School of Computer Science

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
DEHRADUN, UTTARAKHAND

MINI PROJECT

Cloud Security for Health Care
Report

Submitted to:

Dr. Khushboo Jain

Submitted by:

Amman Hussain 500091927

Arnav Sharma 500091791

Cloud Security for Healthcare: A Grounded Theory Approach

Abstract

Cloud computing (CC) has emerged as a pivotal technological advancement in the United States healthcare sector. While offering benefits such as cost reduction, scalability, resource sharing, and high availability, CC also brings forth significant concerns, particularly in privacy and security. This study employs Grounded Theory methodology to delve into these concerns within cloud-based Healthcare Information Management Systems (HIMS) in the U.S. The research focuses on healthcare organizations' strategies to mitigate these challenges through in-depth interviews and document analysis, constructing a theoretical framework showcasing CC's impact on HIMS privacy and security.

Keywords: Cloud Computing, Privacy, Security, Health Information Management Systems (HIMS), Grounded Theory Methodology

1. Introduction

Cloud computing (CC) has witnessed widespread adoption across organizations for hosting critical applications and storing sensitive data. However, concerns surrounding its security uncertainties have influenced adoption rates, especially in critical sectors like healthcare. Gartner's Cloud Shift research predicts a substantial increase in cloud adoption, with public cloud solutions expected to constitute over half of IT spending in key segments by 2025. The healthcare sector is witnessing a transition towards cloud infrastructure, with a projected surge in the global healthcare cloud infrastructure market.

This study adopts a grounded theory research design to develop insights into the privacy and security impacts of CC on HIMS. CC fosters coordination, communication, and collaboration within the healthcare sector, leading to significant improvements in care delivery. Cloud-based HIMS adoption is poised to revolutionize healthcare delivery, although the rapid adoption of CC in healthcare raises critical questions about its implications on patient data security and privacy, particularly in light of regulations like the Health Insurance Portability and Accountability Act (HIPAA).

1.1 Methodology

The research employs Grounded Theory methodology, a qualitative research strategy involving in-depth interviews and document analysis with healthcare professionals and IT specialists interacting with cloud-based HIMS. Through thematic analysis and constant comparison, the research aims to construct a theoretical framework showcasing CC's impact on HIMS privacy and security. This framework will provide valuable insights for healthcare organizations to adopt and implement cloud-based HIMS compliant with U.S. data privacy regulations.

1.2 Key Findings and Analysis

The study explores the challenges and benefits associated with cloud-based HIMS adoption in the healthcare sector. While CC offers advantages such as scalability, flexibility, and cost-effectiveness, concerns persist regarding data privacy, security breaches, and regulatory compliance. Healthcare organizations are implementing various strategies to mitigate these challenges, including robust encryption protocols, access controls, and compliance with regulatory frameworks like HIPAA.

1.3 Implications and Future Directions

The research findings underscore the need for healthcare organizations to carefully evaluate the security implications of adopting cloud-based HIMS. By adhering to best practices in cloud security and compliance, healthcare providers can leverage the benefits of CC while safeguarding patient data privacy and security. Future research directions may include longitudinal studies to assess the long-term impact of cloud-based HIMS adoption on healthcare delivery and patient outcomes.

2. Background of the Study

Recent research has extensively explored cloud computing (CC) within the healthcare sector, focusing on its impact on patient care delivery and associated data security and privacy concerns. Mehrtak et al. highlight the simplification of user collaboration, reduction in infrastructure and service costs, and improvements in agility, scalability, and flexibility as key advantages of adopting cloud technology in healthcare. However, they caution about potential drawbacks, particularly in confidentiality, privacy, and service costs, which make healthcare organizations hesitant about CC utilization.

Mehraeen et al. addressed challenges related to interoperability between cloud-hosted information systems and legacy applications within healthcare organizations. Despite numerous benefits, challenges persist in healthcare data privacy, transparency, risk management, compliance, and information security. Maslin and Rahimli conducted a SWOT analysis to investigate CC adoption in healthcare, highlighting concerns related to data security and compliance issues.

Reference explored how emerging CC technology contributes to healthcare provision, emphasizing the development of a cloud-based clinical information system, "Collaborative Care Solution." However, security risks, service interruptions, and reliance on single cloud service providers remain deterrents to CC adoption. Abrar et al. focused on the risk analysis of cloud sourcing in healthcare, highlighting the shared security responsibility model of CC and concerns hampering adoption.

The proposed research aims to assess and evaluate cybersecurity risks in cloud-based HIMS, particularly concerning patient data security and privacy. This will involve participant interviews and a review of existing literature identifying security risks primarily associated with cloud storage data breaches. Concerns regarding the privacy and security of healthcare information stored in the cloud have escalated as cloud-based HIMS gained popularity.

The Cloud Maturity Model (CMM), described by SEAGATE, offers a structured approach for organizations to assess their readiness for cloud migration and optimize cloud-based services. This model will be instrumental in evaluating the cloud adoption readiness of healthcare organizations, focusing on managing patient data privacy and security in the cloud.

In conclusion, the study aims to provide healthcare organizations with recommendations and guidelines to effectively determine their cloud roadmap and prepare healthcare personnel for managing patient data when hosted in the cloud.

2.1. Problem Statement

The healthcare sector, recognized as a critical infrastructure, faces unique challenges in protecting patient data, especially with the increasing adoption of CC. Reports highlight the growing market for healthcare cloud infrastructure and the rising incidents of healthcare data breaches. The need for secure and compliant healthcare technology platforms is more pressing than ever, with the digitization of healthcare services like Electronic Health Records (EHR) introducing benefits and security threats. The reliance on EHR and the digitization of healthcare services compels a rigorous examination of the privacy and security implications of CC.

2.2. Research Question

This study employs a qualitative grounded theory design methodology to gain insight into the impact of CC on the privacy and security of HIMS in patients' Protected Health Information (PHI) in the U.S. The research question (RQ1) is:

- How has the cloud-based computing approach to HIMS improved the privacy and security of patients' PHI in the U.S.?

2.3. Significance

This study is of utmost importance as it addresses the critical need for robust privacy and security measures in HIMS containing sensitive patient information. With the rising incidence of data breaches in healthcare, understanding the implications of CC on patient data confidentiality and security is crucial. By exploring CC adoption in healthcare, this research aims to guide organizations in enhancing their cybersecurity measures, ultimately contributing to safeguarding patient well-being and trust in the healthcare system.

3. Related Work

The cloud-based computing approach has emerged as a prevalent technological solution for organizations, irrespective of size, scope, and location. This technology has provided a platform that transcends the traditional limitations of brick-and-mortar organizations, driving its rapid adoption and implementation across a broad spectrum of business sectors. Organizations face a dual scenario in adopting and implementing CC: either overhaul their legacy on-premises applications and data services in favour of CC or integrate these existing systems with CC, making it central to all mission-critical applications and database services operations.

The adoption of CC within the U.S. healthcare sector is particularly noteworthy, classified as part of the country's critical infrastructures. This sector utilizes CC to host mission-critical applications and manage workloads that include sensitive patient care information for processing and data storage. The technological benefits of CC, such as its virtualized web service enabling constant accessibility, along with features supporting scalability, elasticity, and high availability of enterprise infrastructure, make it an attractive technology for the healthcare industry. By adopting CC, the healthcare sector can meet increasing patient care demands, including telehealth services, and reduce costs associated with managing and storing the growing volume of patient data. Consequently, CC's adoption in healthcare presents an ideal case study for researching the impact on patient data privacy and security.

3.1. Shared Responsibility in Cloud Computing: A Thematic Exploration

Organizations transitioning to cloud computing encounter challenges securing cloud computing solutions and architectures. However, this study focuses on the impacts of adopting cloud privacy and security within HIMS and does not delve into detailed discussions of cloud architecture and infrastructure security.

A critical aspect of CC security and privacy is understanding the security responsibilities of cloud consumers relative to the chosen cloud deployment and service model. Cloud Service Providers (CSPs) are obligated to secure the cloud's underlying infrastructure, while cloud customers are responsible for securing contents within the cloud, including services, applications, and data. The shared responsibility model educates adopters on securing cloud workloads and addressing CC security and privacy challenges akin to traditional on-premises data and application security.

Cloud customers must ensure administrators and personnel interacting with cloud services possess the necessary skills and permissions to meet security, privacy, and business requirements. Despite the growing adoption of cloud technology for business innovation, some industries and sectors are slow to embrace it, often due to a potential cloud skills gap.

The shortage of cloud skills among employees has contributed to increased data breaches and malware attacks against cloud-hosted technologies, primarily due to improperly configured cloud resources and services. As cloud service adoption increases, so does the likelihood of cloud misconfigurations, a leading challenge in cloud security and data privacy.

3.2. Exploration of Cloud-Based Technology Adoption in Healthcare

This study will explore the privacy and security impact of cloud-based technology adoption in the healthcare sector. It aims to analyse cloud customers' comprehension of the shared responsibility model concerning privacy and security impacts on healthcare organizations' cloud-based information management systems.

Before adopting cloud computing for database and application hosting, organizations must define business requirements for cloud adoption, encompassing an understanding of CC technology in terms of cost, usage benefits, and performance metrics, including data security, privacy, and productivity.

A comprehensive cost and usage benefit analysis is critical before adopting CC technology, encompassing all cloud adoption variables, such as cost, accessibility, storage features, data security, and privacy. The study will subsequently discuss theories to define the roadmap for adopting CC as a service in the healthcare sector and the associated implications and challenges concerning cloud privacy and security.

3.2. Healthcare Cloud Adoption: Insight from Grounded Theory and TOE Framework

Grounded Theory has been employed in information technology and management research, including studies on CC. This inductive qualitative research methodology posits that theories should emerge from data, ensuring that the developed theory aligns with empirical findings. The study expands upon previous research on cloud-based adoption in healthcare, addressing their limitations and filling the existing knowledge gaps.

The Technology Organization-Environment (TOE) framework aids in identifying relevant factors and variables influencing CC adoption in healthcare organizations. Various studies have applied this framework to analyse factors influencing new information technology innovations. The scalability, flexibility, and cost-effectiveness of cloud technology, coupled with organizational and environmental factors, play a pivotal role in its adoption in healthcare.

Digital health technology's significance is increasingly evident, with the rise in the use of digital health tools among physicians. Cloud-based technologies offer robust data collection, processing, transmission, and storage solutions. However, selecting CSPs experienced in healthcare-specific regulations, such as HIPAA, is critical.

3.3. Cloud Computing Implementation in Healthcare: Strategies and Challenges

As cloud computing becomes a leading innovative application and database hosting platform, its adoption in healthcare has been extensively studied. This body of research primarily examines CC's characteristics, features, benefits, and the privacy and security challenges associated with its implementation in healthcare.

The digitization of healthcare organizations and the enhancement of patient record sharing and interoperability through EHR are pivotal in rapidly adopting technologies like CC. Advancements in information technology, notably CC, have revolutionized patient care delivery. However, the ubiquity and convenience of cloud-based data storage also introduce significant security challenges.

Cybersecurity maturity models in healthcare organizations utilizing CC solutions emphasize adhering to security standards and best practices, such as those outlined by ISO and IEC. Additionally, HIPAA is crucial for managing healthcare information security within CC architectures.

Conclusion

In conclusion, the study delved into the critical realm of cloud security within the healthcare sector, focusing on the adoption, implications, and challenges associated with cloud computing (CC) in Healthcare Information Management Systems (HIMS). Through the employment of Grounded Theory methodology and the Technology Organization-Environment (TOE) framework, the research has shed light on various dimensions of cloud adoption in healthcare and its impact on patient data privacy and security.

The shared responsibility model in cloud computing emerged as a central theme, highlighting the crucial role of both Cloud Service Providers (CSPs) and healthcare organizations in ensuring data confidentiality, integrity, and availability. Understanding the security responsibilities under this model is paramount for mitigating risks and maintaining compliance with healthcare regulations like HIPAA.

In essence, the findings of this study provide valuable insights and guidelines for healthcare organizations to navigate the intricacies of cloud security effectively. By fostering a deeper understanding of the shared responsibility model and leveraging frameworks like TOE, healthcare entities can make informed decisions, optimize cloud infrastructure, and ultimately enhance patient data protection and trust in the healthcare ecosystem. Moving forward, collaborative efforts between stakeholders, ongoing research, and knowledge-sharing will be instrumental in ensuring the secure and responsible adoption of cloud computing in healthcare.