

Course Overview: Research Methodology in Computer Science

Course Code: AI800

Weighting: 30%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: July 13, 2025

Hand-in Date: July 19, 2025

Submission Method: Online via E-Learning

Between Digitization and Hacking: The Digital Home Facing Cybersecurity Challenges

Bushra Ali Alharby

Problem Statement:

With the rapid development of digitization and artificial intelligence, humans have transformed from mere technology users to "digital beings" living and interacting within the digital space. This transformation, despite its great promise, creates profound challenges that threaten individual security. Cyberattacks are no longer limited to the theft of personal data and information; they extend to the very essence of human identity and their sense of security and privacy.

Most previous studies have focused on the technical aspects of cybersecurity or institutional solutions, largely ignoring the direct human experience and the representation of the digital human in security discourse. Although some research, such as Petersons (2024) and Nifakos et al. (2021), has addressed both technical and human challenges, few studies have delved into understanding the role of humans as actors rather than mere victims, as Klimburg-Witjes & Wentland (2021) did, which analyzed the discourse of the "imperfect user."

Therefore, there is an urgent need for a study that explores the digital human's position in the face of ever-increasing cyber threats, and how their image and responses are constructed through security discourse and the technologies used. This research aims to fill this gap through a deeper analysis of the digital human's experience and how to address cybersecurity challenges from a holistic perspective that combines technical, social, and psychological dimensions.

Research Objectives:

To this research aims to provide an in-depth understanding of the digital human's position in the face of increasing cybersecurity challenges in the era of accelerating digitization. To achieve this primary objective, **the research seeks:**

1. To analyze the concept of the "digital human": Identify the various dimensions of human existence and interactions in the digital space, with a focus on identity, privacy, and personal data.

2. To identify the most prominent cybersecurity challenges facing the digital human: Investigate the main types of breaches and threats (such as social engineering, identity theft, digital tracking, and privacy violations) that directly target individuals.

3. To examine how the image of the "digital human" is constructed and represented in security discourse: Analyze the narratives and concepts used in security discourse (such as "imperfect user" or "human vulnerability") and how these perceptions influence individuals' understanding of their role and responsibilities in cybersecurity.

4. To evaluate the psychological and social impact of cybersecurity breaches on the digital human: Explore how cybersecurity incidents affect individuals' sense of security, trust, and well-being in their digital lives.

5.To Propose recommendations to enhance digital human protection: Based on the findings, provide guidelines and suggestions to improve security awareness, design more effective data protection policies, and develop security education methods that empower individuals rather than place blame on them.

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 essence of an individual's identity and sense of security, which impacts their privacy. This literature review aims to analyze recent

studies that have addressed the position of the digital human in the face of cybersecurity challenges, focusing on the role of human factors, the impact of attacks, and how user understanding is constructed in security discourse.

- The literature indicates that modern security systems, such as those based on artificial intelligence, are increasingly important in securing cyberspace, as demonstrated by **Meduri et al.'s (2024)** study. However, these systems often focus on purely technical solutions, neglecting the human dimension in their approach to security.
- Other studies highlight the role of human factors as a critical component of the cybersecurity equation. **Petersons (2024)** addressed the general challenges of cybersecurity in the digital age, providing a broad framework for the risks facing individuals and organizations. In a more specific context, **Nifakos et al. (2021)** The impact of human factors on cybersecurity within healthcare organizations, emphasizing the sensitivity of data and the direct impact of individuals in this sector. **Klimburg-Witjes & Wentland (2021)** offer a profound critique of how the "imperfect user" is constructed in security discourse. They analyze how human error is portrayed as a vulnerability, placing responsibility on users and shaping their understanding of their role in cybersecurity.
- To enhance understanding of the direct impact of breaches on individuals, some research presents real-life case studies. In this regard, **Ingrida & Wibowo (2024)** shed light on human security by analyzing the Bjorka hacking incident, demonstrating how cyber breaches can directly impact individuals' personal and social security. **In parallel, Rahim (2024)** focused on cyberthreats in healthcare IT, a vital sector where highly sensitive personal data is collected, making any breach deeply human, impacting the privacy and dignity of digital humans.

- This review indicates that understanding the digital human in the context of cybersecurity still needs further exploration. Existing studies, despite their importance, often focus on specific aspects (technical, institutional, or discourse analysis) without offering a holistic perspective that effectively links the human's existence as a digital entity, the threats they face, and how their protection is articulated in security discourses and practices. This calls for research that integrates these diverse dimensions to provide a more comprehensive understanding of how the digital human confronts the growing challenges of cybersecurity.

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.
