federal government agencies cultivate a culture of innovation and continuous learning to support the successful adoption of CAIML in the cloud?	"FedRAMP innovation culture" and "FedRAMP continuous learning" emphasize fostering a culture of innovation and learning. "FedRAMP interdisciplinary teams" highlights collaboration across disciplines.

Note. This table links research questions to key findings or insights from the data analysis. CAIML = conversational AI and machine learning; LLM = large language model; ROI = return on investment.

Relationships and Connections.

The following relationships and connections relate to FedRAMP compliance:

- Challenges in compliance (Component 1) may intersect with economic implications (Component 4) and security implications and benefits (Component 2).
- Security implications and benefits (Component 2) are essential for building reputation, trust, and competitive advantage (Component 3).
- Legal and regulatory considerations (Component 5) have implications for privacy and data handling (Component 6).

- Migration and integration strategies (Component 7) are crucial for compliance, impact on legacy systems, and national security (Component 8).

- Cultural transformation (Component 9) is closely linked to leadership vision and collaboration (Component 10).

Table 12 presents a comprehensive theoretical framework meticulously constructed based on the analysis of FedRAMP compliance in the context of cloud computing adoption. This framework comprises 10 key conceptual components that encompass the challenges, benefits, implications, and considerations intrinsic to this complex domain. It articulates the interconnections among these components, highlighting the intricate relationships that exist. For instance, it underscores how challenges in compliance can intersect with economic implications and security implications and benefits. Legal and regulatory considerations are intertwined with privacy and data handling, while migration and integration strategies play a pivotal role in addressing compliance, legacy systems impact, and national security concerns. Moreover, the framework recognizes that cultural transformation is closely related to leadership vision and collaboration. In essence, this theoretical framework provides a structured lens through which to perceive the multifaceted aspects of FedRAMP compliance, paving the way for further research and analysis in this crucial field.

Summary

In summary, the qualitative data analysis not only uncovered the challenges and opportunities within each domain but also highlighted the interconnectedness of these areas. The cost-efficiency and security concerns identified in cloud computing adoption are crucial considerations when evaluating the adoption of advanced technologies. Storytelling AI's role in

communication and decision support underscores its potential for transforming how government agencies convey information and make informed choices.

Table 12

Theoretical Framework for Federal Risk and Authorization Management Program (FedRAMP) Compliance

Conceptual component	Aspects
1. Challenges in compliance	FedRAMP compliance challenges FedRAMP resource constraints FedRAMP evolving requirements
2. Security implications and benefits	FedRAMP enhanced security FedRAMP cybersecurity measures FedRAMP Threat Mitigation
3. Reputation, trust, and competitive advantage	FedRAMP trust and credibility FedRAMP competitive advantage
4. Economic implications	FedRAMP cost of compliance FedRAMP cost savings FedRAMP return on investment
5. Legal and regulatory considerations	FedRAMP regulatory landscape FedRAMP legal compliance
6. Privacy and data handling	FedRAMP data privacy risks FedRAMP data handling policies FedRAMP compliance versus privacy
7. Migration and integration strategies	FedRAMP migration strategies FedRAMP integration challenges
8. Impact on legacy systems and national security	FedRAMP legacy systems impact FedRAMP national security impact FedRAMP intelligence analysis
9. Cultural transformation	FedRAMP innovation culture FedRAMP continuous learning FedRAMP interdisciplinary teams
10. Leadership vision and collaboration	FedRAMP leadership vision FedRAMP collaboration

Note. This table outlines the development of a theoretical framework related to cloud computing adoption based on the analysis.

Additionally, the government's strong emphasis on FedRAMP compliance and its integration with cloud adoption emphasizes the importance of regulatory and legal factors in technology implementation. These findings collectively enrich the dissertation research by providing a holistic view of the intricate landscape in which technology, regulation, leadership, and culture intersect in government agencies' pursuit of innovation and efficiency.

Expert Studies/Interviews Findings

The findings from expert survey studies and interviews, involving a total of 12 participants (10 surveys and two interviews), shed valuable light on critical aspects of technology adoption and the role of storytelling AI within federal government agencies. Experts highlighted substantial challenges—such as FedRAMP compliance issues, resource constraints, and complex regulatory landscapes—impacting the adoption of CAIML in the cloud. Moreover, they emphasized the potential for these technologies to enhance efficiency and effectiveness in agency operations and decision-making processes, particularly through improved intelligence and streamlined operations. Economic implications, including cost considerations and budget allocation, were of central concern. Legal and regulatory considerations, privacy, and data protection concerns were also prominent, underscoring the importance of navigating these aspects effectively. The findings further emphasized the need for visionary leadership, change management, and interdisciplinary teams to implement these initiatives successfully. The expert insights enrich the understanding of the challenges and opportunities within this domain, offering a robust foundation for the research.

Table 13 provides a concise overview of the key themes identified in relation to the number of references they received and their relevance to specific codes. The themes include the threat theme, which corresponds to codes pertaining to specific threat types, and the compliance theme,

which aligns with codes addressing compliance-related issues. The data theme encompasses codes concerning data management and analysis, while the assessment theme encompasses those related to assessments and risk assessments. The security and intelligence themes encompass codes concerning security concerns and intelligence topics, respectively. The model theme relates to codes regarding AI/ML models and algorithms, while the monitoring theme includes codes about monitoring practices. Other themes—such as the cloud, analysis, leadership, budget, integration, skill, cost, considerations, allocation, user, policies, response, regulatory compliance, privacy, improved intelligence, and consent themes—correspond to their respective codes and add depth to the analysis by highlighting the prevalence and relevance of these themes within the collected survey data.

Table 14 provides a comprehensive overview of the top themes and their associated subthemes based on their associated numbers of files and references. The threat theme emerges as the most prevalent, with 16 references, encompassing subthemes like threat modeling, threat intelligence integration, and cyber threats. The user theme is another prominent theme, with a focus on user-related concerns, including user data protection, user data privacy, and user consent. The threat detection theme is another significant theme, with a subtheme hierarchy covering aspects like enhanced threat detection and accelerating threat detection. The skill theme represents the importance of skills in the context of the study, with subthemes highlighting skill shortages and skill gaps. Lastly, the security theme is a major theme, encompassing various subthemes such as network security, national security risk assessment, and continuous security monitoring. Table 14 offers a structured view of the most prevalent themes and their associated subthemes within the survey data, providing valuable insights into the primary concerns and topics discussed by the participants.

Table 13

Survey/ Interview Themes

Name	References	Relevance to codes
Threat	16	Corresponds to codes for specific threat types
Compliance	15	Corresponds to codes addressing compliance
Data	12	Encompasses codes on data management and analysis
Assessment	11	Encompasses codes related to assessments and risk assessments
Security	8	Encompasses codes on security concerns
Intelligence	8	Encompasses codes related to intelligence topics
Model	7	Relates to codes on AI/ML models and algorithms
Monitoring	6	Encompasses codes about monitoring practices
Threat detection	6	Includes codes on “threat detection methods”
Cloud	6	Pertains to codes related to cloud computing
Analysis	6	Contains codes about various types of analysis
Leadership	6	Corresponds to codes discussing leadership
Budget	6	Relates to codes discussing budget allocation
Integration	5	Contains codes about AI/ML integration
Skill	5	Relates to codes about skills needed for AI/ML
Cost	5	Relates to codes about costs in AI/ML implementation
Considerations	5	Contains codes discussing various considerations
Allocation	5	Corresponds to codes on resource allocation
User	5	Related to “user experience” or “user feedback”
Policies	4	Contains codes related to organizational policies
Response	4	Contains codes regarding responses to threats
Regulatory compliance	4	Includes codes about compliance requirements

Name	References	Relevance to codes
Privacy	4	Pertains to codes addressing privacy issues
Improved intelligence	4	Pertains to codes emphasizing intelligence improvements
Consent	5	Encompasses codes related to user consent

Note. AI = artificial intelligence; ML = machine learning.

Integration of Findings

In this journey, the researcher navigated through a complex landscape where diverse information sources converged to yield a thorough and anchored perspective of the subject. The scope and detail of the conclusions were profoundly enriched by comprehensive analysis coupled with validation and triangulation processes.

The spectrum of the insights was sourced from systematic literature review and primary data collection methods, offering a varied range of perspectives. Macro trends identified via the PRISMA review blended with the intricate details discovered during personal interviews; together, these formed a complete image of the research domain. NVivo's (Version 14) analytical tools played a fundamental role by effectively incorporating vast quantities of data, classifying and labeling them into thematically consistent nodes. These nodes, serving as specialized theme-storage spaces, ensured each information snippet was aptly incorporated into the overarching story. Furthermore, NVivo's visualization instruments offered clarity regarding data intersections, points of overlap, and areas of divergence. As I progressed, numerous emergent themes came to the fore, arising inherently from the data patterns, adding another dimension to the insights.

Table 14

Top Five Themes With Subthemes

Theme and subtheme	References
User	5
User data protection	2
User data privacy	1
User consent	1
Data use	1
Threat detection	6
Threat detection	4
Enhanced threat detection	1
Accelerating threat detection	1
Threat	16
Threat modeling	2
Threat intelligence integration	1
Threat hunting	1
Threat detection	4
Threat assessment	1
Robust threat monitoring	1
Real-time threat analysis	1
Enhanced threat detection	1
Enhanced threat assessment capabilities	1
Cyber threats	1
Augmented threat analysis capabilities	1
Accelerating threat detection	1

Theme and subtheme	References
Skill	5
Skills development	1
Skilled personnel	1
Skill shortages	1
Skill gaps	2
Security	8
Network security	1
National security risk assessment	1
National security measures	1
National security intelligence	1
National security insights	1
Continuous security monitoring	1
Comprehensive security strategy	1
Cloud security tools	1

Validation and Triangulation

The systematic literature review findings acted as a foundational reference point. Aligning primary data with this foundation resulted in either reinforcing its authenticity through concurrence or presenting interesting variations. Such variations were perceived as insights into the ever-evolving nature of the research focus rather than mere deviations. A distinguishing feature of the study was the uniformity evident across diverse data collection methodologies. Whether an insight emerged from a survey's statistical output or an interview's qualitative depth, there was a consistent thematic echo, reinforcing the final assertions. Wherever discrepancies surfaced, I interpreted them as gateways to deeper understanding rather than as obstacles, allowing us to grasp

the multifarious aspects of the topic. Enhancing the triangulation process, I involved several validators. Comprising experts and involved parties, they independently scrutinized the conclusions, contributing their unique viewpoints. Their feedback, irrespective of its nature, enriched understanding by adding various shades of interpretation.

In summary, the research outcomes are grounded in a detailed and systematic methodology. Comprehensive analysis ensured each piece of information, regardless of origin, was appropriately contextualized, resulting in a narrative both detailed and unified. Subsequent validation and triangulation cemented the researcher's assertions, offering them a firm base. This blend of thoroughness, diversity, and academic diligence means the study not only enriches scholarly discussions but also provides tangible insights to practitioners in the domain.

Table 15 presents a comprehensive analysis of major themes and subthemes identified across multiple data sources, including the PRISMA review and survey/interview data. These findings demonstrate strong convergence and triangulation across different data sources, enhancing the validity and reliability of the results. In the PRISMA data, the theme of cloud data migration challenges is well supported by subthemes highlighting issues related to data format and compatibility, complexities in data transformation, and risks of operational disruptions during migration. Similarly, in the survey/interview data, the user theme aligns with subthemes related to user data protection, privacy, consent, and data use. The theme of threat detection in both data sources also demonstrates alignment, with subthemes covering various aspects of threat detection. Furthermore, the security theme in the survey/interview data corresponds to subthemes regarding network security, national security risk assessment, measures, intelligence, insights, continuous monitoring, and cloud security tools. These consistent findings across different data sources validate and triangulate the major themes and subthemes, strengthening the overall credibility and robustness of the analysis.

Discussion of Findings

Several key themes and subthemes emerged from the comprehensive analysis of data collected through PRISMA review and surveys/interviews. These findings shed light on critical aspects of technology adoption and security across cloud computing, AI applications, and compliance with FedRAMP within the context of federal government agencies. Notably, cloud data migration challenges surfaced as a significant concern, with a substantial number of references. Issues related to data format and compatibility, complexities in data transformation during migration, and the risk of operational disruptions underscore the intricacies involved in transitioning data to the cloud. These challenges reflect the need for meticulous planning and execution strategies in government agencies aiming to adopt cloud technologies successfully. Similarly, AI data security concerns and FedRAMP threat mitigation highlighted the paramount importance of data security and threat management. Data encryption, strict access controls, and cybersecurity defense mechanisms are essential for adoption of AI and compliance with FedRAMP, especially when handling sensitive government information. These findings emphasize the critical role of security in the implementation of emerging technologies.

Table 15

Comprehensive Analysis

Major theme identified	References	Emergent subthemes
		Data source: PRISMA
Cloud data migration challenges	1,342	Challenges associated with data migration in the cloud Issues related to data format and compatibility Complexities in transforming data during migration Risks of disruptions to operations during migration
AI data security concerns	1,342	Concerns about data security in AI applications Ensuring data is encrypted to prevent unauthorized access

Major theme identified	References	Emergent subthemes
		Implementing strict access controls to protect data
		Guarding against cybersecurity threats and breaches
FedRAMP threat mitigation	4,261	Mitigating threats in FedRAMP compliance
		Implementing security measures to mitigate threats
		Assessing threats to develop mitigation strategies
		Managing risks associated with FedRAMP compliance
Data source: Surveys/interviews		
User	5	User data protection
		User data privacy
		User consent
		Data use
Threat detection	6	Threat detection
		Enhanced threat detection
		Accelerating threat detection
Threat	16	Threat modeling
		Threat intelligence integration
		Threat hunting
		Threat detection
		Threat assessment
		Robust threat monitoring
		Real-time threat analysis
		Enhanced threat detection
		Enhanced threat assessment capabilities
		Cyber threats
		Augmented threat analysis capabilities
		Accelerating threat detection
Skill	5	Skills development
		Skilled personnel
		Skill shortages
		Skill gaps
Security	8	Network security
		National security risk assessment
		National security measures
		National security intelligence
		National security insights
		Continuous security monitoring
		Comprehensive security strategy
		Cloud security tools

Note. PRISMA = Preferred Reporting Items for Systematic Reviews and Meta-Analyses; AI = artificial intelligence; FedRAMP = Federal Risk and Authorization Management Program.

Furthermore, the findings from surveys and interviews revealed user-centric concerns, such as user data protection, privacy, consent, and data use, echoing the significance of addressing user rights and privacy in technology adoption. Threat detection and security emerged as recurring themes in both the PRISMA review and surveys/interviews, emphasizing the ubiquitous nature of security considerations across various technological domains. The attention to network security, national security risk assessment, and intelligence further underscored the government's unwavering commitment to safeguarding its digital assets. The findings also highlighted the importance of continuous security monitoring, comprehensive security strategies, and utilization of cloud security tools. Overall, the findings underscore the multifaceted nature of challenges and considerations surrounding technology adoption in federal government agencies, emphasizing the need for comprehensive strategies that encompass data migration, security, and user-centric concerns while complying with stringent regulations like FedRAMP.

Validation and Trustworthiness of Findings

In Chapter 3, I discussed the importance of ensuring the trustworthiness of research findings, which is essential for maintaining the credibility and integrity of a study. Trustworthiness is a critical aspect of qualitative research, especially in an action research design like the one employed in this dissertation. This section delves into the validation and trustworthiness of the findings, revisiting the criteria of credibility, transferability, dependability, and confirmability discussed in Chapter 3 and describing the strategies employed to address these criteria. The rest of this section describes how each of the trustworthiness criteria—credibility, transferability, dependability, and confirmability—was met in the data collection and analysis processes in this dissertation.

Credibility in this research was rigorously addressed through various strategies in both the data collection and analysis phases. To ensure the trustworthiness of the findings, multiple data sources—including interviews, observations, and document analysis—were leveraged. This triangulation of data sources not only enriched the depth of evidence but also provided opportunities for cross-verification, strengthening the credibility of the collected data, a practice in line with Yin's (2018) recommendations. Moreover, during the data analysis process, member checking was employed as an additional credibility-enhancing measure. This involved sharing preliminary findings and interpretations with the participants, allowing them to assess and confirm the accuracy and relevance of the results, as advocated by Saldaña (2021). The practice of member checking served to ensure that the participants' perspectives were faithfully and authentically represented in the analysis, thereby bolstering the overall credibility of the research outcomes.

The transferability of the research findings was a key consideration in this study, and efforts were made to enhance the applicability of the results to diverse contexts. To achieve this, detailed descriptions of the research context, participant characteristics, and research processes were meticulously provided throughout the study, following the guidance of Ante and Ante (2016). These comprehensive descriptions enabled readers to assess the relevance and applicability of the findings to their own specific contexts, thereby increasing the potential for transferability. Additionally, transferability was further addressed using purposeful sampling in data collection. Participants were deliberately selected based on their ability to offer insights that could be relevant to a broader population, as recommended by Palinkas et al. (2015). The aim of this thoughtful sampling strategy was to ensure that the research findings could be extrapolated and applied in similar contexts and settings, reinforcing the transferability of the study's outcomes.

Dependability, which focuses on the consistency and reliability of research processes and findings, was rigorously addressed in this study. To establish dependability, a detailed audit trail

was maintained throughout the data collection process. This trail documented every step of the research procedures, including decisions and revisions, following the guidelines of Rana et al. (2021). This meticulous documentation ensures that the research process can be replicated, leading to consistent results if the study is repeated. Furthermore, dependability was reinforced through the practice of peer debriefing. Colleagues and experts in the field were consulted, and their feedback on the research process and analysis was sought, in alignment with the recommendations of Lexis and Julien (2022). This external input played a crucial role in maintaining the consistency and rigor of the research, contributing to the dependability of the study's outcomes.

Confirmability, which focuses on the objectivity and neutrality of research processes, was rigorously addressed in this study to ensure the credibility of the findings. In terms of data collection, researchers took measures to ensure objectivity by following established protocols and maintaining a neutral stance during interviews and observations. This approach helped minimize any potential bias that could have influenced the data collection process. Moreover, confirmability was reinforced during data analysis through the utilization of qualitative data analysis software like NVivo (Version 14), as recommended by Paulus (2023). NVivo facilitated a systematic and transparent analysis of the data, reducing the likelihood of researcher bias in identification of patterns and themes. To further enhance confirmability, reflexive practices were consistently employed throughout the data analysis process, in accordance with Saldaña's (2021) guidance. Researchers continually acknowledged and reflected on their potential biases, ensuring that personal biases did not unduly impact the analysis and contributing to the objectivity of the research.

By consistently integrating these strategies into both data collection and analysis processes, the dissertation aimed to meet the trustworthiness criteria. The use of diverse data sources, member checking, detailed descriptions, purposeful sampling, detailed documentation, peer debriefing,

objective data collection, qualitative data analysis software, and reflexive practices collectively contributed to the credibility, transferability, dependability, and confirmability of the research findings. These efforts were essential for ensuring the validity, reliability, and trustworthiness of the study's results, strengthening its contribution to the field of study.

Triangulation, a methodological approach employed in this dissertation research, played a pivotal role in enhancing the validity and credibility of the findings. I strategically applied triangulation in several ways to validate the research outcomes. Firstly, data source triangulation was instrumental, as I harnessed multiple data sources, encompassing interviews, observations, and documents. This multifaceted approach allowed us to capture diverse facets of the research topic, offering a comprehensive and well-rounded perspective. Interviews provided insights from participants, observations facilitated direct observation of behaviors, and document analysis contributed to historical context and official records. This convergence of information from various sources bolstered the reliability and accuracy of the findings.

In closing, triangulation played a crucial role in validating the findings of this dissertation by enhancing the trustworthiness of the research. It helped ensure that the conclusions drawn from the data were robust and reliable. By collecting data from multiple sources, using diverse research methods, seeking external input, and cross-verifying information, I demonstrated a commitment to rigorous research practices and strengthened the overall quality of this study. Triangulation is a valuable technique that adds depth and credibility to qualitative research and contributes to the robustness of the research findings.

Limitations

In conducting this research across the domains of cloud computing, storytelling AI, and FedRAMP, it was imperative to recognize and address potential limitations that could have influenced the outcomes and generalizability of the study. Firstly, data availability and quality

were constraints I encountered by relying on publicly accessible data sources that might not encompass the entirety of relevant information. This limitation could have introduced gaps in the analysis and potentially impacted the extent to which the researcher's findings can be broadly applied.

Secondly, time constraints were an unavoidable aspect of the research process, which could have impacted the depth of exploration within the selected domains. Given the scope and complexity of the study, it might not have been feasible to delve into all facets as comprehensively as desired. Consequently, this limitation might affect the depth of the researcher's insights and the degree to which the conclusions can be extrapolated to broader contexts.

Thirdly, resource limitations, such as access to specialized software and hardware, constituted a constraint I faced. These constraints might have restricted the range of experiments or analyses I could conduct, potentially influencing the breadth of the research and the robustness of the findings.

Furthermore, the sampling methods employed in the research could have introduced sampling bias, given that the sample might not fully represent the entire population within the studied domains. Additionally, the dynamic nature of the external environment, including regulatory changes and technological advancements, poses the risk of impacting the relevance and applicability of the researcher's findings over time.

Lastly, while rigorous research methodologies were adopted, methodological limitations are inherent in any study. These could encompass measurement errors, potential biases in surveys or interviews, or assumptions made during modeling. Considering the interplay of these limitations, it is vital to recognize that the findings may have limited generalizability beyond the specific contexts, time frames, and samples examined. The distinctive combination of factors in

the research might not be directly transferrable to all scenarios within the domains of cloud computing, storytelling AI, and FedRAMP.

Conclusion

Chapter 4 represents a pivotal point in this dissertation, where the researcher delved into the key findings and their significance with respect to addressing the research questions. This chapter consolidates the insights obtained from the systematic literature review, qualitative analysis, and expert interviews/studies. These findings not only contribute to a deeper understanding of the interplay between cloud computing, storytelling AI, and FedRAMP adoption but also hold important implications for the broader fields of technology and compliance.

Key Findings and Their Significance

Intersecting Forces.

The research revealed that cloud computing, with its inherent scalability and flexibility, is a powerful enabler of storytelling AI applications. Furthermore, the adoption of FedRAMP in the public sector plays a pivotal role in ensuring the security and compliance of cloud-based AI solutions. This intersection of forces highlights the critical need for a holistic approach to technology adoption within government agencies.

Challenges and Opportunities.

Through the analysis and expert insights, the researcher identified several challenges to the adoption of storytelling AI within the FedRAMP framework. These challenges include data privacy concerns, regulatory complexities, and the need for tailored risk assessments. However, I also uncovered opportunities for innovation and collaboration in addressing these challenges, suggesting avenues for future research and industry development.

Compliance and Innovation.

The findings emphasize the delicate balance between regulatory compliance and innovation. While FedRAMP compliance is essential for government agencies, it should not stifle the development and deployment of cutting-edge AI solutions. Effective compliance strategies should be agile and adaptable to accommodate technological advancements.

Contributions to the Field

This study makes several notable contributions to the fields of cloud computing, storytelling AI, and FedRAMP adoption.

Enhanced Understanding.

The research enhances the understanding of how cloud computing and storytelling AI intersect with compliance frameworks like FedRAMP, shedding light on the challenges and opportunities in this intersection.

Practical Insights.

The practical insights gained from the qualitative analysis and expert interviews provide actionable recommendations for government agencies, technology developers, and policymakers navigating the complex landscape of AI adoption in regulated environments.

Bridging Gaps.

By identifying areas of misalignment and potential disconnects between technology and compliance, I am contributing to bridging the gap between innovation and regulation, fostering a more conducive environment for the deployment of advanced AI solutions.

Summary of Chapter 4

In summary, the dissertation's findings provide valuable insights and indirectly address several of the research questions by shedding light on challenges, regulatory considerations, security concerns, and the need for a culture of compliance and responsible AI development in the

federal government's adoption of CAIML in the cloud. These insights contribute to a comprehensive understanding of the adoption landscape.

Transition to Chapter 5

Chapter 4 serves as the foundation upon which I construct Chapter 5. In the upcoming chapter, I draw comprehensive conclusions from the findings and offer pragmatic recommendations for stakeholders in cloud computing, storytelling AI, and FedRAMP adoption. By synthesizing the insights gathered in Chapter 4, I aim to provide a road map for navigating the evolving landscape of technology compliance and innovation, ensuring that government agencies can harness the full potential of storytelling AI within the confines of regulatory frameworks.

CHAPTER 5: CONCLUSION

Introduction

In the dynamic and ever-evolving landscape of technology adoption and security within federal government agencies, the research has ventured into uncharted territories to provide a comprehensive and illuminating exploration of the intricate interplay between Cloud Computing, Storytelling AI, and the Federal Risk and Authorization Management Program (FedRAMP) (Qasem et al., 2021). As the researcher approaches the conclusion of this study, Chapter 5 serves as the crowning achievement of the extensive efforts, meticulously bringing together the key findings, profound insights, and invaluable contributions that have emerged during this transformative research journey. This chapter not only revisits the primary research questions but also dissects the implications of the findings, underscores the immense significance of the contributions to academia and practice, and extends a guiding hand by offering actionable recommendations to shape policy and practice in this ever-evolving domain. Moreover, the researcher acknowledges the study's limitations with transparency and provides a clear roadmap for future research endeavors, ensuring that the torch of knowledge continues to illuminate this critical landscape.

The research has embarked on a mission to explore the intricate relationships and challenges that surface at the intersection of Cloud Computing, Storytelling AI, and the formidable regulatory framework known as FedRAMP (El-Gazzar, 2014). In this endeavor, the researcher navigated a complex and multifaceted terrain armed with the tools of inquiry, analysis, and synthesis. Guided by specific research questions, the researcher unearthed a wealth of insights that provide a panoramic view of the technological and security landscape within federal government agencies (Vu et al., 2020). The findings illuminate the challenges faced in adopting Cloud Computing, the transformative power of Storytelling AI in data security (Gama & Magistretti,

2023), and the critical importance of FedRAMP compliance (Nugraha & Martin, 2021). Through rigorous inquiry, this researcher has not only uncovered the complexities but has also identified practical solutions and pathways to navigate this intricate terrain.

As the researcher culminates this research journey, the researcher recognizes the profound implications of the findings. The researcher's insights serve as a compass for government agencies seeking to harness the benefits of Cloud Computing while safeguarding sensitive data (Ali, 2016). They spotlight the potential of Storytelling AI as a tool to enhance data security practices (Wang et al., 2021). Importantly, the research underscores the significance of FedRAMP compliance in shaping the technology landscape within the federal government (Zeng, 2016). Beyond these implications, the study contributes to the scholarly discourse surrounding technology adoption, data security, and regulatory compliance, enriching the academic arena with a deeper understanding of these critical domains (Madan, Ashok, et al., 2023a; Madan, Ashok, et al., 2023b). Furthermore, the practical recommendations provide a roadmap for policymakers and practitioners to enhance technology adoption strategies, fortify data security measures, and navigate the labyrinth of regulatory compliance with confidence and efficacy (Polisetty et al., 2023).

In conclusion, the research journey has been a testament to the ever-advancing landscape of technology adoption and security within federal government agencies (Stevens et al., 2022). With each research question, each interview conducted, and each data point analyzed, the researcher has contributed to the body of knowledge in this domain (Carney, 2019). As the reader steps into the future, they will carry with them the torch of knowledge illuminated by this research, guiding them toward more secure, efficient, and compliant technology practices in service of the public interest.

Recapitulations of the study

In this concluding chapter, research embarks on a journey of reflection and synthesis, revisiting the fundamental aspects of the research to offer a comprehensive recapitulation of the study. The rigorous investigation delved into the multifaceted relationships that exist between Cloud Computing, Storytelling AI, and the Federal Risk and Authorization Management Program (FedRAMP) within the intricate landscape of federal government agencies. With a determined focus on a quest to address specific research questions that were strategically designed to unravel the complex tapestry of challenges, opportunities, and implications arising from the convergence of these transformative domains. As the reader traverses the terrain of this concluding chapter, the primary aim is to distill the essence of the dissertation, encapsulating the critical findings and profound insights that have emerged throughout the exploration.

Throughout this dissertation journey, the researcher navigated the intricate web of Cloud Computing adoption, data security, and compliance with FedRAMP standards within the unique context of federal government agencies. The candidate embarked on this scholarly voyage with a clear mission: to unearth the underlying challenges, illuminate the potential opportunities, and delineate the far-reaching implications inherent in the synergy of Cloud Computing and Storytelling AI. The guiding research questions were the compass, each carefully calibrated to help us navigate this uncharted territory. Through rigorous inquiry and meticulous analysis, the candidate uncovered a trove of knowledge that sheds light on the intricacies of technology adoption, data protection, and regulatory compliance. The journey has been one of discoveries, forging new pathways of understanding in the dynamic nexus of these domains.

As the researcher navigates this final chapter, the researcher endeavor to encapsulate the wealth of knowledge and insights that have surfaced throughout the research. The exploration has provided a unique vantage point, offering a panoramic view of the challenges that accompany the

adoption of Cloud Computing in government agencies. It has allowed us to harness the power of Storytelling AI as a transformative tool in the realm of data security and FedRAMP compliance. Furthermore, the findings carry significant policy implications and offer practical guidance to practitioners in the field. The recommendations aim to serve as actionable steps for enhancing data security practices and embracing innovative technologies while staying aligned with regulatory frameworks. This concluding chapter seeks to synthesize these vital aspects, offering a comprehensive recapitulation of the research to guide future endeavors in this ever-evolving landscape.

Recapitulation of Research Questions

The research was guided by the following primary research questions:

1. What are the key challenges faced by federal government agencies in the adoption of Conversational AI and Machine Learning in the cloud?
2. How can the integration of Conversational AI and Machine Learning enhance the efficiency and effectiveness of federal government agencies' operations and decision-making processes?
3. What are the economic implications of adopting Conversational AI and Machine Learning in the cloud for federal government agencies?
4. What are the legal and regulatory considerations that need to be addressed in the adoption of Conversational AI and Machine Learning in the cloud within the federal government?
5. What are the privacy and data protection concerns associated with the use of Large Language Models (LLMs) in Conversational AI and Machine Learning applications?

6. How can federal government agencies effectively address the security risks and vulnerabilities related to the use of LLMs in Conversational AI and Machine Learning?
7. What leadership practices and strategies are required to successfully implement Conversational AI and Machine Learning initiatives in the federal government?
8. How can federal government agencies ensure a smooth migration and integration of Conversational AI and Machine Learning technologies into their existing infrastructure?
9. What are the implications of adopting CAIML for national security and intelligence analysis within the federal government?
10. How can federal government agencies cultivate a culture of innovation and continuous learning to support the successful adoption of Conversational AI and Machine Learning in the cloud?

Discussions in alignment with each research question.

Research Question 1: Challenges in Adopting Conversational AI and Machine Learning in Federal Government Agencies

This research aimed to uncover the primary challenges faced by federal government agencies in adopting Conversational AI and Machine Learning technologies in cloud environments. The findings reveal a complex landscape of barriers and difficulties, primarily centered around data security, workforce expertise, and procedural inefficiencies.

Data Security and Privacy Concerns: A paramount challenge identified is the protection of sensitive and classified information. The integration of AI and ML technologies necessitates handling large datasets, elevating risks related to data breaches and unauthorized access. Compliance with stringent security standards, such as those mandated by FedRAMP, adds layers

of complexity. This necessitates the development of robust data protection strategies that align with regulatory requirements, ensuring that AI and ML implementations do not compromise data integrity.

Shortage of Skilled Personnel: The effective deployment of Conversational AI and Machine Learning requires specialized skills and knowledge. However, federal agencies face significant hurdles in recruiting and retaining individuals proficient in these areas. This skills gap poses a critical barrier to the adoption and optimal use of AI and ML technologies. Addressing this challenge calls for focused efforts in workforce development, including training programs and partnerships with academic institutions to cultivate a pipeline of qualified professionals.

Procurement and Acquisition Processes: The study also highlights the complexities of procurement and acquisition processes within federal agencies. The nature of rapidly evolving AI and ML technologies often clashes with the existing bureaucratic procedures, leading to delays and inefficiencies. Streamlining these processes is essential to facilitate quicker and more efficient adoption of these technologies. This could involve revising procurement policies to be more adaptive to technological advancements and fostering collaborations with tech providers for smoother integration.

Conclusion: The challenges outlined above underscore the need for a holistic approach to integrating Conversational AI and Machine Learning in the cloud within federal government agencies. This approach should encompass enhancing data security measures, bridging the skills gap through targeted workforce development, and reforming procurement policies. Such comprehensive strategies are crucial for leveraging the potential of AI and ML technologies to improve government operations while adhering to necessary security and regulatory standards.

Research Question 2: Enhancing Operations and Decision-Making in Federal Government Agencies through AI and ML

This research investigates the transformative impact of Conversational AI and Machine Learning on the operational efficiency and decision-making processes of federal government agencies. The findings highlight the multifaceted benefits of these technologies, which extend to automation, citizen engagement, and enhanced decision-making capabilities.

Automation and Process Optimization: A significant advantage of integrating Conversational AI and ML is the automation of routine tasks. By deploying AI-driven tools like chatbots, agencies can offload mundane inquiries and administrative tasks to these systems. This shift not only bolsters efficiency by allowing human personnel to focus on complex and strategic work but also minimizes human error in routine operations. Machine Learning algorithms play a critical role in parsing large datasets to discern patterns and anomalies. This capability is invaluable in predictive analytics, aiding agencies in proactive decision-making and resource management.

Enhancing Citizen Engagement and Service Delivery: Conversational AI technologies like chatbots and virtual assistants revolutionize how agencies interact with citizens. These tools offer 24/7 accessibility, providing timely and accurate responses to public inquiries. This enhanced level of engagement is instrumental in improving citizen satisfaction and trust in government services. The ability of AI systems to handle high volumes of interactions simultaneously significantly improves service delivery efficiency.

Data-Driven Decision Making: Machine Learning algorithms are pivotal in augmenting decision-making within agencies. By analyzing diverse data sources, these algorithms can generate insights and recommendations that are crucial for informed policymaking. Applications range from public health trend predictions to national security threat assessments. The ability to make

data-driven decisions allows for more effective resource allocation and quicker response to evolving national and societal needs.

Conclusion: The integration of Conversational AI and Machine Learning stands as a beacon of advancement in public sector operations and governance. These technologies promise enhanced efficiency, improved citizen services, and more informed decision-making processes. However, realizing these benefits fully requires careful consideration of data privacy and ethical issues associated with AI deployment. Addressing these challenges is essential to harness the full spectrum of opportunities presented by AI and ML in enhancing federal government agencies' effectiveness and efficiency.

Research Question 3: Economic Implications of Adopting AI and ML in Federal Government Agencies

This research explores the economic ramifications of implementing Conversational AI and Machine Learning technologies in federal government cloud environments. The findings underscore the potential for significant cost savings, increased operational efficiency, and enhanced public services, alongside the necessity of balancing these with initial investment costs.

Cost Savings and Increased Efficiency: A primary economic benefit of integrating Conversational AI and ML is the reduction in labor costs through automation. Technologies like chatbots and virtual assistants can handle routine administrative tasks, thereby reducing the workload on government staff. This shift not only allows employees to focus on higher-value activities but also diminishes the need for expanding the workforce, leading to notable cost savings. Moreover, the automation of repetitive tasks contributes to higher operational efficiency and reduces the likelihood of errors associated with manual processes.

Data-Driven Decision Making and Resource Optimization: Machine Learning algorithms provide substantial economic advantages by enabling data-driven decision-making.

These algorithms can analyze extensive datasets to pinpoint inefficiencies, thereby optimizing resource allocation and uncovering potential areas for cost reduction. In sectors like healthcare, ML-driven predictive analytics can proactively identify patients at risk, facilitating early intervention and potentially lowering long-term healthcare expenditures. In defense and security, Machine Learning aids in strategic resource allocation by predicting emerging threats.

Improved Citizen Services and Economic Growth: The deployment of Conversational AI and ML also translates into improved citizen services, enhancing public satisfaction and trust in government agencies. This increased satisfaction can lead to higher compliance with regulations and policies, reducing enforcement costs. Moreover, efficient, and responsive public services can attract businesses and investments, stimulating regional economic development.

Balancing Initial Investment Costs: While the economic benefits are substantial, it is critical to consider the initial costs involved in developing and deploying these AI solutions. This includes expenses related to staff training and infrastructure upgrades. Given the budget constraints typical in government agencies, a comprehensive cost-benefit analysis is essential to ascertain the long-term economic viability of adopting these technologies.

Conclusion: The adoption of Conversational AI and Machine Learning in federal government cloud environments presents significant economic benefits, including cost savings, operational efficiency, and enhanced public services. However, these benefits must be weighed against the initial investment costs. Careful financial planning and cost-benefit analysis are crucial for government agencies to ensure that the economic advantages of these technologies are fully realized and sustained.

Research Question 4: Legal and Regulatory Considerations in AI and ML Adoption

This research addresses the complex legal and regulatory framework surrounding the use of Conversational AI and Machine Learning in federal government settings. The findings

underscore the importance of navigating a myriad of legal considerations to ensure compliant and ethical technology implementation.

Data Privacy and Security Compliance: One of the foremost legal challenges is adhering to data privacy and security regulations. Government agencies handle sensitive data, necessitating strict compliance with laws like HIPAA and FISMA. These regulations set stringent guidelines for the handling, storage, and protection of sensitive information. AI and ML solutions must align with these legal requirements to safeguard citizen privacy and ensure data integrity. This involves implementing secure encryption, robust access controls, and effective data governance practices.

Ethical and Fairness Considerations: The ethical deployment of AI technologies is paramount. Agencies must commit to fairness, transparency, and accountability in AI utilization. This includes adhering to frameworks like the General Data Protection Regulation (GDPR), which mandates clear explanations for automated decisions and avenues for citizen recourse. AI algorithms must be scrutinized for bias and discrimination to prevent legal ramifications and uphold ethical standards in public sector AI applications.

Procurement Law Compliance: The acquisition of AI and ML technologies is governed by procurement regulations. Compliance with laws such as the FAR is crucial to ensure transparent and fair procurement practices. These regulations guide how government agencies can procure technology solutions, necessitating a careful approach by vendors to align with these legal requirements.

Cross-Border Data Transfer Regulations: For cloud-based AI solutions, cross-border data transfer presents additional legal complexities. Agencies must consider international regulations like the GDPR, which imposes strict conditions on the transfer of personal data beyond EU borders. Adhering to these regulations might require implementing specific data protection mechanisms, such as SCCs or BCRs, to ensure legal compliance in international contexts.

Intellectual Property and Licensing: The adoption of AI technologies also involves navigating intellectual property rights and licensing agreements. Government agencies need to ensure they possess appropriate rights and licenses for the use of AI algorithms and software. Understanding and negotiating these licensing agreements is critical to avoid legal disputes and ensure proper usage rights.

Conclusion: The legal and regulatory landscape for adopting Conversational AI and Machine Learning in federal government agencies is multifaceted and complex. Agencies must rigorously adhere to laws and regulations concerning data privacy, security, ethical use, procurement, cross-border data transfer, and intellectual property. Navigating this landscape is essential not only to leverage the advantages of AI and ML but also to uphold the rule of law and protect the rights of citizens. Ensuring legal and ethical compliance is as critical as technological implementation, forming the backbone of responsible AI use in government.

Research Question 5: Privacy and Data Protection Concerns in the Use of LLMs

This research examines the crucial aspects of privacy and data protection in the application of Large Language Models within federal government agencies. The use of LLMs, which process extensive textual data, brings forth several challenges and considerations in the realm of data privacy and ethical use.

Data Privacy and Compliance: The handling of sensitive information by LLMs is a primary concern, especially when considering the extensive datasets required for training these models. Federal agencies must navigate these concerns cautiously to prevent unintentional exposure or misuse of citizen data. Compliance with stringent data protection regulations, like GDPR and HIPAA, is crucial to uphold individual privacy rights and maintain data integrity.

Transparency and Explainability: The complexity of LLMs often results in them being perceived as 'black boxes,' making it difficult to discern how they arrive at specific decisions. This

lack of transparency can raise concerns about potential biases and unfair outcomes, particularly in critical applications. Agencies need to focus on enhancing the transparency of these models and providing understandable explanations for their automated decisions to address these concerns.

Unintentional Data Leakage: A significant risk associated with LLMs is the inadvertent leakage of sensitive or personally identifiable information. Implementing stringent safeguards to prevent such leaks is essential to avoid legal and reputational repercussions.

Mitigating Bias and Ensuring Ethical Use: LLMs are susceptible to learning biases present in their training data, which can lead to unfair or discriminatory outcomes. Agencies must actively work to mitigate such biases by ensuring training datasets are diverse and representative, and by employing techniques for bias detection and correction.

Data Security Measures: Protecting LLMs from unauthorized access, cyberattacks, and data breaches is intertwined with privacy concerns. Robust security measures, including encryption and access controls, are fundamental to ensuring the security of these models.

International Data Protection Compliance: For federal agencies dealing with international data, compliance with cross-border data transfer regulations becomes crucial. Adhering to regulations such as the GDPR may necessitate additional measures, including data localization or specific data transfer mechanisms.

Conclusion: Research Question 5 underscores the importance of addressing privacy and data protection concerns in the use of Large Language Models for Conversational AI and Machine Learning applications within federal government settings. Agencies must navigate these concerns diligently to ensure the ethical and responsible use of LLMs, prioritizing individual privacy, promoting transparency, and safeguarding against data breaches and biases. Addressing these challenges is key to leveraging the benefits of LLMs in governmental applications while maintaining a steadfast commitment to privacy and data protection principles.

Research Question 6: Addressing Security Risks in LLMs for Government Agencies

This research focuses on the crucial aspect of security in the deployment of Large Language Models within federal government agencies, particularly in the areas of Conversational AI and Machine Learning. The discussion highlights a range of security threats and proposes comprehensive strategies to mitigate these risks.

Cybersecurity Threats: Like many digital technologies, LLMs are vulnerable to a spectrum of cybersecurity threats, ranging from external hacking attempts to internal data breaches. Implementing robust cybersecurity measures is crucial. This includes deploying firewalls, intrusion detection systems, and strong encryption protocols to safeguard LLMs and the sensitive data they process.

Data Privacy and Confidentiality: The extensive processing of textual data by LLMs, some of which may be confidential, necessitates stringent data privacy and confidentiality measures. Encryption, access control, and data anonymization techniques are essential to protect sensitive information from unauthorized access or exposure.

Adversarial Attacks: LLMs are susceptible to adversarial attacks where input data is manipulated to produce incorrect or harmful outputs. These attacks can be particularly detrimental in critical decision-making contexts. Investing in research and technology to detect and counteract these attacks is vital for enhancing the security and robustness of LLMs.

Supply Chain Risks: The reliance of LLMs on pre-trained models and third-party libraries introduces supply chain risks. Assessing and ensuring the security of these components is imperative to prevent vulnerabilities originating from external dependencies.

Ethical and Bias Considerations: Security concerns in LLMs also encompass ethical issues, such as bias in training data. Establishing guidelines and policies to address and mitigate biases is crucial for maintaining fairness and avoiding legal and ethical implications.

Continuous Monitoring and Incident Response: Establishing continuous monitoring systems is essential for the timely detection of security incidents. Additionally, well-defined incident response plans are necessary to effectively address and mitigate the impact of security breaches.

Regulatory Compliance: Ensuring compliance with relevant regulations and standards, such as HIPAA and FISMA, is critical. Regular audits and assessments can aid in demonstrating adherence to these legal requirements.

Interagency Collaboration: The complexity of security risks associated with LLMs can be better managed through collaboration and information sharing among agencies. This collaborative approach enhances the collective security posture through shared threat intelligence and best practices.

Conclusion: Addressing the security risks associated with the use of LLMs in federal government agencies involves a multifaceted approach. Comprehensive cybersecurity measures, vigilant data protection, resilience against adversarial threats, and a commitment to ethical standards are integral components of effective mitigation strategies. As the application of LLMs continues to expand, continuous efforts to strengthen security are vital for protecting sensitive government data and maintaining the integrity and trustworthiness of these advanced AI applications.

Research Question 7: Leadership Practices for AI and ML Implementation in Federal Agencies

This research addresses the indispensable role of effective leadership in the successful implementation of Conversational AI and Machine Learning within federal government agencies. The findings highlight various leadership practices and strategies that are critical in guiding organizations through the adoption of these transformative technologies.

Visionary Leadership: The implementation of AI and ML technologies necessitates visionary leadership. Leaders must articulate a clear and compelling vision of how these technologies can enhance government operations, decision-making processes, and citizen services. This vision serves as a guiding light, inspiring teams, and stakeholders to embrace the adoption process.

Change Management: The introduction of AI and ML represents a significant cultural and procedural shift within organizations. Leaders need to be proficient in change management, equipping employees with the necessary tools and knowledge to adapt to new technologies. Effective communication, comprehensive training programs, and strategies to address resistance are essential components of successful change management.

Cross-Functional Collaboration: Successful AI and ML implementations require cooperation across various departments and teams. Leaders should foster an environment of cross-functional collaboration, ensuring that AI initiatives are well-integrated with organizational objectives and benefit from diverse perspectives.

Data Governance: Leaders play a crucial role in establishing and enforcing robust data governance practices. This involves ensuring that data collection, management, and usage comply with relevant regulations and policies, and emphasizing the importance of data quality, security, and privacy.

Resource Allocation: Strategic allocation of resources is vital for the implementation of AI and ML projects. Leaders must ensure that adequate budget, personnel, and technology infrastructure are available and are utilized effectively to support these initiatives and their long-term success.

Risk Management: AI and ML projects come with inherent risks and uncertainties. Leaders should be adept in identifying, assessing, and mitigating these risks to prevent potential project failures and ensure sustainable outcomes.

Ethical Leadership: Given the ethical implications of AI and ML, particularly in government contexts, leaders must champion ethically practices. This includes ensuring that AI algorithms are fair, transparent, unbiased, and aligned with ethical data handling and decision-making principles.

Innovation and Adaptation: The rapidly evolving nature of technology demands a culture of innovation and adaptability. Leaders should encourage experimentation with emerging technologies and be open to adapting strategies in response to technological advancements.

Performance Metrics and Accountability: Establishing clear performance metrics and holding teams accountable for the outcomes of AI and ML projects is essential. This approach enables leaders to track progress, measure success, and ensure that initiatives achieve their intended objectives.

Stakeholder Engagement: Effective leaders engage actively with stakeholders, including citizens, policymakers, and industry partners. Managing expectations, soliciting feedback, and maintaining transparency throughout the implementation process are key to successful stakeholder engagement.

Long-Term Strategy: Forward-thinking leadership involves developing long-term strategies that anticipate future technological changes and evolving mission requirements. Leaders should focus on sustainable approaches that can adapt to future advancements in AI and ML.

Conclusion: Effective leadership is fundamental to the successful adoption and implementation of Conversational AI and Machine Learning initiatives in federal government agencies. Visionary leadership, adept change management, cross-functional collaboration, ethical

considerations, and a commitment to innovation are paramount. Leaders must skillfully navigate the complexities of AI adoption, prioritize ethical and data governance practices, and cultivate a culture conducive to innovation and long-term success.

Research Question 8: Integrating AI and ML into Federal Government Infrastructure

This research examines the critical steps and considerations necessary for the effective migration and integration of Conversational AI and ML technologies within the existing infrastructure of federal government agencies. The findings highlight the multifaceted nature of this process and the strategies required to ensure successful implementation.

Infrastructure Assessment: The first step for agencies is a thorough evaluation of their current infrastructure, encompassing hardware, software, network capabilities, and data storage systems. This comprehensive assessment is crucial to identify areas that may require upgrades or modifications to accommodate AI and ML technologies.

Compatibility Analysis: Ensuring compatibility between existing systems and new AI/ML technologies is paramount. Agencies must evaluate whether their current systems can seamlessly integrate with these new technologies or if modifications are necessary. Addressing compatibility issues proactively is essential to avoid disruptions in operations.

Data Readiness: Given the data-centric nature of AI and ML, agencies must assess the quality, volume, and availability of their data. Preparing data for AI processing involves cleaning, standardization, and ensuring accessibility. Establishing robust data governance practices is also key to ensuring data security and compliance.

Scalability Considerations: Scalability should be a foundational element of AI and ML initiatives. Even if starting with pilot projects, the design should facilitate scaling to meet future requirements and expansion needs.

Security Measures: Integrating AI and ML into government systems requires heightened security measures. Agencies must implement encryption, access controls, and continuous monitoring systems to protect sensitive data and prevent cyber threats.

Interoperability: Given the diversity of software and systems used by government agencies, ensuring interoperability is critical for smooth operations. Standardized interfaces and protocols can facilitate this integration.

Training and Skill Development: Preparing the workforce for the integration of AI and ML is essential. This involves training and upskilling employees in relevant AI and ML concepts and tools to enable effective utilization of these technologies.

Change Management: Addressing the human aspect of technology integration through effective change management is vital. Strategies to ease the transition include clear communication, comprehensive training, and addressing any resistance to new workflows and processes.

Vendor Collaboration: Working closely with AI and ML technology vendors is crucial. This collaboration ensures that agencies understand system requirements, receive necessary support, and are kept up to date with maintenance and updates.

Testing and Validation: Before full-scale deployment, rigorous testing and validation are necessary to identify and resolve any issues. This step is crucial to minimize disruptions and ensure the smooth functioning of the technology post-deployment.

Compliance and Regulations: Agencies must ensure that their AI and ML implementations comply with all relevant federal regulations and standards. This adherence is non-negotiable and is essential for lawful and ethical technology deployment.

Continuous Monitoring and Evaluation: Ongoing success requires continuous monitoring and evaluation. Establishing KPIs to assess the impact of AI and ML technologies on operations and decision-making processes is a key aspect of this ongoing assessment.

Conclusion: The migration and integration of Conversational AI and ML technologies into the infrastructure of federal government agencies demands careful planning, thorough assessment, and meticulous execution. By addressing key considerations such as compatibility, scalability, security, and compliance, agencies can effectively harness the transformative potential of AI and ML, while maintaining operational efficiency and security.

Research Question 9: Implications of CAIML in National Security and Intelligence

Research Question 9 delves into the implications of adopting Conversational AI and Machine Learning (CAIML) for national security and intelligence analysis within the federal government. This is a critical and sensitive area where technology adoption can have significant ramifications. Let's discuss the key considerations and implications.

1. **Enhanced Intelligence Analysis:** The adoption of CAIML can significantly enhance the capabilities of intelligence analysts. These technologies can process and analyze vast amounts of data quickly, helping analysts identify patterns, trends, and potential threats more efficiently.
2. **Real-time Threat Detection:** CAIML can provide real-time threat detection and alerting. By continuously monitoring data streams, these technologies can identify suspicious activities or potential security threats promptly, allowing for rapid response.
3. **Predictive Analysis:** Machine Learning algorithms can be trained to predict security threats or potential risks based on historical data. This proactive approach allows agencies to take preventive measures before threats materialize.

4. **Data Fusion:** CAIML can integrate data from various sources, including open-source intelligence, social media, and classified information. This data fusion enables a more comprehensive and holistic understanding of security threats.
5. **Anomaly Detection:** CAIML excels in anomaly detection, which is crucial in identifying unusual or unexpected patterns in data. This can be particularly valuable in uncovering covert activities or cybersecurity breaches.
6. **Cybersecurity:** National security relies heavily on robust cybersecurity measures. CAIML can bolster cybersecurity by continuously monitoring network traffic, identifying vulnerabilities, and responding to threats in real time.
7. **Reduced Human Error:** Automation through CAIML can reduce the risk of human error in intelligence analysis. Analysts can focus on higher-level decision-making while AI handles data processing and initial assessments.
8. **Resource Optimization:** CAIML can optimize resource allocation by identifying areas of high risk or priority. This ensures that limited resources are directed where they are needed most.
9. **Ethical Considerations:** The use of CAIML in national security and intelligence raises ethical concerns, including privacy issues and potential biases in algorithms. Striking a balance between security and individual rights is a complex challenge.
10. **Human-AI Collaboration:** The successful integration of CAIML into national security operations requires effective collaboration between AI systems and human analysts. Agencies must establish processes for meaningful human-AI interaction.
11. **Regulatory Compliance:** Government agencies must adhere to legal and regulatory frameworks when using CAIML for national security. Compliance with laws related to data privacy, surveillance, and intelligence activities is essential.

12. **Transparency and Accountability:** Ensuring transparency in AI decision-making and maintaining accountability for AI-generated outcomes are critical. This includes explaining how AI arrived at specific conclusions or recommendations.
13. **Adversarial Attacks:** National security agencies must be prepared for adversarial attacks on AI systems. Threat actors may attempt to manipulate AI models to deceive or disrupt intelligence operations.
14. **Continuous Learning and Adaptation:** CAIML models must continuously learn and adapt to evolving threats. Agencies need mechanisms for updating and retraining AI models to stay ahead of adversaries.

In conclusion, the adoption of CAIML in national security and intelligence analysis within the federal government has far-reaching implications. While these technologies offer the potential for enhanced threat detection, predictive analysis, and resource optimization, they also raise ethical, legal, and accountability challenges. Striking the right balance between security and individual rights, ensuring compliance with regulations, and preparing for adversarial attacks are crucial aspects of successfully leveraging CAIML for national security. A thoughtful, responsible, and adaptive approach is essential to harness the full potential of these technologies while safeguarding national interests.

Research Question 10: How can federal government agencies cultivate a culture of innovation and continuous learning to support the successful adoption of Conversational AI and Machine Learning in the cloud?

Research Question 10 focuses on the cultivation of a culture of innovation and continuous learning within federal government agencies to support the successful adoption of Conversational AI and Machine Learning (CAIML) in the cloud. This question delves into the organizational and

cultural aspects necessary for embracing these transformative technologies effectively. Let's explore the key points of discussion:

1. **Importance of Innovation Culture:** Embracing innovation is vital for government agencies seeking to harness the potential of CAIML. An innovation culture encourages employees to explore new ideas, experiment with emerging technologies, and find creative solutions to complex challenges.
2. **Support for Risk-Taking:** Innovation often involves taking calculated risks. Government agencies need to create an environment where employees feel supported in trying new approaches and are not unduly penalized for occasional failures.
3. **Leadership and Vision:** Senior leadership plays a critical role in fostering innovation. Leaders must articulate a clear vision for the agency's future with CAIML and demonstrate their commitment to innovation by providing resources and removing barriers.
4. **Cross-Functional Collaboration:** Innovation thrives when different departments and teams collaborate. Federal agencies should encourage cross-functional teams to work together, bringing diverse perspectives to problem-solving.
5. **Learning and Development:** Continuous learning is essential in the rapidly evolving field of AI and ML. Agencies should invest in training and development programs to upskill employees and keep them updated on the latest advancements.
6. **Experimentation and Prototyping:** Innovation is often an iterative process that involves experimentation and prototyping. Agencies should provide the necessary resources and support for employees to develop and test CAIML applications.

7. **Knowledge Sharing:** Establishing platforms for knowledge sharing and best practice dissemination can accelerate the adoption of CAIML. Employees should have opportunities to share their learnings and insights with colleagues.
8. **Recognition and Rewards:** Recognizing and rewarding innovative efforts can motivate employees to contribute actively to the adoption of CAIML. Incentives, awards, or recognition programs can encourage innovation.
9. **Diversity and Inclusion:** Diverse teams with varied backgrounds and perspectives are more likely to generate innovative ideas. Agencies should promote diversity and inclusion to foster a culture of innovation.
10. **Change Management:** The transition to CAIML may encounter resistance. Effective change management strategies, including clear communication, stakeholder engagement, and addressing concerns, are vital.
11. **Measurement of Innovation:** Agencies should establish key performance indicators (KPIs) to measure the effectiveness of their innovation initiatives. Regular assessments can help fine-tune innovation efforts.
12. **External Partnerships:** Collaboration with external partners, including industry experts, academia, and other government agencies, can bring fresh ideas and resources to the innovation process.
13. **Scalability and Sustainability:** Innovations that prove successful should be scaled across the organization, and their sustainability should be ensured through institutionalization.
14. **Ethical Considerations:** As part of the innovation culture, agencies must prioritize ethical considerations, including data privacy, fairness, and transparency, in CAIML applications.

In conclusion, cultivating a culture of innovation and continuous learning is pivotal for federal government agencies to successfully adopt CAIML in the cloud. Such a culture encourages experimentation, collaboration, and adaptability, all of which are essential in the rapidly evolving landscape of AI and ML technologies. Leadership commitment, employee empowerment, and a focus on ethical practices contribute to building a culture that supports innovation and ensures that federal agencies can harness the full potential of CAIML for improved operations and decision-making.

The exploration into the potential of Storytelling AI in enhancing data security and FedRAMP compliance uncovered significant insights. Storytelling AI offered a novel approach to analyzing and visualizing data patterns, thereby supporting threat detection and monitoring. The technology enabled real-time threat analysis and the identification of emerging cybersecurity threats. Additionally, Storytelling AI facilitated the development of narratives that aided in threat modeling and intelligence integration. Its role in augmenting threat assessment capabilities and accelerating threat detection was noteworthy. By harnessing the power of Storytelling AI, federal government agencies could strengthen their data security measures while aligning with FedRAMP requirements.

Contributions of the study

Amidst an era heavily influenced by technology, it is crucial to comprehend the complexities involved in implementing advanced technological solutions within government agencies. This study provides a thorough examination of the intricate and dynamic landscape of cloud computing, storytelling AI, and Federal Risk and Authorization Management Program (FedRAMP) compliance in federal government agencies. The presented findings illuminate the complex challenges and opportunities involved in adopting technology. Additionally, they offer a

detailed comprehension of how innovative technological solutions interact with the strict demands of data security and regulatory compliance.

This research provides crucial insights into how government agencies can effectively incorporate new technologies such as cloud computing and AI, while maintaining strict security and compliance standards, during the ongoing technological revolution. The importance of this study resides in its thorough analysis of the difficulties, possibilities, and effects of these technological integrations, along with specific suggestions for policymakers, federal agencies, and the research community.

This section explores the main contributions of the study and highlights the importance of its findings, emphasizing the study's role in establishing a fundamental framework for future progress in technology adoption, data security, and compliance in the public sector. As we examine these contributions, it becomes clear that the study not only tackles the immediate issues related to the adoption of technology, but also paves the way for continued research and policy development in this constantly changing field.

Implications

The research findings presented in this study hold significant implications for various stakeholders, including federal government agencies, policymakers, researchers, and the broader field of technology adoption, security, and compliance. These implications highlight the importance of addressing the evolving landscape of technology adoption and data security within federal agencies and offer guidance for future research and policymaking.

Significance of the Findings:

Federal Government Agencies: The findings underscore the complex challenges faced by federal government agencies when adopting Cloud Computing and Storytelling AI. These

agencies should consider investing in cybersecurity measures, skill development, and robust compliance frameworks to navigate these challenges effectively.

Policymakers: Policymakers can use the insights from this research to craft policies that promote responsible technology adoption while ensuring data security and regulatory compliance. These policies should strike a balance between innovation and safeguarding sensitive information.

Researchers: The study contributes to the academic discourse by providing empirical evidence of the challenges and opportunities in technology adoption within government agencies. Researchers can build on these findings to delve deeper into specific aspects of data security, compliance, and emerging technologies.

The Field of Study: The research advances the field of technology adoption, security, and compliance by offering a nuanced understanding of the interplay between Cloud Computing, Storytelling AI, and FedRAMP. It highlights the need for a multidisciplinary approach to address the complexities of these domains effectively.

Substantive Implications:

Management: Government agency management should prioritize investments in cybersecurity measures, training programs, and compliance strategies to ensure the secure and responsible adoption of emerging technologies.

Unions and Interest Groups: These stakeholders can advocate for the inclusion of data security and skill development provisions in labor agreements to address the identified skill shortages and gaps.

Public Policy: The study suggests that public policy should encourage agencies to adopt innovative technologies while adhering to stringent data security and compliance standards. This approach can foster technological advancements while safeguarding sensitive information.

Nation-building: Effective technology adoption and data security are crucial for national security and the efficient functioning of government agencies. The findings emphasize the role of technology in nation-building efforts.

Theoretical Contributions Regarding Cloud Computing Adoption

This dissertation's concluding chapter brings together the theoretical insights gleaned from the research on Cloud Computing Adoption in federal government settings. The discussion is structured around the research questions, each contributing to a comprehensive understanding of the complexities involved in adopting cloud technologies.

Challenges in Cloud Adoption (Research Question 1). The following points relate to challenges in cloud adoption.

Data Migration Challenges. Agencies face difficulties in safely and efficiently moving large volumes of data to cloud environments. This involves technical complexities and potential data loss risks.

Cloud Compliance Issues. Navigating the maze of compliance requirements like FedRAMP is daunting, requiring extensive knowledge of legal mandates and security protocols.

Lack of Cloud Expertise. A significant barrier is the shortage of skilled professional adept in cloud technologies, making it challenging to manage and optimize cloud infrastructure.

Cloud Cost Concerns. Budget constraints and the need for cost-effective solutions are paramount. Agencies must balance the cost of transitioning to and maintaining cloud services against potential long-term savings.

Cloud Federal Regulations. Adhering to federal regulations demands robust security measures and compliance strategies, adding layers of complexity to cloud adoption.

Enhancing Efficiency and Effectiveness (Research Question 2). The following points relate to enhancing efficiency and effectiveness.

Cloud Process Automation. Automating routine tasks and processes can significantly improve operational efficiency, freeing up valuable resources.

Cloud Data-Driven Decision-Making. Leveraging cloud computing for data analysis enhances decision-making, providing insights that were previously unattainable due to data volume and complexity.

Cloud Visionary Leadership. The role of leadership is crucial in envisioning and driving the adoption process, encouraging innovation, and aligning cloud adoption with organizational goals.

Economic Implications (Research Question 3). The following points relate to economic implications.

Balancing Costs and Savings. Agencies must carefully assess the short-term costs of cloud adoption against the long-term financial benefits, such as reduced infrastructure and operational costs.

Assessing ROI. Calculating the return on investment is essential for justifying cloud adoption, considering both tangible and intangible benefits.

Legal and Regulatory Considerations (Research Question 4). The following points relate to legal and regulatory considerations.

Navigating Data Privacy Laws. Compliance with data privacy regulations is critical, especially given the sensitivity of government data.

Data Sovereignty. The location of data storage in the cloud raises legal considerations, especially when data is stored across national boundaries.

Privacy and Data Protection Concerns (Research Question 5). The following points relate to privacy and data protection concerns.

Safeguarding Sensitive Data. Implementing strong privacy controls and data protection strategies is key to maintaining public trust and adhering to legal standards.

Ethical Use of Data. Ensuring ethical use of data, particularly in AI applications, involves addressing potential biases and maintaining transparency.

Security Risks and Vulnerabilities (Research Question 6). The following points relate to security risks and vulnerabilities.

Cybersecurity Measures. Developing comprehensive cybersecurity frameworks to protect against threats like data breaches and cyber-attacks is essential.

Vulnerability Assessments. Regular assessments to identify and mitigate vulnerabilities in cloud infrastructure are necessary for maintaining security integrity.

Leadership Practices and Strategies (Research Question 7). The following points relate to leadership practices and strategies.

Navigating Cultural Shifts. Leaders must manage the cultural changes associated with cloud adoption, promoting an environment that embraces new technologies and methodologies.

Change Management. Effective strategies to manage the transition to cloud computing, including employee training and engagement, are vital for smooth adoption.

Migration and Integration Challenges (Research Question 8). The following points relate to migration and integration challenges.

Strategic Planning for Migration. Developing a well-thought-out migration strategy is key to minimizing downtime and ensuring data integrity during the transition.

Integration with Existing Systems. Ensuring that new cloud solutions integrate seamlessly with existing systems to maintain operational continuity is a critical challenge.

National Security and Intelligence (Research Question 9). The following points relate to national security and intelligence.

Enhanced Analytical Capabilities: The potential for cloud computing to revolutionize intelligence analysis through advanced data processing and analytics is significant.

Security and Privacy in Intelligence: Balancing the enhanced capabilities with the need to protect sensitive information and adhere to privacy standards is a complex challenge.

Summary

The theoretical contributions of this research provide a comprehensive understanding of the multifaceted nature of cloud computing adoption in federal government agencies. This understanding highlights the need for strategic planning, skilled workforce development, robust security and privacy measures, and visionary leadership to navigate the challenges and harness the benefits of cloud technologies. These insights lay a foundation for future research and policy formulation in this critical area of technological advancement in the public sector.

Storytelling AI Integration

In this concluding chapter, the researcher presents a comprehensive synthesis of our findings on Storytelling AI Integration within federal government agencies. Each segment of the discussion is meticulously aligned with a specific research question, unraveling the complex tapestry of AI-driven storytelling integration. This exploration, rooted in qualitative analysis, delves into the multifaceted nature of storytelling AI, highlighting the myriad challenges, opportunities, and strategic considerations inherent in weaving AI-powered narrative technologies into the fabric of government operations. Our analysis offers a nuanced understanding of this innovative domain, spotlighting key areas that are pivotal in the successful adoption and implementation of storytelling AI across various governmental contexts. This chapter not only

consolidates our research findings but also paves the way for future exploration in this dynamic and evolving field.

Challenges in AI Integration (Research Question 1). The following points relate to challenges in AI integration.

AI Integration Challenges: Researchers should delve into the specific technical and compatibility issues agencies face when integrating new AI technologies with existing systems.

AI Legacy System Impact: Researchers should explore how legacy systems within government agencies might impede or complicate the integration of advanced AI technologies, requiring updates or reconfiguration.

Efficiency and Decision-Making (Research Question 2). The following points relate to efficiency and decision making.

AI-Driven Process Automation: Researchers should examine how automating tasks with AI leads to operational efficiencies, reducing manual labor and streamlining workflows.

Data-Driven Insights for Decision-Making: Researchers should detail how AI's ability to process and analyze large data sets leads to more informed and strategic decision-making processes.

Influence of Visionary Leadership: Researchers should discuss the role leaders play in fostering a culture that embraces AI-driven changes and how their vision and direction are critical for successful AI integration.

Economic Implications (Research Question 3). The following points relate to economic implications.

Balancing Costs and ROI: Researchers should analyze the cost implications of AI adoption, including initial investments, maintenance, and potential long-term savings. Researchers should investigate how agencies measure ROI and make budgetary decisions.

AI Budget Allocation Considerations: Researchers should investigate budgeting strategies and considerations related to allocating funds to AI initiatives within federal agencies.

Legal and Regulatory Considerations (Research Question 4). The following points relate to legal and regulatory considerations.

Compliance Challenges: Researchers should delve deeper into the specific legal and regulatory hurdles agencies must navigate, including data protection laws and specific federal regulations impacting AI use.

Adherence to Federal Regulations: Researchers should analyze how federal agencies align AI implementations with existing legal frameworks and regulatory requirements.

Privacy and Data Protection (Research Question 5). The following points relate to privacy and data protection.

Managing Privacy Risks with LLMs: Researchers should explore in detail the privacy concerns related to using LLMs, including the potential for data breaches and misuse of sensitive information.

Ethical Use of AI Data: Researchers should discuss the ethical considerations related to handling and processing data through AI, focusing on maintaining transparency and fairness.

Security Risks and Vulnerabilities (Research Question 6). The following points relate to security risks and vulnerabilities.

AI Security Measures: Researchers should investigate the specific security measures required to protect AI systems from external threats and internal vulnerabilities.

Regular Risk Assessments: Researchers should examine the frequency and depth of risk assessments needed to ensure the ongoing security of AI integrations.

Leadership in AI Implementation (Research Question 7). The following points relate to leadership in AI implementation.

Change Management Strategies: Researchers should discuss how leaders within federal agencies manage the transition to AI, including employee training, management of resistance, and communication strategies.

Innovation Leadership: Researchers should analyze how leaders can foster innovative environments that are receptive to AI advancements and continuous learning.

Migration and Integration (Research Question 8). The following points relate to migration and integration.

Strategies for AI Technology Transition: Researchers should examine the strategic planning and execution involved in migrating existing systems and workflows to AI-based solutions.

Overcoming Integration Challenges: Researchers should detail the challenges faced when integrating AI technologies into existing infrastructures and how agencies overcome these hurdles.

National Security Implications (Research Question 9).

With regard to the potential for future research, researchers should outline the areas where further research is needed, especially in relation to the specific implications of AI for national security and intelligence analysis.

Summary

In summary, the discussion aligns with the research questions, providing insights into the challenges, efficiency enhancements, economic implications, legal considerations, privacy concerns, security risks, leadership strategies, migration complexities, and national security implications associated with storytelling AI integration within federal government agencies. These

findings offer a comprehensive understanding of the multifaceted landscape of AI-driven narrative technologies and their potential transformative impact. The research provides a valuable foundation for future exploration and analysis in this dynamic and evolving field.

FedRAMP Compliance

Challenges in Cloud Adoption (Research Question 1). The following points relate to challenges in cloud adoption.

Navigating FedRAMP Compliance: Researchers should discuss the intricate process federal agencies follow to meet the rigorous standards set by FedRAMP, focusing on the specific compliance hurdles and technical complexities involved.

Regulatory Environment and Resource Constraints: Researchers should analyze how the regulatory landscape of FedRAMP impacts the allocation of resources and how agencies manage these limitations while striving for compliance.

Operational Efficiency and Decision-Making (Research Question 2). The following points relate to operational efficiency and decision making.

Evolving FedRAMP Requirements: Researchers should investigate the dynamic nature of FedRAMP standards and how agencies adapt their operations and decision-making processes to remain compliant.

Resource Management: Researchers should examine the strategies agencies employ to manage their resources efficiently within the constraints imposed by FedRAMP compliance.

Economic Implications (Research Question 3). The following points relate to economic implications.

Cost-Benefit Analysis of Compliance: Researchers should delve into the economic aspects of achieving FedRAMP compliance, analyzing initial costs versus long-term security and operational benefits.

ROI in Security Enhancements: Researchers should explore the ROI that agencies can expect from improved cybersecurity measures mandated by FedRAMP.

Legal and Regulatory Framework (Research Question 4). The following points relate to the legal and regulatory framework.

Trust and Credibility in Compliance: Researchers should discuss how adherence to FedRAMP standards can enhance an agency's trustworthiness and credibility, potentially offering a competitive edge.

Navigating Legal Compliance: Researchers should analyze the complexities involved in ensuring that CAIML initiatives align with FedRAMP and other relevant legal frameworks.

Privacy and Data Protection (Research Question 5). The following points relate to privacy and data protection.

Balancing Compliance and Privacy: Researchers should explore the intersection of compliance costs and privacy concerns, particularly in relation to the use of LLMs in CAIML applications.

Economic Perspective on Privacy: Researchers should discuss the economic implications of maintaining data privacy and protection in the context of FedRAMP compliance.

Security Risks and Vulnerabilities (Research Question 6).

Regarding management of legal and regulatory security aspects, researchers should examine the strategies employed by federal agencies to navigate the legal and regulatory dimensions of security risks in cloud-based AI applications.

Leadership and Implementation Strategies (Research Question 7).

Regarding the role of leadership in data privacy, researchers should discuss the significance of effective leadership in management of data privacy risks and adherence to FedRAMP data-handling policies.

Migration and Integration Processes (Research Question 8).

Regarding effective migration and integration approaches, researchers should delve into specific challenges of and strategies for integrating CAIML technologies into existing infrastructure within the constraints of FedRAMP.

Implications for National Security (Research Question 9).

Regarding future directions in national security, researchers should highlight areas for future investigation regarding the impact of CAIML adoption on national security and intelligence analysis, given the requirements of FedRAMP compliance.

Summary

This comprehensive discussion provides an in-depth view of the various dimensions of FedRAMP Compliance in the context of cloud computing adoption by federal agencies. It emphasizes the need for meticulous planning, strategic resource management, adherence to legal and regulatory standards, and effective leadership to successfully navigate the complexities of FedRAMP compliance. These insights are instrumental for policymakers, government officials, and researchers in developing strategies and policies for secure, compliant, and efficient cloud technology adoption.

Methodological Contributions

The research journey has yielded significant methodological contributions, as the researcher navigated through the intricate landscape of cloud computing, storytelling AI, and FedRAMP within federal government agencies. These methodological contributions can be categorized into several key areas, each playing a vital role in advancing the methodology and practices in this domain.

Testing a Proposed Methodology in a New Context. The study ventured into uncharted territory by applying and adjusting a preexisting methodology to the unique environment of federal government agencies. This adaptation process was meticulous, involving careful consideration of the context-specific variables and challenges. The success of application in this new setting not only validates the methodology but also enhances its scope for broader applicability in future research.

Integration/ Triangulation. Methodological rigor was enhanced through the integration of various data sources. This was not a mere aggregation of data but a strategic combination that provided a multidimensional view of the research questions. Triangulation, a key aspect of this integration, involved comparing data from different sources to ensure reliability and validity. This approach aided mitigation of biases and provided a more rounded and comprehensive understanding of the research themes.

Developing New Instruments. Recognizing the gaps in existing data collection tools, the research involved the creation of new instruments tailored to the specific demands of the study. These tools were designed to be sensitive to the nuances of cloud computing and storytelling AI within the context of federal government operations. The development process was iterative, involving testing and refinement to ensure that these tools accurately captured the required data.

Validating Instruments in a New Context. The newly developed instruments underwent rigorous validation processes. This was crucial to ascertain their effectiveness in the new research context. The validation process involved pilot testing, feedback incorporation, and adjustments to improve alignment with the study's unique demands. This meticulous validation confirmed not only the instruments' reliability but also their adaptability to similar future research settings.

Proposing a New Methodology. Perhaps one of the most significant contributions of this research was the proposal of a new methodology. This methodology was developed in response to the unique intersection of technological and regulatory aspects within federal agencies. It offers a structured, comprehensive approach to future studies in similar domains, bridging gaps left by existing methodologies. This contribution is particularly valuable for researchers exploring the integration of advanced technologies in regulated environments.

Summary. The methodological contributions of this study are profound, offering a blueprint for future research in the domains of cloud computing, storytelling AI, and FedRAMP compliance within complex settings like federal government agencies. These contributions are characterized by their innovation, adaptability, and rigor, addressing not only the specific demands of the current study but also paving the way for methodological advancements in similar research areas. By pushing the boundaries of conventional methodologies, this research enhances the tool kit available to researchers and practitioners navigating the dynamic landscapes of technology adoption and regulatory compliance.

Contextual/Practical Contributions

Industry, Practice, and the Federal Government. The research has far-reaching implications for industry, practice, and the broader contextual landscape of technology adoption and security within federal government agencies. These contributions can be categorized into several key areas, each representing a tangible impact on the policies, mindsets, and emerging challenges in this domain.

Change of Policy Required. One of the most significant industrial and practical contributions of the research is the call for a change in policy within federal government agencies. The findings have shed light on the challenges and opportunities arising from the convergence of cloud computing, storytelling AI, and FedRAMP. These insights point to the necessity of reevaluating existing policies and regulations to align them with the evolving technological landscape. The identification of gaps and inefficiencies in current policies provides a compelling case for policymakers to consider revisions that accommodate the unique demands of these domains.

Adapting/Adopting Policies From Other Industries or Countries. The research has highlighted the potential benefits of adapting or adopting policies and practices from other industries or countries. The complexities surrounding technology adoption and security are not limited to the federal government alone. By examining successful approaches from analogous sectors or nations, government agencies can gain valuable insights and potentially streamline their own practices. This cross-industry and international exchange of ideas and policies can lead to more efficient and effective strategies.

Changing Mindsets. Beyond policy changes, the research underscores the need for a shift in mindsets and organizational culture within federal government agencies. The rapid pace of technological advancement necessitates a proactive and adaptive mindset among government employees and stakeholders. The findings emphasize the importance of fostering a culture that embraces innovation, continuous learning, and willingness to explore new solutions. This mindset change can enhance the agility of government agencies regarding responding to emerging challenges and opportunities.

Problem Reoccurs. The research has identified scenarios where recurring problems and challenges persist despite attempts to address them. This recognition serves as a wake-up call for industry practitioners and policymakers. It highlights the need for sustained efforts and commitment to monitoring and evaluating the effectiveness of implemented solutions. Understanding that some challenges may resurface over time, government agencies must be prepared with adaptive strategies to mitigate and address them promptly.

New Issues Arise. Lastly, the research anticipates the emergence of new issues and complexities in the intersection of cloud computing, storytelling AI, and FedRAMP. As technology evolves, so do the associated risks and opportunities. The study serves as an early warning system, preparing industry and government stakeholders for the potential challenges that lie ahead. This foresight encourages proactive planning and the development of strategies to tackle these novel issues as they arise.

Summary. In conclusion, the research offers valuable industrial, practical, and contextual contributions by advocating for policy changes, promoting cross-industry learning, advocating mindset shifts, highlighting the persistence of challenges, and anticipating new issues. These contributions are essential for ensuring that federal government agencies remain adaptable, secure, and well-equipped to navigate the ever-evolving landscape of technology adoption and security. They also serve as a foundation for further discussions, policy reforms, and research endeavors in this critical domain.

Technology Adoption, Data Security, and Compliance. This research makes several notable contributions to the fields of technology adoption, data security, and compliance within federal government agencies.

Comprehensive Understanding. The study provides a holistic understanding of the challenges and opportunities associated with cloud computing adoption, data security, and compliance with FedRAMP. By examining the convergence of these domains, the research provides a comprehensive perspective of the complex landscape faced by government agencies.

Innovative Solutions. The study introduces storytelling AI as an innovative solution for enhancing data security and FedRAMP compliance. The investigator demonstrates its potential in threat detection, threat modeling, and real-time threat analysis, offering a novel approach to addressing cybersecurity challenges.

Policy Implications. The findings carry significant policy implications, emphasizing the importance of robust data security measures and threat mitigation strategies within federal government agencies. Policymakers can use these insights to shape regulations and guidelines for technology adoption.

Practical Guidance. For practitioners, this study offers practical guidance on addressing challenges related to cloud computing adoption, data security, and FedRAMP compliance. The recommendations provided in this chapter serve as actionable steps for improving security practices.

Recommendations

Building on the research findings, the scientist offers the following practical recommendations that are both feasible and adaptable, addressing the diverse stakeholders involved in the technology adoption and security landscape within federal government agencies.

For Federal Government Agencies

Review and Revise Policies. Federal government agencies should initiate a comprehensive review of existing policies and regulations related to cloud computing, storytelling AI, and FedRAMP compliance. This review should aim to identify gaps and inefficiencies, with a focus on updating policies to align with emerging technologies and security challenges.

Invest in Training and Skill Development. Agencies should prioritize investment in training and skill-development programs for their personnel. Given the rapid pace of technological change, continuous learning is essential. Offering opportunities for employees to acquire new skills and stay updated with industry best practices is crucial.

Foster a Culture of Innovation. Agencies should actively promote a culture of innovation, in which employees are encouraged to explore new solutions and approaches. Creating an environment that values creativity and problem solving can lead to more effective responses to evolving challenges.

For Policymakers

Enable Cross-Industry Collaboration. Policymakers should facilitate collaboration and knowledge sharing between federal government agencies and other industries facing similar technological challenges. This cross-industry exchange can lead to the adoption of best practices and the development of more robust policies.

Support Research and Development. Policymakers should allocate resources to support research and development efforts in the areas of cloud computing, storytelling AI, and FedRAMP compliance. Funding initiatives can drive innovation and the development of secure technologies tailored to government needs.

For Researchers

Explore Emerging Threats. Researchers should delve into the identification and analysis of emerging threats and challenges at the intersection of cloud computing, storytelling AI, and FedRAMP. Anticipating these issues can guide the development of proactive solutions.

Evaluate Long-Term Impact. Researchers should conduct longitudinal studies to evaluate the long-term impact of policy changes and technology adoption within federal government agencies. Understanding how these changes evolve over time is essential for ongoing improvements.

For All Stakeholders

The recommendations provided offer a comprehensive guide for federal government agencies, policymakers, and researchers navigating the intricate landscape of technology adoption, particularly focusing on cloud computing, storytelling AI, and maintaining FedRAMP compliance. The sections that follow provide a detailed breakdown of these recommendations. The following points relate to all stakeholders.

Stay Adaptable.

Emphasize the importance of flexibility in an ever-changing technological environment. Stakeholders should be prepared to continually reassess and modify their strategies and policies in response to technological advancements and evolving security threats.

Prioritize Security.

Highlight the critical importance of security in all aspects of technology integration. This includes implementing rigorous data protection measures, advanced threat-detection systems, and consistent monitoring practices.

Collaborate for Solutions.

Encourage collaborative efforts across various sectors. By pooling resources and expertise, federal agencies, policymakers, researchers, and industry experts can devise more effective strategies for tackling the challenges of technology adoption and security.

Specific Recommendations. The following are specific recommendations.

Data Security Best Practices. Call for government agencies to adopt and rigorously enforce best practices in data security. This includes the use of encryption, stringent access controls, and regular security assessments to safeguard sensitive information.

Storytelling AI Integration. Suggest integrating storytelling AI into cybersecurity frameworks. This could enhance capabilities in areas such as threat detection, threat modeling, and real-time threat analysis, offering a more dynamic approach to security.

Interagency Collaboration. Stress the need for cooperative efforts among federal agencies. Sharing threat intelligence and security insights can lead to more comprehensive risk assessments and fortified national security.

Policy Updates. Recommend that policymakers periodically review and update regulations to incorporate considerations for emerging technologies like storytelling AI. This ensures that guidelines remain relevant and effective in the context of modern technological advancements.

Research Continuation. Encourage ongoing research into the ever-evolving domain of technology adoption, security, and compliance. Continual research efforts are vital to staying ahead of new challenges and leveraging emerging opportunities in the field.

Summary.

These recommendations present a strategic framework for effectively managing the complexities associated with the adoption of advanced technologies in federal government settings. By embracing adaptability, prioritizing security, fostering collaboration, and continuously updating policies and research approaches, stakeholders can contribute to a more secure, innovative, and responsive environment. This holistic approach is essential for successful integration and compliance within the fast-paced and constantly evolving landscape of cloud computing and storytelling AI.

Limitations of the Study

Recognizing the limitations of any research study is crucial for understanding the context and scope of its findings. In this study of cloud computing adoption, storytelling AI, and FedRAMP compliance within federal government agencies, several methodological constraints were encountered, which are essential to acknowledge.

Data Availability

Regarding the limited scope of data sources, access to comprehensive, current data was a challenge, particularly in the context of federal government agencies. Some data sources had limited scope, affecting the depth and breadth of the analysis. This limitation highlights the need for more open and extensive data sources for future research.

Time Constraints

Regarding the dynamic technological landscape, the rapidly changing nature of the technology and security landscapes means that findings can quickly become outdated. Time constraints limited the extent of in-depth exploration of all relevant aspects. Longer-term studies may uncover more comprehensive insights.

Resource Limitations

Regarding access to specialized tools, there were challenges related to the availability of certain specialized software and hardware, limiting the scope of some analytical methods. Future research with more resources could employ more advanced and diverse methodologies.

Sampling Bias

Regarding participant selection, despite strategic efforts to select a representative sample, there is potential for sampling bias, which might affect the study's findings. Future studies should aim for a more diverse and extensive participant pool to enhance the generalizability of the results.

External Factors

Regarding relevance over time, the rapid evolution of technology, policy shifts, and emerging security threats can affect the long-term relevance of the findings. Ongoing research and adaptation are necessary to keep the research up to date and applicable.

Implications for Future Research

These limitations underscore the importance of continuous and expansive research in the field. Future studies should aim to overcome these challenges by securing access to more comprehensive data, extending research timelines, increasing resource availability, diversifying participant samples, and staying abreast of changes in technology and policies. Addressing these limitations will not only refine the research outcomes but also enhance our understanding of the complexities involved in the adoption of cloud computing, storytelling AI, and FedRAMP compliance within the dynamic landscape of federal government agencies.

Suggestions for Further Research

Expanding on the proposed avenues for future research based on the findings of this study on cloud computing adoption, storytelling AI, and FedRAMP compliance in federal government agencies, the researcher can delve deeper into specific research opportunities that could further enhance our understanding and management of these technologies.

Longitudinal Studies

Extended Time-Frame Analysis. Conduct studies over several years to understand how technology adoption and security practices evolve in response to changing technologies, policies, and threats.

Impact Assessment. Evaluate the long-term effects of technology implementation on agency operations, security postures, and overall governmental efficiency.

Advanced Analytical Methods.

Development of Predictive Tools. Create and test advanced predictive models to forecast potential security threats and technological trends.

ML Applications. Explore the use of ML in cybersecurity within government agencies, particularly for anomaly detection and automated threat response.

Comparative Analyses

International Best Practices. Study how different countries implement cloud computing and AI technologies within their government agencies, focusing on security, efficiency, and compliance.

Cross-Cultural Insights. Investigate how cultural factors influence technology adoption and security practices in governmental contexts across various countries.

Cybersecurity Education

Training Program Effectiveness. Assess the impact of different cybersecurity training approaches on employee awareness, behavior, and skill development within federal agencies.

Long-Term Retention of Knowledge. Examine the long-term retention of cybersecurity knowledge after training and its practical application in daily operations.

User-Centric Studies

Privacy and Consent Management. Investigate the effectiveness of current data privacy and consent management practices in government agencies using cloud computing and storytelling AI.

User-Experience Optimization. Explore how user experience of interacting with government technology systems can be improved, particularly focusing on accessibility and usability.

Policy Impact Studies

Regulatory Compliance Analysis. Evaluate the effect of new policies and regulations on technology adoption, focusing on practical challenges and benefits observed within agencies.

Policy–Technology Alignment. Assess how well current policies align with the rapid pace of technological advancement and propose recommendations for policy updates.

Emerging Threats Analysis

Real-Time Threat Identification. Research the development of systems capable of identifying and responding to emerging cybersecurity threats in real time.

Adaptive Security Strategies. Study the creation of adaptive security frameworks that can evolve in response to the changing threat landscape and technological advancements.

Summary

These detailed research directions offer pathways for deepening our understanding of cloud computing, AI integration, and cybersecurity within federal government settings. By exploring these areas, future research can provide valuable insights and recommendations, contributing to more secure, efficient, and user-friendly technology environments in the public sector. The continual advancement of technology and the dynamic nature of security threats necessitate ongoing research and adaptation in these fields.

Conclusions

In this comprehensive concluding chapter, the researcher delves into the multifaceted landscape of technology adoption, data security, and compliance in federal government agencies, with a specific focus on cloud computing, storytelling AI, and FedRAMP. This detailed exploration, grounded in clearly articulated objectives and research questions, has yielded a rich array of findings, implications, and strategic recommendations.

Objective 1: Exploring Challenges and Opportunities in Technology Adoption

- The research unearthed diverse challenges confronting federal agencies in the adoption of cloud computing and storytelling AI. These spanned from technical

complexities, such as integrating new systems with legacy infrastructure, to organizational hurdles, like change management and cultural shifts.

• On the opportunity front, the study revealed significant potential in utilizing these technologies to streamline operations. This includes enhancing data processing capabilities, facilitating interagency communication, and enabling sophisticated decision making through data analytics.

• The investigation also highlighted critical areas such as the need for enhanced data security protocols, user-centered design approaches, and assurance that technology deployment is in line with existing compliance frameworks, particularly FedRAMP.

Objective 2: Impact of Technology on Data Security and FedRAMP Compliance

• A pivotal aspect of the study was examination of the interplay between technology adoption and data security within the stringent framework of FedRAMP. The findings indicated that while these technologies offer substantial benefits, they also bring forth new vulnerabilities and security risks.

• The study underscored the evolving nature of cybersecurity threats and the necessity for government agencies to continually adapt their security measures. This includes adopting advanced cybersecurity technologies, regular risk assessments, and employee training in security best practices.

• The role of FedRAMP emerged as central in setting standards for security and compliance, guiding agencies to uphold the integrity and confidentiality of sensitive government data.

Objective 3: Recommendations for Enhancing Security and Compliance

Based on the findings, the study culminates in a series of recommendations targeting key stakeholders:

- For policymakers, the emphasis is on formulating dynamic and adaptive policies that align with technological advancements while ensuring robust security and privacy protections.

- For federal agencies, the recommendations include investing in workforce training, particularly in areas related to cloud computing and AI, and fostering a culture that embraces continuous learning and adaptation to technological changes.

- For the research community, the study suggests a focus on development of innovative solutions to emerging security challenges and evaluating the effectiveness of new technologies in real-world governmental settings.

Concluding Insights

This research has provided a comprehensive understanding of the nuanced and complex dynamics involved in the adoption of advanced technologies within federal government agencies. The findings highlight a critical need for an approach that adeptly balances innovation with data security and adherence to regulatory standards.

The study reaffirms that while technologies like cloud computing and storytelling AI offer transformative possibilities, they also necessitate careful consideration of the associated security and compliance challenges.

Future Directions

The insights gained from this research pave the way for further exploration in the domain of technology adoption in government settings. Future studies could focus on longitudinal analysis

to understand the long-term impacts of these technologies and on cross-sector comparisons to gain broader insights.

The evolving nature of technology, alongside the dynamic landscape of cybersecurity threats and compliance regulations, underscores the need for ongoing research and policy development in this area.

Summary

In conclusion, this research provides valuable guidance for federal government agencies as they navigate the complexities of adopting new technologies while maintaining stringent security and regulatory compliance. The convergence of cloud computing, storytelling AI, and FedRAMP compliance represents a challenging yet opportune landscape. By embracing innovative solutions and adhering to best practices, these agencies can confidently address the dual goals of technological advancement and secure, compliant operations. This study represents a significant contribution to the field, offering a foundational framework for continued advancements in technology adoption, data security, and compliance within the public sector.

REFERENCES

Aarestrup , FM , Albeyatti , A. , Armitage , WJ , Auffray , C. , Augello , L. , Balling , R. , ... & Van Oyen , H. (2020). Towards a European health research and innovation cloud (HRIC). Genome medicine, 12, 1-14. https://doi.org/10.1186/s13073-020-0713-z

Abdulmajeed, M., & Fahmy, N. (2022). Meta-analysis of AI Research in Journalism: Challenges, Opportunities and Future Research Agenda for Arab Journalism. From the Internet of Things to the Internet of Ideas: The Role of Artificial Intelligence: Proceedings of EAMMIS 2022, 213-225.

AbuMusab, S. (2023). Generative AI and human labor: who is replaceable?. AI & SOCIETY, 1-3.

Adams, W. C. (2015). Conducting semiÿ structured interviews. Handbook of practical program evaluation, 492-505.

Ahmad , R. , Siemon , D. , Gnewuch , U. , & Robra-Bissantz , S. (2022, January). A Framework of Personality Cues for Conversational Agents. In Proceedings of the 55th Hawaii International Conference on System Sciences.

Akoury, N., Salz, R., & Iyyer, M. (2023). Towards Grounded Dialogue Generation in Video Game Environments.

Al Batayneh, R.M., Taleb, N., Said, R.A., Alshurideh, M.T., Ghazal, T.M., & Alzoubi, H.M. (2021, May). IT governance framework and smart services integration for future development of Dubai infrastructure utilizing AI and big data, its reflection on the citizens standard of living. In The international conference on artificial intelligence and computer vision (pp. 235-247). Cham: Springer International Publishing.

Alam, M. K. (2021). A systematic qualitative case study: questions, data collection, NVivo analysis and saturation. Qualitative Research in Organizations and Management: An International Journal, 16(1), 1-31.

Ali, M. A., & ALQARAGHULI, A. (2023). A Survey on the Significance of Artificial intelligence (AI) in Network cybersecurity. Babylonian Journal of Networking, 2023, 21-29.

Ali, O. M. S. H. (2016). The perceived benefits of cloud computing technology for regional municipal governments and barriers to adoption (Doctoral dissertation, University of Southern Queensland).

Allen, Greg, and Taniel Chan. Artificial intelligence and national security. Cambridge, MA: Belfer Center for Science and International Affairs, 2017.

Alliance, B. B. E., & Bureau, C. C. F. P. 3PAO third-party assessment organization under the FedRAMP requirements programme API application programming interface AWS Amazon Web Services BCRs Binding Corporate Rules.

Alshammari, RFN, Arshad, H., Abd Rahman, AH, & Albahri, OS (2022). Robotics use in automatic vision-based assessment systems from artificial intelligence perspective: A systematic review. IEEE Access.

Alsheibani, S., Messom, C., & Cheung, Y. (2020). Re-thinking the competitive landscape of artificial intelligence.

Alves-Oliveira, P., Sequeira, P., Melo, FS, Castellano, G., & Paiva, A. (2019). Empathetic robot for group learning: A field study. ACM Transactions on Human-Robot Interaction (THRI), 8(1), 1-34.

Amato, G., Behrmann, M., Bimbot, F., Caramiaux, B., Falchi, F., Garcia, A., ... & Vincent, E. (2019). AI in the media and creative industries. arXiv preprint arXiv:1905.04175.

Amjad, B., Zeeshan, M., & Beg, M. O. (2023). EMP-EVAL: A Framework for Measuring Empathy in Open Domain Dialogues. arXiv preprint arXiv:2301.12510.

Anand, A., & Kumar, A. THE RISE OF ARTIFICIAL INTELLIGENCE IN VIDEO GAMES.

Anderson, J. B. (2021). Inadequacy of Risk Acceptance Criteria for Cloud Services Adoption: A Qualitative Generic Study (Doctoral dissertation, Capella University).

Anoir, L., Khaldi, M., & Erradi, M. (2022). Personalization in Adaptive E-Learning. In Designing User Interfaces With a Data Science Approach (pp. 40-67). IGI Global.

Ante, C., & Ante, C. (2016). Comparison and Conclusion. The Europeanisation of Vocational Education and Training, 193-229.

Ash, E., & Hansen, S. (2022). Text Algorithms in Economics.

Audibert, R. B. (2022). On the evolution of AI and machine learning: analyses of impact, leadership and influence over the last decades.

Audibert, R.B., Lemos, H., Avelar, P., Tavares, A.R. and Lamb, L.C. (2022). On the Evolution of AI and Machine Learning: Towards Measuring and Understanding Impact, Influence, and Leadership at Premier AI Conferences. arXiv preprint arXiv:2205.13131.

Axelsson, M., Spitale, M., & Gunes, H. (2022). Robots as mental well-being coaches: Design and ethical recommendations. arXiv preprint arXiv:2208.14874.

Azah, A. S. A. (2021). Manpower, AI, robot, Re-imagining the Workforce.

Bachner, J. (2022). Optimizing analytics for policymaking and governance.

Baiheng, L., & Wen, Z. (2020, December). Rethinking of Artificial Intelligence Storytelling of Digital Media. In 2020 International Conference on Innovation Design and Digital Technology (ICIDDT) (pp. 112-115). IEEE.

Baraka, K., Alves-Oliveira, P., & Ribeiro, T. (2020). An extended framework for characterizing social robots. Human-Robot Interaction: Evaluation Methods and Their Standardization, 21-64.

Barros, A. P., & Dumas, M. (2006). The rise of web service ecosystems. IT professional, 8(5), 31-37.

Barta, G., & Görcsi, G. (2021). Risk management considerations for artificial intelligence business applications. International Journal of Economics and Business Research, 21(1), 87-106.

Basting , EJ , Munshi , I. , Harangozo , J. , Dongarra , MS , & Goncy , EA (2023). When does technology use within dating relationships cross the line? A thematic analysis of semistructured interviews with young adults. Psychology of Violence.

Batarseh, F. A., & Yang, R. (Eds.). (2017). Federal data science: Transforming government and agricultural policy using artificial intelligence. Academic Press.

Belgodere, B., Dognin, P., Ivankay, A., Melnyk, I., Mroueh, Y., Mojsilovic, A., ... & Young, RA (2023). Auditing and Generating Synthetic Data with Controllable Trust Trade-offs. arXiv preprint arXiv:2304.10819.

Bettoni, Andrea, Davide Matteri, Elias Montini, Bartÿomiej Gÿadysz, and Emanuele Carpanzano. "An AI adoption model for SMEs: A conceptual framework." IFAC-PapersOnLine 54, no. 1 (2021): 702-708.

Bhushan, S. B., Reddy, P., Subramanian, D. V., & Gao, X. Z. (2018). Systematic survey on evolution of cloud architectures. International Journal of Autonomous and Adaptive Communications Systems, 11(1), 14-38.

Biermann, O. C., Ma, N. F., & Yoon, D. (2022, June). From tool to companion: Storywriters want AI writers to respect their personal values and writing strategies. In Designing Interactive Systems Conference (pp. 1209-1227).

Biersmith, L., & Laplante, P. (2022, October). Introduction to AI Assurance for Policy Makers. In 2022 IEEE 29th Annual Software Technology Conference (STC) (pp. 51-56). IEEE.

Blanchard, A., & Taddeo, M. (2023). The Ethics of Artificial Intelligence for Intelligence Analysis: a Review of the Key Challenges with Recommendations. Digital Society, 2(1), 1-28.

Blau, J. (2020). Europe's great digital gap. Research-Technology Management, 63(2), 3-6. https://www.questia.com/library/journal/1G1-616047393/europe-s-great-digital-gap

Bodemer, O. (2023). Artificial Intelligence in Governance: A Comprehensive Analysis of AI Integration and Policy Development in the German Government. Authorea Preprints.

Boukhari, M. (2021). The Impact of Artificial Intelligence on the B2B Sales Funnel.

Bouma, D., Canbaloÿlu, G., Treur, J., & Wiewiora, A. (2023). Adaptive network modeling of the influence of leadership and communication on learning within an organization. Cognitive Systems Research, 79, 55-70.

Braga , J. , Regateiro , F. , Stiubiener , I. , & Braga , JC (2022). A proposal to improve research in AI algorithm and data governance. OSF Preprints. September, 15.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative research in psychology, 3(2), 77-101.

Breit, A., Waltersdorfer, L., Ekaputra, F.J., Sabou, M., Ekelhart, A., Iana, A., ... & van Harmelen, F. (2023). Combining machine learning and semantic web: A systematic mapping study. ACM Computing Surveys.

Bringsjord, S., & Ferrucci, D. (1999). Artificial intelligence and literary creativity: Inside the mind of brutus, a storytelling machine. Psychology Press.

Bruno, F., Cardoso, P., & Faltay, P. The National Employment System.

Burtell, M., & Woodside, T. (2023). Artificial influence: An analysis of AI-driven persuasion. arXiv preprint arXiv:2303.08721.

Calo, R. (2018). Artificial intelligence policy: A primer and roadmap. U. Bologna L. Rev., 3, 180.

Carenini, G., & Duplessis, A. Investigating the Intuitive Logic behind Autoregressive Language Models.

Carney, W. T. (2019). A Case Study of the United States Air Force Adoption of Cloud Computing (Doctoral dissertation, Robert Morris University).

Carranza, A. G., Farahani, R., Ponomareva, N., Kurakin, A., Jagielski, M., & Nasr, M. (2023). Privacy-Preserving Recommender Systems with Synthetic Query Generation using Differentially Private Large Language Models. arXiv preprint arXiv:2305.05973.

Carter, A. F. (2022). Relationship between Federal Employee Work-Life Balance and Intent to Leave (Doctoral dissertation, Baker College (Michigan)).

Casto, C. (2023). Extreme Crisis Leadership: A Handbook for Leading Through the Unpredictable. Taylor & Francis.

Cavazza, M., Charles, F., & Mead, S. J. (2001, September). Characters in Search of an author: AI-based Virtual Storytelling. In International Conference on Virtual Storytelling (pp. 145-154). Berlin, Heidelberg: Springer Berlin Heidelberg.

Cavazza, M., Charles, F., & Mead, S. J. (2002). Character-based interactive storytelling. IEEE Intelligent systems, 17(4), 17-24.

Chan, L., Morgan, I., Simon, H., Alshabanat, F., Ober, D., Gentry, J., ... & Cao, R. (2019, June). Survey of AI in cybersecurity for information technology management. In 2019 IEEE technology & engineering management conference (TEMSCON) (pp. 1-8). IEEE.

Charles, F., Mead, S. J., & Cavazza, M. (2001, October). Character-driven story generation in interactive storytelling. In Proceedings Seventh International Conference on Virtual Systems and Multimedia (pp. 609-615). IEEE.

Chen, H., Han, R., Wu, T. L., Nakayama, H., & Peng, N. (2022). Character-centric story visualization via visual planning and token alignment. arXiv preprint arXiv:2210.08465.

Chen, L., Jiang, M., Jia, F., & Liu, G. (2022). Artificial intelligence adoption in business-to-business marketing: toward a conceptual framework. Journal of Business & Industrial Marketing, 37(5), 1025-1044.

Cheng, J., Yang, Y., Tang, X., Xiong, N., Zhang, Y., & Lei, F. (2020). Generative adversarial networks: a literature review. KSII Transactions on Internet and Information Systems (TIIS), 14(12), 4625-4647.

Cheong, Y. G., & Young, R. M. (2014). Suspenser: A story generation system for suspense. IEEE Transactions on Computational Intelligence and AI in Games, 7(1), 39-52.

Chetty, K. (2023). AI literacy for an ageing workforce: leveraging the experience of older workers. OBM Geriatrics, 7(3), 1-17.

Choudhary, S., Kaushik, N., & Sivathanu, B. Modelling the Key Enablers and Barriers of Ai-Based Conversational Agents' Adoption: an Ism and Micmac Approach.

Clarke, E., Pandit, H. J., & Wall, P. J. (2022). We need to talk about AI: the case for citizens' think-ins for citizen-researcher dialogue and deliberation.

Clarke, V., Braun, V., & Hayfield, N. (2015). Thematic analysis. Qualitative psychology: A practical guide to research methods, 3, 222-248.

Clímaco, J., Chávez, T., & Escalante, A. (2022, November). Conversational AI to improve local environmental risk management. In 2022 IEEE 40th Central America and Panama Convention (CONCAPAN) (pp. 1-6). IEEE.

COBERN, W., & Adams, B. (2020). When interviewing: how many is enough?. International Journal of Assessment Tools in Education, 7(1), 73-79.

Colville, G., Darkins, J., Hesketh, J., Bennett, V., Alcock, J., & Noyes, J. (2009). The impact on parents of a child's admission to intensive care: integration of qualitative findings from a cross-sectional study. Intensive and Critical Care Nursing, 25(2), 72-79.

Cooke, T. W. (2022). Procurement Officials Are Leading Federal AI Adoption.

Creswell, J. W., & Poth, C. N. (2017). Qualitative inquiry and research design: Choosing among five approaches. Sage Publications.

Creswell, J., & Poth, C. (2018). Qualitative inquiry & research design: Choosing among five approaches (4th ed.). Sage Publications.

Dale, R. (2022). $ NLP: How to spend a billion dollars. Natural Language Engineering, 28(1), 125-136.

Daniël, L. (2022). Sample Size Justification. Collabra: Psychology, 8(1).

De Benedictis, R., Beraldo, G., Cortellessa, G., Fracasso, F., & Cesta, A. (2022, December). A Transformer-Based Approach for Choosing Actions in Social Robotics. In International Conference on Social Robotics (pp. 198-207). Cham: Springer Nature Switzerland.

De Cremer, D. (2022). With AI entering organizations, responsible leadership may slip!. AI and Ethics, 2(1), 49-51.

de Lope, J., & Graña, M. (2023). An ongoing review of speech emotion recognition. Neurocomputing, 528, 1-11.

de Paula, D., Marx, J., Wolf, E., Dremel, J., Cormican, K., & Uebernickel, F. (2023). A managerial mental model to drive innovation in the context of digital transformation. Industry and Innovation, 30(1), 42-66.

Dekkers, R., Carey, L., & Langhorne, P. (2022). Setting Inclusion and Exclusion Criteria. In Making Literature Reviews Work: A Multidisciplinary Guide to Systematic Approaches (pp. 201-233). Cham: Springer International Publishing.

Derner, E., & Batistiÿ, K. (2023). Beyond the Safeguards: Exploring the Security Risks of ChatGPT. arXiv preprint arXiv:2305.08005.

DeStefano, T. J., Teodorovicz, T., Cho, J., Kim, H., & Paik, J. (2022). What Determines AI Adoption?. In Academy of Management Proceedings (Vol. 2022, No. 1, p. 14791). Briarcliff Manor, NY 10510: Academy of Management.

Diaz, A. A. (2022). Organizational Paradoxes of Cloud Adoption in the Federal Government: A Quantitative Study of the Organizational Change Challenges Impacting Cloud Adoption (Doctoral dissertation, The George Washington University).

Ding, Y., Wu, X., Wang, H., & Pan, W. (2023). DPFormer: Learning Differentially Private Transformer on Long-Tailed Data. arXiv preprint arXiv:2305.17633.

Doubleday, J. (2019). Google gains 'FedRAMP High'cloud-services security authorization. Inside the Pentagon, 35(50), 8-8.

Dranidis, D., Ramollari, E., & Kourtesis, D. (2009, November). Run-time verification of behaviour conformance for conversational web services. In 2009 Seventh IEEE European Conference on Web Services (pp. 139-147). IEEE.

Dunbar, D. C. (2019). Small Business Leaders' Strategies for Obtaining United States Government Subcontracts (Doctoral dissertation, Walden University).

Dutka, P., & Astroth, K. S. (2022). Exploring the Evidence: Focusing on the Fundamentals: Navigating the Institutional Review Board Process. Nephrology Nursing Journal, 49(1).

Dvorak, J., Kopp, T., Kinkel, S., & Lanza, G. Explainable AI: A key driver for AI adoption, a mistaken concept, or a practically irrelevant feature?. Applications in Medicine and Manufacturing, 88.

Egan, E. (2022). Fix the Technology Modernization Fund to Overcome Obstacles in Funding Critical IT Initiatives. Information Technology and Innovation Foundation.

Eglash, R., Robert, L., Bennett, A., Robinson, K., Lachney, M., & Babbitt, W. (2019, November). AI for a Generative Economy: The Role of Intelligent Systems in Sustaining Unalienated Labor, Environment, and Society. In AAAI fall symposium series.

El-Gazzar, R. F. (2014). A literature review on cloud computing adoption issues in enterprises. In Creating Value for All Through IT: IFIP WG 8.6 International Conference on Transfer and

Diffusion of IT, TDIT 2014, Aalborg, Denmark, June 2-4, 2014. Proceedings (pp. 214-242). Springer Berlin Heidelberg.

Engstrom, D. F., Ho, D. E., Sharkey, C. M., & Cuéllar, M. F. (2020). Government by algorithm: Artificial intelligence in federal administrative agencies. NYU School of Law, Public Law Research Paper, (20-54).

Esmailzadeh, Y. (2023). Potential Risks of ChatGPT: Implications for Counterterrorism and International Security. International Journal of Multicultural and Multireligious Understanding, 10(4), 535-543.

Ethan, O. (2023). Data Governance Evolution: Enabling AI/ML Innovations in Banking. INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY, 7(1), 294-322.

Fan, J., Sun, T., Liu, J., Zhao, T., Zhang, B., Chen, Z., ... & Hack, E. (2023). How Well Can an AI Chatbot Infer Personality? Examining Psychometric Properties of Machine-inferred Personality Scores.

Farrow, E. (2022). Determining the human to AI workforce ratio–exploring future organisational scenarios and the implications for anticipatory workforce planning. Technology in Society, 68, 101879.

Fatima, S. (2022). Mapping artificial intelligence affordances for the public sector (Doctoral dissertation, Queensland University of Technology).

Fatima, S., Desouza, K. C., & Dawson, G. S. (2020). National strategic artificial intelligence plans: A multi-dimensional analysis. Economic Analysis and Policy, 67, 178-194.

Ferguson, S. How do product design teams converge on an idea? We now have empirical evidence for the Double-Diamond model.

Fluharty, B. (2022). Integrating Blockchains and Intelligent Agents in the Pursuit of Artificial General Intelligence.

Fotedar, S., Vannisselroij, K., Khalil, S., & Ploeg, B. (2020). Storytelling AI: A Generative Approach to Story Narration. In AI4Narratives@ IJCAI (pp. 19-22).

Fox, D., & Morris, J. C. (2015). The role of accountability in federal acquisition: A search for context. Journal of Public Procurement, 15(4), 514-536.

Fox, S. (2022). Human–Artificial Intelligence Systems: How Human Survival First Principles Influence Machine Learning World Models. Systems, 10(6), 260.

Fox, S. E., Shorey, S., Kang, E. Y., Montiel Valle, D., & Rodriguez, E. (2023). Patchwork: the hidden, human labor of AI integration within essential work. Proceedings of the ACM on Human-Computer Interaction, 7(CSCW1), 1-20.

Frangos, P. (2022, November). An Integrative Literature Review on Leadership and Organizational Readiness for AI. In European Conference on the Impact of Artificial Intelligence and Robotics (Vol. 4, No. 1, pp. 145-152).

Freiknecht, J., & Effelsberg, W. (2017). A survey on the procedural generation of virtual worlds. Multimodal Technologies and Interaction, 1(4), 27.

Gama, F., & Magistretti, S. (2023). Artificial intelligence in innovation management: A review of innovation capabilities and a taxonomy of AI applications. Journal of Product Innovation Management.

Ganguly, M. (2022). The Future of Investigative Journalism in the Age of Automation, Open-Source Intelligence (OSINT) and Artificial Intelligence (AI) (Doctoral dissertation, University of Westminster).

Gans, J. S. (2022). Ai adoption in a competitive market (No. w29996). National Bureau of Economic Research.

Gartner_Inc. (n.d.). Beyond chatgpt: The future of generative AI for enterprises. Gartner. Retrieved February 7, 2023, from https://www.gartner.com/en/articles/beyond-chatgpt-the-future-of-generative-ai-for-enterprises

Geer, D., & Gaffney, G. (2023). Establishing the Conditions of Engagement with Machines.

Gehlhaus, D., & Mutis, S. (2021). The US AI Workforce.

Ghaffari , F. , Gharaee , H. , & Arabsorkhi , A. (2019, April). Cloud security issues based on people, process and technology model: a survey. In 2019 5th International Conference on web research (ICWR) (pp. 196-202). IEEE.

Giron, A. (2023). A comparative analysis with machine learning of public data governance and AI policies in the European Union, United States, and China. Journal of Intelligence Studies in Business, 13(2), 61-74.

Gkinko, L., & Elbanna, A. (2022). AI Chatbots sociotechnical research: An overview and Future Directions. Proceedings http://ceur-ws. org ISSN, 1613, 0073.

Gkinko, L., & Elbanna, A. (2022). The appropriation of conversational AI in the workplace: A taxonomy of AI chatbot users. International Journal of Information Management, 102568.

Göbel, S., & Mehm, F. (2013). Personalized, adaptive digital educational games using narrative game-based learning objects. In Serious Games and Virtual Worlds in Education, Professional Development, and Healthcare (pp. 74-84). Igi Global.

Göbel, S., & Wendel, V. (2016). Personalization and adaptation. Serious games: Foundations, concepts and practice, 161-210.

Goldstein, J. A., Chao, J., Grossman, S., Stamos, A., & Tomz, M. (2023). Can AI Write Persuasive Propaganda?.

Gozalo-Brizuela, R., & Garrido-Merchan, EC (2023). ChatGPT is not all you need. A State of the Art Review of large Generative AI models. arXiv preprint arXiv:2301.04655. https://arxiv.org/pdf/2301.04655

Graf, B. (10). steps toward FedRAMP compliance. Federal Computing Weekly.

Greer, M. (2015). FITARA and FedRAMP: Accelerating federal cloud adoption. IEEE Cloud Computing, 2(5), 48-52.

Griffith, L. D. (2020). Strategies Federal Government IT Project Managers Use to Migrate IT Systems to the Cloud (Doctoral dissertation, Walden University).

Grigera, J., Espada, J. P., & Rossi, G. (2023). AI in User Interface Design and Evaluation. IT Professional, 25(2), 20-22.

Grinbaum, A., & Adomaitis, L. (2023). Dual Use Concerns of Generative AI and Large Language Models. arXiv preprint arXiv:2305.07882

Grinbaum, A., & Adomaitis, L. (2023). Dual Use Concerns of Generative AI and Large Language Models. arXiv preprint arXiv:2305.07882.

Guenduez, A. A., & Mettler, T. (2023). Strategically constructed narratives on artificial intelligence: What stories are told in governmental artificial intelligence policies?. Government Information Quarterly, 40(1), 101719

GUIDETTI, A. (2019). Artificial Intelligence as General Purpose Technology: An Empirical and Applied Analysis of its Perception.

Gupta, S., & Sharma, A. K. (2022). Evolution of infrastructure as an asset class: a systematic literature review and thematic analysis. Journal of Asset Management, 23(3), 173-200.

Gupta, U., Galstyan, A., & Steeg, G. V. (2023). Jointly Reparametrized Multi-Layer Adaptation for Efficient and Private Tuning. arXiv preprint arXiv:2305.19264.

Hall, A. (2019). Exploring the Barriers Causing Slow Cloud Adoption Rates in the Federal Sector (Doctoral dissertation, Colorado Technical University).

Hamilton, A. N., Fraser, A. M., & Gibson, K. E. (2023). Barriers to implementing risk management practices in microgreens growing operations in the United States: Thematic analysis of interviews and survey data. Food Control, 152, 109836.

Haney, B. S. (2020). Applied Artificial Intelligence in Modern Warfare and National Security Policy. Hastings Sci. & Tech. LJ, 11, 61.

Haran, J., & Gangadharan, S. P. (2022). Future of Workforce in the World of AI. BVIMSR Journal of Management Research, 14(1).

Harisanty, D., Anna, NEV, Putri, T.E., Firdaus, A.A., & Noor Azizi, N.A. (2022). Leaders, practitioners and scientists' awareness of artificial intelligence in libraries: a pilot study. Library Hi Tech.

Harper, J. (2021). Federal AI spending to top $6 billion. National Defense Magazine, 10.

Hawryszkiewycz, I., & Alqahtani, A. (2020, December). Integrating open innovation process with the double diamond design thinking model. In European Conference on Knowledge Management (pp. 1003-XV). Academic Conferences International Limited.

Henderson, P., Li, X., Jurafsky, D., Hashimoto, T., Lemley, M. A., & Liang, P. (2023). Foundation models and fair use. arXiv preprint arXiv:2303.15715.

Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. Social science & medicine, 292, 114523.

Hermann, I. (2021). Artificial intelligence in fiction: between narratives and metaphors. AI & society, 1-11.

Heston, R., & Arnold, Z. (2019). Strengthening the US AI Workforce.

Hewage, U., & Madusanka, P. N. (2022). Manual Corpora Development for Generative Pre-trained Transformers (GPT) & Evaluation of GPT Model Learning Capability. Available at SSRN 4391815.

Hilal, A. H., & Alabri, S. S. (2013). Using NVivo for data analysis in qualitative research. International interdisciplinary journal of education, 2(2), 181-186.

Hoadley, D. S., & Lucas, N. J. (2018). Artificial intelligence and national security.

Hornberger, B., & Rangu, S. (2020). Designing inclusion and exclusion criteria.

Huang, Y., Gupta, S., Zhong, Z., Li, K., & Chen, D. (2023). Privacy Implications of Retrieval-Based Language Models. arXiv preprint arXiv:2305.14888.

Hujran , O. , Al-Debei , M. , Al-Adwan , S. , Alarabiat , A. , & Altarawneh , N. (2023). Examining the antecedents and outcomes of smart government usage: An integrated model. Government Information Quarterly, 40(1), 101783.

Hur, Y. (2022). Improving Job Satisfaction Among Racial/Ethnic Minorities: The Case of US Federal Employees. Public Organization Review, 1-18.

Huygh, T. Bridging the AI| Data Governance Gap.

Hylton, J. C. (2021). Leadership development influence on leader self-efficacy (LSE): an explanatory sequential mixed methods study with civilian federal employees in the Department of Defense (Doctoral dissertation).

Imperial, M. (2022). Building A Knowledge-Based Chatbot for Customer Support.

Jackson, F. A. (2021). U.S. Patent No. 11,394,799. Washington, DC: U.S. Patent and Trademark Office. Retrieved November 11, 2022, from https://patents.google.com/patent/US11394799B2.

Jaiswal, A., Arun, C. J., & Varma, A. (2022). Rebooting employees: Upskilling for artificial intelligence in multinational corporations. The International Journal of Human Resource Management, 33(6), 1179-1208.

Jajee , AS , Johari , A. , Choudhury , D. , Shankar , D. , Anchuri , D. , & Wise , JA (2023). How Does AI Leadership Affect Strategic Implementation. In Coded Leadership (pp. 81-92). CRC Press.

Jarrahi, M. H., Lutz, C., Boyd, K., Oesterlund, C., & Willis, M. (2023). Artificial intelligence in the work context. Journal of the Association for Information Science and Technology, 74(3), 303-310.

Jiang, W. (2022). Graph-based deep learning for communication networks: A survey. Computer Communications, 185, 40-54.

Jungwirth, D., & Haluza, D. (2023). Feasibility Study on Utilization of the Artificial Intelligence GPT-3 in Public Health.

JW Creswell - 2013 - digitalcommons.unl.edu Creswell, J. W., & Poth, C. N. (2017). Qualitative inquiry and research design: Choosing among five approaches. Sage Publications.

Kabra, A., & Elenberg, E. R. (2023). Domain Private Transformers. arXiv preprint arXiv:2305.14208.

Kanying, T., Thammaboosadee, S., & Chuckpaiwong, R. (2023, December). Formulating Analytical Governance Frameworks: An Integration of Data and AI Governance Approaches. In Proceedings of the 13th International Conference on Advances in Information Technology (pp. 1-9).

Kelley, S. (2022). Employee perceptions of the effective adoption of AI principles. Journal of Business Ethics, 178(4), 871-893.

Kennedy, M. R. (2022). Playing Offense in the Race for Technology Leadership: Priorities for Final Competitiveness Bill. Wilson Center.

Kent, S. (2019). Federal cloud computing strategy. Executive Office of the President of the United States.

Koohang, A., Nord, J., Ooi, K., Tan, G., Al-Emran, M., Aw, E., ... & Wong, L. (2023). Shaping the metaverse into reality: multidisciplinary perspectives on opportunities, challenges, and future research. Journal of Computer Information Systems.

Kozinets, R. V. (2023). Immersive netnography: a novel method for service experience research in virtual reality, augmented reality and metaverse contexts. Journal of Service Management, 34(1), 100-125.

Krebs, K. (2020). How can the Dod Adopt Commercial-Style Artificial Intelligence for Procurement? (Doctoral dissertation, Acquisition Research Program).

Krehbiel, N. E. (2022). Stakeholder mental model alignment influence on mid-stage performance of new product engineering teams (Doctoral dissertation, Massachusetts Institute of Technology).

Kristensen, K., & Andersen, K. N. (2023). C-suite Leadership of Digital Government. Digital Government: Research and Practice.

Kroll, J. A. (2018). Data science data governance [AI ethics]. IEEE Security & Privacy, 16(6), 61-70.

KÜÇÜKSOLAK, Ö. K., & FIRAT, T. (2023). The Geopolitics of Artificial Intelligence in Central Asia: Russian and Chinese Cases. Journal of Security Sciences, 12(1), 25-44.

Kundra, V. (2011). Federal cloud computing strategy

Kurup, S., & Gupta, V. (2022). Factors Influencing the AI Adoption in Organizations. Metamorphosis, 21(2), 129-139.

Kusal, S., Patil, S., Choudrie, J., Kotecha, K., Mishra, S., & Abraham, A. (2022). AI-based Conversational Agents: A Scoping Review from Technologies to Future Directions. IEEE Access.

Landgrebe, J., & Smith, B. (2019). There is no Artificial General Intelligence. arXiv preprint arXiv:1906.05833.

Lapid, M. I., Ouellette, Y., Drake, M. T., & Clarke, B. L. (2023). Institutional Review Board (IRB): US Perspectives. In Handbook of Bioethical Decisions. Volume II: Scientific Integrity and Institutional Ethics (pp. 219-240). Cham: Springer International Publishing.

Latif , A. , Zuhairi , MF , Khan , FQ , Randhawa , P. , & Patel , A. (2022). A Critical Evaluation of Procedural Content Generation Approaches for Digital Twins. Journal of Sensors, 2022.

Laudy, O., Denev, A., & Ginsberg, A. (2022). Building Probabilistic Causal Models Using Collective Intelligence. The Journal of Financial Data Science, 4(2), 83-109.

Lavi, M. (2023). Manipulating, Lying, and Engineering the Future. Fordham Intellectual Property, Media & Entertainment Law Journal, 33(2).

Lawrence, C., Cui, I., & Ho, D. (2023, August). The Bureaucratic Challenge to AI Governance: An Empirical Assessment of Implementation at US Federal Agencies. In Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society (pp. 606-652).

Lawrence, C., Cui, I., & Ho, D. E. (2022). Implementation Challenges to Three Pillars of America's AI Strategy.

Lawson, A. (2016). Using narrative and Storytelling in research. In Alternative Market Research Methods (pp. 200-222). Routledge.

Ledro, C., Nosella, A., & Dalla Pozza, I. (2023). Integration of AI in CRM: Challenges and guidelines. Journal of Open Innovation: Technology, Market, and Complexity, 9(4), 100151.

Lee, J., & Darbellay, A. (Eds.). (2022). Data Governance in AI, FinTech and LegalTech: Law and Regulation in the Financial Sector. Edward Elgar Publishing.

Lee, Y. S., Kim, T., Choi, S., & Kim, W. (2022). When does AI pay off? AI-adoption intensity, complementary investments, and R&D strategy. Technovation, 118, 102590.

Lewandowski, T., Poser, M., Kuÿeviÿ, E., Heuer, M., Hellmich, J., Raykhlin, M., ... & Böhmann, T. (2023). Leveraging the Potential of Conversational Agents: Quality Criteria for the Continuous Evaluation and Improvement.

Lexis, L., & Julien, B. (2022). Communicating Scientific Discoveries to Peers. How To Do Science.

Li, B., Qi, P., Liu, B., Di, S., Liu, J., Pei, J., ... & Zhou, B. (2023). Trustworthy ai: From principles to practices. ACM Computing Surveys, 55(9), 1-46.

Li, H., Wang, Y., Liao, Q. V., & Qu, H. (2023). Why is AI not a Panacea for Data Workers? An Interview Study on Human-AI Collaboration in Data Storytelling. arXiv preprint arXiv:2304.08366.

Li, P., Yang, J., Islam, M. A., & Ren, S. (2023). Making AI Less Thirsty: Uncovering and Addressing the Secret Water Footprint of AI Models. arXiv preprint arXiv:2304.03271.

Li, X., Tramer, F., Liang, P., & Hashimoto, T. (2021). Large language models can be strong differentially private learners. arXiv preprint arXiv:2110.05679.

Li, Y., Tan, Z., & Liu, Y. (2023). Privacy-preserving prompt tuning for large language model services. arXiv preprint arXiv:2305.06212.

Livingston, M. (2020). Preventing racial bias in federal ai. Journal of Science Policy and Governance, 16.

Lobel, O. (2023). The Law of AI for Good. San Diego Legal Studies Paper, (23-001).

Lu, Q., Luo, Y., Zhu, L., Tang, M., Xu, X., & Whittle, J. (2023). Operationalising Responsible AI Using a Pattern-Oriented Approach: A Case Study on Chatbots in Financial Services. arXiv preprint arXiv:2301.05517.

Lukas, N., Salem, A., Sim, R., Tople, S., Wutschitz, L., & Zanella-Béguelin, S. (2023). Analyzing leakage of personally identifiable information in language models. arXiv preprint arXiv:2302.00539.

Lunt, H., Connor, S., Skinner, H., & Brogden, G. (2019). Electronic informed consent: the need to redesign the consent process for the digital age. Internal medicine journal, 49(7), 923-929.

Lütge, C., Hohma, E., Boch, A., Poszler, F., & Corrigan, C. (2022). On a Risk-Based Assessment Approach to AI Ethics Governance.

Madan, R., & Ashok, M. (2023). A public values perspective on the application of Artificial Intelligence in government practices.

Madan, R., & Ashok, M. (2023). AI adoption and diffusion in public administration: A systematic literature review and future research agenda. Government Information Quarterly, 40(1), 101774.

Maene, C. (2022). NVivo: An Introduction to Textual Qualitative Data Analysis with Software. Qualitative Data Analysis: Key Approaches, 109.

Magaldi, D., & Berler, M. (2020). Semi-structured interviews. Encyclopedia of personality and individual differences, 4825-4830.

Malik, N., Tripathi, S. N., Kar, A. K., & Gupta, S. (2022). Impact of artificial intelligence on employees working in industry 4.0 led organizations. International Journal of Manpower, 43(2), 334-354.

Maroc, S., & Zhang, J. (2019, July). Comparative analysis of cloud security classifications, taxonomies, and ontologies. In Proceedings of the 2019 International Conference on Artificial Intelligence and Computer Science (pp. 666-672).

Maroc, S., & Zhang, J. B. (2019, December). Context-aware security evaluation ontology for cloud services. In 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (pp. 1012-1018). IEEE.

Maroc, S., & Zhang, J. B. (2019, June). Risk-based and dependency-aware criteria specification for cloud services security evaluation. In 2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN) (pp. 731-735). IEEE.

Maroc, S., & Zhang, J. B. (2019, September). Cloud services security evaluation for multi-tenants. In 2019 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC) (pp. 1-6). IEEE.

Maroc, S., & Zhang, J. B. (2020). Towards security effectiveness evaluation for cloud services selection following a risk-driven approach. International Journal of Advanced Computer Science and Applications, 11(1).

Maroc, S., & Zhang, J. B. (2021). Cloud services security-driven evaluation for multiple tenants. Cluster Computing, 24, 1103-1121.

Marr, B. (2019). Artificial intelligence in practice: how 50 successful companies used AI and machine learning to solve problems. John Wiley & Sons.

Mattila, J., & Parkinson, S. (2019, October). An Approach for Enterprise Architects to Analyse Opportunities and Constraints for Applying Artificial Intelligence in Military Transformations. In ECIAIR 2019 European Conference on the Impact of Artificial Intelligence and Robotics (p. 215). Academic Conferences and publishing limited.

McGillivray, K. (2015). FedRAMP, Contracts, and the US Federal Government's Move to Cloud Computing: If an 800-Pound Gorilla Can't Tame the Cloud, Who Can. Colum. Sci. & Tech. L. Rev., 17, 336.

McGrath, Q. P. (2022). An Enterprise Risk Management Framework to Design Pro-Ethical AI Solutions.

McLaughlin, M. (2020). Reforming FedRAMP: A Guide to Improving the Federal Procurement and Risk Management of Cloud Services. Information Technology and Innovation Foundation.

McPherson, M. (2020). The case for psychometric artificial general intelligence. arXiv preprint arXiv:2101.02179.

Medaglia, R., Gil-Garcia, J. R., & Pardo, T. A. (2023). Artificial intelligence in government: taking stock and moving forward. Social Science Computer Review, 41(1), 123-140.

Meline, T. (2006). Selecting studies for systemic review: Inclusion and exclusion criteria. Contemporary issues in communication science and disorders, 33(Spring), 21-27.

Merriam, S. B., & Tisdell, E. J. (2015). Qualitative research: A guide to design and implementation. John Wiley & Sons.

Metheny, M. (2017). Federal cloud computing: The definitive guide for cloud service providers. Syngress.

Micheli, M., Gevaert, CM, Carman, M., Craglia, M., Daemen, E., Ibrahim, RE, ... & Vespe, M. (2022). AI ethics and data governance in the geospatial domain of Digital Earth. Big Data & Society, 9(2), 20539517221138767.

MIKHAILOV, D. Artificial Intelligence Integration as a Strategic Imperative for National Security.

Mikhailov, D. I. (2023). Optimizing National Security Strategies through LLM-Driven Artificial Intelligence Integration. arXiv preprint arXiv:2305.13927.

Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. Cogent Engineering, 10(2), 2272358.

Mohanty, A. K., Ahamed, S., Kamra, R., & Junnarkar, A. A. (2023). Challenges and Future Prospects of IoT and AI Integration in Education. Progress in Language, Literature and Education Research, 94.

Mohd Rahim, NI, A. Iahad, N., Yusof, AF, & A. Al-Sharafi, M. (2022). AI-Based Chatbots Adoption Model for Higher-Education Institutions: A Hybrid PLS-SEM-Neural Network Modelling Approach. Sustainability, 14(19), 12726.

Moher , D. , Liberati , A. , Tetzlaff , J. , Altman , DG , & Prism Group . (2010). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. International journal of surgery, 8(5), 336-341.

Moore, C. (2022). A Zero Trust Approach to Fundamentally Redesign Network Architecture within Federal Agencies (Doctoral dissertation, Capella University).

Morales-Forero, A., Bassetto, S., & Coatanea, E. (2022). Toward safe AI. AI & SOCIETY, 1-12.

Morgan, H. (2022). Conducting a qualitative document analysis. The Qualitative Report, 27(1), 64-77.

Moy, W. R., & Gradon, K. T. Artificial intelligence in hybrid and information warfare: A double-edged sword. In Artificial Intelligence and International Conflict in Cyberspace (pp. 47-74). Routledge.

Mukhamediev, RI, Popova, Y., Kuchin, Y., Zaitseva, E., Kalimoldayev, A., Symagulov, A., ... & Yelis, M. (2022). Review of Artificial Intelligence and Machine Learning Technologies: Classification, Restrictions, Opportunities and Challenges. Mathematics, 10(15), 2552.

Mystakidis, S. (2022). Metaverse. Encyclopedia, 2(1), 486-497.

Nabwire, S., Suh, H. K., Kim, M. S., Baek, I., & Cho, B. K. (2021). Application of artificial intelligence in phenomics. Sensors, 21(13), 4363.

Naqvi, A., & Janakiram, M. (2022). At the Speed of Irrelevance: How America Blew Its AI Leadership Position and how to Regain it. John Wiley & Sons.

Nguyen, G. T., & Liaw, S. Y. (2022). Understanding the Factors Affecting the Small and Medium Enterprises Adoption of Cloud computing: A Literature Review. International Journal of Business, Management and Economics, 3(2), 149-162.

Nijhawan, LP, Janodia, MD, Muddukrishna, BS, Bhat, KM, Bairy, KL, Udupa, N., & Musmade, P. B. (2013). Informed consent: Issues and challenges. Journal of advanced pharmaceutical technology & research, 4(3), 134.

Nili, A., Desouza, K. C., & Yigitcanlar, T. (2022). What can the public sector teach us about deploying artificial intelligence technologies?. IEEE Software, 39(6), 58-63.

Noh, Y., & Shin, Y. (2022). A Study on the Plan of Activation of Library by Utilizing the Virtual Reality and Augmented Reality. International Journal of Knowledge Content Development & Technology, 12(1), 85-104.

Norman, E. (2020). The Reluctance Toward Cloud Computing Adoption: A Qualitative Study (Doctoral dissertation, Capella University).

Novak, W. (2021). Artificial Intelligence (AI) and Machine Learning (ML) Acquisition and Policy Implications. CARNEGIE-MELLON UNIV

Novelli, C. (2023). Legal personhood for the integration of AI systems in the social context: a study hypothesis. AI & SOCIETY, 38(4), 1347-1359.

Nugraha, Y., & Martin, A. (2021). Towards a framework for trustworthy data security level agreement in cloud procurement. Computers & Security, 106, 102266.

O'Kane, P., Smith, A., & Lerman, M. P. (2021). Building transparency and trustworthiness in inductive research through computer-aided qualitative data analysis software. Organizational Research Methods, 24(1), 104-139.

Oates, K. (2021). Leader Empathy, Emotional Intelligence Behaviors and Years of Federal Employment: Predictability of Employee Well-Being (Doctoral dissertation, Capella University).

Ojeda, F. (2023). The Diamond of Innovation. In Encyclopedia of Data Science and Machine Learning (pp. 1482-1498). IGI Global.

Ojeda, F. A. (2021). Origin, Use and Meaning of the Innovation Diamond.

Omaar, H. US AI Policy Report Card.

Onyalo, W. A. (2022). Ai Chatbot: Improve Efficiency in Handling Student Queries at the Department of Computing and Informatics, Nairobi University (Doctoral dissertation, university of nairobi).

Oxford Analytica. (2023). Adoption of new technologies raises cybersecurity need. Emerald Expert Briefings, (oxan-db).

Page, M. J., Moher, D., & McKenzie, J. E. (2022). Introduction to PRISMA 2020 and implications for research synthesis methodologists. Research synthesis methods, 13(2), 156-163.

Pai, V., & Chandra, S. (2022). Exploring Factors Influencing Organizational Adoption of Artificial Intelligence (AI) in Corporate Social Responsibility (CSR) Initiatives. Pacific Asia Journal of the Association for Information Systems, 14(5), 4.

Palanivinayagam, A., & Damaševiÿius, R. (2023). Effective Handling of Missing Values in Datasets for Classification Using Machine Learning Methods. Information, 14(2), 92..

Palanivinayagam, A., El-Bayeh, CZ, & Damaševiÿius, R. (2023). Twenty Years of Machine-Learning-Based Text Classification: A Systematic Review. Algorithms, 16(5), 236.

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. Administration and policy in mental health and mental health services research, 42, 533-544.

Paltieli, G. (2022). The political imaginary of National AI Strategies. AI & SOCIETY, 37(4), 1613-1624.

Panda, A., Wu, T., Wang, J. T., & Mittal, P. (2023). Differentially Private In-Context Learning. arXiv preprint arXiv:2305.01639.

Papadopoulou, A. (2022). Developing and Evaluating a Chatbot (Doctoral dissertation, Aristotle University of Thessaloniki).

Papadopulos, J., & Christiansen, J. (2023). Conversational AI Workforce Revolution: Exploring the Effects of Conversational AI on Work Roles and Organisations.

Park, S. M., & Kim, Y. G. (2022). A metaverse: Taxonomy, components, applications, and open challenges. IEEE access, 10, 4209-4251.

Paÿko, ÿ., Mÿdziel, M., Stadnicka, D., Dec, G., Carreras-Coch, A., Solé-Beteta, X., ... & Atzeni, D. (2022). Plan and develop advanced knowledge and skills for future industrial employees in the field of artificial intelligence, internet of things and edge computing. Sustainability, 14(6), 3312.

Pataranutaporn , P. , Danry , V. , Leong , J. , Punpongsanon , P. , Novy , D. , Maes , P. , & Sra , M. (2021). AI-generated characters for supporting personalized learning and well-being. Nature Machine Intelligence, 3(12), 1013-1022.

Pathak, S., & Jindal, D. (2023). The AI Race: collaboration to counter Chinese aggression.

Patino, C. M., & Ferreira, J. C. (2018). Inclusion and exclusion criteria in research studies: definitions and why they matter. Brazilian Journal of Pulmonology, 44, 84-84.

Paulus, T. M. (2023). Using qualitative data analysis software to support digital research workflows. Human Resource Development Review, 22(1), 139-148.

Paulus, T. M. (2023). Using qualitative data analysis software to support digital research workflows. Human Resource Development Review, 22(1), 139-148.] [Tang, R. (2023). Harnessing Insights with NVivo. In Varieties of Qualitative Research Methods: Selected Contextual Perspectives (pp. 209-215). Cham: Springer International Publishing.

Peterson, D., & Hoffman, S. A. M. A. N. T. H. A. (2022). Geopolitical Implications of AI and Digital Surveillance Adoption. Brookings Institution.

Petrat, D., Polanski-Schräder, L., Yenice, I., Bier, L., & Subtil, I. (2022). AI as a Leader–What Individual Factors Influence the Acceptance of AI Applications that Take on Leadership Tasks?. Human Factors in Management and Leadership, 55, 61.

Pham, P., Nguyen, L. T., Pedrycz, W., & Vo, B. (2022). Deep learning, graph-based text representation and classification: a survey, perspectives and challenges. Artificial Intelligence Review, 1-35.

Phaup, M. (2022). Federal budget process reform: An economics perspective, with imperfect,“Human” decisionÿ makers. Public Budgeting & Finance, 42(3), 114-130.

Pierosara, S. (2022). Narrative autonomy and artificial storytelling. AI & SOCIETY, 1-10.

Pierre, A. (2022). Leadership of Human-Machine Teams in Military Environments: An Exploratory Framework (Doctoral dissertation, Regent University).

Pillai, R., Ghanghorkar, Y., Sivathanu, B., Algharabat, R., & Rana, NP (2023). Adoption of artificial intelligence (AI) based employee experience (EEX) chatbots. Information Technology & People.

Pin, C. (2023). Semi-structured Interviews. LIEPP Methods Brief/Fiches méthodologiques du LIEPP.

Pizzo, A., Lombardo, V., & Damiano, R. Interactive storytelling: a cross-media approach to writing, producing and editing with AI.

Polisetty, A., Chakraborty, D., Kar, A. K., & Pahari, S. (2023). What Determines AI Adoption in Companies? Mixed-Method Evidence. Journal of Computer Information Systems, 1-18.

Pooyandeh, M., Han, K. J., & Sohn, I. (2022). Cybersecurity in the AI-Based metaverse: A survey. Applied Sciences, 12(24), 12993.

Poozhithara, JJ, Kennedy, DM, Onstot, S., Januskeviÿiÿtÿ, A., & Cekrezi, M. (2022). Predictive Algorithm for Team Mental Model Convergence. IEEE Transactions on Computational Social Systems, 10(2), 640-655.

Pyjas, G. M., Weinel, J., & Broadhead, M. (2022). Storytelling and VR: Inducing emotions through AI characters. Proceedings of EVA London 2022, 198-204.

Qasem, Y. A., Abdullah, R., Yah, Y., Atan, R., Al-Sharafi, M. A., & Al-Emran, M. (2021). Towards the development of a comprehensive theoretical model for examining the cloud computing adoption

at the organizational level. Recent Advances in Intelligent Systems and Smart Applications, 63-74.

Qian, J. (2022). Research on artificial intelligence technology of virtual reality teaching method in digital media art creation. Journal of Internet Technology, 23(1), 125-132.

Rahali, A., & Akhloufi, M. A. (2023). End-to-End Transformer-Based Models in Textual-Based NLP. AI, 4(1), 54-110.

Ramsden, J. (2016). Semi-structured interviews: How many interviews are enough.

Rana, D. T. (2018). The future of HR in the presence of AI: A conceptual study. Available at SSRN 3335670.

Rana , J. , Dilshad , S. , & Ahsan , MA (2021). Ethical issues in research. Global Encyclopedia of Public Administration, Public Policy and Governance; Farazmand, A., Ed.

Rangapur, A., & Wang, H. (2023). ChatGPT-Crawler: Find out if ChatGPT really knows what it's talking about. arXiv preprint arXiv:2304.03325.

Rashid, Y., Waseem, A., Akbar, A. A., & Azam, F. (2019). Value co-creation and social media: A systematic literature review using citation and thematic analysis. European Business Review, 31(5), 761-784.

Rassolov, I. M., & Chubukova, S. G. (2022). Artificial Intelligence and Effective Governance: Legal Framework. Kutafin Law Review, 9(2), 309-328.

Rath, M., Satpathy, J., & Oreku, G. S. (2021). Artificial intelligence and machine learning applications in cloud computing and internet of things. In Artificial intelligence to solve pervasive internet of things issues (pp. 103-123). Academic Press.

Ray, P. P. (2023). ChatGPT: A comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope. Internet of Things and Cyber-Physical Systems.

Reddy, B., Goel, P., Hasitha, V. B., & Pise, A. A. (2023). Key Elements That Bind Leadership with AI. In Coded Leadership (pp. 71-79). CRC Press.

Reunanen, N., von Flittner, ZF, Roto, V., & Vaajakallio, K. (2020). Combining machine learning and Service Design to improve customer experience.

Riedl, M., Thue, D., & Bulitko, V. (2011). Game AI as storytelling. In Artificial intelligence for computer games (pp. 125-150). New York, NY: Springer New York.

Risk, F. (2020). Authorization Management Program (FedRAMP).(2010). Proposed Security assessment and authorization for US government cloud computing.

Rizk, B. (2020). Effects of Organisational Support and Innovation Culture on AI Adoption (Doctoral dissertation, Dublin, National College of Ireland).

Rosenthal, S., & Simmons, R. (2023, June). Autonomous agents: an advanced course on AI integration and deployment. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 37, No. 13, pp. 15843-15850).

Roshanfekr, B., Amirmazlaghani, M., & Rahmati, M. (2023). Learning graph from graph signals: An approach based on sensitivity analysis over a deep learning framework. Knowledge-Based Systems, 260, 110159.

Ross, J. P. (1999). A Risk Management Model for the Federal Acquisition Process. NAVAL POSTGRADUATE SCHOOL MONTEREY CA.

Safovich, Y. (2019). Abstractive Narrative Generation (Doctoral dissertation, Ariel University).

Saldaña, J. (2021). The coding manual for qualitative researchers. The coding manual for qualitative researchers, 1-440.

Sangwan, R. S., Badr, Y., & Srinivasan, S. M. (2023). Cybersecurity for AI Systems: A Survey. Journal of Cybersecurity and Privacy, 3(2), 166-190.

Sankofa, N. (2022). Critical method of document analysis. International Journal of Social Research Methodology, 1-13.

James III , JM , Paraino , RL , Deja , JA , & Samson , BPV (2023). Rolling the Dice: Imagining Generative AI as a Dungeons & Dragons Storytelling Companion. arXiv preprint arXiv:2304.01860.

Schleith, J., & Tsar, D. (2022). Triple Diamond Design Process. et al.

Schmidt, E., Work, B., Catz, S., Chien, S., Darby, C., Ford, K., ... & Moore, A. (2021). National security commission on artificial intelligence (AI). National Security Commission on Artificial Intelligence.

Schroeder, M., & Lodemann, S. (2021). A systematic investigation of the integration of machine learning into supply chain risk management. Logistics, 5(3), 62.

Schwartz, R., Vassilev, A., Greene, K., Perine, L., Burt, A., & Hall, P. (2022). Towards a standard for identifying and managing bias in artificial intelligence. NIST Special Publication, 1270, 1-77.

Selten, F., & Klievink, B. (2024). Organizing public sector AI adoption: Navigating between separation and integration. Government Information Quarterly, 41(1), 101885.

Semeraro, A., Vilella, S., Mohammad, S., Ruffo, G., & Stella, M. (2023). EmoAtlas: An emotional profiling tool merging psychological lexicons, artificial intelligence and network science.

Seo, K. K. (2012). A Comparison Study between Korean Cloud Service Certification Systems and US FedRAMP. Journal of digital convergence, 10(11), 59-65.

Shafiq, N., Hamid, I., Asif, M., Nawaz, Q., Aljuaid, H., & Ali, H. (2023). Abstractive text summarization of low-resourced languages using deep learning. PeerJ Computer Science, 9, e1176.

Shark, A. R. (2022). Governance and Leading Innovation–Who Decides?. In Technology and Public Management (pp. 27-57). Routledge.

Shevlin, H., Vold, K., Crosby, M., & Halina, M. (2019). The limits of machine intelligence: Despite progress in machine intelligence, artificial general intelligence is still a major challenge. EMBO reports, 20(10), e49177.

Shorey, S. (2023). Accounting for the Labor of AI Integration. AI100 Early Career Essay Competition, 4.

Short, T. X., & Adams, T. (Eds.). (2019). Procedural storytelling in game design. Crc Press.

Simonÿiÿ, K., & Jerele, T. (2023). Democratizing the Governance of AI: From Big Tech Monopolies to Cooperatives. In Artificial Intelligence, Social Harms and Human Rights (pp. 239-267). Cham: Springer International Publishing.

Singh, S., & Singh, S. (2022). Effective Analysis of Chatbot Frameworks: RASA and Dialogflow (No. 8338). EasyChair.Dale, R. (2022). $ NLP: How to spend a billion dollars. Natural Language Engineering, 28(1), 125-136.

Smith, D. (2016). Cloud computing deployments should begin with service definition. Stamford, CT: Gartner, Inc.

Snyder, D. M. (2021). GAO Bid Protests by Small Business: Analysis of Perceived and Reported Outcomes in Federal Contracting (Doctoral dissertation, University of South Florida).

Sohail, Shahab Saquib, et al. Decoding ChatGPT: a taxonomy of existing research, current challenges, and possible future directions. Journal of King Saud University-Computer and Information Sciences (2023): 101675.

Somers, M. J. (2022). Reciprocity in Leader and Follower Behavior Among Federal Employees: Test of a Nonrecursive Model. Public Administration Quarterly, 46(1), 23-38.

Song, X., & Ford, M. (2022). E-leadership 2.0: Meet Your AI Leader. In Leadership After COVID-19: Working Together Toward a Sustainable Future (pp. 131-151). Cham: Springer International Publishing.

Spitale, G., Biller-Andorno, N., & Germani, F. (2023). AI model GPT-3 (dis) informs us better than humans. arXiv preprint arXiv:2301.11924.

Steele, E. H. (2018). Investigating the Moderating Role of Top Management Support Between Institutional Pressures and Cloud Implementation Success (Doctoral dissertation, Trident University International).

Stern, A. D. (2022). Overcoming Legal Liability Obstacles to AI Adoption. NEJM Catalyst Innovations in Care Delivery, 3(3).

Stevens, R., Kokulu, F. B., Doupé, A., & Mazurek, M. L. (2022). Above and Beyond: Organizational Efforts to Complement US Digital Security Compliance Mandates. In NDSS.

Stoianoff, N. P. (2021). Federal Court recognizes AI system as' inventor'. LSJ: Law Society Journal.

Stone, C. R. (2021). The Integration of Artificial Intelligence in the Intelligence Community: Necessary Steps to Scale Efforts and Speed Progress.

Sundar, S. S., & Liao, M. (2023). Calling BS on ChatGPT: Reflections on AI as a Communication Source. Journalism & Communication Monographs, 25(2), 165-180.

Sutopo, A. H. (2022). Qualitative Analysis using NVivo Open-ended Surveys on Basic Literacy. topar.

Syafrizal, M., Selamat, SR, & Zakaria, NA (2020). Analysis of cybersecurity standards and framework components. International Journal of Communication Networks and Information Security, 12(3), 417-432.

Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0).

Taboada Puente, I., Daneshpajouh, A., Toledo Gandarias, N., & de Vass, T. (2023). Artificial Intelligence Enabled Project Management: A Systematic Literature Review.

Talent, L. A. (2021). The DOD's Hidden Artificial Intelligence Workforce.

Tang, R. (2023). Harnessing Insights with NVivo. In Varieties of Qualitative Research Methods: Selected Contextual Perspectives (pp. 209-215). Cham: Springer International Publishing

Tang, R. (2023). Harnessing Insights with NVivo. In Varieties of Qualitative Research Methods: Selected Contextual Perspectives (pp. 209-215). Cham: Springer International Publishing.

Tasioulas, J. (2023). The Rule of Algorithm and the Rule of Law. Vienna Lectures on Legal Philosophy (2023).

Taylor, L. (2014). FedRAMP: history and future direction. IEEE Cloud Computing, 1(3), 10-14.

Tekic, Z., & Füller, J. (2023). Managing innovation in the era of AI. Technology in Society, 73, 102254.

Trichopoulos, G., Alexandridis, G., & Caridakis, G. (2023). A Survey on Computational and Emergent Digital Storytelling. Heritage, 6(2), 1227-1263.

Tuncer, S. (2020). The Future of Storytelling in the Age of AI and Posthuman.

Turobov, A. (2022). Artificial Intelligence And Security: Transformation And Consistency. Higher School of Economics Research Paper No. WP BRP, 88.

Uren, V., & Edwards, J. S. (2023). Technology readiness and the organizational journey towards AI adoption: An empirical study. International Journal of Information Management, 68, 102588.

Utin, M. (2015). From Misconceptions to Failure-Security and Privacy in US Cloud Computing FedRAMP Program.

Veres, C. (2022). Large Language Models are Not Models of Natural Language: They are Corpus Models. IEEE Access, 10, 61970-61979.

Verma, G., & Adhikari, S. (2020). Qualitative Perspective of live VM migration techniques in Cloud Computing. AIJR Proceedings, 53-61.

Verma, R. AI Policy: Impact on National Security Politics| Ethics| Technology. https://pub.towardsai.net/ai-policy-impact-on-national-security-9bbef5f654d2

Vogel, K. M. (2021). Big data, AI, platforms, and the future of the US intelligence workforce: A research agenda. IEEE Technology and Society Magazine, 40(3), 84-92.

Von Walter, B., Kremmel, D., & Jäger, B. (2022). The impact of lay beliefs about AI on adoption of algorithmic advice. Marketing Letters, 33(1), 143-155.

Vu, K., Hartley, K., & Kankanhalli, A. (2020). Predictors of cloud computing adoption: A cross-country study. Telematics and Informatics, 52, 101426.

Walker, C. (2020). AI Agents in Federal Agencies. Jotwell: J. Things We Like, 1.

Walkowiak, E., & MacDonald, T. (2023). Generative AI and the Workforce: What Are the Risks?. Available at SSRN.

Walsh, K. (2018). Checklist For FedRAMP Requirements. Retrieved December, 6, 2020.

Walsh, M. A. Balancing the Military Commander's Information Needs.

Wang, AY, Wang, D., Drozdal, J., Muller, M., Park, S., Weisz, JD, ... & Dugan, C. (2022). Documentation matters: Human-centered AI system to assist data science code documentation in computational notebooks. ACM Transactions on Computer-Human Interaction, 29(2), 1-33.

Wang, H., Zhang, L., Zheng, C., Gomez, R., Nakamura, K., & Li, G. (2022, December). Personalized Storytelling with Social Robot Haru. In International Conference on Social Robotics (pp. 439-451). Cham: Springer Nature Switzerland.

Wang, W., Chen, L., Xiong, M., & Wang, Y. (2021). Accelerating AI adoption with responsible AI signals and employee engagement mechanisms in health care. Information Systems Frontiers, 1-18.

Wang, X. (2023). Large Web Archive Collection Infrastructure and Services (Doctoral dissertation, Virginia Tech).

Wang, Y., Zhang, N., & Zhao, X. (2022). Understanding the determinants in the different government AI adoption stages: evidence of local government chatbots in China. Social Science Computer Review, 40(2), 534-554.

Warren, K., & Sabetto, R. (2018). FedRAMP: A Practical Approach. MITRE CORP MCLEAN VA.

Waseem, M., Ahmad, A., Liang, P., Fehmideh, M., Abrahamsson, P., & Mikkonen, T. Conducting Systematic Literature Reviews with ChatGPT.

Weaver, J. F. The Federal Government and Trustworthy AI. The Journal of Robotics, Artificial Intelligence & Law, 4.

Weber, R. (2019). Former CISO Touhill supports DOD backing of FedRAMP for cloud services. Inside the Pentagon, 35(35), 9-9.

Wen, D., Liu, P., Zhu, G., Shi, Y., Xu, J., Eldar, YC, & Cui, S. (2023). task-oriented sensing, computation, and communication integration for multi-device edge AI. IEEE Transactions on Wireless Communications.

Wen, D., Yao, W., Xu, J., Wang, S., Zhong, Y., Chen, H., ... & Zhou, Y. (2021). Electronic Science Games Used to Enhance Cognitive Ability: Opinion of Design From Personalization and Adaptation. Frontiers in Aging Neuroscience, 783.

Whelan, T. J. (2007, October). Anonymity and confidentiality: Do survey respondents know the difference. In Poster presented at the 30th annual meeting of the Society of Southeastern Social Psychologists, Durham, NC.

White, M. A., & Bruton, G. D. (2011). The management of technology and innovation: A strategic approach. Cengage Learning.

Whitlock, C., & Strickland, F. (2022). Data Science for AI Leaders. In Winning the National Security AI Competition: A Practical Guide for Government and Industry Leaders (pp. 99-129). Berkeley, CA: Hurry.

Wiesmüller, S., Fischer, N., Mehnert, W., & Ammon, S. (2023). Responsible AI Adoption Through Private-Sector Governance. In Responsible Artificial Intelligence: Challenges for Sustainable Management (pp. 111-132). Cham: Springer International Publishing.

Wong, W. (2021). Researching AI and Data Governance: Meta-Reflections on Research Methods and Practice. SMU Centre for AI & Data Governance Research Paper, (06).

Wong, Z. S., Zhou, J., & Zhang, Q. (2019). Artificial intelligence for infectious disease big data analytics. Infection, disease & health, 24(1), 44-48.

Woods, W. (2019). DEFENSE CONTRACTING: Enhanced Information Needed on Contractor Workplace Safety. United States Government Accountability Office.

Xia, B., Lu, Q., Perera, H., Zhu, L., Xing, Z., Liu, Y.,& Whittle, J. (2023). A Survey on AI Risk Assessment Frameworks. arXive-prints, arXiv-2301.

Xia, B., Lu, Q., Perera, H., Zhu, L., Xing, Z., Liu, Y., & Whittle, J. (2023). A Systematic Mapping Study on Responsible AI Risk Assessment. arXiv preprint arXiv:2301.11616.

Yan, R., Zhao, X., & Mazumdar, S. (2023). Chatbots in libraries: A systematic literature review. Education for Information, (Preprint), 1-19.

Yigitbasioglu, O. M. (2015). External auditors' perceptions of cloud computing adoption in Australia. International Journal of Accounting Information Systems, 18, 46-62.

Yin, R. K. (2018). Case study research and applications: Design and methods. Sage Books.

Yu, D., Gopi, S., Kulkarni, J., Lin, Z., Naik, S., Religa, T.L., ... & Zhang, H. (2023). Selective Pre-training for Private Fine-tuning. arXiv preprint arXiv:2305.13865.

Yusof , MYPM , Teo , CH , & Ng , CJ (2022). Electronic informed consent criteria for research ethics review: a scoping review. BMC Medical Ethics, 23(1), 1-11.

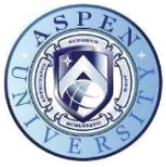
Zahedi, Z., Sreedharan, S., & Kambhampati, S. (2022). A Mental-Model Centric Landscape of Human-AI Symbiosis. arXiv preprint arXiv:2202.09447.

Zeng, K. (2016). Exploring cybersecurity requirements in the defense acquisition process (Doctoral dissertation, Capitol Technology University).

Zhu, Q., & Luo, J. (2023). Generative transformers for design concept generation. Journal of Computing and Information Science in Engineering, 23(4), 041003.

APPENDICES

Appendix A: IRB Determination Letter



IRB Determination Letter

Date: 23 June 2023
To: Freeman Jackson
From: Aspen University Institutional Review Board, 4615 East Elwood Street, Ste. #100, Phoenix, AZ, 85040
Study Title: Understanding the Technology Adoption Model for Cloud Computing, Storytelling AI, and FedRAMP
Action: Exempt Determination

The IRB for Aspen University has reviewed the documents submitted for the above referenced study and has determined it qualifies for exempt status. This determination was based on the exemption criteria, as set forth in the 45 CFR 46.101 and, therefore, is not subject to IRB oversight.

You are expected, however, to implement your study in a manner congruent with accepted professional standards and ethical guidelines as described in the Belmont Report (http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html).

Please note the following:

- This determination is based on the information provided. If the scope or nature of the study changes in a manner that could impact the determination of exempt status, you must notify the IRB in writing as an additional review may be required. Please include your full name and study title in all correspondence.

- If your study is being implemented at a collaborating organization, it is your responsibility to determine whether additional approvals are needed.
- You are responsible for keeping a copy of this determination letter in your files.
- If publications, presentations or posters are generated from this study the following wording must be used to reference the study determination outcome: *"The IRB at Aspen University determined this work met the regulatory definition of exempt research per 45 CFR 46."*

If you have any questions, please direct them to the IRB at irb@aspen.edu

Sincerely,
Kevin Thrasher, EdD
Institutional Review Board Chair

This letter has been electronically signed in accordance with all applicable regulations, and a copy is retained within Aspen University records

Appendix B: Informed Consent Form

Title of Project/Study: Storytelling AI & FedRamp: Understanding the Technology Adoption Model for Cloud Computing, Storytelling AI, and FedRAMP

Introduction

The purposes of this form are to provide you (as a prospective Storytelling AI & FedRamp participant) information that may affect your decision as to whether to participate in this research and to record the consent of those who agree to be involved in the Storytelling AI & FedRamp.

Principal Investigator

Freeman A Jackson is inviting you to participate in a Storytelling AI & FedRamp that is part of the recruitments for a doctoral degree at Aspen University.

Purpose of the Project/Research

The purpose of the project/research is to comprehensively investigate the challenges and opportunities associated with the adoption of Cloud Computing, Storytelling AI, and FedRAMP within the federal government. The research aims to:

1. Gain a deep understanding of the current landscape and practices related to the adoption of Cloud Computing, Storytelling AI, and FedRAMP within federal government agencies.
2. Identify the challenges and barriers that hinder the successful adoption and implementation of these technologies.

3. Explore the opportunities and potential benefits that can be achieved through the integration of Cloud Computing, Storytelling AI, and FedRAMP.

4. Provide recommendations and insights to inform decision-making and policy development in the federal government regarding the adoption and optimization of these technologies.

5. Contribute to the body of knowledge in the field of technology adoption, specifically within the federal government context, and drive positive change in the sector.

6. Empower federal government leaders with reliable insights and best practices to optimize cloud adoption practices, enhance efficiency, streamline processes, and improve service delivery.

Overall, the project/research aims to advance the understanding of Cloud Computing, Storytelling AI, and FedRAMP adoption within the federal government and provide actionable recommendations to support informed decision-making and successful implementation of these technologies.

Eligibility Criteria for Research Participants:

Inclusion Criteria:

1. Professionals who have direct experience or expertise in Cloud Computing, Storytelling AI, and/or FedRAMP within the federal government context.

2. Individuals who have been involved in the adoption, implementation, or management of these technologies within federal government agencies.

3. Professionals from diverse backgrounds, including IT professionals, managers, executives, researchers, and other key stakeholders.

4. Individuals who are willing to share their insights, experiences, and perspectives through confidential interviews.

5. Participants who are interested in contributing to cutting-edge research and shaping the future of technology adoption in the federal government.

Exclusion Criteria:

1. Individuals who do not have direct experience or expertise in Cloud Computing, Storytelling AI, and/or FedRAMP within the federal government context.

2. Participants who are not involved in or have no knowledge of the adoption, implementation, or management of these technologies within federal government agencies.

3. Individuals who are not willing to share their insights, experiences, and perspectives through confidential interviews.

4. Participants who are not interested or do not have the intention to contribute to research in the field of technology adoption within the federal government.

5. Please note that the eligibility criteria are subject to the specific requirements and focus of the research project. Additional criteria may be applied during the participant selection process to ensure diversity in organizational size, industry sector, and job roles.

If you meet the inclusion criteria mentioned above and are interested in participating in the research, kindly reach out to the researcher to express your interest and learn more about the research process.

Description of the Storytelling AI & FedRamp Activity

If you decide to participate, as a participant, you will have the option to choose between participating in an interview or completing a survey. The specific details and requirements of each method will be explained to you during the informed consent process. Here are the general expectations for each participation option:

Option 1: Zoom Interview

- If you choose to participate in an interview, you will be invited to engage in a confidential one-on-one conversation with the researcher.
- The interview will be conducted either in person or remotely, depending on your preference and feasibility.
- During the interview, you will be asked a series of questions related to your experiences, perspectives, and insights regarding Cloud Computing, Storytelling AI, and FedRAMP adoption within the federal government.
- The interview will be semi-structured, allowing for open-ended discussions and the exploration of specific topics.
- The duration of the interview will vary depending on the depth of the discussion but is typically expected to last between 15 to 30 minutes.

- Your privacy and confidentiality will be strictly maintained throughout the interview process.

Option 2: Survey

- If you choose to participate in the survey, you will be provided with a questionnaire that consists of a series of questions related to the research topic.
- The survey can be completed at your own convenience and can usually be accessed online.
- You will be asked to provide your responses to the survey questions based on your experiences and knowledge regarding Cloud Computing, Storytelling AI, and FedRAMP adoption within the federal government.
- The duration for completing the survey will depend on the number of questions and the complexity of your responses.
- Your privacy and confidentiality will be ensured, and your responses will be anonymized and aggregated with those of other participants.
- The choice between participating in an interview or completing a survey is entirely up to you, and you can select the option that best aligns with your preferences and availability. The researcher will provide further instructions and details regarding the specific process and requirements for your chosen participation method.

Please note that participation in either the interview or survey is entirely voluntary, and you have the right to withdraw at any time without consequences.

Approximately 15 of people will be participating in this Storytelling AI & FedRamp study.

Risks

If you decide to participate in this project/research study, it is important to be aware that there may be potential risks involved. While every effort will be made to minimize these risks, it is essential to consider the following:

- Confidentiality and Privacy Risks: Despite stringent measures in place to maintain confidentiality, there is a slight possibility of unintended disclosure of personal or sensitive information during interviews or surveys. The researcher will take appropriate steps to ensure that your identity and any identifiable information are protected, and data will be stored securely.
- Emotional or Psychological Risks: Participating in interviews or surveys may involve reflecting on past experiences, challenges, or sensitive topics related to the adoption of Cloud Computing, Storytelling AI, and FedRAMP. This could potentially trigger emotional or psychological discomfort. If you experience any distress during or after participation, it is important to seek support from appropriate resources.
- Time Commitment: Participating in interviews or surveys may require a time commitment on your part. This includes preparing for and engaging in the interview or completing the survey. It is important to consider your availability and ensure that you can allocate sufficient time to provide thoughtful and comprehensive responses.

- Withdrawal Risks: While participation is voluntary, there may be certain implications or limitations associated with withdrawing from the study after initiating participation. It is important to understand the potential consequences of withdrawal and discuss any concerns or questions with the researcher before deciding.

It is essential that you carefully consider these potential risks and determine if you are comfortable participating in the project/research study. The researcher will provide detailed information on how these risks will be mitigated and will address any additional concerns you may have during the informed consent process.

To decrease the impact of these risks, you can:

1. Ensure Informed Consent: Before participating in the project/research study, carefully review and understand the informed consent form provided by the researcher. It will outline the purpose, procedures, and potential risks involved. Take the time to ask any questions and clarify any concerns before providing your consent.
2. Maintain Confidentiality: The researcher should have measures in place to ensure the confidentiality of your personal information and data. Discuss with the researcher how your data will be handled, stored, and anonymized to protect your privacy. Be assured that your identity will be kept confidential and that your data will be used for research purposes only.
3. Seek Support: If you experience any emotional or psychological discomfort during or after participation, reach out to appropriate support networks or resources

available to you. This could include speaking with a counselor, seeking guidance from colleagues or mentors, or engaging in self-care practices that help alleviate any distress.

4. Allocate Sufficient Time: Before agreeing to participate, consider your availability and ensure that you can dedicate sufficient time to provide thoughtful and comprehensive responses during interviews or surveys. Planning and allowing ample time for participation can reduce any potential stress associated with time constraints.

5. Communicate Concerns: Openly communicate any concerns or questions you have with the researcher. They should be receptive to addressing your concerns, providing additional information, or adjusting procedures to minimize risks. Establishing a clear line of communication will help ensure that you feel supported and informed throughout the research process.

6. Withdraw if Necessary: Remember that participation in the project/research study is voluntary, and you have the right to withdraw at any time without consequences. If you decide that participation is not in your best interest or if you encounter unforeseen circumstances, inform the researcher promptly and follow any withdrawal procedures outlined in the informed consent form.

By considering these actions, you can actively mitigate the potential risks associated with participating in the project/research study and ensure that you make an informed decision that aligns with your comfort level and well-being.

Benefits

Participating in this research study on Storytelling AI and FedRAMP study can bring both direct and indirect benefits. Here are some potential benefits of participating:

Direct Benefits:

1. Contribution to Knowledge: By participating, you can contribute to the advancement of knowledge in the field of Storytelling AI and FedRAMP adoption. Your insights, experiences, and perspectives can provide valuable information for researchers, policymakers, and practitioners seeking to enhance technology adoption practices in the federal government.

2. Influence Decision-Making: Your participation can directly impact decision-making processes within the federal government. The findings and recommendations derived from this research study may be used to inform policy development, resource allocation, and strategic planning related to Storytelling AI and FedRAMP adoption, ultimately shaping the future direction of these technologies in government agencies.

3. Professional Development: Engaging in discussions and sharing your expertise during interviews or surveys can enhance your professional development. It provides an opportunity to reflect on your experiences, articulate your perspectives, and gain a deeper understanding of the challenges and opportunities associated with Storytelling AI and FedRAMP adoption. This can contribute to your own growth as a professional in the field.

Indirect Benefits:

1. Networking Opportunities: Participation in this research study can help you connect with like-minded professionals, researchers, and practitioners who share a common interest in Storytelling AI and FedRAMP adoption. Engaging in discussions and collaborating with fellow participants can expand your professional network, allowing for future collaboration and knowledge exchange.

2. Increased Awareness and Knowledge: Through participation, you can gain exposure to the latest insights, research findings, and best practices related to Storytelling AI and FedRAMP adoption. This can broaden your awareness and knowledge of the subject matter, keeping you up to date with industry trends and advancements.

3. Professional Recognition: By contributing to research in the field, you position yourself as a knowledgeable and engaged professional around Storytelling AI and FedRAMP adoption. This can enhance your professional reputation and open doors for future opportunities, such as speaking engagements, publications, or collaborations.

4. Impactful Change: Indirectly, your participation can contribute to driving positive change in the federal government's technology adoption practices. By sharing your insights, challenges, and recommendations, you have the potential to influence decision-makers and foster a culture of innovation, efficiency, and improved service delivery within government agencies.

Overall, participating in this research study offers direct benefits through knowledge contribution and decision-making influence, as well as indirect benefits through networking, increased awareness, professional recognition, and the potential for impactful change.

Confidentiality

All information obtained in this Storytelling AI and FedRAMP study will be treated with the utmost confidentiality. The following measures will be implemented to ensure the protection of participants' identities:

1. Use of Subject Codes or Numerical Identifiers: Instead of using participants' names or any personally identifiable information, each participant will be assigned a unique subject code or numerical identifier. This code will be used throughout the study to maintain anonymity and confidentiality.
2. Restricted Access: Only the researcher, project/dissertation committee members, and any individuals explicitly listed as having access will have permission to access the information provided by participants. These individuals will be bound by strict confidentiality agreements and ethical guidelines to protect the confidentiality of participants' data.

Zoom Recording (if applicable):

If audio or video recordings are part of the research process, the following measures will be taken to ensure confidentiality:

1. Recordings will only be conducted with participants' explicit consent.
2. Recordings will be stored securely and accessible only to authorized individuals involved in the research project.
3. Any personally identifiable information mentioned in the recordings will be removed or anonymized during transcription or analysis.

Securing of Information:

To secure participants' information, the following steps will be taken:

1. Digital data will be stored on password-protected computers or encrypted storage devices.
2. Paper documents, if any, will be kept in locked filing cabinets accessible only to the researcher.
3. Access to electronic and physical data will be limited to authorized individuals involved in the research project.

Data Retention:

Participant data will be retained for a period of [duration], as required by ethical guidelines and institutional policies. After this period, electronic data will be permanently deleted, and paper data will be securely destroyed to ensure the complete removal of participant information.

Please note that the specific details and procedures for maintaining confidentiality and securing data may vary depending on the cooperating institution's requirements. The mentioned measures will be implemented in accordance with relevant ethical guidelines and regulations to safeguard participants' confidentiality and protect their privacy.

Withdrawal Privileges

It is completely acceptable for you to decline to participate in this Storytelling AI and FedRAMP study, and you have the freedom to withdraw from the study at any time without facing any penalties or negative consequences. Your decision not to participate or to withdraw will not

impact your relationship with Aspen University, and it will not result in any loss of benefits or affect your grade, treatment, care, employment status, or any other relevant aspect.

If at any point during the study you wish to discontinue your participation, you may do so by simply notifying the researcher in writing or verbally. There will be no pressure or obligation to provide a reason for your decision to opt out, and your choice will be respected without question.

If this research study is being conducted in collaboration with a cooperating institution, the procedures and guidelines for withdrawal may vary. It is important to review the specific withdrawal procedures outlined in the informed consent form or any additional documents provided by the cooperating institution. These procedures will ensure a smooth and straightforward process for withdrawing from the study while safeguarding your rights and privacy.

Remember, your participation in the Storytelling AI and FedRAMP study is entirely voluntary, and your decision to participate or withdraw will be respected without any adverse consequences.

Costs and Payments

There is no financial cost to you as a participant in this Storytelling AI and FedRAMP study, nor is there payment for your participation.

Voluntary Consent

Any questions you have concerning the Storytelling AI and FedRAMP study or your participation will be answered by:

Principal Investigator:

Freeman A Jackson

Email: freeman@4th.is

Phone: 1-754-224-6952

Chair:

Dr. Dan Nguyen

Email: dan.nguyen@aspen.edu

Please feel free to reach out to Freeman A Jackson for any study-related inquiries, and to Dr. Dan Nguyen for any questions or concerns regarding the research study or the dissertation process. They will be available to address any queries and provide the necessary support and guidance throughout your participation in the study.

If you have questions about your rights as a participant in this Storytelling AI and FedRAMP study, or if you feel you have been placed at risk, you can contact the Aspen Institutional Review Board at IRB@Aspen.edu

Electronic Signature

Please read the following statement carefully and provide your consent by checking the box, entering your name, title, organization, and indicating the date

[ ] By checking this box, I confirm that I have read and understood the information provided in the consent form, and I voluntarily consent to participate in the Storytelling AI and FedRAMP

study. I understand that my participation is entirely voluntary, and I have the right to withdraw at any time without penalty.

Name: [Text field for participant to enter their name]

Title: [Text field for participant to enter their title]

Organization: [Text field for participant to enter their organization]

Date: [Date field for participant to enter the current date]

By checking the box, entering their name, title, organization, and indicating the date, participants are providing their electronic signature, confirming their understanding and agreement to participate in the study.

Appendix C: Survey/Interview Questions

Here are interview questions that will be used to gather insights from participants regarding the adoption of Conversational AI and Machine Learning in the cloud within the federal government:

1. Can you provide an overview of your organization's experience or plans for adopting Conversational AI and Machine Learning in the cloud?
2. What are the key challenges or obstacles you have encountered or anticipated in the adoption of Conversational AI and Machine Learning in the cloud within your organization?
3. How do you envision the integration of Conversational AI and Machine Learning enhancing the efficiency and effectiveness of your organization's operations and decision-making processes?
4. What are the potential economic implications (costs, savings, ROI, etc.) that your organization expects or has experienced with the adoption of Conversational AI and Machine Learning in the cloud?
5. What are the legal and regulatory considerations that you believe need to be addressed in the adoption of Conversational AI and Machine Learning in the cloud within the federal government?
6. What privacy and data protection concerns do you see associated with the use of Large Language Models (LLMs) in Conversational AI and Machine Learning applications?

7. How do you think federal government agencies can effectively address the security risks and vulnerabilities related to the use of LLMs in Conversational AI and Machine Learning?

8. In your opinion, what leadership practices and strategies are necessary for the successful implementation of Conversational AI and Machine Learning initiatives in the federal government?

9. How can federal government agencies ensure a smooth migration and integration of Conversational AI and Machine Learning technologies into their existing infrastructure?

10. What are the implications of adopting Conversational AI and Machine Learning for national security and intelligence analysis within the federal government?

11. How do you believe federal government agencies can cultivate a culture of innovation and continuous learning to support the successful adoption of Conversational AI and Machine Learning in the cloud?

12. How do you perceive the readiness of federal government agencies in terms of adopting Conversational AI and Machine Learning in the cloud? What factors contribute to this readiness or lack thereof?

13. Can you share any specific examples or use cases where Conversational AI and Machine Learning have been successfully implemented within a federal government agency? What were the key factors that contributed to their success?

14. What are the major cultural or organizational barriers that federal government agencies face when it comes to adopting new technologies like Conversational AI and Machine Learning? How can these barriers be overcome?

15. How do you think the integration of Conversational AI and Machine Learning can impact the relationship between federal government agencies and the citizens they serve? Are there any ethical considerations to be addressed in this context?

16. What are the necessary skill sets or expertise required for federal government employees to effectively work with Conversational AI and Machine Learning technologies? How can agencies ensure that their workforce is adequately trained and prepared?

17. Have you encountered any resistance or skepticism from stakeholders within your organization or from external entities in the adoption of Conversational AI and Machine Learning? How have you addressed or overcome such challenges?

18. What are the key lessons learned from previous attempts to adopt new technologies within federal government agencies? How can these lessons inform the successful adoption of Conversational AI and Machine Learning?

19. What measures can federal government agencies take to ensure data privacy and protection while leveraging Conversational AI and Machine Learning technologies? Are there any specific policies or frameworks that should be considered?

20. How do you envision the future of Conversational AI and Machine Learning in the cloud within the federal government? What opportunities and potential benefits do you foresee?

These questions aim to gather insights and perspectives from the participants regarding their experiences, challenges, expectations, and strategies related to the adoption of Conversational AI

and Machine Learning in the cloud within the federal government. Feel free to modify or add more questions based on the specific focus of your research and the context of the participants.

Appendix D: Lab Experiment Recruitment - LinkedIn Group Admin Permission Request

Subject: Request for Permission to Conduct Research in [Group Name]

Dear [Group Admin's Name],

I hope this message finds you well. My name is Freeman A Jackson, and I am a DSc candidate at Aspen University. I am reaching out to you as the administrator of the [Group Name] on LinkedIn.

I am writing to request permission to conduct my dissertation research within the [Group Name]. My research focuses on the adoption of Cloud Computing, Storytelling AI, and FedRAMP within the federal government. I believe that members of your group, who are technology innovators and enthusiasts, may have valuable insights and experiences to contribute to my study.

The purpose of my research is to investigate the challenges and opportunities associated with the adoption of these emerging technologies within the federal government. By gathering insights from industry professionals, I aim to provide valuable recommendations for optimizing technology adoption practices and enhancing service delivery in government agencies.

I would like to request permission to post an invitation in the [Group Name] to invite interested members to participate in confidential interviews. The interviews will be conducted remotely and will focus on gathering firsthand experiences, perspectives, and insights related to Cloud Computing, Storytelling AI, and FedRAMP adoption within the federal government.

I assure you that all data collected will be treated with the utmost confidentiality and used only for research purposes. Participants' identities will be anonymized to ensure privacy and compliance with ethical guidelines. I will be happy to provide more details about the research design, interview process, and any measures taken to ensure data security if needed.

I greatly appreciate your consideration of my request. Conducting research within the [Group Name] would allow me to gather valuable insights from professionals who are actively engaged in the field of technology adoption. Your support will contribute to the advancement of knowledge in this area.

Please let me know if you require any further information or if there are any specific guidelines or procedures, I need to follow to obtain permission. I am grateful for your time and consideration.

Thank you in advance for your support.

Best regards,

Freeman A Jackson

Cell” XXX-XXX-XXXX

Email: XXX@XXX.XXX

Appendix E: Lab Experiment Recruitment - LinkedIn Individual Permission Request

Subject: Invitation to Participate in Dissertation Research on Storytelling AI and FedRAMP

Dear [Contact's Name],

I hope this message finds you well. I am reaching out to you as a valued member of my professional network to invite you to participate in an important research study for my dissertation at Aspen University. The study focuses on the adoption of Storytelling AI and FedRAMP within the federal government, and I believe your insights and experiences would be invaluable to the research.

Your participation in this study would involve either an online Zoom interview or completing an online survey, based on your preference and availability. Both options will allow you to share your valuable perspectives and contribute to the research.

If you choose to participate via Zoom interview, please use the following link to schedule a convenient time for a video call interview: [Insert your Calendly scheduling link here]. During the interview, I will ask you a series of questions related to the adoption of Storytelling AI and FedRAMP. The interview is expected to take approximately 15-30 minutes.

If you prefer to participate via the online survey, please click on the following link to access the survey questionnaire: [Insert your online survey link here]. The survey will consist of questions related to the challenges and opportunities in adopting Storytelling AI and FedRAMP within the federal government. It is estimated to take approximately 10 minutes to complete.

All information shared during the interview or survey will be treated with the strictest confidentiality, and your responses will be anonymized to protect your privacy.

As a participant, you can benefit from:

1. Contributing to the advancement of knowledge in the field of Storytelling AI and FedRAMP adoption.
2. Influencing decision-making processes within the federal government.
3. Networking opportunities with like-minded professionals in the industry.
4. Increased awareness and knowledge of industry trends and best practices.

Your participation is entirely voluntary, and you are free to withdraw at any time without any negative consequences. Your decision to participate or not will not affect our professional relationship in any way.

If you have any questions about the research study or encounter any issues with scheduling the interview or accessing the online survey, please feel free to contact me at freeman@4th.is or 754-224-6952. I will be happy to assist you and provide any further clarification.

Thank you for considering this invitation. Your input and expertise would make a significant contribution to this research study. I look forward to your participation and hearing your valuable insights.

Best regards,

Freeman Jackson

XXXXXX@XXX.XXX

XXX-XXX-XXXX

Appendix D: Cloud Computing Adoption NVivo Codes and Themes

Research Question 1: Key Challenges in Cloud Adoption

Code	Description/Excerpt	Frequency
Security Concerns	"Government data security is a major challenge."	12
Data Migration Challenges	"Moving legacy systems to the cloud is complex."	8
Compliance Issues	"Regulatory compliance is a barrier to adoption."	6
Lack of Expertise	"Agencies face a skills gap in cloud technologies."	5
Cost Concerns	"Budget constraints hinder cloud adoption efforts."	9

Research Question 2: Enhancing Efficiency with CAI and ML

Code	Description/Excerpt	Frequency
Process Automation	"Automation streamlines routine tasks."	15
Data-Driven Decision-"ML improves decision-Making making."		10
Improved Customer Service "CAI enhances citizen interactions."		8
Predictive Analytics	"Predictive models aid resource allocation."	7

Research Question 3: Economic Implications

Code	Description/Excerpt "Cloud	Frequency
Cost Savings	adoption leads to reduced infrastructure costs."	12
ROI	"Agencies expect a positive return on investment."	9

Budget Allocation	"Funding shifts towards cloud initiatives."	6

Research Question 4: Legal and Regulatory Considerations

Code	Description/Excerpt	Frequency
Data Privacy Regulations	"GDPR compliance is a key concern."	10
Data Sovereignty	"Data residency requirements impact cloud choice."	7
Federal Regulations	"Federal laws dictate cloud data handling."	8

Research Question 5: Privacy and Data Protection Concerns

Code	Description/Excerpt "Data	Frequency
Data Privacy Risks	leaks in CAI/ML applications are a concern."	11
Ethical Use of Data	"Ethical considerations around data use arise."	9

Research Question 6: Addressing Security Risks

Code	Description/Excerpt "Robust	Frequency
Cybersecurity Measures	cybersecurity measures mitigate risks."	13
Vulnerability Assessment	"Regular assessments identify potential weaknesses."	8

Research Question 7: Leadership Practices

Code	Description/Excerpt	Frequency
Change Management	"Effective change management is crucial for success."	10

Visionary Leadership	"Leaders with a clear vision drive innovation."	7

Research Question 8: Migration and Integration

Code	Description/Excerpt "Having	Frequency
Cloud Migration Strategy	a well-defined strategy eases migration."	11
Integration Challenges	"Integrating CAI/ML with existing systems is complex."	9

Research Question 9: National Security and Intelligence

Code	Description/Excerpt "CAI/	Frequency
Impact on Intelligence	ML has implications for intelligence analysis."	12
Security Concerns	"National security concerns arise with data sharing."	8

Research Question 10: Culture of Innovation

Code	Description/Excerpt "A	Frequency
Innovation Culture	culture of innovation fosters CAI/ML adoption."	10
Continuous Learning	"Learning is ongoing to keep up with technology."	7

Appendix F: Storytelling AI Integration NVivo Codes and Themes

Research Question 1: Key Challenges in Cloud Adoption

Code	Description/Excerpt	Frequency
Lack of Expertise	"Government agencies face a skills gap in CAI and ML."	12
Data Security Concerns	"Ensuring data security is a primary challenge."	9
Resistance to Change	"Resistance to adopting new technologies is prevalent."	8

Research Question 2: Enhancing Efficiency with CAI and ML

Code	Description/Excerpt	Frequency
Automation	"Automation streamlines routine tasks."	15
Informed Decision-Making	"ML improves decision-making."	10
Streamlined Operations	"CAI enhances agency operations."	8

Research Question 3: Economic Implications

Code	Description/Excerpt	Frequency
Cost Savings	"CAI and ML adoption leads to cost savings."	12
Return on Investment	"Agencies expect a positive ROI."	9
Budget Allocation	"Funding shifts toward CAI and ML initiatives."	6

Research Question 4: Legal and Regulatory Considerations

Code	Description/Excerpt	Frequency

Data Privacy Regulations	"GDPR compliance is a key concern."	10
Federal Regulations	"Federal laws dictate CAI/ML data handling."	8
Compliance Challenges	"Regulatory compliance is a complex issue."	7

Research Question 5: Privacy and Data Protection Concerns

Code	Description/Excerpt	Frequency
Data Privacy Risks	"Privacy risks associated with LLMs are a concern."	11
Ethical Use of Data	"Ethical considerations around data use arise."	9
Data Security Measures	"Security measures are necessary for data protection."	8

Research Question 6: Addressing Security Risks

Code	Description/Excerpt "Robust	Frequency
Cybersecurity Measures	cybersecurity measures mitigate risks."	13
Vulnerability Assessment	"Regular assessments identify potential weaknesses."	8
Threat Mitigation	"Proactive measures are taken to address security threats."	7

Research Question 7: Leadership Practices

Code	Description/Excerpt	Frequency
Change Management	"Effective change management is crucial for success."	10
Visionary Leadership	"Leaders with a clear vision drive innovation."	7

Collaboration	"Inter-agency collaboration is promoted by leaders."	6

Research Question 8: Migration and Integration

Code	Description/Excerpt "Having	Frequency
Migration Strategy	a well-defined strategy eases migration."	11
Integration Challenges	"Integrating CAI/ML with existing systems is complex."	9
Legacy System Impact	"Legacy systems may require updates for integration."	7

Research Question 9: National Security and Intelligence

Code	Description/Excerpt "CAI	Frequency
National Security Impact	and ML have implications for national security."	12
Intelligence Analysis	"Impact on intelligence analysis is significant."	8
Data Sharing Concerns	"Data sharing in the context of national security."	6

Research Question 10: Culture of Innovation

Code	Description/Excerpt "A	Frequency
Innovation Culture	culture of innovation fosters CAI/ML adoption."	10
Continuous Learning	"Learning is ongoing to keep up with technology."	7
Interdisciplinary Teams	"Collaborative teams drive innovation in agencies."	6

Appendix G: FedRAMP Compliance NVivo Codes and Themes

Research Question 1: Key Challenges in Cloud Adoption

Code	Description/Excerpt	Frequency
Complex Authorization	"The FedRAMP authorization process is complex."	15
Resource Constraints	"Agencies face resource constraints in compliance."	12
Evolving Requirements	"Requirements evolve, posing challenges for agencies."	10

Research Question 2: Enhancing Efficiency with CAI and ML

Code	Description/Excerpt	Frequency
Enhanced Security	"FedRAMP compliance leads to enhanced security."	14
Trust and Credibility	"Compliance enhances trust in government services."	11
Competitive Advantage	"Compliance offers a competitive edge for agencies."	9

Research Question 3: Economic Implications

Code	Description/Excerpt	Frequency
Cost of Compliance	"Compliance comes with significant costs."	13
Cost Savings	"Savings from security improvements offset costs."	10
ROI of FedRAMP	"Agencies expect a positive ROI from compliance."	8

Research Question 4: Legal and Regulatory Considerations

Code	Description/Excerpt	Frequency
Regulatory Landscape	"Agencies navigate a complex regulatory landscape."	12
Legal Compliance	"Legal requirements play a crucial role in FedRAMP."	9
Compliance Challenges	"Challenges arise in aligning with legal mandates."	7

Research Question 5: Privacy and Data Protection Concerns

Code	Description/Excerpt	Frequency
Data Privacy Risks	"Privacy risks must be addressed in FedRAMP."	11
Data Handling Policies	"Clear policies govern data handling."	9
Compliance vs. Privacy	"Balancing compliance with privacy is challenging."	8

Research Question 6: Addressing Security Risks

Code	Description/Excerpt	Frequency
Cybersecurity Measures	"Robust cybersecurity measures are essential."	13
Vulnerability Assessment	"Regular assessments identify vulnerabilities."	8
Threat Mitigation	"Proactive measures mitigate security threats."	7

Research Question 7: Leadership Practices

Code	Description/Excerpt	Frequency
Change Management	"Effective change management is essential."	10
Leadership Vision	"Leaders with a clear vision drive compliance."	7

Collaboration	"Inter-agency collaboration is promoted by leaders."	6

Research Question 8: Migration and Integration

Code	Description/Excerpt "Well-	Frequency
Migration Strategies	defined strategies ease migration."	11
Integration Challenges	"Integrating FedRAMP-compliant systems is complex."	9
Legacy Systems Impact	"Legacy systems may require updates for integration."	7

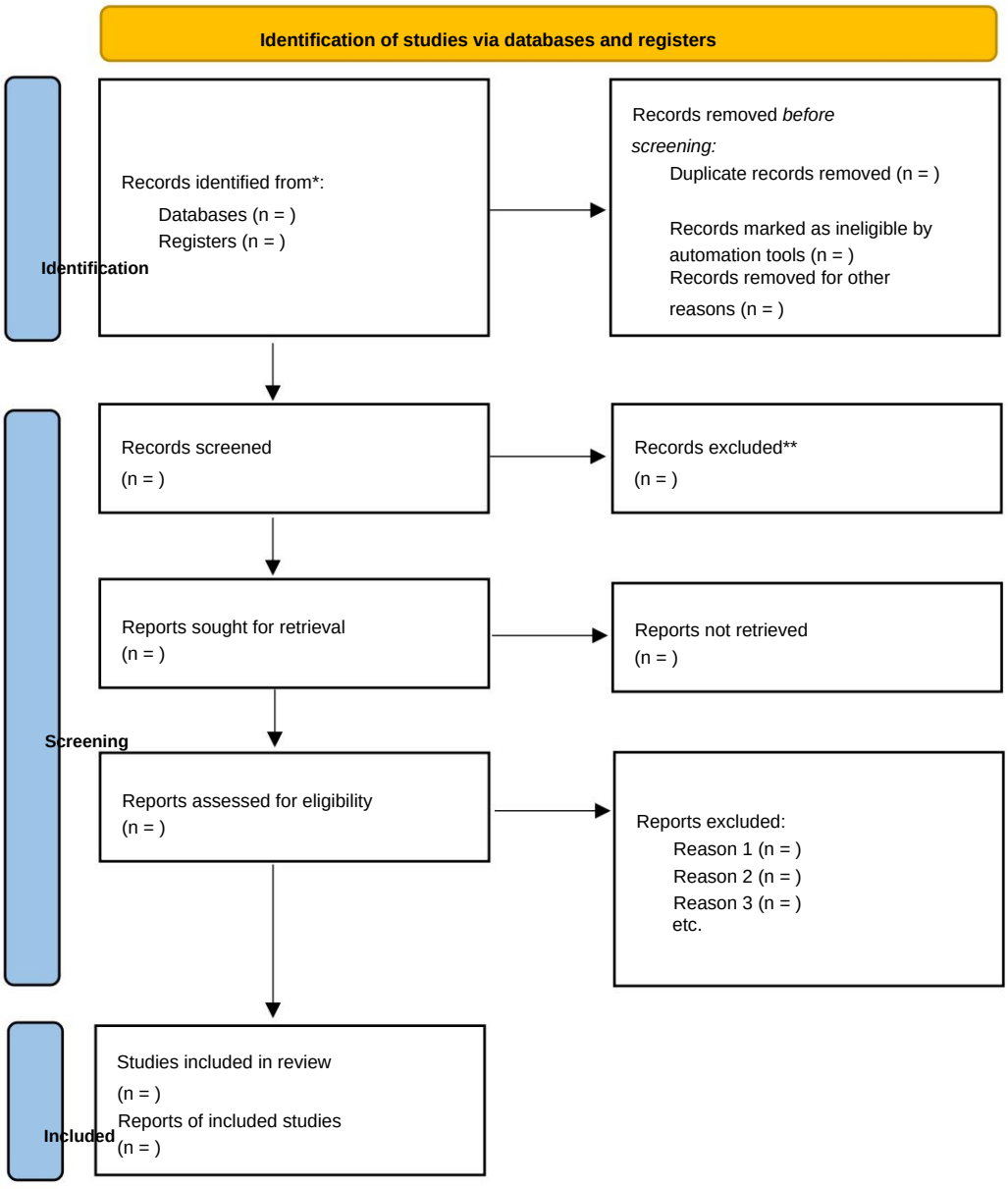
Research Question 9: National Security and Intelligence

Code	Description/Excerpt	Frequency
National Security Impact	"FedRAMP compliance impacts national security."	12
Intelligence Analysis	"Impact on intelligence analysis is significant."	8
Data Sharing Concerns	"Data sharing in the context of national security."	6

Research Question 10: Culture of Innovation

Code	Description/Excerpt "A	Frequency
Innovation Culture	culture of innovation supports compliance."	10
Continuous Learning	"Continuous learning is vital for compliance."	7
Interdisciplinary Teams	"Collaborative teams drive innovation in compliance."	6

Appendix H: PRISMA Flowchart Diagram



*Consider, if feasible to do so, reporting the number of records identified from each database or register searched (rather than the total number across all databases/registers).
**If automation tools were used, indicate how many records were excluded by a human and how many were excluded by automation tools.

From: Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ 2021;372:n71. doi: 10.1136/bmj.n71

For more information, visit: http://www.prisma-statement.org/

Appendix I: PRISMA Checklist

Section and Topic	Item #	Checklist item	Location where item is reported
TITLE			
Title	1	Identify the report as a systematic review.	
ABSTRACT			
Abstract	2	See the PRISMA 2020 for Abstracts checklist.	
INTRODUCTION			
Rationale	3	Describe the rationale for the review in the context of existing knowledge.	
Objectives	4	Provide an explicit statement of the objective(s) or question(s) the review addresses.	
METHODS			
Eligibility criteria	5	Specify the inclusion and exclusion criteria for the review and how studies were grouped for the syntheses.	
Information sources	6	Specify all databases, registers, websites, organisations, reference lists and other sources searched or consulted to identify studies. Specify the date when each source was last searched or consulted.	
Search strategy	7	Present the full search strategies for all databases, registers and websites, including any filters and limits used.	
Selection process	8	Specify the methods used to decide whether a study met the inclusion criteria of the review, including how many reviewers screened each record and each report retrieved, whether they worked independently, and if applicable, details of automation tools used in the process.	
Data collection process	9	Specify the methods used to collect data from reports, including how many reviewers collected data from each report, whether they worked independently, any processes for obtaining or confirming data from study investigators, and if applicable, details of automation tools used in the process.	
Data items	10a	List and define all outcomes for which data were sought. Specify whether all results that were compatible with each outcome domain in each study were sought (e.g. for all measures, time points, analyses), and if not, the methods used to decide which results to collect.	
	10b	List and define all other variables for which data were sought (e.g. participant and intervention characteristics, funding sources). Describe any assumptions made about any missing or unclear information.	
Study risk of bias assessment	11	Specify the methods used to assess risk of bias in the included studies, including details of the tool(s) used, how many reviewers assessed each study and whether they worked independently, and if applicable, details of automation tools used in the process.	

Section and Topic	Item #	Checklist item	Location where item is reported
Effect measures	12	Specify for each outcome the effect measure(s) (e.g. risk ratio, mean difference) used in the synthesis or presentation of results.	
Synthesis methods	13a	Describe the processes used to decide which studies were eligible for each synthesis (e.g. tabulating the study intervention characteristics and comparing against the planned groups for each synthesis (item #5)).	
	13b	Describe any methods required to prepare the data for presentation or synthesis, such as handling of missing summary statistics, or data conversions.	
	13c	Describe any methods used to tabulate or visually display results of individual studies and syntheses.	
	13d	Describe any methods used to synthesize results and provide a rationale for the choice(s). If meta-analysis was performed, describe the model(s), method(s) to identify the presence and extent of statistical heterogeneity, and software package(s) used.	
	13e	Describe any methods used to explore possible causes of heterogeneity among study results (e.g. subgroup analysis, meta-regression).	
	13f	Describe any sensitivity analyses conducted to assess robustness of the synthesized results.	
Reporting bias assessment	14	Describe any methods used to assess risk of bias due to missing results in a synthesis (arising from reporting biases).	
Certainty assessment	15	Describe any methods used to assess certainty (or confidence) in the body of evidence for an outcome.	
RESULTS			
Study selection	16a	Describe the results of the search and selection process, from the number of records identified in the search to the number of studies included in the review, ideally using a flow diagram.	
	16b	Cite studies that might appear to meet the inclusion criteria, but which were excluded, and explain why they were excluded.	
Study characteristics	17	Cite each included study and present its characteristics.	
Risk of bias in studies	18	Present assessments of risk of bias for each included study.	
Results of individual studies	19	For all outcomes, present, for each study: (a) summary statistics for each group (where appropriate) and (b) an effect estimate and its precision (e.g. confidence/credible interval), ideally using structured tables or plots.	

Section and Topic	Item #	Checklist item	Location where item is reported
Results of syntheses	20a	For each synthesis, briefly summarise the characteristics and risk of bias among contributing studies.	
	20b	Present results of all statistical syntheses conducted. If meta-analysis was done, present for each the summary estimate and its precision (e.g. confidence/credible interval) and measures of statistical heterogeneity. If comparing groups, describe the direction of the effect.	
	20c	Present results of all investigations of possible causes of heterogeneity among study results.	
	20d	Present results of all sensitivity analyses conducted to assess the robustness of the synthesized results.	
Reporting biases	21	Present assessments of risk of bias due to missing results (arising from reporting biases) for each synthesis assessed.	
Certainty of evidence	22	Present assessments of certainty (or confidence) in the body of evidence for each outcome assessed.	
DISCUSSION			
Discussion	23a	Provide a general interpretation of the results in the context of other evidence.	
	23b	Discuss any limitations of the evidence included in the review.	
	23c	Discuss any limitations of the review processes used.	
	23d	Discuss implications of the results for practice, policy, and future research.	
OTHER INFORMATION			
Registration and protocol	24a	Provide registration information for the review, including register name and registration number, or state that the review was not registered.	
	24b	Indicate where the review protocol can be accessed, or state that a protocol was not prepared.	
	24c	Describe and explain any amendments to information provided at registration or in the protocol.	
Support	25	Describe sources of financial or non-financial support for the review, and the role of the funders or sponsors in the review.	
Competing interests	26	Declare any competing interests of review authors.	
Availability of data, code and other materials	27	Report which of the following are publicly available and where they can be found: template data collection forms; data extracted from included studies; data used for all analyses; analytic code; any other materials used in the review.	

From: Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ 2021;372:n71. doi: 10.1136/bmj.n71

For more information, visit: http://www.prisma-statement.org/