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

TYPE Original Research
PAGE NO. 203-209
DOI 10.37547/tajet/Volume07Issue09-15

Check for updates

Integrating AI Technologies Into Information Security Systems

Sergei Beliachkov
Head of Department, Platform Cybersecurity Center, JSC Sberbank-Technologies, Moscow, Russia

OPEN ACCESS

SUBMITTED 01 August 2025
ACCEPTED 12 August 2025
PUBLISHED 27 September 2025
VOLUME Vol.07 Issue 09 2025

CITATION
Sergei Beliachkov. (2025). Integrating AI Technologies Into Information Security Systems. The American Journal of Engineering and Technology, 7(09), 203–209. https://doi.org/10.37547/tajet/Volume07Issue09-15

Abstract: This article explores the integration of artificial intelligence (AI) technologies into information security systems, aiming to enhance the effectiveness of threat detection and response. The research is grounded in a comprehensive review of existing literature. It examines AI's capabilities in processing large volumes of data, forecasting potential threats, and automating their identification. The discussion also addresses associated vulnerabilities, including issues related to the quality of training datasets, susceptibility to adversarial attacks, and algorithmic bias. Special attention is given to the development of technological solutions designed to protect AI-driven systems themselves. These include data encryption, access control mechanisms, anomaly detection systems, behavioral analytics, and architectural strategies such as multi-layered defense and containerization. The findings presented are relevant to cybersecurity researchers and practitioners, machine learning specialists, and developers of intelligent systems engaged in building interdisciplinary approaches to threat analysis, prediction, and mitigation in today's complex digital environments. This material is also of value to professionals seeking to bridge theoretical frameworks with practical implementation in the context of rapidly evolving digital ecosystems and critical infrastructure.

Keywords: Artificial intelligence; information security; cybersecurity automation; threat detection; encryption; access control; adaptive learning; multi-layered defense.

1. Introduction

Modern security systems are under increasing pressure

to adapt rapidly to multilayered and continuously evolving threats, driven by the integration of heterogeneous technologies into unified digital infrastructures. Recent DDoS attack statistics from the first quarter of 2025 underscore the severity of this trend: the telecommunications sector accounted for 28% of all incidents, marking it as the most vulnerable industry for several consecutive years. It was followed by the financial sector (21%) and government organizations (16%), with political and commercial motives dominating attack drivers (StormWall, Izvestia, April 10). The total number of attacks during this period surged by 71% compared to the same quarter in 2024. The financial sector alone experienced a 36% increase, resulting in significant service disruptions, particularly affecting mobile banking access. Government institutions faced a 29% rise in attack volume, primarily from politically motivated hacktivists targeting public services. Retail accounted for 14% of cases (+22%), the entertainment industry for 9% (+12%), and the oil and gas sector for 7%, with a record-breaking 48% increase in attacks. Spikes in cyber incidents also aligned with major events: a 3.5-fold rise in attacks on online retailers during International Women's Day, a surge against streaming platforms during the New Year holidays, and targeted assaults on energy companies during periods of economic sanctions [11].

Artificial intelligence (AI) has shown significant promise in handling vast data streams, forecasting cyber threats, and automating incident detection—making it a highly relevant instrument for protecting information systems [1, 2].

Within the scientific paradigm where information security faces unprecedented challenges, the integration of AI technologies is emerging as a strategic research direction. Several authors have focused on the methodological foundations and principles underpinning the use of AI in security systems. Hudson J. [1], for example, proposes innovative database protection methods for AI models, emphasizing the need for dynamic, self-learning systems. Similarly, Lysenko S. et al. [2] highlight the potential of machine learning algorithms to automate threat detection and mitigation, substantially enhancing the adaptability of security infrastructures. Gadde H. [7] advances this perspective by exploring how AI can be integrated into failure detection and recovery algorithms for high-availability databases, underscoring the value of a comprehensive approach that merges traditional safeguards with contemporary computing technologies.

Alongside methodological advancements, there is a growing emphasis on applying AI within specialized domains of cybersecurity. Damaraju A. [3, 4] addresses the challenges of securing cloud environments and the future of cybersecurity in the 5G and 6G era, revealing how emerging communication technologies necessitate a fundamental rethinking of traditional protective frameworks. Chirra D. R. [5] examines the application of AI in proactive threat intelligence for smart grids, contributing to risk minimization in critical infrastructure systems. In a similar vein, Reddy V. M. and Nalla L. N. [8] explore real-time data processing challenges in e-commerce, emphasizing the need for AI algorithms capable of managing high volumes of dynamic data. Syed F. M. and ES F. K. [10] illustrate how AI can strengthen multifactor authentication in healthcare access control systems—where both security and speed are of paramount importance.

Another key research direction involves the development of specialized tools for risk management and improved deployment of AI technologies. Venugopal R. et al. [6] propose a structured framework for selecting risk management tools, helping systematize decision-making when integrating AI into enterprise security infrastructures. Goriparthi R. G. [9], in turn, focuses on hybrid AI frameworks that optimize distributed edge computing processes, aiming to balance performance and scalability.

It is also worth noting that statistical data was sourced from [11], as published on the en. website.

Overall, the literature reveals a wide spectrum of approaches to AI integration in cybersecurity systems—from foundational methodologies and algorithmic innovation to practical applications across various sectors. However, certain contradictions emerge. Some researchers advocate for full automation of security processes, while others stress the importance of retaining flexibility and adaptability to address context-specific challenges. Furthermore, strategic management of AI solutions in cybersecurity remains underexplored, particularly concerning the interplay between technical system characteristics and organizational implementation frameworks. These gaps highlight the need for continued research aimed at bridging theoretical models with actionable strategies to develop universal and adaptive protection systems.

The aim of this paper is to examine the key challenges

arising from the integration of AI technologies into information security systems, with a focus on advanced database protection techniques.

The scientific contribution lies in the proposed approach that combines encryption methods, modern access control mechanisms, and anomaly detection algorithms with adaptive AI models to create a unified, self-learning cybersecurity system. This approach not only expands the theoretical boundaries of how information protection is understood but also opens new avenues for practical application in the face of real-world cyber threats.

The core hypothesis is that integrating database security techniques—such as encryption and access control—with adaptive AI models will reduce vulnerabilities in contemporary cybersecurity systems and improve their capacity for rapid threat detection and response. It is expected that this holistic approach will raise the overall level of protection for information assets by enabling swift adaptation to the dynamic nature of cyber threats.

The study is based on a structured analysis of relevant literature in the field.

2. Analysis Of AI Capabilities And Vulnerabilities In Information Security Systems

Modern AI algorithms demonstrate high efficiency in processing large volumes of data, detecting anomalous patterns, and forecasting cyber threats. Leveraging machine learning techniques enables AI-driven systems to analyze data in real time, significantly reducing the time needed to detect incidents—an essential factor for rapid response [1]. Automating threat detection through AI contributes to more accurate and timely identification of attacks, minimizing human error and enhancing the overall security posture of information systems [2]. Further insights into the effectiveness of AI in detecting cyberattacks can be found in the work of Damaraju A. [3], who emphasizes the value of self-learning systems capable of adapting to emerging threats by continuously updating their models.

Despite these advantages, integrating AI into information security is accompanied by several serious vulnerabilities. One of the primary concerns is the dependence of AI models on the quality of input data. Data poisoning attacks, in which training data is manipulated or corrupted, can distort AI models and compromise their effectiveness [1]. Additionally, adversarial attacks—wherein attackers introduce subtle, imperceptible changes to input data—can mislead AI systems, causing incorrect threat classifications [2]. Another issue is algorithmic bias, which can arise from poorly curated training datasets and lead to systematic detection errors for certain types of attacks [3]. These vulnerabilities underscore the need for not only continuous monitoring and updating of AI models but also for their integration with traditional cybersecurity methods to create a robust, multi-layered defense system.

A comparative analysis of AI capabilities and vulnerabilities in information security is presented in Table 1.

Table 1: Comparative analysis of AI capabilities and vulnerabilities in information security (compiled on the basis of data from [1–3])

Aspect	Capabilities / Advantages	Vulnerabilities / Risks	Notes / Mitigation Measures
Data Processing and Analysis	Rapid handling of large datasets; detection of anomalies and threat prediction	Dependence on data quality; risk of data manipulation (data poisoning)	Verification of data sources; implementation of data integrity control mechanisms
Automated Threat Detection	Real-time detection of cyberattacks; use of deep learning to identify complex threats	Risk of false positives and model exploitation; need for regular algorithm updates	Integration with traditional monitoring systems; calibration techniques to reduce false alerts
Adaptability	Continuous learning	Risk of algorithmic bias;	Use of adversarial training;

Aspect	Capabilities / Advantages	Vulnerabilities / Risks	Notes / Mitigation Measures
and Self-learning	from historical data; ability to adapt to new threat types	susceptibility to adversarial attacks	regular model evaluation and dataset refinement

The analysis shows that integrating AI into information security systems can significantly improve the effectiveness of cyberattack detection and response. High-speed data processing, the ability to uncover novel threats, and the adaptability of AI models are key strengths that support more agile defense mechanisms. However, these technologies are not without their weaknesses. Issues such as data manipulation, susceptibility to adversarial attacks, and algorithmic bias necessitate a comprehensive approach to securing AI systems.

To mitigate these risks, best practices include rigorous data verification, continuous updates and refinement of training datasets, and the integration of AI with conventional defense tools.

In conclusion, a holistic understanding of both the advantages and vulnerabilities of AI technologies is essential for developing an effective and adaptive information security framework—one that is capable of countering both current and emerging cyber threats.

3. Technological Solutions For Protecting AI Systems

Integrating artificial intelligence technologies into information security systems requires a comprehensive suite of technological solutions designed to minimize AI model vulnerabilities and safeguard critical data. Contemporary protection methods include database-level security measures, the integration of anomaly detection and behavioral analysis algorithms, and the implementation of advanced architectural strategies to enable multi-layered defense. These approaches not only enhance the effectiveness of threat detection and response but also reduce the risk of exploiting weaknesses associated with AI training and operation [5].

At the core of AI system protection is the preservation of data confidentiality and integrity—especially for the datasets used in model training and execution. Key protective measures include:

- Data encryption. The use of modern cryptographic algorithms such as AES (Advanced Encryption Standard) helps secure data both at rest and in transit. This reduces the likelihood of unauthorized access or data manipulation.
- Access control. Implementing strict access control mechanisms—including role-based access control (RBAC) and multi-factor authentication (MFA)—ensures restricted data access and mitigates the risk of leaks [6, 7].

A fundamental requirement for modern AI systems is continuous activity monitoring and the prompt detection of anomalous events that may signal a cyberattack. Several technologies contribute to this capability:

- Network and user pattern analysis. Machine learning algorithms and deep neural networks can detect real-time deviations from normal behavior, enabling accurate identification of attacks such as adversarial manipulation and data forgery attempts [1].
- Behavioral analytics. Automated systems based on user and network node behavior build dynamic threat models that adapt to the evolving cybersecurity landscape. This reduces false positives and improves detection precision [3, 8].

Robust AI protection also depends on architectural design strategies that enable isolation and resilience across critical system components:

- Defense in Depth. This approach involves deploying multiple layers of protection—from traditional tools such as firewalls and intrusion detection/prevention systems (IDS/IPS) to specialized AI modules that monitor system status in real time [5].
- Containerization and microservices architecture. These technologies isolate key system components, reducing the attack surface—particularly relevant for distributed AI models [3].
- Regular testing and vulnerability assessment. Systematic penetration testing, security audits, and simulated attack scenarios help identify weaknesses and

refine system architecture [2].

A comparative overview of technological solutions used to protect AI systems is provided in Table 2.

Table 2: Comparative analysis of technological solutions for the protection of AI systems (based on data from [2, 3, 5, 7])

Technological Solution	Description	Advantages	Risks and Mitigation Measures
Data Encryption	Use of AES algorithms to secure data at rest and in transit	Ensures confidentiality; prevents unauthorized access	High computational load; requires regular updates of cryptographic keys
Access Control (RBAC, MFA)	Restricts access via role-based permissions and multi-factor authentication	Reduces data leak risks; improves access control precision	Credential compromise risk; requires anomaly monitoring and timely updates to authentication
Anomaly Detection & Behavioral Analytics	Uses machine learning to monitor network activity and detect behavioral deviations	Accelerates cyberattack detection; reduces false positives	Risk of misclassification; continuous model adaptation needed
Multi-layered Architecture & Containerization	Isolates critical system components using containers and microservices architecture	Limits attack impact; enhances infrastructure resilience	Complex integration and management; regular vulnerability testing essential

These technological measures show that integrating database-level protections, anomaly detection algorithms, and advanced architectural designs significantly enhances the security of AI systems. Encryption and access control ensure foundational defense against external threats, while behavioral analytics and multi-layered architectures support timely incident detection and containment.

However, effective implementation requires ongoing monitoring, updating, and testing to mitigate risks related to the unique vulnerabilities of AI training and operation. Continued research and the application of current best practices will be critical in building resilient and adaptive cybersecurity systems capable of countering today's evolving threat landscape.

4. Security Automation And Development Prospects

As cyber threats grow in complexity and the volume of processed data increases, automation has become a critical component of modern information security strategies. The integration of artificial intelligence (AI) technologies accelerates threat detection and incident response while enhancing decision-making quality through real-time analytics and self-learning algorithms [9]. This section examines the opportunities for security automation, the associated challenges and risks, and the future trajectory of integrated protection systems.

One key area of automation is the use of AI for rapid cyberattack detection and the deployment of automatic response mechanisms. Machine learning–based systems can process vast data streams, detect anomalous patterns, and swiftly identify potential threats—significantly reducing reaction times [10]. These solutions operate on real-time analytics, shifting the focus from passive monitoring to active threat prevention, including isolating compromised network segments and blocking suspicious activity.

Automation offers a range of advantages: minimizing

response delays, reducing dependence on human analysts, and optimizing the workload of security operations centers. However, despite its effectiveness, the use of AI in automated protection is not without challenges. A major concern is the potential use of similar AI technologies by malicious actors to bypass defenses or craft new types of attacks, such as adversarial examples [1]. Moreover, excessive reliance on automation may lead to underestimating the context of complex incidents—highlighting the need for a balanced approach that combines automated responses with expert evaluation [3, 5].

The future of security automation lies in deeper integration of AI into comprehensive monitoring and response systems. Adaptive learning approaches are expected to evolve, enabling systems to continuously refine their models based on new data and incident patterns. Current research underscores the importance of hybrid solutions that merge classical cybersecurity techniques with advanced AI analytics. Another promising direction is the development of federated learning, which preserves data privacy while enabling collective model training across distributed systems [1].

To further explore the benefits and risks of security automation, Table 3 presents a comparative overview of key elements.

Table 3: Comparative analysis of key elements of security automation and their associated advantages and risks (based on data from [1, 2])

Automation Element	Description	Advantages	Challenges and Mitigation Measures
Automated Threat Detection	Use of deep learning and anomaly detection algorithms to identify suspicious activity in real time	Faster detection, quicker attack identification, reduced false positives	Vulnerable to adversarial attacks; requires multi-layered result verification and regular model updates
Automated Response	Isolation of compromised nodes, blocking suspicious activity, and automated operator alerts	Rapid incident containment, reduced damage, minimized human error	Potential false positives; integration with expert systems needed for accurate response interpretation
Adaptive Self-learning	Systems that continuously learn from historical and new data, adjusting models in real time	Ongoing model relevance, resilience to novel attack types, reduced algorithm obsolescence	Needs training data quality control; risk of bias; requires regular validation and correction mechanisms

AI-driven security automation enhances the speed and accuracy of threat detection, with clear benefits in reducing response times and limiting reliance on manual oversight. However, effective implementation requires careful consideration of current challenges—particularly the risks posed by adversarial manipulation and potential misinformation in automated systems.

Looking forward, the development of adaptive self-learning and hybrid technologies capable of integrating diverse data sources while upholding robust security standards is essential. Such a comprehensive approach will enable the creation of resilient, dynamically evolving cybersecurity systems, capable of responding effectively to the continuously shifting threat landscape of the digital age.

5. Conclusion

This study presented a comprehensive analysis of the capabilities and vulnerabilities associated with integrating artificial intelligence technologies into information security systems. The findings demonstrate that AI significantly enhances the speed and accuracy of cyber threat detection by leveraging large-scale data

processing algorithms, anomaly pattern recognition, and automated response mechanisms. At the same time, identified vulnerabilities—such as data manipulation risks, adversarial attacks, and potential algorithmic bias—underscore the need for robust, multi-faceted defense strategies that combine advanced encryption methods, strict access control, and multi-layered system architecture.

Automation technologies play a particularly critical role in strengthening cybersecurity resilience. By accelerating threat detection and reducing reliance on human intervention, automation becomes essential in the face of increasingly sophisticated cyberattacks. A promising direction for future research lies in the advancement of adaptive, self-learning models capable of adjusting their parameters in real time based on incoming data. The integration of federated learning also emerges as a key opportunity, enabling collaborative model training across distributed systems while preserving data privacy.

Further research should focus on improving data quality control mechanisms, minimizing susceptibility to adversarial attacks, and optimizing the synergy between automated solutions and expert analysis. Taken together, the present study offers a valuable contribution to the development of scientifically grounded strategies for safeguarding digital assets in an ever-evolving cyber landscape.

6. References

1. Hudson J. Artificial Intelligence and Cybersecurity Integration: Modern Database Techniques for Securing AI Models. – 2024. – pp.3-23.
2. Lysenko S. et al. The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats //Economic Affairs. – 2024. – Vol. 69. – pp. 43-51.
3. Damaraju A. Cloud Security Challenges and Solutions in the Era of Digital Transformation //International Journal of Advanced Engineering Technologies and Innovations. – 2024. – Vol. 1 (3). – pp. 387-413.
4. Damaraju A. The Future of Cybersecurity: 5G and 6G Networks and Their Implications //International Journal of Advanced Engineering Technologies and Innovations. – 2024. – Vol. 1 (3). – pp. 359-386.
5. Chirra D. R. AI-Based Threat Intelligence for Proactive Mitigation of Cyberattacks in Smart Grids //Revista de Inteligencia Artificial en Medicina. – 2023. – Vol. 14 (1). – pp. 553-575.
6. Venugopal R. et al. Third Party Risk Management Tool Selection Framework (TPRMTSF) //Srinidhi, Third Party Risk Management Tool Selection Framework (TPRMTSF)(June 03, 2024). – 2024. – Vol. 10. - pp. 1-10.
7. Gadde H. AI-Powered Fault Detection and Recovery in High-Availability Databases //International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. – 2024. – Vol. 15 (1). – pp. 500-529.
8. Reddy V. M., Nalla L. N. Real-time Data Processing in E-commerce: Challenges and Solutions //International Journal of Advanced Engineering Technologies and Innovations. – 2024. – Vol. 1 (3). – pp. 297-325.
9. Goriparthi R. G. Hybrid AI Frameworks for Edge Computing: Balancing Efficiency and Scalability //International Journal of Advanced Engineering Technologies and Innovations. – 2024. – Vol. 2 (1). – pp. 110-130.
10. Syed F. M., ES F. K. AI and Multi-Factor Authentication (MFA) in IAM for Healthcare //International Journal of Advanced Engineering Technologies and Innovations. – 2023. – Vol. 1 (2). – pp. 375-398.
11. The main targets of DDoS attacks in 2025 are named [Electronic resource] Access mode: https://en.iz.ru/en/1868631/2025-04-10/main-targets-ddos-attacks-2025-are-named (date of request: 04/14/2025).