Journal of Information Systems Engineering and Management
2025, 10(9s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Phenomenological Inquiry into IT Professionals' Perspectives on AI-Powered Cybersecurity Systems for Intrusion Detection

Hondor Saragih[1*], Mukhlis Lubis[2], Andi Subhan Amir[3], Choirul Anam[4], Supendi[5]
[1]Universitas Pertahanan, Jawa Barat, Indonesia,
**Corresponding Author: hondor.saragih@idu.ac.id*
[2]Sekolah Tinggi Agama Islam Negeri Mandailing Natal
mukhlizlubiz@gmail.com
[3]Hasanuddin University
asa@unhas.ac.id
[4]Universitas Kadiri
choirulanam@unik-kediri.ac.id
[5]Universitas Linggabuana PGRI Sukabumi
doktorgurufatih@gmail.com

ARTICLE INFO

Received: 02 Nov 2024

Revised: 22 Dec 2024

Accepted: 05 Jan 2025

ABSTRACT

Cybersecurity has become a critical field in protecting digital infrastructure, with increasing reliance on AI-powered systems for intrusion detection. However, the integration of AI into cybersecurity raises concerns about trust, effectiveness, and the human role in decision-making. Despite significant advancements, there is limited understanding of how IT professionals experience and interact with AI-driven intrusion detection systems in real-world settings. This study aims to explore these experiences and identify factors influencing trust and acceptance of AI in security contexts. Using a phenomenological approach, the research delves into the subjective perspectives of IT professionals, uncovering insights into their interactions with AI systems. Through in-depth interviews and thematic analysis, the findings highlight the dual role of AI as an assistant rather than a complete replacement for human decision-making, while also revealing challenges related to false positives and the need for human oversight. These results contribute to a more nuanced understanding of human-AI collaboration in cybersecurity, emphasizing the ongoing importance of human expertise. The study's implications suggest that future research should focus on optimizing AI systems for better alignment with user trust and expectations.

Keywords: Cybersecurity, Artificial Intelligence (AI), Intrusion Detection, Professional IT Experience, Automated Security Systems, Phenomenological Analysis

Introduction

Cybersecurity has become one of the most critical issues in the digital era, as cyber threats continue to grow in sophistication and diversity (Nunes et al., 2019). Organizations worldwide face significant challenges in protecting their data and systems from attacks that can compromise integrity and user trust. In recent years, artificial intelligence (AI) technology has been widely applied to address these issues, particularly in intrusion detection and threat response (Varma et al., 2023). With its ability to process vast amounts of data and identify patterns that may be overlooked by humans, AI offers great potential in enhancing the effectiveness and efficiency of cybersecurity systems.

However, despite AI's innovative solutions, its adoption in cybersecurity remains fraught with challenges. While AI systems can quickly detect threats and even predict upcoming attacks, the reliability and trustworthiness of automated decisions made by AI continue to be debated. One of the primary challenges is the high rate of false positives—false alarms generated by the system, which can overwhelm security teams with irrelevant alerts (Skoumperdis et al., 2023). Additionally, AI has limitations in handling more complex attacks or those that do not follow easily recognizable patterns (Hussain, 2024). In this regard, IT professionals still find it necessary to conduct manual verification, highlighting the crucial interplay between human expertise and machine capabilities in cybersecurity.

Previous research has largely focused on the development and evaluation of AI technologies in cybersecurity, but little attention has been given to the subjective experiences of IT professionals who interact directly with these technologies (Jothishri et al., 2024). A deep understanding of their perceptions, the challenges they face, and the meaning they ascribe to AI-based security systems remains limited (Ogiela & Ogiela, 2024). Therefore, it is essential to explore these experiences through a phenomenological approach, which focuses on how individuals interpret and make sense of the phenomena they encounter in their social and professional contexts.

The objective of this study is to bridge this gap by exploring the experiences and perspectives of IT professionals who utilize AI-based security systems for intrusion detection (Preuveneers & Joosen, 2024). Using a phenomenological approach, this research aims to understand how IT professionals interact with these technologies, how they develop trust in such systems, and the challenges they face in leveraging AI as a tool for threat detection (Cheng et al., 2020). This study seeks to provide deeper insights into the dynamics between humans and technology in an environment that increasingly relies on automation and artificial intelligence.

Research on the experiences of IT professionals in using AI-based security systems has become an increasingly important field in cybersecurity studies and human-computer interaction (Kumar & Pande, 2021). As reliance on automated systems grows, understanding how individuals adapt to, trust, and manage these technologies becomes crucial. Previous studies have extensively discussed the technical effectiveness of AI in intrusion detection, such as the speed of analysis and system accuracy (Pasha et al., 2022). However, research specifically highlighting how users experience, understand, and respond to AI systems in their work context remains limited.

One of the main challenges in exploring these subjective experiences lies in the dominant methodological approach used in cybersecurity research (Mohamed, 2023). Many previous studies have adopted a quantitative approach, measuring system performance through metrics such as detection rates, false positive rates, and response times. While this approach provides valuable insights into AI performance, it falls short in capturing the human experience dimension of using these technologies (Khilenko et al., 2023). For example, how IT professionals build trust in AI, how they handle system-generated alerts, and how they adjust their workflows to accommodate AI's limitations are aspects that are difficult to quantify numerically.

The limitations of quantitative approaches in understanding these subjective dimensions highlight the need for more exploratory and experience-based methods. Qualitative studies in the fields of human-computer interaction (HCI) and technology trust have shown that factors such as system transparency, AI result interpretability, and individual professional experience significantly contribute to the acceptance and effectiveness of automated technologies (Gafni & Levy, 2024). However, most of these studies remain at a conceptual level or rely on surveys with limited responses, failing to provide an in-depth exploration of how user experiences evolve in real workplace settings.

Therefore, this study adopts a phenomenological approach to bridge this methodological gap by exploring how IT professionals experience, understand, and interpret AI's role in cybersecurity (Alzahrani, 2023). By focusing on participants' direct experiences and subjective reflections, this approach enables a richer understanding of how AI influences decision-making, trust, and work dynamics within cybersecurity systems.

While many practical solutions have been implemented to address challenges in AI-based intrusion detection, existing approaches often focus on measuring system performance, such as detection accuracy or the number of false positives (Eze & Shamir, 2024). These studies provide useful technical insights, but they fail to explore the subjective experiences of IT professionals who interact directly with these systems. One commonly used practical solution is the full automation of threat detection systems, allowing AI to make decisions with minimal human intervention (Alneyadi & Normalini, 2025). While this enhances efficiency in certain aspects, this approach often overlooks how automated decisions affect users' trust, comfort, and emotional responses to the system.

However, this quantitative approach has limitations in capturing deeper experiential dimensions, such as how IT professionals understand, evaluate, and adapt to AI-driven decisions. These limitations result in a more superficial and less holistic understanding of human-AI interactions in the cybersecurity context. For example, while AI systems can generate alerts rapidly, how an IT professional perceives and interprets these alerts in their work context—

whether they feel comfortable trusting AI's decisions or prefer human intervention—is an aspect that remains largely unaddressed in technical studies.

To bridge this gap, a phenomenological approach offers a more in-depth alternative. By focusing on subjective experiences and the meanings individuals ascribe to these phenomena, phenomenology enables a more holistic and profound understanding of how IT professionals interact with AI-based intrusion detection systems. This approach provides space to explore users' emotions, trust, and challenges in real-world situations. Therefore, it is crucial to directly investigate the experiences of IT professionals to gain a more comprehensive insight into the essence of AI utilization in threat detection—an area that remains underexplored in the existing literature.

Previous research has extensively explored the implementation of AI-based intrusion detection systems in cybersecurity, primarily focusing on the technical effectiveness and operational efficiency of these systems. Many studies have examined quantitative outcomes, such as detection accuracy rates or the number of false positives, yet they have paid less attention to the subjective experiences of IT professionals who use these systems in their daily work. Studies in the fields of human-computer interaction (HCI) and trust in technology have also provided insights into how users develop trust in automated systems. However, few have delved into how the personal experiences and deep perceptions of IT professionals influence their decision-making in AI-driven scenarios. Thus, this study aims to fill this gap by focusing on understanding users' subjective experiences with AI in intrusion detection.

The phenomenological method was chosen to address this research gap, as this approach allows for an in-depth exploration of the experiences and meanings derived by individuals who interact with technology. Phenomenology focuses on understanding how individuals experience and assign meaning to specific phenomena—in this case, the use of AI-based systems in cybersecurity. Through in-depth interviews and thematic analysis, this study seeks to understand IT professionals' emotions, trust, and challenges, as well as how they interpret alerts or decisions generated by AI. Consequently, phenomenology provides a more suitable approach to answering questions related to subjective experiences and meanings that are often overlooked in quantitative research.

This article is structured into several key sections to systematically present the findings. It begins with an introduction discussing the background and significance of this research, followed by a more detailed examination of the phenomenon under study—the interaction between IT professionals and AI systems in cybersecurity. Next, the methodological approach of phenomenology is explained, including data collection and analysis processes aimed at uncovering participants' subjective experiences. The research findings are then presented in the form of key themes identified from interviews and observations, concluding with a discussion and summary of the study's contributions to understanding human-AI collaboration in cybersecurity.

Method

Study Design

This study employs a phenomenological approach to explore the experiences of IT professionals in using AI-based security systems for intrusion detection. This approach was chosen because it focuses on gaining a deep understanding of participants' subjective experiences when interacting with increasingly automated technologies in the cybersecurity context.

In this study, interpretative phenomenology is used to uncover the deeper meanings behind participants' experiences, including their perceptions, challenges, and reflections on AI systems. This approach allows for an exploration of how IT professionals develop understanding and trust in AI technology for threat detection, as well as how they navigate the challenges arising from the implementation of such systems. By examining these experiences, this study provides broader insights into the human-AI interaction within the realm of cybersecurity.

Participants

The participants in this study are IT professionals with direct experience using AI-based security systems for intrusion detection. A purposive sampling approach was employed to ensure that participants have relevant engagement with the studied phenomenon.

The inclusion criteria for this study are as follows:

- A minimum of three years of experience in the field of cybersecurity.
- Active involvement in the use or management of AI-based intrusion detection systems in their workplace.
- Holding roles such as security analyst, security engineer, or IT security manager in industries or institutions that implement AI-driven security systems.

A total of 10 to 15 participants were included in the study. Participants' identities were kept confidential to protect their privacy and to ensure compliance with ethical research standards.

Data Collection

Data for this study were collected through semi-structured interviews, conducted either in person or online, depending on participants' preferences and availability. The interviews followed an open-ended question guide designed to explore participants' experiences, challenges, and perceptions regarding AI-based security systems.

Each interview lasted between 45 to 60 minutes, allowing for in-depth exploration while minimizing participant burden. A comfortable and distraction-free environment was ensured during the interviews to encourage participants to share their experiences openly. All interviews were audio-recorded with participants' consent and later transcribed verbatim for analysis.

In addition to interviews, direct observations were conducted to monitor participants in real workplace settings as they interacted with AI-based intrusion detection systems. These observations provided additional insights into the interaction patterns between IT professionals and AI systems in real-world cybersecurity operations.

Data Analysis

Data were analyzed using a phenomenological thematic analysis method to identify patterns and key themes within participants' experiences. The analysis process followed several stages:

1. Transcription and In-Depth Reading – Each interview was transcribed verbatim and repeatedly reviewed to grasp the essence of participants' experiences.
2. Initial Coding – Segments of data reflecting significant experiences and meanings were open-coded to capture key insights.
3. Theme Identification – Codes with similarities or interconnections were categorized into major themes that encapsulate the deeper meanings of the studied phenomenon.
4. Theme Structuring and Interpretation – Identified themes were further analyzed within the context of IT professionals' experiences, linking them to theoretical frameworks on technology trust and human-computer interaction.

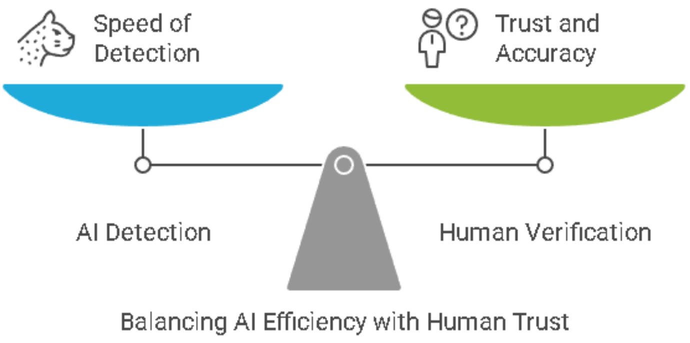
The analysis was conducted using qualitative data analysis (QDA) software, such as NVivo, to facilitate systematic data organization and categorization. This approach ensured a structured and rigorous examination of participants' subjective experiences.

Results

This study explores the experiences of IT professionals in using AI-based security systems for intrusion detection. Through in-depth interviews and observations, several key themes emerged, reflecting their perceptions, challenges, and interactions with this technology.

Trust in AI for Cybersecurity: Between Convenience and Skepticism

Most participants acknowledged that AI has a significant advantage in detecting anomalies faster than humans. However, trust in AI-generated automated decisions remains a dilemma. Some IT professionals stated that while AI can provide early warnings, they still feel the need to conduct manual verification before making final decisions.



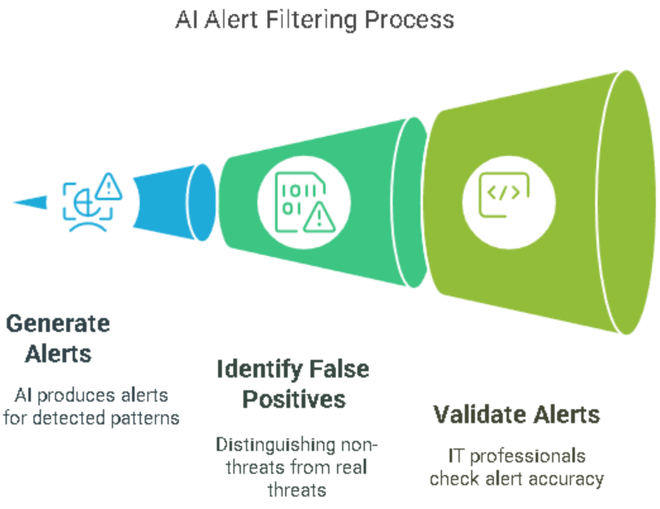
One participant expressed:

"AI is often able to detect suspicious activities that I might have missed. However, I can't fully trust the system because there have been instances where its decisions seemed unreasonable or lacked clear context."

This experience highlights that AI is perceived as an assistive tool that enhances threat detection efficiency but cannot fully replace human analysis. The trust IT professionals place in AI systems appears to depend on how transparent and interpretable the system's decisions are.

Challenges of False Positives and False Negatives: Increased Workload for IT Professionals

One of the primary challenges highlighted by participants is the high rate of false positives generated by AI systems. AI often detects patterns that do not actually represent real threats, leading to excessive alerts. As a result, IT professionals must filter and validate each alert, ultimately adding to their workload.


AI Alert Filtering Process
Generate Alerts
AI produces alerts for detected patterns
Identify False Positives
Distinguishing non-threats from real threats
Validate Alerts
IT professionals check alert accuracy

A security analyst shared:

"Every day, I receive hundreds of notifications from AI about potential attacks. Unfortunately, many of them are just false alarms that do not actually pose a threat. This makes my team and me more selective, and at times, we even ignore some alerts that might be important."

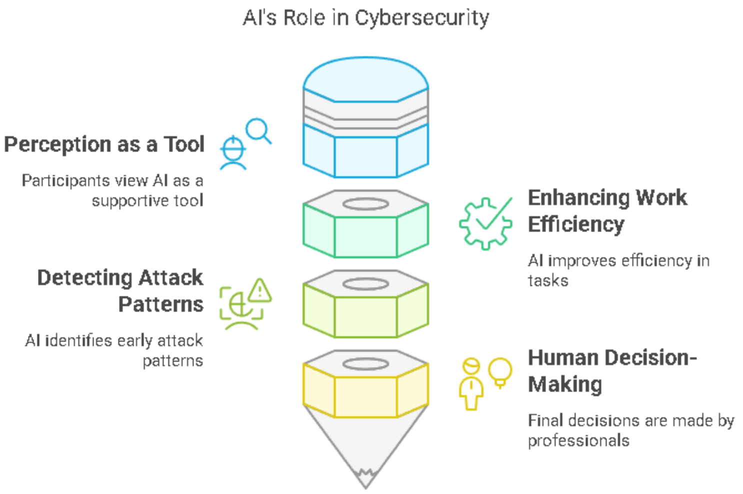
On the other hand, false negatives, or the AI's failure to detect actual attacks, also remain a concern. One participant pointed out that sophisticated attacks, such as Advanced Persistent Threats (APT), often go undetected because AI operates primarily based on predefined attack patterns.

"I once encountered a case where AI failed to detect an ongoing attack because the attack pattern did not match AI's dataset. This is very concerning because it means we still have to rely on human oversight."

These findings indicate that while AI can enhance threat detection efficiency, its limitations necessitate human intervention to ensure the system operates optimally.

Human-AI Collaboration: AI as an Assistant, not a Replacement

Most participants perceive AI as a supporting tool that enhances their work efficiency rather than a system capable of completely replacing human roles in cybersecurity. AI is considered more suitable for detecting early attack patterns, while the final decision-making remains in the hands of IT professionals.


AI's Role in Cybersecurity
Perception as a Tool
Participants view AI as a supportive tool
Enhancing Work Efficiency
AI improves efficiency in tasks
Detecting Attack Patterns
AI identifies early attack patterns
Human Decision-Making
Final decisions are made by professionals

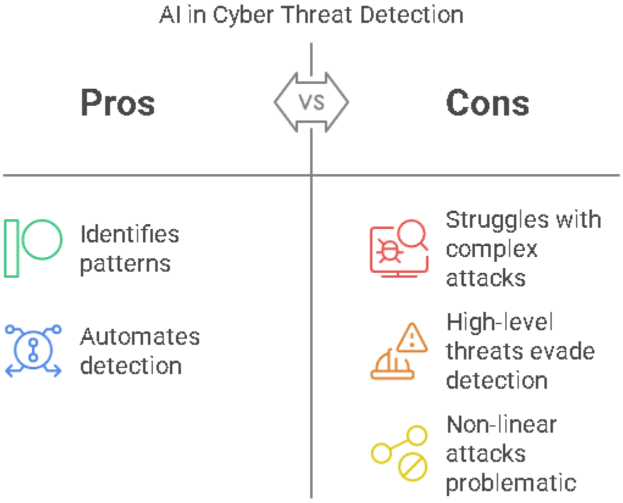
An IT security manager stated:

"AI is great for filtering information and providing initial data, but I would never fully delegate security decisions to a machine. I need to understand the reasoning behind AI alerts before taking action."

This experience reinforces the idea that while AI provides significant benefits in automating threat detection, its effectiveness in cybersecurity systems still heavily relies on human expertise for data interpretation and validation.

AI Limitations in Handling Complex Attacks: Unforeseen Threats

Several participants revealed that AI still struggles with understanding complex and dynamically evolving attack patterns. Non-linear attacks or those carried out by high-level threat actors often evade AI detection because they do not follow easily identifiable patterns.


AI in Cyber Threat Detection
Pros
VS
Cons
Identifies patterns
Automates detection
Struggles with complex attacks
High-level threats evade detection
Non-linear attacks problematic

A security engineer shared their experience:

"We once encountered an attack that was carried out gradually over a long period. AI didn't recognize this activity as a threat because it was executed very carefully and slowly. If we had relied solely on AI without manual investigation, we might have lost highly valuable data."

This finding indicates that while AI is effective in identifying known threats, it still has limitations in anticipating sophisticated attacks that lack clear patterns. Thus, human expertise remains essential in cybersecurity to address unpredictable and advanced threats.

The findings of this study reveal that while AI holds significant potential in cybersecurity, there are still major challenges in its implementation, particularly regarding user trust, false positive rates, and AI's limitations in handling complex threats. IT professionals generally perceive AI as a support tool that enhances efficiency, rather than a system capable of fully replacing human roles in cybersecurity.

The experiences shared by participants highlight the importance of human-AI collaboration in cybersecurity systems. Final decision-making still requires human intervention, especially in cases where AI fails to grasp the broader context of a threat. Therefore, the design of AI-based security systems should prioritize transparency, reliability, and human interaction to ensure greater acceptance and trust among IT professionals.

Discussion

This study reveals that while AI-based intrusion detection systems have great potential to enhance efficiency in cybersecurity, the experiences of IT professionals who interact directly with this technology are more complex and nuanced (Ali & Shah, 2024). The key findings indicate that although IT professionals acknowledge AI's ability to detect threats quickly, they still experience uncertainty and a tendency to verify the system's outputs (Lysenko et al., 2024). This reflects a tension between trust in technology and the need to maintain human control over security decision-making.

These findings directly address the research question posed in the introduction: How do IT professionals experience using AI-based systems for intrusion detection? The study demonstrates that while IT professionals rely on AI for initial threat detection, they still feel the need to perform manual verification and intervene in AI-driven decision-making when faced with uncertainty or false positives (Smmarwar et al., 2023). This highlights that although AI-based systems can accelerate threat identification, trust and reliability remain significant challenges in the full adoption of automation (Kelly et al., 2023). These experiences reinforce the notion that AI, while beneficial, cannot entirely replace human roles in scenarios requiring more complex situational judgment.

In the context of existing literature, these findings align with human-computer interaction (HCI) theories, which suggest that regardless of technological advancements, human factors continue to play a crucial role in their utilization. Previous studies on trust in technology also support this research, indicating that while users tend to trust technology for certain tasks, they remain skeptical when decisions are fully automated. Furthermore, these findings expand the literature on human-AI collaboration in cybersecurity, where prior research has predominantly focused on AI system performance, while this study highlights the subjective experiences of those involved in these systems (Dehghantanha et al., 2024). Therefore, this study makes a significant contribution to the understanding of how IT professionals build and maintain their relationship with advanced technology in daily cybersecurity practice (Mahalle et al., 2024).

The findings of this research provide significant insights from both theoretical and practical perspectives. Scientifically, this study deepens our understanding of the relationship between humans and technology in the context of cybersecurity, where IT professionals continue to play a significant role despite the presence of automation. The practical implication is that developers of AI-based security systems need to consider user trust and reliance on human supervision in system design (Kaushik, 2022). These findings emphasize the necessity of designing interfaces and workflows that support human-AI collaboration, allowing IT professionals to verify and interact with the system flexibly. More broadly, these results are also relevant for organizations integrating AI technology into their security frameworks, as it is crucial to understand that while technology can accelerate processes, human involvement in decision-making remains indispensable (Kim & Park, 2020). From social and professional perspectives, these findings indicate that although AI technology in cybersecurity is rapidly advancing, there is a need to establish a relationship of mutual trust between humans and machines, which will enhance the effectiveness and success of such systems.

Although this research provides valuable insights into IT professionals' experiences with AI-based intrusion detection systems, several limitations should be acknowledged (Buhas et al., 2024). One of these is the relatively small number of participants (10–15 individuals), which may affect the generalizability of the findings to a broader population. Additionally, the participants in this study come from specific industry sectors that utilize AI for network security, meaning their experiences may not fully represent IT professionals outside this context. Moreover, this study's focus on subjective experiences may not comprehensively capture the technical or managerial challenges associated with implementing AI-based security systems (Cau & Spano, 2024). Therefore, the findings of this research are primarily descriptive and exploratory, and further studies with larger and more diverse samples are needed to confirm or expand upon these findings.

This study opens avenues for further research into understanding the subjective dimensions of human-AI collaboration in other professional contexts, such as the healthcare or financial industries, where AI-based systems are also increasingly adopted (Al Humaid Alneyadi & Normalini, 2023). Future studies could explore the dynamics of human-machine relationships in more complex situations, including how cultural or organizational factors influence the acceptance and trust of technology. Additionally, further investigations could examine the impact of training or prior experience on IT professionals' perceptions of AI-based security systems (Alalwan, 2022). The long-term contribution of this research is to inform the design of more inclusive and collaborative technology, optimizing the synergy between human capabilities and machine intelligence in addressing the evolving threats in cybersecurity.

Conclusion

This study explored the experiences of IT professionals with AI-powered cybersecurity systems for intrusion detection, addressing the need for deeper insights into human-AI collaboration in the cybersecurity field. The findings revealed that while AI systems are viewed as effective tools for detecting anomalies, professionals still maintain skepticism about fully trusting automated decisions, especially in complex or unforeseen situations. Additionally, challenges such as false positives and the need for human oversight were identified as key factors affecting the acceptance and effectiveness of these systems. These insights contribute to a more nuanced understanding of how professionals engage with AI in security contexts and highlight the ongoing role of human expertise in cybersecurity. Future research could further investigate how organizational factors or training programs influence the acceptance of AI systems, or explore how different sectors adapt to the integration of AI in their security frameworks. Ultimately, this study paves the way for refining the design of AI-driven security systems that foster a balanced collaboration between humans and machines.

Conflict of Interest Statement

The authors declare no conflicts of interest regarding this study.

References

[1] Al Humaid Alneyadi, M. R. M., & Normalini, M. K. (2023). FACTORS INFLUENCING USER'S INTENTION TO ADOPT AI-BASED CYBERSECURITY SYSTEMS IN THE UAE. *Interdisciplinary Journal of Information, Knowledge, and Management*, *18*, 459–486. Scopus. https://doi.org/10.28945/5166

[2] Alalwan, J. A. A. (2022). Roles and Challenges of AI-Based Cybersecurity: A Case Study. *Jordan Journal of Business Administration*, *18*(3), 437–456. Scopus. https://doi.org/10.35516/jjba.v18i3.196

[3] Ali, A., & Shah, M. (2024). What Hinders Adoption of Artificial Intelligence for Cybersecurity in the Banking Sector. *Information (Switzerland)*, *15*(12). Scopus. https://doi.org/10.3390/info15120760

[4] Alneyadi, M. R. M. A. H., & Normalini, Md. K. (2025). INTELLIGENT PROTECTION: A STUDY OF THE KEY DRIVERS OF INTENTION TO ADOPT ARTIFICIAL INTELLIGENCE (AI) CYBERSECURITY SYSTEMS IN THE UAE. *Interdisciplinary Journal of Information, Knowledge, and Management*, *20*. Scopus. https://doi.org/10.28945/5430

[5] Alzahrani, A. A. (2023). Using Artificial Intelligence and Cybersecurity in Medical and Healthcare Applications. *Information Sciences Letters*, *12*(3), 1579–1590. Scopus. https://doi.org/10.18576/isl/120343

[6] Buhas, V., Ponomarenko, I., Buhas, N., & Hulak, H. (2024). *Cybersecurity Role in AI-Powered Digital Marketing* (Proshkin V., Vakaliuk T., Osadchyi V., & Osadcha K., Eds.; Vol. 3665, pp. 1–11). CEUR-WS; Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85191413962&partnerID=40&md5=05572d83fc85d067213be19d922971d0

[7] Cau, F. M., & Spano, L. D. (2024). *Mitigating Human Errors and Cognitive Bias for Human-AI Synergy in Cybersecurity* (Breve B., D. of C. S. University of Salerno Via Giovanni Paolo II, 132, Fisciano, Desolda G., D. of C. S. University of Bari "Aldo Moro" Via Orabona, 4, Bari, Deufemia V., D. of C. S. University of Salerno Via Giovanni Paolo II, 132, Fisciano, Spano L.D., & D. of M. and C. S. University of Cagliari Via Ospedale, 72, Cagliari, Eds.; Vol. 3713, pp. 1–8). CEUR-WS; Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85198713587&partnerID=40&md5=2f4ab94d4d9e44c72f178e607f792cef

[8] Cheng, K. S., Pan, R., Pan, H., Li, B., Meena, S. S., Xing, H., Ng, Y. J., Qin, K., Liao, X., Kosgei, B. K., Wang, Z., & Han, R. P. S. (2020). ALICE: a hybrid AI paradigm with enhanced connectivity and cybersecurity for a serendipitous encounter with circulating hybrid cells. *Theranostics*, *10*(24), 11026–11048. Scopus. https://doi.org/10.7150/thno.44053

[9] Dehghantanha, A., Yazdinejad, A., & Parizi, R. M. (2024). *Autonomous Cybersecurity: Evolving Challenges, Emerging Opportunities, and Future Research Trajectories*. 1–10. Scopus. https://doi.org/10.1145/3689933.3690832

[10] Eze, C. S., & Shamir, L. (2024). Analysis and Prevention of AI-Based Phishing Email Attacks. *Electronics (Switzerland)*, *13*(10). Scopus. https://doi.org/10.3390/electronics13101839

[11] Gafni, R., & Levy, Y. (2024). The role of artificial intelligence (AI) in improving technical and managerial cybersecurity tasks' efficiency. *Information and Computer Security*, *32*(5), 711–728. Scopus. https://doi.org/10.1108/ICS-04-2024-0102

[12] Hussain, M. J. (2024). *A Survey Based on Behavior Analysis of Artificial Intelligence Using Machine Learning Process*. 1694–1701. Scopus. https://doi.org/10.1109/ICSES63445.2024.10763264

[13] Jothishri, S., Upender, T., Ravikumar, R. J., Sailaja, Y., Yuvabharathi, E., & Agnestreesa, J. (2024). *AI Cyber Security: Enhancing Network Security with Deep Learning for Real-Time Threat Detection and Performance Evaluation*. 2024 3rd International Conference for Advancement in Technology, ICONAT 2024. Scopus. https://doi.org/10.1109/ICONAT61936.2024.10774912

[14] Kaushik, K. (2022). Blockchain Enabled Artificial Intelligence for Cybersecurity Systems. In *Studies in Big Data* (Vol. 111, pp. 165–179). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-031-05752-6_11

[15] Kelly, B. S., Quinn, C., Belton, N., Lawlor, A., Killeen, R. P., & Burrell, J. (2023). Cybersecurity considerations for radiology departments involved with artificial intelligence. *European Radiology*, *33*(12), 8833–8841. Scopus. https://doi.org/10.1007/s00330-023-09860-1

[16] Khilenko, V., Akhmetov, B., Berdibayev, R., Lakhno, V., Harchenko, Y., Hwang, W.-L., & Khylenko, V. (2023). Increasing the Speed of Banking Cybersecurity Systems Based on Intelligent Data Analysis and Artificial Intelligence Algorithms for Predicting Cyberattacks. I. *Cybernetics and Systems Analysis*, *59*(4), 519–525. Scopus. https://doi.org/10.1007/s10559-023-00587-x

[17] Kim, J., & Park, N. (2020). Blockchain-based data-preserving AI learning environment model for AI cybersecurity systems in IoT service environments. *Applied Sciences (Switzerland)*, *10*(14). Scopus. https://doi.org/10.3390/app10144718

[18] Kumar, K., & Pande, B. P. (2021). Applications of Machine Learning Techniques in the Realm of Cybersecurity. In *Cyber Security and Digital Forensics* (pp. 295–316). wiley; Scopus. https://doi.org/10.1002/9781119795667.ch13

[19] Lysenko, S., Bobro, N., Korsunova, K., Vasylchyshyn, O., & Tatarchenko, Y. (2024). The Role of Artificial Intelligence in Cybersecurity: Automation of Protection and Detection of Threats. *Economic Affairs (New Delhi)*, *69*, 43–51. Scopus. https://doi.org/10.46852/0424-2513.1.2024.6

[20] Mahalle, A. V., Waghmare, V. N., Dhore, A., Raut, R. M., Barbudhe, V. K., Zanjat, S. N., & Gaidhani, V. A. (2024). Machine learning algorithms for data-driven intelligent systems. In *Data-Driven Systems and Intelligent Applications* (pp. 52–61). CRC Press; Scopus. https://doi.org/10.1201/9781003388449-4

[21] Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering*, *10*(2). Scopus. https://doi.org/10.1080/23311916.2023.2272358

[22] Nunes, R. C., Colomé, M., Barcelos, F. A., Garbin, M., Paulus, G. B., & Silva, L. A. D. L. (2019). A Case-Based Reasoning Approach for the Cybersecurity Incident Recording and Resolution. *International Journal of Software Engineering and Knowledge Engineering*, *29*(11–12), 1607–1627. Scopus. https://doi.org/10.1142/S021819401940014X

[23] Ogiela, M. R., & Ogiela, L. (2024). AI-Based Cybersecurity Systems. In *Lecture Notes on Data Engineering and Communications Technologies* (Vol. 202, pp. 166–173). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-031-57916-5_15

[24] Pasha, S. A., Ali, S., & Jeljeli, R. (2022). Artificial Intelligence Implementation to Counteract Cybercrimes Against Children in Pakistan. *Human Arenas*. Scopus. https://doi.org/10.1007/s42087-022-00312-8

[25] Preuveneers, D., & Joosen, W. (2024). An Ontology-Based Cybersecurity Framework for AI-Enabled Systems and Applications. *Future Internet*, *16*(3). Scopus. https://doi.org/10.3390/fi16030069

[26] Skoumperdis, M., Vakakis, N., Diamantaki, M., Medentzidis, C.-R., Karanassos, D., Ioannidis, D., & Tzovaras, D. (2023). A Novel Self-learning Cybersecurity System for Smart Grids. In *Power Systems* (pp. 337–362). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-031-20360-2_14

[27] Smmarwar, S. K., Gupta, G. P., & Kumar, S. (2023). *XAI-AMD-DL: An Explainable AI Approach for Android Malware Detection System Using Deep Learning* (Tomar G.S. & Bansal J., Eds.; pp. 423–428). Institute of Electrical and Electronics Engineers Inc.; Scopus. https://doi.org/10.1109/AIC57670.2023.10263974

[28] Varma, A. J., Taleb, N., Said, R. A., Ghazal, T. M., Ahmad, M., Alzoubi, H. M., & Alshurideh, M. (2023). A Roadmap for SMEs to Adopt an AI Based Cyber Threat Intelligence. In *Studies in Computational Intelligence* (Vol. 1056, pp. 1903–1926). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-031-12382-5_105