Contents

[1. Introduction 3](#_Toc192800202)

[1.1. Research Aim 5](#_Toc192800203)

[1.2. Objectives 5](#_Toc192800204)

[1.3. Rationale 5](#_Toc192800205)

[2. Literature Review 7](#_Toc192800206)

[2.1. The Impact of AI on Human Interaction: Redefining Communication Norms 7](#_Toc192800207)

[2.1.1 Maximizing Effectiveness 7](#_Toc192800208)

[2.1.2 Customizing User Interactions 8](#_Toc192800209)

[2.1.3 Obstacles: Decreased Sympathy and Genuineness 8](#_Toc192800210)

[2.1.4 Greater Reliance on AI 8](#_Toc192800211)

[2.2. Six Human-Cantered Artificial Intelligence Grand Challenges 9](#_Toc192800212)

[2.2.1 Social and Ethical Implications 9](#_Toc192800213)

[2.2.2 Human-Centered AI Principles and Objectives 9](#_Toc192800214)

[2.2.3 Research Directions in HCAI 10](#_Toc192800215)

[2.2.4 Recommendations for Ethical and Transparent AI 10](#_Toc192800216)

[2.2.5 Importance of Collaboration and Standardization 11](#_Toc192800217)

[2.2.6 Summary 11](#_Toc192800218)

[3. Methodology and Research Design 12](#_Toc192800219)

[3.1. Research Design 12](#_Toc192800220)

[3.2. Data Collection Methods: 12](#_Toc192800221)

[3.2.1 Surveys – A detailed primary survey will aim to gather information on: 12](#_Toc192800222)

[3.2.2 Survey Structure: 12](#_Toc192800223)

[3.2.3 Survey Distribution: 13](#_Toc192800224)

[3.2.4 User Testing 13](#_Toc192800225)

[3.2.5 User Testing Process: 13](#_Toc192800226)

[3.3. Sampling Strategy 14](#_Toc192800227)

[3.4. Data Analysis Methods 14](#_Toc192800228)

[3.4.1 Descriptive Statistics: 15](#_Toc192800229)

[3.4.2 Inferential Statistics: 15](#_Toc192800230)

[3.5. Challenges and Risk Management 15](#_Toc192800231)

[3.6. Conclusion 16](#_Toc192800232)

[3.7. Ethical Considerations 16](#_Toc192800233)

[3.8. Informed Consent 16](#_Toc192800234)

[3.9. Confidentiality and Anonymity 17](#_Toc192800235)

[3.10. Voluntary Participation and Right to Withdraw 17](#_Toc192800236)

[3.11. Data Protection and Security 18](#_Toc192800237)

[3.12. Avoidance of Harm 18](#_Toc192800238)

[3.13. Bias and Representation 18](#_Toc192800239)

[4. Project Plan 20](#_Toc192800240)

[5. Bibliography 24](#_Toc192800241)

[6. Appendix 25](#_Toc192800242)

**AI's Triple Impact: Redefining Interaction, Security, and Experience**

# Introduction

Robust AI is now regarded as one of the most vital blocks of technology as it improves security systems and even augments human interaction with different technological interfaces. The development of AI has greatly impacted many facets of life such as User Interfaces, Cybersecurity, and User Experience. This study seeks to analyse the comprehensiveness of the transformation brought to these three spheres concerning AI- algorithms and machine learning models in action.

Modern AI has profoundly upgraded the way the average user engages and interacts with technological systems. Nowadays, Machine Learning systems like virtual assistants and recommendation systems are more responsive and self-sufficient, and thus, more useful. In addition, NLP and conversation AI boost machines’ understanding of human language and language structures enabling users to interact with machines and robots as they would with a real person. The rise of AI technology-enabled instantaneously responsive bots and AI assistants to take charge of customer service roles – maintaining as well as advancing the communication construction of different fields.

AI responsibilities extend beyond just user engagement as they are also responsible for preventing user interaction's impact on cybersecurity and restraining fears about digital threats and data breaches. Cybercriminals are technologically advanced, which means they have advanced security measures to counter their tactics, and simple security defaults would never work. Cybersecurity systems that are powered by AI make use of machine learning algorithms to identify patterns, anomalies, and potential threats in real-time. This helps organizations address risks, respond to cyberattacks, and identify vulnerabilities proactively. When it comes to authentication, AI significantly improves security through biometric verification, facial recognition, and behavioural analysis to combat identity theft and unauthorized access (Sharma, 2021).

AI users' experience effects are deeply felt and go far beyond e-commerce systems and streaming services suggesting ultra-personalized content. Even adaptive user interfaces which change based on user interactions improve ease of use with AI. Features like transcription, real-time language translation, and assistance for the disabled are now possible thanks to AI.

With the development of Artificial Intelligence, business processes across sectors continue to be transformed, driving innovation and diversification. Businesses are taking advantage of AI systems to streamline customer service, and security measures, and tailor services to specific requirements. The adoption of AI solutions is indisputable and can disrupt entire industries, including healthcare, finance, retail, and even entertainment. But there are growing concerns about privacy, the potential for human job displacement, and bias algorithms as people start to rely on AI more. These concerns need to be addressed through a single strategy that guarantees AI progress in unison with ethical and legal measures.

This study attempts to analyse the effects of AI on user interaction, cybersecurity, and overall user experience. This study provides recommendations based on case studies, market data, and developments in the field that are designed to help businesses understand the increasing complexities of innovations powered by AI. Grasping the triple threat of AI is necessary for addressing digital age challenges and for balanced integration of AI technology into society along with ensuring security, ease of use, and engagement. Such analysis allows us to expand on the existing knowledge of the great capabilities of AI and the new domains and realms it can influence.

## Research Aim

## To conduct a thorough analysis on how Artificial Intelligence affects user interaction, cybersecurity, and user experience, with a specific focus on how AI technologies enhance engagement through adaptive interfaces, strengthen cybersecurity through automated threat detection, anomaly detection and risk management, and refine user experiences through predictive analytics and personalized content delivery. It will also assess the issues of ethics and the practicality of using AI virtually in all domains, including social media, and the concern of privacy, bias in AI and the balance between automation and human oversight to ensure responsible and effective AI integration across various industries

## Objectives

* Analyze how AI-enhanced technologies improve cybersecurity, user interaction, and user experience, focusing on threat and anomaly detection, adaptive security measures, and automated remediation
* Analyse the efficacy of authentication methods that rely on AI technology, particularly those involving biometrics and behavioral profiling and real-time verification, in enhancing security and user convenience.
* Highlight the gaps and challenges AI brings into the realm of cybersecurity, including but not limited to adversarial cybersecurity and data privacy issues, and trust issues in AI-driven interactions.
* Examine the social and ethical issues arising from using AI in security, such as bias in AI-based assessment of risks, surveillance concerns, and AI-driven decision-making transparency.
* Investigate how AI-centred security solutions for security, user interaction, and user experience are applied across different sectors like finance, healthcare, and e-commerce, highlighting sector-specific challenges and benefits.

## Rationale

Given the speed at which AI is changing technologies, examining its effects across different domains is critical. The research attempts to fill the gap created by the growing introduction of AI in user interaction, cyber security measures, and user interfaces—all three most important features of modern digital ecosystems. Businesses can adapt their strategies to improve engagement, security, and user interfaces by learning AI’s impact in these areas.

The increase in cyber threats requires including AI-based measures to protect sensitive information. Proactive risk mitigation measures are becoming the norm, and almost all traditional methods of cybersecurity are outdated. A more pressing issue stems from the fact that users are increasingly demanding more engaging and authentic interactions with machines, and AI is at the center of addressing this need. This work investigates the issues of ethics and privacy concerns along with everything else that AI does to improve digital interactions.

This study aims to inform businesses, policymakers, and developers on how to harness AI’s impact on user interaction, cybersecurity, and user experience effectively and responsibly by analyzing how AI-driven technologies enhance engagement, strengthen security frameworks, and refine digital experiences. It states the opportunities that AI can be possessed and how regulatory measures must be put in place to ensure ethical use. These findings will assist in decreasing risks economically and politically while making sure that the combination of AI is made in a way that meets the users’ and security countermeasures’ requirements (Russell, 2020).

# Literature Review

## The Impact of AI on Human Interaction: Redefining Communication Norms

The incorporation of AI within day-to-day activities has drastically changed how humans engage with each other and raised multiple issues. (Misnawati, Yusriadi, Astri, Abbas, & Asbar, 2025) study of how AI technologies like chatbots, virtual assistants, and personalization algorithms are changing communication patterns in the digital age. This literature review highlights AI's role in enhancing communication with the aid of efficiency and personalization, along with the opposing factors of decreased empathy, overreliance on technology, and inauthentic interactions.

Chatbots and virtual assistants have eliminated wait time by providing users with immediate responses (Mou, 2017). These AI technologies serve as important tools in increasing accessibility across customer service and streamlining mundane inquiries, leaving complex issues to human agents. (Misnawati, Yusriadi, Astri, Abbas, & Asbar, 2025) state that this AI-powered facilitation increased the speed of information exchange, but also offered users accurate and consistent information, which enhanced the overall quality of communication (Farhan, 2023).

## Maximizing Effectiveness

AI has improved business productivity a great deal by aiding in the automation processes. AI facilitates the automation of mundane functions which enables human efforts to be reallocated towards tasks that require cognition and empathy. For instance, AI-powered scheduling assistants can handle appointments along with their reminders, thereby easing the burden on memory. According to (Misnawati, Yusriadi, Astri, Abbas, & Asbar, 2025) this automated approach not only improves concern over time but sustains quality control by eliminating the possibility of human mistakes, therefore increasing trust and efficiency in operations (Farhan, 2023).

## Customizing User Interactions

The vast amount of data, AI can manipulate translates to significant user interaction improvements. Personalization algorithms examine users’ preferences and actions to predict and provide specific content, recommended products, and other services. Such modification also improves a user’s trust in the system and, in turn, boosts their engagement with the system. (Misnawati, Yusriadi, Astri, Abbas, & Asbar, 2025), however, warn that improving user experience through personalizing services comes at the cost of privacy and data protection, which creates the need for constraints on personal information and ethical implications of personalization endeavours

## Obstacles: Decreased Sympathy and Genuineness

AI assistance in communication comes with several obstacles to overcome, especially when it comes to human interaction dynamics. According to (Misnawati, Yusriadi, Astri, Abbas, & Asbar, 2025) reliance on advanced telecommunication tools can reduce empathy where interactions that require deep emotional connections are handled by machines (Misnawati, Yusriadi, Astri, Abbas, & Asbar, 2025), creating an emotional disconnect. Furthermore, the abundance of AI content raises issues of authenticity by having users question the difference between human and machine sets of communication. This can end up creating issues with digital communication trust.

## Greater Reliance on AI

AI technology has been shown to provide ease, which in turn demands a higher level of satiation, leading to greater dependence AI can show the ease of access within seemingly complex procedures that can be carried out effortlessly, but leads to concern about problem-solving abilities being neglected (Misnawati, Yusriadi, Astri, Abbas, & Asbar, 2025). In addition, these systems can pose risks when compromised further reminding users that a certain level of control needs to be maintained to prepare for the complete disablement of AI.

## Six Human-Cantered Artificial Intelligence Grand Challenges

Human-Centered Artificial Intelligence, or HCAI, is an upcoming area of research interest, which makes people the most important aspect of the AI lifecycle to make sure that AI technologies are developed for the benefit of people and their safety. The paper by Ozmen Garibay, Brent Winslow, Salvatore Andolina, Margherita Antona, and Anja Bodenschatz focuses on six grand challenges of HCAI and proposes the creation of AI that is trustworthy, comprehensible, non-discriminatory, and answerable (Ozlem Ozmen Garibay, 2023). As AI’s presence in human life increases, its usage needs to be constructive, especially concerning healthcare, business, transportation, and even eco-friendly practices (Affairs., 2018). The six challenges are:

# Trustworthiness: Ensuring that AI systems can be trusted by users and, most importantly, by the high-stake domains like finance & healthcare.

1. **Comprehensibility:** Ensuring AI is understandable for non-experts to facilitate user engagement and responsible decision-making.
2. **Non-Discrimination**: Addressing the bias in AI systems to ensure fairness and inclusivity.
3. **Accountability:** Establishing clear mechanisms for holding AI systems and their teams accountable for mistakes
4. **Transparency:** Providing insight on how AI systems make decisions in sectors like criminal justice, finance, and healthcare.
5. **Sustainability:** Designing AI systems that contribute positively to the environment and society and promoting eco-friendly practices and well-being.

## Social and Ethical Implications

AI technology has crept into the deepest parts of human communication, requiring scrutiny of its social and ethical implications. (Misnawati, Yusriadi, Astri, Abbas, & Asbar, 2025) accentuated the need to construct adaptive policies and use a human-centered approach to AI technology that helps in forming healthy human relationships. This also includes tackling concerns such as the privacy of data, the lack of consent, or the possibility of AI reproducing the existing biases in training data. If these factors are considered beforehand, developers and policymakers can create AI systems that improve human interaction and communication while ensuring ethical thresholds are not breached (Ozlem Ozmen Garibay, 2023).

## Human-Centered AI Principles and Objectives

Core principles of HCAI also address the need for AI systems to improve the basic cognitive functions of humans, assist in emotional regulation, and manage any possible adverse effects. Research has highlighted the need for making AI systems fair, unbiased, and ethical as a top priority. Garibay et al. argued that doing this effectively calls for a deliberate concerted action between technology, policy, and academic institutions, which underscores the need for proper governance and design of AI systems (Ozlem Ozmen Garibay, 2023).

## Research Directions in HCAI

A large portion of research work is focused on the improvement of human-AI interaction, algorithmic transparency, and privacy-preserving AI. Some of the efforts like that of DAPRA’s Explainable AI program are geared towards implementing interpretable AI which helps in user trust and accountability. Other areas of research include:

* Responsible AI design principles geared towards enhanced human well-being.
* Evaluation methodologies regarding the deployment of ethical AI.
* Governance models for independent oversight and auditing.

Despite progress, gaps remain in defining standardized policies, establishing industry-wide ethical norms, and addressing challenges related to bias and fairness in AI decision-making (Ozlem Ozmen Garibay, 2023).

## Recommendations for Ethical and Transparent AI

To tackle the six grand challenges presented that there are primary, high-level recommendations that highlight accountability for specific parties which include researchers, developers, policymakers, and corporations. These include:

* Governance frameworks that support AI policies at local and global fronts (Dwivedi, 2021).
* Policies that establish codes of practices, and industry-specific AI ethical standards.
* A strong focus on inter- and multi-disciplinary work to deal with the problem of AI comprehensively.
* Creating systems for regular monitoring and assessment of AI technologies.
* Developing privacy-preserving AI using secure data laundering.

Governance policies must deal with the environmental and social aspects of the project of ESG principles and FIRE governance (Fairness, Inclusivity, Responsibility and Ethics) principles.

## Importance of Collaboration and Standardization

International collaboration, a shared language, and multidisciplinary workgroups are vital for the seamless execution of HCAI. In AI’s development, Piloting agreements between industry and academia and establishing unified standards and regulatory systems are of utmost importance. Papers, conferences, and specialized training are instrumental in nurturing responsible AI development.

## Summary

The research on HCAI highlights the challenges, offers advice, and points out topics on which more research is required; it shows the significance of all relevant stakeholders in the future benefits of AI use in society. In addressing user interaction, cybersecurity, and user experience, this research highlights the need for AI technologies that are trustworthy, comprehensible, non-discriminatory, and accountable. The above-mentioned challenges provide the foundation for ensuring secure digital interaction of AI, enhancing user satisfaction, and raising the level of cybersecurity through the lens of tackling ethical concerns raised regarding bias and privacy. Ethical considerations for AI development, governance models for it, and AI’s application in humanitarian fields can create more inclusive, accessible, and secure AI systems. By introducing these principles, we can achieve a just, equitable, and technologically advanced society with AI systems that are responsible, inclusive, and human-centered, which in turn shall benefit user interaction, security, and experience.

# Methodology and Research Design

The goal of this research is to assess the effects of AI on user interaction, security, and experience with the aid of primary data collection and statistical treatment. This will be done by conducting surveys and user tests to gain objective measurements on the use of AI in different sectors.

## Research Design

This part relies heavily on **quantitative** data to show how AI influences human-machine interaction, the methods of dealing with cybersecurity issues, and user satisfaction levels. Such an approach guarantees that the information collected is factual, quantifiable, and applicable to the general population (Creswell, 2018).

## Data Collection Methods:

### 3.2.1 **Surveys** – A detailed primary survey will aim to gather information on:

* User Interaction: Perceived effectiveness and engagement in utilizing AI-powered interfaces such as chatbots, voice assistants, and recommendation systems.
* Security: Confidence in AI-based security features such as biometric identification, fraud recognition, AI-driven encryption, and issues of privacy in data and information technology.
* User Experience: Users’ contentment on how well AI adapts, the functionality of interfaces, and AI facilitating the physically challenged to access services.

### 3.2.2 Survey Structure:

* Questions will be in closed form, and answers will require selecting from a range of choices (for example, from 1 to 5 on ease of use or security perception).
* Multiple-choice questions for demographic and AI usage patterns
* Questions where users are placed in particular cases for them to assess AI system performance.
* Ranking questions for AI feature preferences (e.g., trust level for AI-powered protective measures)

### 3.2.3 Survey Distribution:

* Conducted online through Google Forms, Typeform, or Qualtrics ensuring accessibility and ease of participation
* Circulated on social platforms like social media, professional LinkedIn groups, AI technology forums, and mailing lists focused on AI users to reach individuals actively engaged with AI-driven systems,
* Stratified random sampling will be applied to ensure a balanced representation across age, industry, AI usage frequency that shall reduce the risk of selection bias.
* Estimated Participation: Minimum of 300 to reach statistical validity (Fowler, 2014).

3.2.4 User Testing – Participants will engage with the AI-driven systems, such as AI chatbots, recommendation engines and biometric authentication systems within an exercise to determine:

* Time taken to complete tasks (Example: Speed of response of AI chatbots and the time taken to perform biometric authentication).
* Correctness of recommended selections made by AI (Example: Recommendation made on an e-commerce website that shall measure the relevance and accuracy of suggestions).
* Effectiveness of security (Example: Effectiveness of AI-based fraud detection that shall measure how accurately the system flags suspicious activity or transactions).
* Post task usability satisfaction rating (Participants will provide feedback on usability, ease of interaction, and satisfaction through a Likert scale).

### 3.2.5 User Testing Process:

* Pre-test briefing – All respondents are presented with and read a scenario about the AI system they will be interacting with.
* Interaction phase – Participants must perform tasks through AI-driven interfaces for the data to capture the time taken and errors made (response time, errors made).
* Post Task Questionnaire: Participants are asked to rate the system from a defined scale on user friendliness, security, and satisfaction level.
* Observational notes – Notes filed by the researcher about users or behaviors and reactions to the acts observed.

Expected participants: **15 to 30** users from diverse demographic and socioeconomic backgrounds to interact with AI features within their natural context.

## Sampling Strategy

In this case, to foster variety, we will employ stratified random sampling techniques.

* Target Population: Any AI user, which includes ordinary consumers, specific industry workers, and technology lovers.
* Sample Size: At least 300 respondents for surveys, 15-30 users for user testing.
* Stratification Criteria:
* Age groups: We’ll divide participants into the following age groups (18-25 years, 26-40, 41-60, above 60 years) to ensure representation from a wide range of generational perspectives. This shall help us in capturing potential differences in AI usage patterns and the adoption of technology across age groups.
* Industries: AI usage differs across different sectors(Healthcare, finance, e-commerce, cybersecurity, education, entertainment) to ensure balanced representation from these industries. Samples will be obtained by targeting professionals from LinkedIn groups & sector focused mailing lists to gather data from individuals who interact with AI in different professional contexts.
* Frequency of AI usage: Participants will be categorized (Occasional users, moderate users, heavy users) to reflect varying levels of interaction with AI technologies. This shall help us in assessing how AI affects users with different levels of engagement and to understand the difference between a beginner and an advanced AI user.
* Technical Expertise: Categorizing participants by expertise(Novice, intermediate, and advanced AI users) shall ensure that we capture a full spectrum of experiences with AI. This accounts for varying levels of understanding and interaction with AI, which may affect user perceptions of security, interaction, and experience.

The above ensures that representation is proportionate and solves the problem of bias sampling, hence increasing the trustworthiness of the results.

## Data Analysis Methods

The data collected through different methods will be analyzed through SPSS to examine patterns, correlations, and the effect of AI on various user groups.

### 3.4.1 Descriptive Statistics:

* Mean, median, and standard deviation to portray how users, security, and satisfaction are experienced and interpreted in AI.
* Use of Frequency distribution to study the patterns of AI implementation in various population groups.

### 3.4.2 Inferential Statistics:

* Correlation Study: Understanding the correlation of AI adoption with security perception and trust. Regression Study: Estimation of the degree of interaction AI driven with engagement, satisfaction, and security confidence.
* T-tests & ANOVA: Examining the satisfaction from interactions with AI across age groups, industries, and experience with AI.

The findings from the user testing will be analysed using performance metrics, and AI engagement will be compared across various user groups using different statistical methods.

## Challenges and Risk Management

* **Difficulties in attaining a diverse sample** – Recruiting AI practitioners from various industries or levels of expertise poses a challenge.

**Response**: We will use professional groups on LinkedIn and AI discussion forum newsletters, along with specialized target email lists, to reach as many participants as possible.

* **Doubts about the survey validity** – Respondents may provide expected answers or ignore parts of the issues on the survey.

**Response**: A pilot survey will be administered to a smaller test group to allow more focused questions to be formulated more neutrally and clearly for the larger test group.

* **Assumptions of the user testing subjects** – The AI testing conditions that are put in place may not be reflective of actual user behaviour.

**Response**: The tasks that require completion will be designed to resemble real use of AI so that the results can be used for the real application of AI.

## Conclusion

This report aims to analyse the interaction output, interface, cybersecurity measures, and user experience features that an AI system provides and analyse it deeply to find out the uses it can be put to. It will enable businesspeople, programmatic designers, and regulatory authority figures to improve the functionality of AI technologies by incorporating security systems, trusting in AI automation systems, and optimizing the business’s AI-driven strategies for user engagement and participation.

## Ethical Considerations

Any research that involves human subjects must address ethical issues, and this project will follow ethical standards that concern the welfare, privacy, and dignity of all participants. Although not many ethical concerns are expected from this study, some key ones will be managed throughout the project focusing on data collection and participation. Some of the ethical issues that we will address are listed beneath:

## Informed Consent

**Issue:** Every person who takes part in the surveys as well as in the interviews has to properly understand that they are free to participate and must be aware of how their information will be used before the research proceeds.

**Strategy:** Every individual participating in the study will be fully briefed beforehand on the aim of the study, why it is being undertaken, what type of information will be collected, and what dangers, if any, are involved. It will be a requirement that the participants sign an explicit written consent form before taking part in the research. An informed consent form will precede the actual surveys and for interviews, written consent will be taken before the interview session.

## Confidentiality and Anonymity

**Issue:** One of the fundamental principles of conducting research ethics is to protect research participants’ identity and confidentiality from unauthorized disclosure is a proper ethical concern.

**Strategy:** Data will be anonymized removing all identifying factors like names or contact details before analysis. Sensitive data collected during the process will remain in the physical custody of the research team so no single participant will be identifiable in any published research and all findings will be multivariate to ensure confidentiality. Participants during the interviews will be allowed to choose whether they wish to remain anonymous or identified via a pseudonym in any reports.

## Voluntary Participation and Right to Withdraw

**Issue:** Participants must be free to choose whether to participate and have the right to withdraw from the study at any point without facing any negative consequences.

**Strategy:** The strategy is that all participants have the right to withdraw from the study at any point with no negative consequences. All participants must be able to choose whether to take part in this study or not and if they do they must understand that they can stop participating without any penalty.

At the start of the research, participants will be instructed that their participation is completely voluntary and that they are free to withdraw at any time without giving any justification for doing so. This will be clearly stated in the informed consent form. Moreover, participants will be advised that failure to complete the study will not influence their relationship with the researchers or the results of the study.

## Data Protection and Security

**Issue:** The protection of sensitive data about the participants needs special care in storage since it needs to be defended from exploitation and leaking.

**Strategy:** Data will be preserved in a secure electronic medium, which is inaccessible to outside parties. Names and email addresses will be stored separately from the primary data. The research will also be conducted under the principles of GDPR on privacy protection, which restricts the use of participants' sensitive data to information that is crucial for the study only. All sensitive information collected in the course of the study will be destroyed, and only aggregated anonymized information will be kept for further studies or publications.

## Avoidance of Harm

**Issue:** It is crucial to ensure that no damage including physical injury, psychological trauma, or emotional distress will be inflicted on the subjects, especially when deploying AI technologies for testing.

**Strategy:** Focusing on users who will interact with the AI systems, participants will be informed of the user testing procedures and their results beforehand. No AI systems will be employed that could elicit distress during sensitive contexts such as security. Moreover, participants need to be assured that there is no expectation about activities that may potentially cause harm or undue stress. If any participant verbalizes discomfort, the option to terminate the session at any time will be available without resulting in any penalties.

## Bias and Representation

**Issue:** Finding representative samples of participants that would guarantee unbiased results regardless of demographic classification.

**Strategy:** A sufficient number of participants with diverse backgrounds, ages, and experience with AI systems, as well as varying professions and levels of sophistication will be purposefully sampled. AI is shown to influence relations, security, and general user experience differently; therefore, the research seeks to include all, or most, of the relevant underrepresented groups so that the results portray the impact accurately. Any bias that tends to emerge from the research process, such as, incompletely defining the scope of the study by employing stratified random sampling and purposive sampling will be undertaken.

# Project Plan

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Tasks** | **Week 1** | **Week 2** | **Week 3** | **Week 4** | **Week 5** | **Week 6** | **Week 7** | **Week 8** | **Week 9** | **Week 10** | **Week 11** |
| **1.Project Initiation** |  |  |  |  |  |  |  |  |  |  |  |
| Define research  objectives | ✅ | ✅ |  |  |  |  |  |  |  |  |  |
| Develop research questions | ✅ | ✅ |  |  |  |  |  |  |  |  |  |
| Research proposal submission | ✅ | ✅ |  |  |  |  |  |  |  |  |  |
| **2.Literature**  **Review** |  |  |  |  |  |  |  |  |  |  |  |
| Collect academic sources |  |  | ✅ | ✅ | ✅ | ✅ |  |  |  |  |  |
| Analyze relevant  literature |  |  | ✅ | ✅ | ✅ | ✅ |  |  |  |  |  |
| Identify research gaps |  |  |  | ✅ | ✅ | ✅ |  |  |  |  |  |
| **3. Methodology**  **Development** |  |  |  |  |  |  |  |  |  |  |  |
| Define research  design |  |  | ✅ | ✅ | ✅ |  |  |  |  |  |  |
| Develop sampling  strategy |  |  | ✅ | ✅ | ✅ |  |  |  |  |  |  |
| Identify ethical consideration |  |  | ✅ | ✅ | ✅ |  |  |  |  |  |  |
| **4.Data Collection** |  |  |  |  |  |  |  |  |  |  |  |
| Conduct surveys |  |  |  |  | ✅ | ✅ |  |  |  |  |  |
| Conduct interviews |  |  |  |  |  | ✅ | ✅ |  |  |  |  |
| Conduct user testing |  |  |  |  |  | ✅ | ✅ |  |  |  |  |
| **5. Data Analysis** |  |  |  |  |  |  |  |  |  |  |  |
| Clean and organize  data |  |  |  |  |  |  | ✅ |  |  |  |  |
| Thematic analysis of qualitative data |  |  |  |  |  |  | ✅ | ✅ |  |  |  |
| Statistical analysis of survey data |  |  |  |  |  |  | ✅ | ✅ | ✅ |  |  |
| **6. Writing and Compilation** |  |  |  |  |  |  |  |  |  |  |  |
| Write findings and discussion |  |  |  |  |  |  |  | ✅ | ✅ |  |  |
| Draft conclusion and recommendations |  |  |  |  |  |  |  | ✅ | ✅ | ✅ |  |
| Proofreading and final review |  |  |  |  |  |  |  |  |  | ✅ | ✅ |
| **7. Final Submission** |  |  |  |  |  |  |  |  |  |  | ✅ |

# Bibliography

Affairs., U. N. (2018). Indigenous peoples’ rights to lands, territories and resources at the centre of UN annual forum.

Colaner, S. (2021). The ethics of artificial intelligence in human communication. AI & Society. 36(2), 543-554. https://doi.org/10.1007/s00146-020- 01049-4.

Creswell, J. W. (2018). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches.*

Dwivedi, Y. K. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice, and policy.

Farhan, A. (2023). The Impact of Artificial Intelligence on Human Workers. Journal Of Communication Education,.

Fowler, F. J. (2014). *Survey Research Methods (5th ed.).*

Misnawati, M., Yusriadi, Y., Astri, Z., Abbas, A., & Asbar, A. (2025). Exploring Teachers' Initial Perceptions of Corpus Linguistics and Their Readiness to Incorporate Corpora in Classroom Instruction: A Qualitative Analysis. *Qualitative Report, 2025, Vol 30, Issue 1, p3024*.

Mou, Y. &. (2017). The media equation and digital technologies: An examination of social responses to chatbots. Computers in Human Behavior.

Ozlem Ozmen Garibay, B. W. (2023). Six Human-Centered Artificial Intelligence Grand Challenges.

Russell, S. &. (2020). *Artificial intelligence: A modern approach (4th ed.).* Pearson.

Sharma, A. &. (2021). Artificial Intelligence in Cyber Security: Techniques and Applications.

# Appendix

## Questionnaire: A survey shall be distributed to the participants that shall have detailed questions with respect to our objective.

## Prototype: Screenshots, mock-ups or AI integration in UX.