The American Journal of Engineering and Technology
ISSN 2689-0984 | Open Access

TYPE Original Research
PAGE NO. 210-214
DOI 10.37547/tajet/Volume07Issue09-16

Check for updates

Role of Artificial Intelligence in Data-Infrastructure Vulnerability Management

Roman Dubinin
Staff Engineer, SOLAR SECURITY JS Moscow, Russia

Danil Temnikov
Lead Engineer EPAM Systems Redmond, USA

OPEN ACCESS

SUBMITTED 08 August 2025
ACCEPTED 14 August 2025
PUBLISHED 30 September 2025
VOLUME Vol.07 Issue 09 2025

CITATION
Roman Dubinin, & Danil Temnikov. (2025). Role of Artificial Intelligence in Data-Infrastructure Vulnerability Management. The American Journal of Engineering and Technology, 7(09), 210–214. https://doi.org/10.37547/tajet/Volume07Issue09-16

Abstract: This article examines the role of artificial intelligence in managing vulnerabilities across data infrastructures. It describes the methods used to identify, analyse and remediate weaknesses, as well as the difficulties encountered during deployment. The purpose of the study is to evaluate how AI is applied to data-security tasks and to assess its capabilities and limitations. A review of academic publications, risk-management models and publicly available information on cyber-attacks provides a broad perspective on the topic. Algorithms for monitoring network activity, forecasting threats and automating vulnerability remediation are discussed. Findings show that AI accelerates remediation processes by handling large data volumes and adapting to shifts in the threat landscape. Persistent challenges include data-quality issues, ethical risks and the possibility that the technology could be misused for illegal purposes. The need for robust, transparent models that resist manipulation is underscored. The material will benefit cybersecurity professionals, AI developers, IT managers and researchers who focus on the ethical aspects of new technologies.

Keywords: artificial intelligence, vulnerability management, cybersecurity, machine learning, deep learning, threat prediction.

Introduction

As the economy evolves and information technologies spread, data protection becomes a critical concern.

Technological change has increased both the number and the sophistication of cyber-threats, calling for new methods of vulnerability management. Traditional defence measures are unable to cope with the volume of information and the complexity of current threats, making new solutions essential.

Artificial intelligence now plays an important role in vulnerability management by enabling anomaly detection, attack prediction and the automation of security measures.

Yet deploying such technologies raises several issues: the explainability of AI decisions, the quality of the data on which those decisions rely and the risk that criminals will exploit the same tools. Ethical use and the configuration of defensive systems to prevent attacks are therefore crucial considerations.

Information security remains a pressing issue owing to the activities of cybercriminals and the ongoing need to develop new protective measures. AI provides organisations with tools for preventing attacks and safeguarding data, but questions relating to ethical risks and long-term applications still require further academic attention.

The objective of this work is to analyse current AI-driven methods for vulnerability management, identify existing problems and offer recommendations that will improve the effectiveness of AI in information-security practice.

Materials and Methods

The use of artificial intelligence in cybersecurity has become a pivotal element of modern information-protection systems. Academic research on this subject spans several areas: threat analysis, risk and vulnerability management, and the ethical implications of deploying AI under new technological conditions.

Many studies investigate AI for analysing network activity and neutralising threats. Alkhatri M. and Alzitawi D. describe how AI can be applied to the behaviour of network protocols, improving attack-detection systems [1]. Similar ideas are pursued by Hassan S. K. and Ibrahim A., who propose automating incident investigation to accelerate decision-making [4]. Uzoka A., Cadet E. and Ojukwu P. U. examine AI for real-time threat analysis, which reduces latency and increases predictive accuracy [10].

The work of Patel T. et al. focuses on protecting critical infrastructure: they present an AI framework tailored to the operational conditions of industrial facilities. This approach handles large data volumes in real time and integrates AI into existing security systems [7].

Vulnerability management and risk assessment are essential aspects of corporate protection. Gajiwala C. models threats while accounting for changing operating environments, improving the precision of vulnerability identification [3]. Mahmoud M. proposes algorithmic techniques for classifying vulnerable infrastructure elements, helping teams focus on the most problematic areas [2]. Nayman G. and Garkavenko D. explore machine-learning capabilities for automating vulnerability management; predictive models rapidly highlight weaknesses, minimising the likelihood of successful attacks [5]. Ilyenko A., Ilyenko S., Yakovenko O., Halych Y. and Pavlenko V. present a model that combines attack prediction with vulnerability management, supporting deeper risk analysis [9].

Ethical questions surrounding AI have become a central topic. Benzaïd C. and Taleb T. emphasise the dual nature of AI: it can reinforce defences but also refine offensive techniques. In the 5G context, AI both strengthens security and increases exposure to new vulnerabilities [6].

AI use in specific technological contexts is actively discussed in several publications. Mamidi S. R. and Zuhair H. analyse AI's role in cloud security, proposing methods for automating data analysis and monitoring of cloud systems—an increasingly important issue as cloud technologies spread and data-protection tasks grow more complex [11][8].

Collectively, the literature demonstrates a wide variety of AI applications in cybersecurity, yet it also reveals contradictions between studies that highlight positive impacts and those that point to potential risks. This underscores the need for further research to clarify AI's dual nature.

For the present work, a review was conducted of other authors' publications, risk-management models and publicly available information on cyber-attacks, enabling a broad examination of the chosen topic.

Results and Discussion

Data infrastructure comprises various elements that can harbour vulnerabilities. These weaknesses may be classified by their origins and the methods used to exploit them. The categories of vulnerable areas in a data infrastructure are shown in Figure 1.

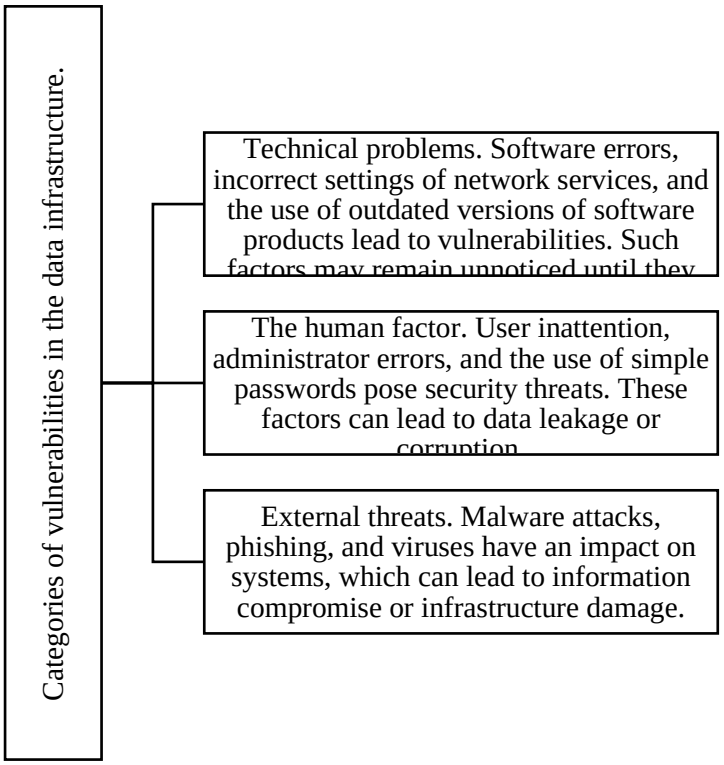

Fig. 1. Categories of vulnerabilities in the data infrastructure [1, 4, 7, 10].

Effective vulnerability management requires a comprehensive system capable not only of detecting weaknesses but also of prioritising their remediation—an especially difficult task when data volumes are large. AI reshapes security practice by making these processes more efficient. Algorithms reveal vulnerabilities by analysing data and system configurations, identifying anomalies that signal either weaknesses or attempts to exploit them. Moreover, AI can discover previously unknown vulnerabilities. Unlike traditional methods, which take time to uncover flaws, AI processes data immediately, enabling rapid responses to change [2, 3].

A further strength of AI is its ability to integrate with existing systems. Security-information-and-event-management platforms gain advanced analytics from AI algorithms. Interaction with access-control systems minimises the risk of unauthorised access by detecting and then blocking suspicious actions [6]. By analysing system interactions, AI can also identify potential threats at an early stage and recommend preventive measures [5, 9]. Table 1 summarises the ways AI may be applied to vulnerability management in data infrastructures.

Table 1. The possibilities of using algorithms based on artificial intelligence in the process of vulnerability management in the data infrastructure [2, 3, 5, 9].

Area of AI application	Capability description
Automation of monitoring and data analysis	In contrast to rule-based systems, AI processes large data volumes in real time to uncover anomalies. Machine-learning algorithms detect deviations in network traffic, training on past attacks to predict emerging threats.
Vulnerability prediction	Drawing on cyber-incident data, AI builds models that forecast new vulnerabilities, allowing security teams to identify in advance which systems are likely to be targeted and which weaknesses may soon be exploited.
Patch-management optimisation	Applying updates demands considerable effort. AI evaluates which patches should be installed first, basing its decisions on threat level, vulnerability location and potential impact. This streamlines the process, cuts costs and sustains performance.

Automated threat response	Modern AI-driven platforms not only detect threats but also react automatically, isolating infected network segments or blocking suspicious processes—an essential feature when qualified specialists are in short supply.
User training and ongoing support	AI plays a direct role in raising staff awareness. Chatbots that simulate genuine phishing attacks teach users to recognise threats, while natural-language-processing tools analyse user actions to identify mistakes.

After vulnerabilities have been detected, AI is applied to evaluate them. This assessment considers multiple factors—including the likelihood of exploitation, the potential impact of incidents and the importance of the assets involved. By analysing information from available sources, AI systems build a risk picture that highlights the threats requiring the highest remediation priority.

Automating vulnerability remediation is another key AI function. Systems can not only recommend fixes but also implement them by installing patches, configuring firewalls, adjusting access policies and blocking exposed components. These actions shorten response times and reduce the window during which attackers can exploit weaknesses.

AI is likewise employed to predict which vulnerabilities may become dangerous in the future. Attack-simulation technologies, weakness assessments and infrastructure-wide security testing reveal flaws before they can be used. Training on cyber-attack data allows systems to adapt to emerging threat types [2, 3].

When AI algorithms are integrated into existing security frameworks, they enhance incident management and sharpen organisational response. By enriching data through open-source analysis and network monitoring, such systems identify malicious activity early and help prevent attacks [6].

AI-driven vulnerability management also analyses new attack vectors, exploitation scenarios and practitioner feedback. Natural-language-processing tools process sources such as vulnerability reports and CVE databases, keeping information current. Machine-learning algorithms and graph databases support data analysis and reveal relationships within network infrastructure, enabling the development of precise vulnerability-management solutions [8, 11]. Table 2 summarises the advantages and drawbacks of using AI for managing vulnerabilities in data infrastructures.

Table 2. Advantages and disadvantages of using artificial intelligence in managing data-infrastructure vulnerabilities (compiled by the author)

Category	Advantages	Disadvantages
Speed and efficiency	– Automation of vulnerability-detection processes. – Rapid threat identification.	– Possible false positives that slow incident response. – Requirement for significant computing resources.
Accuracy	– Improved detection of complex vulnerabilities through data analysis. – Ability to predict future weaknesses.	– AI can err in new or atypical scenarios. – Performance depends directly on data quality.
Reduction of human error	– Less reliance on manual analysis.	– Risk of losing control if systems are misconfigured.
Cost-effectiveness	– Lower spending on vulnerability management.	– High initial investment in developing and deploying AI-based systems.
Flexibility	– Capacity to adapt to new threats.	– Configuration challenges for task-specific requirements.

In sum, AI-based algorithms have a direct impact on vulnerability management by introducing new approaches to automated analysis and threat prediction. Realising their full potential, however, requires an implementation strategy that addresses both technological and organisational factors.

Conclusion

The technology-driven economy demands robust data protection. Ongoing advances in this field are accompanied by a rising number of cyber-threats, making it essential to develop effective vulnerability-management methods. Traditional security approaches no longer address weaknesses efficiently, given the explosive growth of information and the increasing sophistication of attacks. In this context, artificial intelligence has become an indispensable instrument for data analysis and real-time decision-making. Its application enables the detection of anomalies and the forecasting of threats. Machine-learning techniques and natural-language processing make it possible to build systems that adapt to emerging risks and recommend measures for eliminating vulnerabilities, although their deployment in security operations involves a range of challenges.

The escalating complexity of cyber-threats and the need for new protection strategies underscore the relevance of this topic. Artificial intelligence in cybersecurity allows not only a rapid response to attacks but also their prevention at early stages. Nonetheless, many issues linked to ethical considerations and technological constraints remain insufficiently explored, warranting further attention in academic research.

References

1. Alkhatri M., Alzitawi D. The role of artificial intelligence in solving cybersecurity problems // International Journal of Academic Research in the field of Business and Social Sciences. – 2024. – Volume 14 (4). – pp.335-345.
2. Mahmud M. Risks and vulnerabilities of using artificial intelligence in information security //The 2023 International Conference on Computational Science and Computational Intelligence. – IEEE, 2023. – pp. 266-269.
3. Gadjiwala S. Artificial intelligence in cybersecurity : advanced threat modeling and vulnerability assessment // International Journal of Scientific Research in the Field of Computer Science, Engineering and Information Technology. - 2024. – Volume 10 (5). – pp.778-788.
4. Hassan S. K., Ibrahim A. The role of artificial intelligence in cybersecurity and incident response //International Journal for the Investigation of Electronic Crimes. – 2023. – vol. 7. – No. 2.
5. Naiman G., Garkavenko D. Methods and tools for vulnerability management of a corporate information system based on machine learning // Modern information security. - 2021. - No. 3. – pp. 24-28.
6. Benzaid S., Taleb T. Artificial intelligence for networks beyond 5G: a means of protection against cybersecurity or attack? //IEEE network. – 2020. – vol. 34. – No. 6. – pp. 140-147.
7. Patel T. et al. A secure intrusion detection system based on artificial intelligence for critical infrastructure with digital twin support //14th International Conference on Information Technology and Knowledge (IKT), 2023. – IEEE, 2023. – pp. 24-29.
8. Zuhair H. The role of artificial intelligence in cybersecurity //Journal of Al-Kut University College. – 2024. – no. Special issue.
9. Ilyenko A., Ilyenko S., Yakovenko O., Galich Yu., Pavlenko V. Prospects for integrating artificial intelligence into cybersecurity systems // Cybersecurity: education, science, technology. - 2024. – Vol. 1. – No. 25. – pp. 318-329.
10. Uzoka A., Kadet E., Ojukwu P. U. The use of artificial intelligence in cybersecurity to improve threat detection, response to them and risk management //Journal of Computer Science and Information Research. P-ISSN. – 2024. – pp. 2709-0043.
11. Mamidi S. R. The role of artificial intelligence and machine learning in improving the security of cloud computing //Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023. – 2024. – Vol. 3. – No. 1. – pp. 403-417.