

Course Overview: Research Methodology in computer Science

Course Code: AI800

Weighting: 20%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: June 28, 2025

Hand-in Date: July 12, 2025

Submission Method: Online via E-Learning

Assignment Report :Between Digitization and Hacking: The Digital Human Facing Cybersecurity Challenges

Bushra Ali Alharby

Table of Contents

1. Introduction to the Study
2. Summary of Research Papers
3. . Critical Analysis
4. . Connections
5. . Conflicts in Findings
6. . Synthesis Matrix
7. . References

Introduction to the Study

In light of the accelerated digital expansion, a human is no longer just a biological entity; they have become endowed with a parallel existence known as the 'digital human' – one that breathes through its data, moves through its platforms, and is defined by its digital fingerprints in cyberspace. While digitization has promised an era of greater efficiency and connectivity, it has also opened wide doors to breaches that do not only affect systems, but also impact the human entity itself: its privacy, psychological security, and digital identity.

This study aims to provide a literary analytical reading of the cybersecurity scene through a new lens: the human at the heart of the digital battle, not merely as an ordinary user or a number in a database, but as a vulnerable entity, exposed to targeting, manipulation, and surveillance. The study is based on a central hypothesis that cyber intrusions are no longer confined to devices, but have become directed at human consciousness itself, through tools such as social engineering, smart phishing, and exploiting weak digital awareness. While many previous studies have addressed the technical aspects of cybersecurity, this study focuses on the neglected human dimension: how does the digital human live under a constant threat? How does digital surveillance affect their freedom? And what is the psychological cost of an unseen intrusion that is felt deeply?

This introduction comes to present and discuss the relevant previous studies, which form the scientific and intellectual foundation for understanding the general context and locating this study within the research map in this field.

Summary of Research Papers:

Paper 1: Cybersecurity challenges in the era of digitalization –(2024)

In light of the profound digital transformation affecting various sectors, healthcare systems have become one of the most vulnerable environments to cyber risks. Digitization in this field not only offers advantages in efficiency and speed of access to information but also opens the door to complex security threats targeting highly sensitive information that touches on the essence of human beings and their privacy .This study aims to provide a comprehensive analysis of the cybersecurity landscape in the digital healthcare environment, highlighting the technical, organizational, and human challenges faced by healthcare institutions in this context, and suggesting strategies to mitigate these risks and enhance cyber resilience.

Paper 2: Influence of Human Factors on Cyber Security within Healthcare Organizations: A Systematic Review (2021)

The tremendous evolution in Internet of Things (IoT) technologies has made smart devices interconnected in all aspects of life: from homes and hospitals to factories and infrastructure. This expansion has brought immense benefits, but it has also been accompanied by a sharp rise in cyber threats . This study aims to analyze how artificial intelligence (AI) technologies can be used to enhance cybersecurity through predictive

threat detection, while reviewing the challenges associated with the use of AI in the IoT environment.

Paper 3 Hacking Humans? Social Engineering and the Construction of the “Deficient User” in Cybersecurity Discourses (2021)

This study addresses the relationship between social engineering and common security perceptions about users in the cybersecurity environment. The researchers highlight how the category of "user" is often presented as the weakest link in the security chain and portrayed in training discourses as a deficient, incompetent entity vulnerable to exploitation, which necessitates "fixing" through guidance and constant indoctrination.

By analyzing the content of cybersecurity lectures and awareness curricula, the study shows how the focus of security policies on "human error" reinforces a simplistic discourse that neglects the social, cultural, and organizational factors shaping individuals' behavior in the digital reality. The study calls for a rethinking of the traditional concept of the weak user by developing more holistic security models that go beyond directly blaming the individual, towards a deeper understanding of the context in which digital usage occurs, including pressures, technological gaps, and psychological and cognitive factors.

Paper 4: Digital Security in Human Security: A Case Study of the Bjorka Hacking Incident (2024)

The study highlights the rising cyber threats in higher education institutions, which have become not just a technical issue, but a national issue that requires political and strategic intervention. It shows that universities are primary targets for attacks due to the nature

of their sensitive data and the openness of their networks, which has increased their vulnerability amid digital transformation and the expansion of e-learning. The study suggests the necessity of building integrated security strategies, updating national legislation, raising security awareness, and enhancing partnerships between institutions and governments to make knowledge security a sovereign issue.

Paper 5: Enhancing Cybersecurity with Artificial Intelligence: Predictive Techniques and Challenges in the Age of IoT (2024)

This study aims to analyze how to enhance cybersecurity as a means to ensure business continuity and resilience in the face of the rapid challenges of the digital age. It indicates that organizations are facing increasing cyber threats that endanger their data, reputation, and continuity, which necessitates the development of effective strategies that not only rely on technical solutions but also encompass organizational and human dimensions. The study focuses on: - The importance of integrating cybersecurity into the strategic planning of businesses.- The necessity of continuously assessing cyber risks and updating protection policies.- Adopting flexible practices that enable organizations to respond quickly to attacks.- Developing an internal security culture through employee training and raising awareness .The study also confirms that digital transformation has created new opportunities but has increased the complexity of the cyber environment, requiring a mix of innovation and caution to ensure a balance between technological advancement and security protection.

Paper 6: Cybersecurity Threats in Healthcare IT: Challenges, Risks, and Mitigation Strategies (2024)-

This study reviews the increasing risks facing information technology systems in the healthcare sector, indicating that healthcare institutions have become primary targets for cyberattacks due to the sensitivity of medical data and the importance of service continuity. The study highlights several challenges, including:- Weak security infrastructure,- The increasing reliance on Internet-connected devices (IoT),- Lack of security awareness among medical professionals,- Difficulty in updating legacy systems. The study also analyzes the impacts of attacks, which can range from data loss, disruption of vital services to threats to patient safety. It suggests a set of mitigation strategies, including:- Adopting multi-layered security solutions,- Training staff on cybersecurity practices,- Developing incident response plans,- Enhancing collaboration between the healthcare sector and security experts. The study concludes that achieving cybersecurity in healthcare requires a combination of technology, policies, and awareness to protect patients and ensure continuity of care.

Critical Analysis

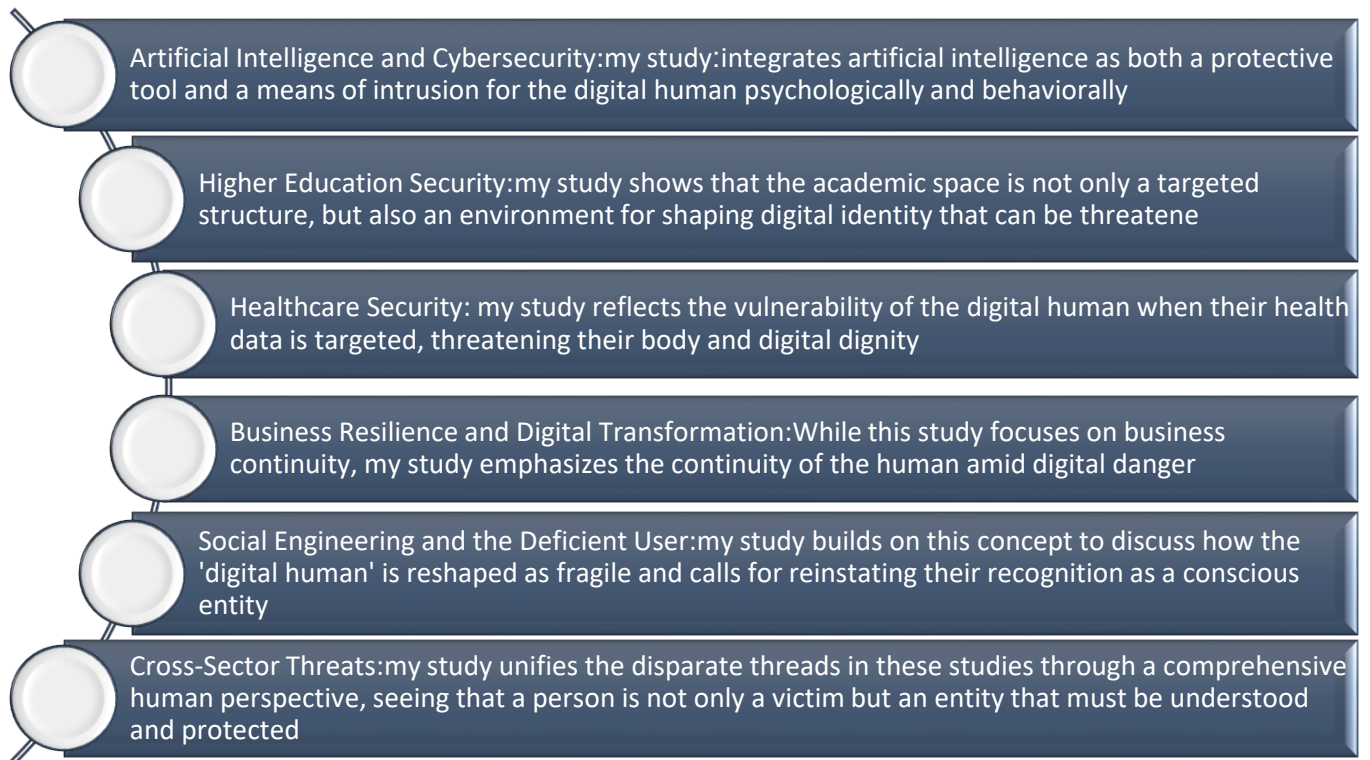
Previous studies show a remarkable diversity in addressing cybersecurity issues, covering multiple angles including: enhancing security using artificial intelligence, protecting infrastructure in higher education institutions, information technology security in the health sector, business resilience strategies, social engineering, and more. This diversity has contributed to forming a rich knowledge framework that aids in understanding the dimensions of the phenomenon. Despite this breadth, critical analysis highlights a number of gaps that underscore the importance of the current study :A tendency towards a purely technical nature: Most studies have focused on technical and organizational solutions, with a clear neglect of the deep human dimension related to

individual experiences in the face of digital threats, which makes them partial in their coverage of the concept of 'breach'. Limited attention to digital identity and self: The 'user' has often been treated as a vulnerable element or the weakest link in the security chain, without a deep analysis of the construction of their digital identity or the implications of breaches on their psychology and behavior.

Weakness of ethical and cultural handling: Studies have not adequately addressed ethical aspects, such as issues of surveillance, manipulation, and digital freedom, or the cultural and social impact of increasing cyber threats, leaving a gap in understanding the full picture. Absence of literary or philosophical approaches: The studies lack any literary reflection or philosophical critique of the digital reality, which marginalizes the experience of humans as emotional and intellectual beings living in a threatened and monitored virtual world. The need to link humans and technology as responsible and breached: Most research views technology merely as a means of protection or danger, without recognizing that the digital human is not just a victim, but also an active, interactive, and sometimes responsible agent for breaches of their own self and society, an issue that this study seeks to address.

Summary of the analysis: These observations highlight the importance of the current research that aims to approach digital human security from a literary-technical perspective, transcending the limits of traditional analysis to re-question the relationship between humans and technology, and breaches as actions that go beyond programming dimensions to touch upon consciousness and existence itself.

Connections:



Communication: My study aims to be a knowledge bridge between pure technical analysis and deep human analysis, by questioning the meaning of humanity in the age of digitization and intrusion

Conflicts in Findings:

When reviewing previous studies, several contradictions and differences in their results emerged, reflecting a variation in analytical approaches and assumptions about the nature of cybersecurity and the role of humans in it: - Contradiction in the perception of the "user": While some studies perceive the user as a vulnerability that should be controlled through training (such as studies in healthcare and education), other studies critique this simplification, such as the study on "social engineering," which reveals how a security discourse is constructed that undermines the individual instead of

empowering them. - Difference regarding the centrality of technology: Some research views artificial intelligence as the ideal savior for cybersecurity, while other studies warn against over-reliance on it due to limitations in explain ability and the risk of deception through "adversarial attacks." - Variance in the priority of protection: There are studies that focus on protecting systems and institutions (such as higher education), while ignoring the psychological or identity impact on the individual user, creating a gap between protecting infrastructure and protecting the digital self. Absence of Consensus on the Ethical Aspect: Previous studies rarely addressed the ethical and social dimensions, leading to the neglect of vital aspects such as freedom of expression, the right to privacy, and digital justice.- The Importance of Studying These Contradictions: My study aims to bridge these gaps and contradictions through a literary-analytical perspective that treats the digital human not only as a subject to be technically protected but as a free being with an entity, rights, and an existence that deserves reflection and protection from commodification and intrusion.

Synthesis Matrix

Paper	Authors & Year	Research Design	Methodology	Key Findings	Limitations
Paper 1 Cybersecurity challenges in the era of digitalization	Edgards Petersons-2024	Applied Research	Technical approach with AI models	AI enhances threat detection but raises ethical challenges	Limited human aspects or social impact

Paper 2 Influence of Human Factors on Cyber Security within Healthcare Organizations: A Systematic Review	Sokratis Nifakos and others, 2021	Case Study	Institutional case with qualitative review	Cyber threats to universities are national-level risks	Focuses mainly on policy level, not individual experience
Paper 3 Hacking Humans? Social Engineering and the Construction of the “Deficient User” in Cybersecurity Discourses	Nina Klimburg-Witjes ¹ and Alexander Wentland-2021	Thematic Analysis	Review and classification of healthcare threats	Healthcare IT systems are highly vulnerable due to outdated infrastructure	Contextual limitation, it cannot be easily generalized.
Paper 4 Digital Security in Human Security: A Case Study of the Bjorka Hacking Incident	Ingrida, N. V., & Wibowo, D. (2024)	Applied Research	Recommendations based on business cases	Integrating cybersecurity with business planning increases resilience	Overly general in strategy, lacks specific implementation
Paper 5 Enhancing Cybersecurity with Artificial Intelligence: Predictive Techniques and Challenges in the Age of IoT	Karthik Meduri and others 2024	Analytical Study	The analysis of the study is qualitative regarding the content of the training.	Users are framed as inherently flawed; training reinforces this view	Lacks concrete policy recommendations
Paper 6 Cybersecurity Threats in Healthcare IT: Challenges, Risks, and	Md Jawadur Rahim, 2024	Systematic Literature Review	Review of 40+ studies	Cybersecurity in health needs layered strategies, better awareness, and policy	Limited focus on psychological or identity dimensions

Mitigation Strategies					
-----------------------	--	--	--	--	--

Conclusion

In this digital age we live in, cyber threats are no longer just a technical issue, but have become intertwined with human daily life, identity, and sense of security. Through this study, we attempted to shed light on the digital human, not merely as a user of technology, but as a party affected by and interacting with this changing and complex reality. We found that many studies focused on systems, technologies, and policies, but did not often pause to consider the human being himself, his emotions, and his existence within this space. This is why this study came to remind us that behind every password and every network, there is a human being with a presence that must be respected and protected. Cybersecurity is not complete with algorithms alone; it needs awareness, culture, and balance that respect the human being as it protects data. This is what we strive for: to have a digital space we trust, where we feel secure as individuals, not just as accounts.

References

1. Petersons, E. (2024). Cybersecurity challenges in the era of digitalization. SSRN.

2. Nifakos, S., et al. (2021). Influence of human factors on cyber security within healthcare organizations: A systematic review. MDPI.
3. Klimburg-Witjes, N., & Wentland, A. (2021). Hacking humans? Social engineering and the construction of the “deficient user” in cybersecurity discourses. Big Data & Society.
4. Ingrida, N. V., & Wibowo, D. (2024). Digital security in human security: A case study of the Bjorka hacking incident. SSRN.
5. Meduri, K., et al. (2024). Enhancing cybersecurity with artificial intelligence: Predictive techniques and challenges in the age of IoT. Sensors, MDPI.
6. Rahim, M. J. (2024). Cybersecurity threats in healthcare IT: Challenges, risks, and mitigation strategies. SSRN.
