Volume XXII, Issue (1) (2026) 172-182

International May Conference on Strategic Management

DOI: 10.5937/IMCSM26172S *Research Article*

THE CYBERSECURITY FUNDAMENTALS OF ARTIFICIAL INTELLIGENCE

Zsolt Szabó Mihály*

Doctoral School on Safety and Security Sciences, Óbuda University, Hungary

Abstract: One of the defining characteristics of the 21st century digital society is the increased reliance on information systems. The daily operations of government institutions, financial organizations, healthcare systems, industrial infrastructures and private users depend to a large extent on the reliability of network and IT systems. In parallel, the volume, complexity and effectiveness of cyber threats are increasing exponentially. Traditional cybersecurity solutions are increasingly unable to effectively manage this rapidly changing and adaptive threat environment.

The rapid development of the digital world has brought new opportunities and challenges. Artificial intelligence (AI) is no longer just a futuristic idea: today it is widely used in everything from automation to data processing to decision support. At the same time, it has also brought about a fundamental transformation in the field of cybersecurity, as AI has become both a supporting and a threatening actor. The aim of this study is to provide a detailed and clear picture of the relationship between artificial intelligence and cybersecurity: basic concepts, technologies, vulnerabilities, defense strategies and future directions.

The aim of this paper is to present the cybersecurity fundamentals of artificial intelligence in a comprehensive and in-depth manner. The paper discusses in detail the technological background of AI, cybersecurity application areas, vulnerabilities of AI-based systems, and possible defense and regulatory strategies. The paper approaches the topic not only from a technical perspective, but also addresses ethical, legal, and social aspects, emphasizing the importance of responsible and secure AI use in the modern digital environment.

Keywords: artificial intelligence (AI), cybersecurity, critical infrastructures, vulnerabilities, risks, defense strategies

* *Corresponding author: szabo.zsoltmihaly@uni-obuda.hu*

Zsolt Mihály Szabó, ORCID: 0000-0001-8407-2180

1. INTRODUCTION

The digitalization and automation have significantly expanded the attack surface of IT systems. Cloud-based infrastructures, mobile communications, Internet of Things (IoT) devices, and industrial control systems (ICS/SCADA) are all offering new entry points for malicious actors. Attacks are no longer isolated incidents, but are often long-term, sophisticated operations carried out by well-organized groups or even state-backed actors. These attacks are often classified as Advanced Persistent Threat (APT), which aim not only to cause immediate damage, but also to obtain information over the long term and to covertly control infrastructures. It is important to emphasize that the use of artificial intelligence (AI) alone is not a universal solution to all security problems (Aditya et al., 2025).

The operation of AI systems depends largely on the quality of the data, the reliability of the learning process, and appropriate supervision. In the case of incorrect, distorted or manipulated data, AI-based decisions can carry serious security risks. In addition, the opacity of complex models also raises legal, ethical and compliance issues, especially in environments where automated decisions have a significant impact on people or organizations (Bányász et al., 2024).

The aim of this paper is to present the cybersecurity fundamentals of AI in a comprehensive and in-depth manner. The paper discusses in detail the technological background of AI, cybersecurity application areas, vulnerabilities of AI-based systems, and possible defense and regulatory strategies. The paper approaches the topic not only from a technical perspective, but also covers ethical, legal and social aspects, emphasizing the importance of responsible and safe use of AI in the modern digital environment.

2. FUNDAMENTALS OF AI IN CYBERSECURITY

The AI systems have now appeared in almost all areas of the digital economy (critical infrastructures, healthcare, finance, public services). The intersection of AI and cybersecurity is particularly important because reliability, security and resilience directly affect public trust and regulatory compliance.

The classic approaches to cybersecurity – such as signature-based antivirus protection, static firewall rules and predefined intrusion detection systems – are fundamentally reactive. These solutions are typically only able to recognize known attack patterns and have limited effectiveness against new, unknown or modified attacks. However, modern threats change dynamically, adapt to defense mechanisms and are often executed using automated tools, which further reduces the effectiveness of traditional methods (Anni et al., 2024).

This is where the application of AI in cybersecurity becomes crucial. AI offers a methodological and technological toolkit that is capable of processing large amounts of data, recognizing complex patterns and making adaptive decisions. Machine learning and deep learning enable security systems to not only operate based on predefined rules, but also to continuously improve their own protection capabilities by learning from observed data.

The application of AI in cybersecurity represents a paradigm shift: defenses are moving from reactive to proactive and predictive. AI-based systems are able to identify anomalies before they develop into specific attacks and predict the likelihood of certain threats. This is especially important in environments where response time is critical, such as financial transactions, critical infrastructures or healthcare systems. At the same time, AI not only strengthens defenses, but also creates new attack possibilities. Attackers themselves are increasingly using AI-based tools, such as automated vulnerability scanning, personalized

phishing campaigns or deepfake technologies. As a result, the emerging "arms race" in cybersecurity is increasingly shifting towards a battle between intelligent systems.

The globalized digital infrastructure – cloud services, IoT devices, mobile communications and industrial automation – has dramatically increased the attack surface. Traditional cybersecurity solutions (rules-based firewalls, signature-based antivirus) are increasingly unable to keep up:

- unknown (zero-day) attacks,
- automated attack tools,
- and adaptive targeted (APT) threats.

The use of AI has become not just a matter of efficiency, but a strategic necessity in cybersecurity.

3. THE CLASSIC MODEL OF CYBERSECURITY SYSTEMS AND AI INTEGRATION

The cybersecurity systems are traditionally designed based on well-defined, layered defense principles aimed at protecting IT infrastructures against various types of threats (Szabó, 2023). These classic models have served the security needs of organizations effectively for a long time, but they are increasingly limited by the increasing complexity of the digital environment and the dynamic nature of threats. The integration of AI in this area does not replace traditional security principles, but rather complements and enhances them.

3.1. Basic principles of the classical cybersecurity model

One of the cornerstones of traditional cybersecurity architectures is the Defense-in-Depth principle (see Table 1), which states that a system should be equipped with multiple, independent layers of protection (Chaudhary et al., 2020). The goal of this approach is to ensure that bypassing a single protection mechanism does not compromise the entire system. The layers of the classic model typically include: perimeter protection (firewalls), network protection (IDS/IPS), endpoint protection (antivirus), application security, and user access management.

Table 1. Defense-in-Depth with AI

Layer	Classic IT security solution	AI-based expansion
Perimeter	Firewall	Anomaly detection ML
Network	IDS/IPS	Behavioral analysis
Endpoint	Antivirus	Predictive malware analysis
User	Password	Biometric + behavioral AI

Traditional systems predominantly use rule- and signature-based solutions. These mechanisms are able to identify threats based on predefined patterns and known attack signatures. While this approach is effective against known attacks, it has a significant drawback in that it is limited in its response to new, modified, or unknown attack forms. Modern threats are often built to exploit these limitations.

The perimeter protection solutions, such as network firewalls, are primarily designed to control inbound and outbound traffic. They use static or semi-dynamic rules to decide whether to allow or deny traffic. Network intrusion detection and prevention systems (IDS/IPS) can detect suspicious patterns, but their decisions are heavily dependent on predefined rule sets

(Karen & Peter, 2010). Endpoint protection systems are designed to protect individual workstations and servers. They traditionally operate based on virus definitions and heuristic rules. Application security and access management typically use role-based authorization management, which relies on static rules and pays little attention to contextual factors such as the user's current behavior or environment.

The main limitation of traditional cybersecurity systems is that they are reactive in nature. They can only act effectively when an attack already shows a recognizable pattern. New types of zero-day attacks and adaptive long-term penetration tests (APTs) often go unnoticed by classic tools. In addition, the huge amount of log and event data generated in modern IT environments is practically impossible to manually analyze, which further increases the workload of security analysts.

3.2. Principles of AI integration

The integration of AI fundamentally changes the way the classic cybersecurity model works. AI-based solutions are able to process large amounts of data in real time, recognize relationships and learn patterns. AI is not just another layer of protection, but a comprehensive, horizontal capability that supports the entire security architecture.

The AI enables behavior-based detection, which does not look for specific attack signatures, but for deviations from normal operation. This approach is particularly effective in detecting unknown attacks. In contrast to classic rule-based systems, AI-based solutions are able to continuously adapt to the changing environment.

In perimeter protection, AI-based traffic analysis can identify anomalous data flow, even if it does not violate specific firewall rules (see Table 1). Network IDS/IPS systems with AI integration dynamically learn normal network behavior and generate alerts when unusual patterns occur (Hornyák, 2025). In endpoint protection, AI enables predictive malware analysis, which can identify potential threats based on the behavior of files and processes (Tabinda, 2025). In access management, AI-based solutions enable context-aware decision-making, taking into account user behavior, geographic location, and device status.

The AI integration is closely linked to modern SIEM and SOAR systems. Security Information and Event Management (SIEM) systems use AI-based analytics to connect and prioritize events from different sources. Security Orchestration, Automation and Response (SOAR) systems, on the other hand, provide automated responses, reducing the need for human intervention and reducing response time (Shanmugavelan & Dinesh, 2024).

The classic model of cybersecurity systems remains an important foundation for protection, but it is no longer sufficient on its own to address modern threats. AI integration provides an opportunity for these systems to become more adaptive, proactive, and efficient. The key to successful integration is a balanced, mutually reinforcing application of classic security principles and AI-based technologies.

4. ANALYSIS OF MI-BASED ATTACKS

The application of AI in cybersecurity is twofold: while it significantly increases the effectiveness of defenses, it also provides new, previously unseen opportunities for attackers. The essence of AI-based attacks is not necessarily to create new attack targets, but to automate, scale, personalize and adapt existing attack methods (Goswami et al., 2024). As a result, attacks become faster, harder to detect and more cost-effective. AI-based attacks can be divided into two main categories:

- attacks against AI (Adversarial Machine Learning, Data Poisoning Attacks, Model Extraction and Model Inversion),
- attacks supported by AI (Authenticated Vulnerability Discovery, Intelligent Social Engineering and Phishing, Deepfake-based Attacks, Adaptive and Self-Optimizing Attacks), where AI serves as a tool to carry out traditional attacks.

4.1. Attacks against AI

The adversarial machine learning is an attack domain that specifically exploits the operating characteristics of machine learning systems. These attacks target the reliability, integrity or confidentiality of AI models. Adversarial examples (Evasion Attacks) are input data that are modified with minimal, often unnoticeable, modifications to the model in order to make the wrong decision (Gundoor, 2024). These attacks typically occur during the inference phase, i.e. they are directed against the already trained model. In a cybersecurity context, this is particularly dangerous because:

- a malicious file can be classified as “harmless”,
- an attacking network traffic can appear to be normal behavior,
- detection can be bypassed without the attacker using a completely new technique.

Such attacks highlight the fact that the decision boundaries of AI models are often unstable, especially for high-dimensional inputs. Data Poisoning Attacks target the training dataset. The attacker aims to inject manipulated or fake data into the learning process, which will distort the model’s behavior in the long term. This type of attack is particularly dangerous in:

- systems that use continuous learning,
- models based on crowdsourcing or open data sources,
- federated learning environments.

A poisoned model may:

- regularly give false positives,
- consistently ignore certain types of attacks,
- appear to work properly while being strategically compromised.

In model extraction, the attacker attempts to reconstruct the functionality or decision logic of the target model by executing a large number of queries on it. This is particularly relevant for cloud-based AI services accessible via APIs.

The goal of model inversion attacks, on the other hand, is to infer from the model:

- sensitive data used for training,
- information that is considered personal or trade secrets.

These attacks do not cause direct inoperability, but pose a confidentiality and data protection risk.

4.2. AI-assisted cyberattacks

In this category, AI is not a target, but a supporting tool that increases the effectiveness of attacks (Kacper, 2025). In automated vulnerability detection, AI-based systems are able to:

- analyze large code bases,
- recognize vulnerability patterns,
- estimate exploit potential.

This significantly shortens the detection phase for attackers and reduces the need for human expertise.

In the case of intelligent social engineering and phishing, modern AI models are able to:

- generate linguistically sophisticated, contextual messages,
- target communication based on public data,
- produce multilingual, culturally adapted content.

This drastically increases the success of phishing attacks, while making them more difficult to detect by traditional filters.

In the case of deepfake-based attacks, deepfake technologies enable:

- spoof voice and video identities,
- impersonate leaders or decision-makers,
- manipulate trust chains.

These attacks pose not only technical but also psychological and organizational risks, especially in financial and government environments.

In the case of adaptive and self-optimizing attacks, with the help of AI, attacks can:

- respond to defensive measures,
- dynamically modify their behavior,
- remain hidden for a long time.

This is especially typical of APT-type attacks, where the goal is not immediate damage, but a long-term presence.

4.3. Strategic implications of AI-based attacks

The proliferation of AI-based attacks is fundamentally changing the strategic landscape of cybersecurity attacks:

- can be scaled more quickly,
- require fewer human resources,
- are harder to attribute.

This creates an asymmetric threat model where even attackers with limited resources can cause significant damage. Defending against AI-based attacks requires:

- adversarial testing,
- the use of robust and explainable models,
- protection of data sources,
- decision-making based on cooperation between humans and AI.

The AI-based attacks represent not only a technological innovation, but also a qualitative leap in the nature of threats. AI is becoming a key factor in both defense and attack, which requires a new way of thinking, new security strategies and stricter regulatory frameworks. Cybersecurity systems of the future must be prepared to operate against intelligent adversaries. AI-based attacks represent a complex, multi-layered threat that can only be effectively responded to with integrated, adaptive and intelligent defense strategies (Nimra & Muhammad, 2025). The attack-defense matrix helps organizations to see the threat space in a structured way and consciously build their AI-based cybersecurity architecture. The attack-defense matrix is an analytical tool that:

- organizes AI-based attack techniques,
- assigns possible defense mechanisms,
- assists in risk analysis and security architecture design.

The matrix is not an operational guide, but a strategic and planning tool. The matrix clearly shows that there is no single universal defense solution. Effective defense is implemented at:

- technical (algorithms),
- infrastructural (data flows),
- organizational (processes),
- human (users) levels.

In many cases, AI-based attack defenses themselves require AI. This creates a dynamic adaptation cycle where defense systems must continuously learn (Islam et al., 2024). The importance of proactive defenses instead of classic reactive security:

- adversarial testing,
- threat hunting,
- predictive analytics
- become necessary.

The role of the attack-defense matrix in security planning:

- provides a basis for risk analysis,
- helps select security controls,
- can support ISO 27001 / NIST / Zero Trust-based planning,
- can also be used for educational and audit purposes.

5. THE QUANTUM-RESISTANT AI MODELS

The quantum-resistant AI models are not a problem of the distant future, but a strategic direction for preparation. Although the practical application of quantum computers is still limited, the long-term reliability of AI-based cybersecurity systems can only be ensured if the quantum threat model is taken into account in the design phase. Secure AI systems of the future will not only be intelligent and adaptive, but also quantum-resilient. AI is now an indispensable tool in cybersecurity — but it is also vulnerable (Noah et al., 2025). The key to protection is reliable data management, model security, continuous testing, explainability and legal and ethical compliance. In the coming years, AI will further shape cybersecurity, while bringing new challenges. AI is a key technological pillar of cybersecurity, which simultaneously:

- increases the effectiveness of defense,
- creates new vulnerabilities,
- requires strategic thinking.

Successful security systems of the future will not only be intelligent, but also explainable, auditable and ethical. The relationship between quantum-resistant AI and cybersecurity is a key issue for the future of information technology and digital security. With the development of quantum computing, classical security mechanisms, especially cryptographic systems, may become increasingly vulnerable.

Quantum-based algorithms, such as the Shor algorithm and the Grover algorithm, have the potential to break current encryption methods, fundamentally undermining the security of digital systems. This challenge is particularly important for AI systems, which are increasingly playing a role in protecting IT infrastructures and processing data.

5.1. The quantum-accelerated attacks

The quantum computers can solve certain mathematical problems that underlie classical encryption algorithms more quickly. This means that in the future, cryptographic systems such

as RSA and Elliptic Difference Cryptography (ECC), which form the backbone of today's computer security systems, will be easily cracked by quantum computers. As a result, AI-based systems that depend on digital signatures, encrypted communications, and data storage protection will become vulnerable (Prem, 2024).

The quantum-accelerated attacks effectively exploit the parallel computing capabilities of quantum computers, which allow attackers to search for and discover adversarial examples more quickly and reduce the cost of brute-force attacks. AI, which relies on pattern recognition and decision-making, could be particularly vulnerable to quantum-based attacks.

5.2. The quantum-resistant cryptography

The quantum-resistant cryptography, also known as post-quantum cryptography (PQC), is one of the most important technological advances in protecting against quantum threats. The guidelines developed by the National Institute of Standards and Technology (NIST) aim to develop cryptographic algorithms that can withstand attacks from quantum computers while still being compatible with today's classical systems. Such algorithms include lattice-based, code-based, hash-based, and multivariate polynomial cryptography solutions (Quang et al., 2025).

Integrating quantum-resistant cryptography into AI systems is essential to maintaining the confidentiality, integrity, and availability of data in the quantum era. Data encryption, API authentication, and model parameter protection are all areas where PQC is needed. AI-based systems, such as federated learning and model updates, can be particularly vulnerable to quantum-accelerated attacks and therefore need to be protected with quantum-resistant encryption.

5.3. Applying Zero Trust

The philosophy of Zero Trust architecture is that communication between network devices and applications should be continuously authenticated, without automatically considering anyone or anything as trustworthy. A Zero Trust approach is key to cybersecurity strategies, especially in environments where data and applications change dynamically, such as cloud infrastructures and AI-based systems (Gopalakrishna, 2024).

Applying Zero Trust to AI systems ensures that every request, data flow, and interface undergoes rigorous verification, minimizing the impact of internal and external threats. AI-driven anomaly detection and behavior-based authentication play key roles in Zero Trust architectures. Quantum-resistant encryption and adversarial training help Zero Trust systems remain protected not only against known but also quantum-accelerated attacks. The following key challenges need to be considered when designing quantum-resistant AI systems:

- Scalability: quantum-resistant algorithms often require more computational resources than classical solutions, which can be challenging when handling large AI models and datasets.
- Compatibility: integrating existing AI systems with quantum-resistant cryptographic solutions can pose technical and logistical challenges, especially in cases where AI algorithms rely on rapid iterations.
- Training and adaptation: developers and security professionals will need to acquire new knowledge about the application of quantum-resistant technologies and post-quantum encryption solutions.

- The future proliferation of quantum computers will inevitably radically transform the cybersecurity landscape. The quantum-resistant AI is therefore not just a security feature, but a new paradigm in the design and operation of digital systems. Combining the NIST Post-Quantum Cryptography Guidelines with the Zero Trust Architecture ensures that AI-based systems will be resistant to quantum threats in the long term (Quang et al., 2025).

Future security solutions must be able to adapt to the challenges of the quantum era, ensuring the reliability and stability of digital systems. Quantum-resistant AI can therefore form the basis of a new generation of cybersecurity systems that can balance performance, scalability, and security.

6. CONCLUSION

The AI has ushered in a new era of cybersecurity, where both defense and offense are AI-driven. Modern cybersecurity strategies are based on the integration of AI, while classic security controls remain essential. Future cybersecurity will depend on the combined strengthening of AI technologies, regulatory frameworks, and human expertise.

The AI is now an indispensable tool in cybersecurity – but it is also vulnerable. The key to protection is reliable data management, model security, continuous testing, explainability, and legal and ethical compliance. In the coming years, AI will continue to shape cybersecurity while bringing new challenges. The AI is a key technological pillar of cybersecurity that simultaneously:

- increases the effectiveness of defense,
- creates new vulnerabilities,
- requires strategic thinking.

Successful security systems of the future will not only be intelligent, but also explainable, auditable, and ethical.

The relationship between quantum-resistant AI and cybersecurity is a key issue for the future of information technology and digital security. With the development of quantum computing, classical security mechanisms, especially cryptographic systems, may become increasingly vulnerable. Quantum-based algorithms, such as the Shor algorithm and the Grover algorithm, can break current encryption methods, fundamentally undermining the security of digital systems. This challenge is particularly important for AI systems, which are increasingly playing a role in protecting IT infrastructures and processing data.

The AI is now one of the most decisive factors in cybersecurity, capable of both strengthening and weakening the information ecosystem. The future cybersecurity strategy is centered on a hybrid model: AI, human expertise, and robust security foundations.

REFERENCES

Aditya, S.; Kashvi, C.; Sunil S.; Krutika P. (2025). Artificial Intelligence (AI) in Cybersecurity: Foundations, Applications, and Research Trends. Implementing Enterprise Cybersecurity With AI pp. 29-56.

Anni, D. S.; Genci, S.; Silvana, Q. (2024). Artificial Intelligence In Cybersecurity Applications. IEEE 28th International Conference on Intelligent Engineering Systems (INES 2024). Piscataway (NJ), USA : Institute of Electrical and Electronics Engineers (IEEE) (2024) pp. 175-180.

Bányász, P. ; Szádeczky, T. ; Váczi, K. B. (2024). The relationship between generative artificial intelligence and cybersecurity. Proceedings of the Central and Eastern European eDem and eGov Days 2024. New York, USA : Association for Computing Machinery (ACM) pp. 209-215.

Chaudhary, H. & Detroja, A. & Prajapati, P. & Shah, P. (2020). A Review of Various Challenges in Cybersecurity using Artificial Intelligence. 10.1109/ICISS49785.2020.9316003.

Gopalakrishna, K. (2024). Zero trust and AI: A synergistic approach to next-generation cyber threat mitigation. World Journal of Advanced Research and Reviews, 2024, 24(03), 3374-3387. Received on 10 November 2024; revised on 16 December 2024; accepted on 18 December 2024. DOI: https://doi.org/10.30574/wjarr.2024.24.3.3883

Goswami, A.; Chirag, M.; Hirenkumar, M.; Ripalkumar, P. (2024). "The Role of AI in Cybersecurity: A Study on the Integration of Artificial Intelligence and Machine Learning in Cybersecurity." International Journal of Research in Computer. Applications and Information Technology (IJRCAIT) 7 (1): 94–113. https://doi.org/10.34218/IJRCAIT_07_01_010.

Gundoor, T. K. (2024). Attacks Against Artificial Intelligence: An Overview. Attacks on Artificial Intelligence The New Facets of Cyber Ecospace. Publisher: CRC Press Taylor and Francise Group. pp. 1-298. https://www.researchgate.net/publication/376207727_Attacks_Against_Artificial_Intelligence_An_Overview

Hornyák, O. (2025). Intelligent – A comprehensive overview of applicable AI Methods with a Focus on IoT Security. Special Issue of the Infocommunication Journal. pp. 61-75. DOI: 10.36244/ICJ.2025.5.8

Islam, S. M., Bari, M. S., Sarkar, A., Khan, A. O. R., & Paul, R. (2024). AI-Powered Threat Intelligence: Revolutionizing Cybersecurity with Proactive Risk Management for Critical Sectors. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 7(01), 1-8.

Kacper, Z. (2025). AI-Powered Cyberattacks: A Comprehensive Review and Analysis of Emerging Threats. Advances in IT and Electrical Engineering vol. 31, 2025, 55-69. https://doi.org/10.7862/re.2025.5

Karen , S.; Peter, M. (2010). Intrusion Detection and Prevention Systems. Handbook of Information and Communication Security. pp. 1-20. https://doi.org/10.1007/978-3-642-04117-4_9

Nimra, B.; Muhammad, Z. Z. (2025). AI-Powered Cyberattacks: Impacts and Defense Strategies. Department of Computer Science, Bahauddin Zakariya University, Multan, Punjab, Pakistan. World Journal of Advanced Research and Reviews, 2025, 25(03), 510-512. DOI: https://doi.org/10.30574/wjarr.2025.25.3.0751

Noah, A.; Emmanuel, C.; Edima, D. E.; Iboro, A. E.; Joshua, O. A. (2025). Quantum-Resistant AI Models for Next-Generation Cyber Defense. Engineering and Technology Journal e-ISSN: 2456-3358 Volume 10 Issue 09 September-2025, Page No.- 7064-7088. DOI: 10.47191/etj/v10i09.23, I.F. – 8.482.

Prem, K. S. (2024). Quantum-Resistant Artificial Intelligence and Machine Learning Architectures for Secure Mortgage and Banking Intelligence Systems. Deep Science Publishing. pp. 1-196. ISBN: 978-93-7185-683-6. DOI:10.70593/978-93-7185-228-9

Quang D. T.; Hien, N.; Tuy, T. N.; Hanho, L. (2025). NIST Post-Quantum Cryptography Standards:A Comprehensive Review of Theoretical Foundations and Implementations. Received 2 December 2025, accepted 3 January 2026, date of publication 14 January

2026, date of current version 28 January 2026. Digital Object Identifier 10.1109/ACCESS.2026.3654142

Shanmugavelan, R.; Dinesh, R. C. (2024). Enhancing Cyber Resilience: Convergence of SIEM, SOAR, and AI in 2024. International Journal of Computing and Engineering. ISSN 2958-7425 (online) Vol. 5, Issue No. 2, pp. 36 - 44.

Szabó, H. (2023). Security Risks of Artificial Intelligence at the Beginning of a New Era. NATIONAL SECURITY REVIEW Volume 11 (2023) Issue 4, pp. 35–46. doi: 10.32561/nsz.2023.4.3

Tabinda, S. (2025). Enhancing Endpoint Security: Integrating Explainable AI, Ransomware Defense, and Data Breach Compliance. Chenab Institute of Information Technology. pp. 1-7. DOI:10.13140/RG.2.2.13568.96008