

The Role of Artificial Intelligence in Enhancing
Cybersecurity of Health Information: Between Technical
Adoption, Human Challenges, and Social Attacks

Bushra Ali Alharby

Research Supervisor

Dr. Mohammed Anbar

Abstract

With the exponential expansion of digital healthcare, patient information has become increasingly vulnerable to cyber threats, both through technology and social skills involving humans.

This study aims to explore the role of artificial intelligence (AI) in enhancing healthcare information security by analyzing the technical and human challenges facing data protection. The study will also understand the experience of the "digital human" in healthcare settings, focusing on human behavior and awareness, complementing technical solutions.

Our methodology utilizes a literature review and previous studies to provide innovative recommendations for enhancing patient privacy protection. These include AI technologies, along with cyber awareness and education.

Chapter 1: Introduction

1.1 Introduction:

Our world today is witnessing a rapid digital transformation, reshaping all areas of life, most notably health and education. In light of this transformation, digital data—especially health information—has become exceptionally important, making it a direct target for increasingly sophisticated cyber threats.

Artificial intelligence (AI) has emerged as a central tool in developing cybersecurity strategies, as it can contribute to early detection of threats, analyze behavioral patterns, and provide more effective predictive solutions than traditional models. As recent studies such as Meduri et al. (2024) demonstrate, AI offers significant potential to enhance the security of healthcare systems.

However, despite this potential, an overemphasis on the technical aspect has overlooked the human dimension in security discourse. According to Petersons (2024) and Klimburg-Witjes & Wentland (2021), the digital human is not only a security vulnerability, but an active player whose motivations and behaviors must be understood and integrated into security solutions.

Social engineering, for example, is one of the most dangerous threats targeting the human factor directly, exploiting users' psychological and behavioral vulnerabilities. This is confirmed by Rahim (2024) in his analysis of threats in the healthcare sector.

Hence, the importance of viewing cybersecurity from a holistic perspective that combines technology and people. Security is no longer just about software and applications; it is a social and psychological context that must be studied in depth to understand how digital humans feel safe or threatened, and how intelligent systems can enhance their confidence rather than marginalize it.

1.2 Theoretical Background:

In light of the accelerating digital transformation, traditional cybersecurity strategies that rely on firewalls and data encryption are no longer sufficient, especially in a sensitive sector like healthcare. Studies (**e.g., Klimburg-Witjes & Wentland, 2021**) have demonstrated that the human element remains the weakest link in the security system, either due to poor security awareness or vulnerability to social engineering techniques.

Here, AI emerges as a promising tool that goes beyond traditional defenses. It can analyze user behavior and detect abnormal patterns, helping to detect threats before they occur, including insider threats or those resulting from social manipulation.

However, the application of AI in a complex environment like healthcare poses unique challenges. According to **Rahim (2024)**, securing sensitive health data requires a delicate balance between technical proficiency and ethical considerations. Studies such as **Meduri et al. (2024)** emphasize the importance of clear governance standards and high transparency to ensure user acceptance and trust.

Real-life incidents, such as the hacking of the Bjorka system as reported by **Ingrida & Wibowo (2024)**, have shown that the impact goes beyond data leakage, but also extends to undermining personal and social security.

Accordingly, this study seeks to frame the digital human as a pivotal element in the cybersecurity equation. It aims to emphasize that building intelligent and effective systems is only possible with a deep understanding of human behavior and their psychological and social needs in the digital space.

1.3 Problem Statement:

With the accelerating digital transformation and the spread of artificial intelligence technologies, humans are no longer merely users of technology, but rather "digital beings" who live, interact, and are hacked within this space. Despite the enormous potential this environment offers, it poses profound challenges that touch upon the essence of privacy and security. Cyberattacks are no longer merely data theft; they threaten the psychological and social structure of individuals.

Research Gap

Despite the abundance of technical research in the field of cybersecurity, the human experience remains marginalized in most analytical frameworks. **Many studies (such as Petersons, 2024 and Nifakos et al., 2021)** have focused on purely

institutional and technical aspects. In contrast, other studies (such as Klimburg-Witjes & Wentland, 2021 and Ingrida & Wibowo, 2024) have attempted to deconstruct the stereotype of the user as a "weak element" and highlight the psychological and social impacts of hacking, but they have not sufficiently focused on the role of humans as a key actor in the security system.

At the same time, AI tools are evolving to enhance security, as Meduri et al. (2024) points out. However, they often lack transparency and ignore the complex human context. Rahim (2024) shows that these systems remain vulnerable to attacks that exploit the human factor, such as social engineering.

Hence, a research gap emerges: the urgent need for an analytical framework that combines the technical and human dimensions and analyzes the relationship between the digital human, technology, and security discourse.

This study aims to fill this gap by providing a critical analysis that highlights the "digital human" not only as a potential victim, but as an active and influential element in the cybersecurity ecosystem. The study seeks to integrate technical, psychological, and social dimensions to provide a deeper and more comprehensive understanding of the digital security experience under AI systems.

1.4 Research Objectives:

This study aims to provide a deep understanding of the role of the "Digital Human" in confronting the growing challenges of cybersecurity, in light of the rapid digital transformation the world is witnessing.

To achieve this primary objective, the study seeks to achieve the following sub-objectives:

1-TO understanding and Protecting the Digital Human: Analyzing the concept of the "Digital Human" and defining the dimensions of their identity, privacy, and online presence. This objective focuses on providing practical solutions to raise security awareness, developing appropriate policies, and designing awareness programs that aim to empower individuals rather than blame them.

2-TO identifying Threats to Individuals: Identifying the most prominent threats directly targeting individuals, such as "social engineering," "identity theft," "digital tracking," and "privacy breach."

3-TO analyzing the Image of the Human in Security Discourse: Examining how the human is portrayed in security discourse, particularly through terms such as "imperfect user" and "human fragility." The study aims to understand the impact of these terms on individuals' awareness of their security responsibilities.

4-TO assessing Psychosocial Impacts: Assessing the psychological and social impacts of cyberattacks on individuals, and studying how they affect their sense of safety, trust, and well-being in their digital environments

The objectives of this study were designed to directly respond to the key challenges identified in the research problem and literature review. Each objective aims to address a specific aspect of these challenges, ensuring a close interconnection between the objectives and significance of the study.

Objective 1: Focuses on analyzing the concept of the "digital human" and presenting strategies for protecting it. This addresses the urgent need for a deeper understanding of individuals' identities, privacy, and agency in the digital world.

Objective 2: Addresses cyber threats that directly target individuals, such as "social engineering" and "identity theft." These challenges are the focus of the research problem, and this objective contributes to a deeper understanding of them.

Objective 3: Addresses how users are portrayed in security discourse, particularly through terms such as "imperfect user." This aspect aims to highlight how this discourse influences individuals' awareness of their security responsibilities.

Objective 4: Explores the psychological and social dimensions of cyber breaches. This dimension is often overlooked in traditional technical solutions, but it is essential for designing human-centered security strategies that take into account their needs.

1.5 cope of the Study

This study focuses on understanding the growing role of artificial intelligence (AI) in enhancing cybersecurity within digital healthcare systems. Particular attention is paid to the human and social dimension, expressed through the concept of the "digital human." We seek to analyze the relationship between cyber threats that directly target individuals, the intelligent technologies used to counter them, and the security practices that shape user awareness.

Principal Study Topics

This study covers several key topics:

Target Environment: Digital healthcare systems containing highly sensitive medical data.

Technical Aspect: AI applications used to monitor threats, predict risks, and improve security responses.

Human Aspect: Analyzing individual behaviors, awareness levels, social engineering risks, and the psychological and social impacts of attacks.

Qualitative Analysis: Reviewing recent literature, case studies, and security discourses, critiquing the stereotype that portrays the user as a vulnerable element.

Scope of Analysis: Not limited to security tools, but also extending to include the effectiveness of communication strategies, social and ethical implications, and the extent to which AI empowers the user.

It should be noted that this study does not include field experiments or experimental models. Instead, it presents an integrated analytical and critical framework that links technology and people in the context of healthcare cybersecurity.

1.6 Significance of the Study:

This study is most important because of the ever-increasing number of cyberattacks targeting health data, which demonstrate the inadequacy of technical solutions alone to provide adequate protection. Therefore, it is essential to explore the complex interactions between technical, human, and social factors within and beyond the digital landscape, as well as the role of "humans" in healthcare.

This study focuses on the following:

Integrating the human body and technology: By understanding how users' communications, awareness, and social media influence email.

Multidimensional interpretation: By shedding light on people who need it (such as social animals), not just electronics.

Providing a comprehensive and multidisciplinary approach: Combining analytics, public groups, and threat understanding.

Continuing support: Providing evidence-based updates to healthcare industries, with the goal of protecting digital technology from the ravages of many.

Chapter 2: Literature Review

2.1 Literature Review:

In light of the accelerating digital expansion, in which humans have become an integral part of the digital space, complex security challenges emerge that go beyond technical aspects to touch upon the core of an individual's identity and sense of security, impacting their privacy. This review aims to analyze recent studies that have addressed the position of the "digital human" in the face of cyber threats, by exploring the role of human factors, analyzing the nature of attacks, and critiquing traditional security discourse.

First: Cybersecurity and Artificial Intelligence

The literature indicates that modern AI-based cybersecurity systems are gaining increasing importance in countering digital threats, as evidenced by **Midori et al.'s (2024) study**, which presented a range of AI technologies used to secure data, but at the same time demonstrated a clear neglect of the human dimension within these systems.

On the other hand, a study by the **World Economic Forum (2025)** highlighted the importance of balancing the adoption of AI technologies in cybersecurity with their risks, emphasizing that imprudent use can lead to a threat to trust, especially when ethical and privacy considerations are ignored.

Second: Human Factors and the "Imperfect" User

Several studies have focused on the importance of the human factor in the cybersecurity equation. Most notable are:

Petersons (2024) provided a comprehensive overview of cybersecurity challenges associated with individuals, emphasizing the need for effective awareness strategies.

Nevakos et al. (2021) highlighted the direct impact of the individual on cybersecurity in healthcare organizations and argued that sensitive data requires security models that integrate the human element at their core.

Klimburg-Witjes and Wentland (2021) offered a scathing critique of how human error is portrayed in security discourse, highlighting the concept of the "imperfect user" as a factor used to blame the individual rather than build a collaborative security environment.

Third: Case Studies and Cybersecurity as a Personal Issue

Through real-life examples, some studies have demonstrated the psychological and social impact of breaches:

Ingrida and Wibowo (2024) provided an analysis of the Björka incident as a case study demonstrating how cyberattacks can undermine individuals' sense of security and privacy.

Rahim (2024) focused on the healthcare sector, explaining how data breaches in this sector deeply impact digital and human dignity.

Fourth: New Contributions to Artificial Intelligence and Cyberhealth

Three important studies have recently joined the list:

CEPS Report (2023) examined the relationship between AI and cybersecurity from a policy perspective, emphasizing the need to integrate transparency and digital governance to enhance trust in technologies.

Tyagi et al. (2024) examined the use of AI to enhance the security of digital health communication, noting the importance of balancing health information protection with user experience.

Soni et al. (2024) reviewed AI and machine learning techniques to improve the security and privacy of eHealth systems, and showed that integrating AI can be effective, provided there is accompanying human awareness.

Previous research in cybersecurity has focused heavily on technical aspects and threat analysis, neglecting the human and psychological aspects of users, especially in the health data environment. Security discourse also places the responsibility on the user, ignoring the limitations of the tools available to them.

This study aims to offer a different perspective on cybersecurity by bridging this gap. We present a conceptual framework that combines artificial intelligence and human factors to provide a more comprehensive understanding of cybersecurity in digital healthcare.

Chapter 3: Research Methodology

3.1 Research Methodology

3.1.1 Research Design

This study adopts a qualitative, descriptive, and analytical approach and aims to understand the role of artificial intelligence technologies in the field of cyber health insurance. Rather than collecting field data, the research relies on a theoretical analysis of previous literature and studies, with the aim of constructing a framework that takes into account social interaction and socio-psychological behavior, represented by the concept of the "digital human."

The research focused on analyzing how humans are represented in cyber expert discourse, exploring digital AI technologies and their privacy, and highlighting the challenges facing people in a completely secure environment.

3.1.2 Data Sources

This study relies solely on secondary data, carefully collected and analyzed from reliable sources, adhering to strict scientific standards, ensuring its suitability for the research objectives, and its practical validity.

These resources include:

Academic studies: Articles published in peer-reviewed journals specializing in cybersecurity, artificial intelligence, and digital studies, with a particular focus on the digital human in healthcare.

Reports: Documents issued by existing and local entities specializing in scientific information and technical analyses that could actually address the topic of digital technology.

Case studies: Investigations of real-life Bluetooth incidents, focusing on monitoring workers within digital human healthcare environments.

Specific literature: This includes frameworks, laws, and strategic documents that define digital identity, privacy protection, and the ethics of using artificial intelligence.

This literature was selected primarily based on its direct relevance to the study topic, particularly: the "digital human," the digital health sector, rapid and behavioral responses to cybersecurity, and the use of AI technologies in threat prediction and data security.

3.1.3 Data Analysis Method

The study also uses thematic analysis as a primary tool for identifying central concepts and ideas represented in texts and secondary sources. The content was categorized and analyzed according to its main summary, representing the areas **most relevant to the study:**

- Artificial Intelligence Technologies: Analyzing the uses of AI in cybersecurity replication and prediction, and the digital defense record.
- Cybersecurity Design Steps: Analyzing and identifying people, particularly social skills, social technologies, and behavior.
- Human Vulnerabilities: Shedding light on the psychological and behavioral aspects that contribute to focusing on the people targeted by threats, and the importance of building awareness among them.
- Privacy and Ethics: Analyzing various issues related to the ethics of using AI and the extent to which individuals' personalities are respected within digital electronics.

This analysis emphasized the construction of a multidimensional interpretive vision of the relationship between humans and smart technology, through the integration of technology and humanity within the cybersecurity framework. It also facilitated understanding and changed how the "digital human" is represented in security discourses and adopted technical mechanisms.

3.1.4 Limitations of the Study

This study is limited to a literature review, without conducting any field interviews or surveys. Therefore, its findings represent a theoretical analytical perspective and may not be fully generalizable. This limitation is due to the nature of the qualitative approach, which focuses on in-depth, contextual understanding rather than quantitative measurement. However, the focus on conceptual analysis enables the

study to identify knowledge gaps and propose frameworks that can be built upon in future research.

3.2 Expected Study Outcomes

This study aims to provide substantive findings that contribute to building a comprehensive understanding of the role of the digital human in the cybersecurity ecosystem. The most prominent expected outcomes are as follows:

Clarifying the concept of the "digital human": The study will contribute to providing a precise and comprehensive definition of the concept of the "digital human," analyzing its cognitive, psychological, and social dimensions in an environment increasingly dependent on digital interaction.

Categorizing threats targeting individuals: The study will classify the most targeted cyber threats against individuals, such as social engineering, identity theft, and digital tracking, in addition to analyzing the psychological effects associated with these threats.

Criticizing the prevailing security discourse: The study will provide a critical analysis of the current security discourse, which tends to place full responsibility on the user, and will instead propose a more equitable and comprehensive discourse that empowers individuals to effectively perform their security role.

Proposing an integrated conceptual framework: The study is expected to provide a framework that combines advanced technical solutions with human considerations, emphasizing the importance of transparency in AI systems and integrating effective awareness programs to empower users.

Highlighting the psychological dimensions of attacks: The study will highlight the emotional and social impacts of cyberattacks on individuals, enhancing our understanding of the human dimension of digital threats and the importance of considering it when developing protection strategies.

3.3.Gantt Chart:

References:

1. Meduri, K., Nandiraju, N., & Krishna, S. V. (2024). *Enhancing cybersecurity with artificial intelligence: Predictive techniques and challenges in the age of IoT*. Sensors.
2. Ingrida, N. V., & Wibowo, D. (2024). *Digital security in human security: A case study of the Bjorka hacking incident*. SSRN.
3. Petersons, E. (2024). *Cybersecurity challenges in the era of digitalization*. SSRN.
4. Rahim, M. J. (2024). *Cybersecurity threats in healthcare IT: Challenges, risks, and mitigation strategies*. SSRN.
5. World Economic Forum. (2024). *Artificial intelligence and cybersecurity: Balancing risks and rewards*. WEF Report.
6. Tyagi, A. K., Hemamalini, V., & Soni, G. (2024). *Digital health communication with artificial intelligence-based cyber security*. National Institute of Fashion Technology, SRM Institute of Science and Technology, MATS University.
7. C SSP. (2024). *Guidelines for secure usage and adoption of artificial intelligence* (Version 1.0).
8. Hadwan, M., & et al. (2024). *Security and privacy in e-health systems: A review of AI and machine learning techniques*. Discover Artificial Intelligence, Springer.
9. Klimburg-Witjes, N., & Wentland, A. (2021). *Hacking humans? Social engineering and the construction of the “deficient user” in cybersecurity discourses*. Big Data & Society.
10. Nifakos, S., Patel, T., Athanasiou, A., & Bonn, S. E. (2021). *Influence of human factors on cyber security within healthcare organizations: A systematic review*. Healthcare, MDPI

Contents

Abstract.....	2
Chapter 1: Introduction	2
1.1 Introduction:.....	2
1.2 Theoretical Background:.....	2
1.3 Problem Statement:	3
1.4 Research Objectives:.....	4
1.5 cope of the Study	7
1.6 Significance of the Study:	8
Chapter 2: Literature Review	8
2.1 Literature Review:	9
Chapter 3: Research Methodology.....	9
3.1 Research Methodology	11
3.1.1 Research Design	11
3.1.2 Data Sources	11
3.1.3 Data Analysis Method.....	12
3.1.4 Limitations of the Study	13
3.2 Expected Study Outcomes	14
3.3.Gantt Chart.....	15
References:	17