The Shivapuri
Volume: XXVII, 2026
DOI: https://doi.org/10.3126/shivapuri.v27i1.90943
Army Command and Staff College, Nepali Army
Shivapuri, Kathmandu, Nepal

Revolutionizing Security: The Role of Artificial Intelligence in Modern Systems

- ***Maj Prakash Bista*** *(prakashbst55@gmail.com)*

Abstract

The rapid advancement of Artificial Intelligence (AI) has fundamentally reshaped contemporary security systems, leading to significant improvements in surveillance, threat detection, and incident response across both physical and digital domains. By leveraging machine learning algorithms, neural networks, and predictive analytics, AI enhances the speed and precision of security operations while reducing human error and reliance on purely manual decision-making. In physical security contexts, AI-driven systems analyze real-time video feeds to detect anomalous behavior, identify individuals, and track suspicious movements with high accuracy. In digital security, AI supports malware detection, network intrusion prevention, and phishing mitigation through continuous learning from evolving threat patterns. Moreover, the integration of AI with big data analytics enables comprehensive risk assessment by processing large volumes of heterogeneous data, thereby facilitating early threat identification and proactive mitigation. Natural language processing techniques further contribute by detecting potential insider threats through the analysis of communication patterns and textual data. This paper adopts a qualitative, literature-based methodology grounded in thematic analysis. This paper draws on secondary data obtained from peer-reviewed journal articles, policy reports, and authoritative industry publications related to AI applications in security systems. The analysis synthesizes existing scholarship to identify dominant trends, operational benefits, and critical challenges associated with AI-driven security frameworks.

The central objective of this paper is to examine how AI is transforming modern security systems while critically assessing the ethical, legal, and governance challenges that accompany its adoption. The findings indicate that although AI significantly

enhances efficiency, predictive capability, and system resilience, persistent concerns related to data privacy, algorithmic bias, transparency, and over-reliance on automated decision-making continue to pose serious risks. This paper underscores the necessity of robust regulatory frameworks, transparent AI decision processes, and sustained human oversight to ensure responsible and trustworthy AI deployment. Ultimately, the paper argues that AI should be viewed not as a replacement for human judgment, but as an augmentative tool that strengthens security systems when embedded within ethical, legal, and organizational safeguards.

Keywords

Artificial Intelligence, Cyber Security, Machine Learning, Modern Security Systems, Predictive Analytics, Surveillance, Threat Detection

Introduction

The entire security industry is experiencing a massive transformation and one of the key factors responsible for it is the widespread adoption of Artificial Intelligence (AI) in both the physical and digital aspects of security. As cyber threats become more sophisticated and the need for securing large areas more intricate, traditional security systems that merely respond to issues are no longer sufficient (Goud, Chinnegowda, & Kaul, 2024). The classic types of security systems, whether they belong to cyberspace or the real world, are largely based on static rules and human vigilance. These methods are not that effective in discovering new or shifting dangers in real-time. However, AI comes with clever algorithms that learn from previous data, detect unusual behaviors, and intervene in time to prevent escalation of problems (Jaggi, Temkar, Nakirekanti, & Bhatt, 2024).

AI's scope includes technologies such as machine learning, deep learning, natural language processing, and predictive analytics. These tools reinforce security systems by detecting threats with a higher degree of certainty, analyzing the situation more accurately and giving more rapid responses (Craw Security, 2025). AI in physical security can go through the video footage, identify people, and notice the suspiciousness of behavior, thus elevating the alertness and shrinking the occurrence of false alarms support that AI could be assisting in the prevention of incidents through early actions (Goud et al., 2024). AI in cyber security is playing the role of a super human analyst by monitoring and analyzing data coming from different fronts, consequently detecting the hacking attempts before they could actually harm the system, taking down the entry points in the systems, and nullifying the phishing practices (Goud et al., 2024).

The combination of AI and big data analytics is a powerful tool in threat prediction prior to their actual manifestation, hence allowing the security to upgrade its role from just being reactive to problems to being preventive by stopping them ahead of time a (AI Said, 2025). The extremely rapid processing and understanding of different data types by AI is one main benefit in the area of security. This very feature helps to detect the elaborate threats consisting of multiple steps and also gets the chance to act (Zhand et al., 2022) quicker so that the threats would not cause any harm. One of the scenarios is that AI can still be in charge of monitoring the global threat information; besides, it can also compare the global with the local activity and in fact, subscribe to the information the security staff can use, all done in seconds. AI's continuous learning capability means that the security systems will be constantly aware of the emerging threats, thus becoming more resourceful as a result of time (Goud et al., 2024).

On the other hand, as in every other case of artificial intelligence use, there are difficulties in the security domain. One of the main problems is that the AI sometimes shows a tendency towards or against a particular group, which could result in discriminatory practices in polygraph tests, for example (AI Said, 2025). Besides, there is the possibility of a hacking attack on the AI system where the attackers take the advantage of feeding the AI with false information to confuse the system, therefore, the AI itself needs to be under very secure measures (Zhang et al., 2022). Another issue is concern about data privacy. The AI systems are using the personal data in huge amounts, and if proper regulations are not set, it could easily result in the sensitive information being misused (Craw Security, 2025). Moreover, the largest part of AI models is operating just like "Black Boxes," where it isn't possible to see inside what is going on, which makes it difficult to know precisely how the decisions are made, thus calling into question accountability and trust (Zhang et al., 2022).

The situation that calls for such a balanced and coordinated approach to the future of security where AI is properly and responsibly integrated in a powerful way that would be protective of everything from critical infrastructures to people and society at large. This paper examines the impact of AI on security, its pros, and cons, and how to design more secure and ethically acceptable systems for the future.

Thesis Statement

This paper argues that the integration of Artificial Intelligence into security systems represents a transformative shift that enhances the ability to predict, adapt to, and respond to threats across both physical and digital domains. However, it also contends that the full

potential of AI can only be realized through ethically grounded implementation, institutional transparency, and sustained human oversight, which are essential for mitigating risks related to algorithmic bias, privacy violations, and adversarial manipulation.

Review of Literature

Artificial Intelligence (AI) has been one of the most revolutionary shifts in the security technology industry. It brought about major changes like threat detection, incident response, and strengthening defenses. In December Mendes and Rios (2023) conducted a thorough review of literature with more than 2300 studies and proved the accessibility and application of AI in security as per NIST cyber security framework leading to detection, protection, response, and recovery. This indicates that AI can surpass the traditional rule while having system in both speed and accuracy. Thematic AI-based threat detection systems enable to be and make use of` machine learning (ML), deep learning (DL), and natural language processing (NLP), which has dramatically increased their capability for detection and management of the threats in real-time. Partnership Rahman, Hossain, Gony, and Rafy (2022) noticed that AI models were capable of identifying the atypical behavior in the network and then, preventing intrusions beforehand. Goud et al. (2024) claimed that the use of big data with AI can lead to predictive modeling thus making security more proactive rather than reactive. Explainable Artificial Intelligence (XAI) has become an important research topic mainly due to the need for transparency in the case of the "Black Box" AI models. According to Zhang et al. (2022), explain ability cultivates trust and guarantees that the artificial intelligence systems comply with legal and moral standards. Srivastava et al. (2022) argue that making the AI transparent diminishes bias and facilitates human oversight during sensitive decision-making processes.

Apart from cyber security, AI is also applied in areas such as physical security and social security. The study of Ahmad et al. (2022) demonstrates that artificial intelligence is incorporated into smart city surveillance systems, which utilize sensor data and video analysis for better environmental awareness. These systems, however, raise privacy and ethical concerns as they are involved in the recording and processing of very personal and sensitive information. According to the Security Convergence Council (2023), the integration of the physical and the digital realms of security are becoming increasingly significant with the proliferation of IoT and cyber-physical systems in the market. A considerable number of research works emphasize the positive side of AI in security; however, there is still a void in the area of long-term studies evaluating the robustness of

AI against attackers. In addition, the ethical concerns raised by Crawford (2024) in connection with military usage, reiterate the demand for regulatory frameworks that would promote innovation while also considering the impacts on humanitarian issues.

Research Gap

Numerous investigations have been conducted on the potential of Artificial Intelligence (AI) to enhance contemporary security systems; however, the majority of them have either concentrated on the advancement of AI algorithms or on their application in specific areas such as cyber-security or physical surveillance. Very few studies have taken an all-encompassing approach, which embraces both the physical and the digital, and thus, have become able to see the unified and predictive role that AI plays in the security systems of the future.

While AI imbues research with its capacity to detect weird activities, to recognize persons by face, and to prevent unauthorized access, it mostly neglects the discussion about the bigger, moral, legal and social, consequences, such as AI's decisions being fair, the process being transparent, and the question of who takes responsibility when mistakes are made. Besides, there is no attention given to the question of how vulnerable AI systems are to the types of attacks that are aimed at deceiving them, and how we might make AI explainable and usable in the day-to-day security environments. Moreover, the area of AI in security systems is still under-researched regarding its long-term benefits and implications, for instance, whether they lower the threat, get quicker in responding or make better decisions over the years. It is imperative to eradicate these voids in order to comprehend fully the conditions under which AI in security systems can be applied safely and effectively and, hence, let innovation take place along with the responsibility.

Research Methodology

This paper employs a qualitative research approach, specifically content analysis, to examine the application of Artificial Intelligence (AI) in contemporary security systems by analyzing existing literature and sources. A diverse range of materials (including books, academic journals, conference papers, credible news outlets, and reputable websites) was collected and systematically reviewed. This paper considers multiple dimensions of AI in security, encompassing cyber security, physical surveillance, threat detection, ethical considerations, and policymaking. To provide a comprehensive and nuanced understanding of both the benefits and challenges associated with AI in security, the gathered evidence was organized and categorized thematically. This methodology not only highlights technological advancements but also integrates social and ethical

perspectives, thereby offering a holistic framework that can inform future research, policy development, and practical implementation in the field of security.

Case Studies

AI has already made a significant impact on the security systems of the world, and its real-life applications are testament to that. Virtually every industry is utilizing AI in one way or another to handle security concerns more intelligently and efficiently. The case studies reflect the transformation created by AI in the domains of the cyber security industry, monitoring systems, and the related advantages and challenges of these new technologies.

Case Study I: AI in Financial Cyber security

An international financial institution has adopted advanced AI-driven cyber protection methods. Using machine learning to monitor network traffic and user activity, the system identifies abnormal behavior early, reducing false alarms by 40% and improving incident response time by 30%. This proactive approach enables the bank to shift from reactive security measures to predictive threat management, significantly enhancing its cyber security posture (Digital Defynd, 2025; AI Multiple, 2025).

Case Study II: AI in Smart City surveillance

A major city implemented an AI-based video analytics system for public safety. The system employs facial recognition and movement tracking to detect unusual activities in real-time. It helps identify high-density areas and potential risks, enabling faster police response. However, its use has also raised ethical and privacy concerns due to the continuous monitoring of public spaces (Business Insider, 2025).

Case Study III: AI in Disaster Response

In disaster-prone regions, AI is leveraged to improve emergency management. It integrates meteorological data, geographic information, and social media feeds to predict potential threats and coordinate evacuation. AI-powered drones assess damage in inaccessible areas, accelerating relief operations and ensuring the safety of rescue personnel (Ferrag et al., 2023).

Table 1

Comparative Table of AI Applications in Security

Case Study	Domain	AI Technologies Used	Key Benefits	Challenges / Concerns
I	Financial Cyber security	Machine Learning, Predictive Analytics	Early detection of anomalies, reduced false alarms (40%), faster incident response (30%), predictive threat management	Risk of system manipulation, reliance on high-quality data
II	Smart City Surveillance	Video Analytics, Facial Recognition	Real-time detection of suspicious behavior, improved public safety, faster police response	Privacy invasion, ethical concerns
III	Disaster Response	AI Analytics, Drones, Big Data	Predictive threat alerts, safe evacuation, faster damage assessment, improved rescue operations	Dependence on data accuracy, high operational cost

Source: Adapted from Ferrag et al. (2023)

Artificial Intelligence has fundamentally reshaped contemporary security systems across multiple domains. In financial cyber security, AI-driven machine learning and predictive analytics facilitate early detection of anomalies, minimize false positives, and accelerate incident response, effectively shifting operations from reactive to anticipatory. In smart city surveillance, advanced video analytics and facial recognition enhance real-time monitoring and situational awareness, although they introduce significant ethical and privacy considerations. In disaster response, AI integrates heterogeneous data sources to predict hazards, coordinate evacuations, and optimize rescue operations, thereby improving operational efficiency and decision-making. Despite these advancements, challenges including data quality dependency, algorithmic bias, and system vulnerabilities underscore the necessity for careful governance, ethical oversight, and sustained human supervision.

The Role of Artificial Intelligence in Modern Security Systems

Artificial Intelligence (AI) has emerged as a transformative force in modern security systems, fundamentally shifting security practices from reactive, rule-based models to proactive and predictive frameworks. By integrating machine learning, deep learning, and natural language processing techniques, AI-enabled systems can continuously analyze vast and heterogeneous data sources, detect anomalous patterns, and respond to potential threats in real time with greater speed and accuracy than traditional methods. This capability is particularly critical in high-risk sectors such as finance, healthcare, energy, and national security, where delayed responses can result in severe consequences. AI enhances threat detection and response by processing network logs, behavioral data, and intelligence reports at a scale beyond human capacity, enabling early intervention and minimizing operational, financial, and reputational damage. Real-world applications in financial institutions and digital platforms demonstrate AI's effectiveness in fraud prevention, compliance monitoring, and risk assessment, highlighting its practical value in operational environments. However, despite these advantages, the deployment of AI in security systems raises significant challenges, including data privacy risks, algorithmic bias, limited transparency in decision-making, and vulnerability to adversarial attacks designed to manipulate AI models. These concerns underscore the necessity of explainable and trustworthy AI frameworks, continuous system monitoring, robust regulatory oversight, and sustained human involvement in decision-making processes. Ultimately, AI should be understood not as a replacement for human judgment but as an augmentative tool that enhances security capabilities when embedded within ethical, legal, and organizational safeguards, thereby ensuring both effectiveness and accountability in modern security systems.

Thematic Analysis of AI-Driven Security Transformation

This paper constitutes its analytical core through a thematic examination of how Artificial Intelligence (AI) is transforming contemporary security systems. Drawing on established scholarly literature and documented industry practices, this paper analyzes AI's proactive role in security, enhanced threat detection and response capabilities, real-world applications across critical sectors, issues of explainability and ethical governance, and emerging technical and regulatory challenges. Rather than presenting original empirical data, this paper relies on a systematic synthesis of secondary sources to identify dominant patterns, operational implications, and structural limitations of AI-driven security frameworks, thereby offering a critical and integrative understanding of AI's role in modern security architectures.

AI as a Proactive Force in Security

The adoption of Artificial Intelligence has significantly transformed the security landscape from a predominantly reactive model to a proactive and predictive one. Traditional security systems largely depend on static rules and predefined signatures, which are increasingly inadequate in addressing complex and evolving threats (Zhou & Jin, 2022). In contrast, AI-enabled systems possess the capacity to continuously learn from data, adapt to changing threat environments, and respond to risks in real time.

Through machine learning (ML), deep learning (DL), and natural language processing (NLP), AI systems can identify abnormal patterns, detect early indicators of compromise, and reinforce defenses before an attack fully materializes (Ferrag et al., 2023; Wang et al., 2023). This shift is particularly critical in sectors such as healthcare, energy, and national security, where delayed responses or system failures can have severe consequences (Sharma et al., 2023; Kumar et al., 2022). Moreover, AI reduces human error by automating repetitive monitoring tasks, thereby enabling cyber security professionals to focus on complex, high-level decision-making (Papanastasiou, 2022; Ferrag et al., 2023).

Enhanced Threat Detection and Response

One of the most significant contributions of AI to modern security systems lies in its ability to enhance threat detection and response accuracy. AI systems can process and analyze vast volumes of data (such as network logs, behavioral records, and threat intelligence reports) that exceed human cognitive capacity (Berman et al., 2019). By employing predictive analytics, AI can anticipate potential attacks and mitigate them before they result in operational, financial, or reputational damage (PwC, 2017).

Advanced AI applications are increasingly embedded in next-generation Security Information and Event Management (SIEM) systems. These systems, often referred to as "Intelligent Security Operations (Sec Ops)," integrate automated investigation, behavioral analytics, and real-time threat correlation, transforming SIEM from a passive monitoring tool into an active defense mechanism (Tech Radar Pro, 2025). This evolution reflects a broader shift toward anticipatory security models that prioritize prevention over post-incident response.

Real-World Implementations of AI in Security

The practical relevance of AI in security is evidenced by its growing adoption across industries. Financial institutions, in particular, have integrated AI to strengthen fraud detection and regulatory compliance. For instance, HSBC has implemented AI-driven

monitoring systems to detect suspicious financial activities, resulting in reduced false positives and improved compliance efficiency (Digital Defynd, 2025). Similarly, Visa has employed AI to rapidly identify abnormal transaction patterns, preventing billions of dollars in fraudulent losses (AI Multiple, 2025).

Master Card's Decision Intelligence system further demonstrates the application of AI in real-time risk assessment by utilizing behavior-based analytics to prevent fraud while adhering to ethical governance standards (Business Insider, 2025). These cases, drawn from secondary literature, illustrate how AI enhances operational efficiency while also highlighting the need for responsible implementation.

Explain ability, Trust, and Ethical AI

Despite its advantages, AI in security systems is frequently criticized for operating as a "black box," where decision-making processes remain opaque and difficult to interpret. This lack of transparency raises concerns regarding accountability, trust, and legal responsibility. Explainable Artificial Intelligence (XAI) has therefore emerged as a critical research area aimed at making AI decisions understandable to human users (Barredo Arrieta et al., 2019). In intrusion detection contexts, explainable intrusion detection systems (X-IDS) are designed to generate interpretable alerts that support informed human judgment (Neupane et al., 2022). Broader frameworks such as "Trustworthy AI" emphasize transparency, accountability, and reliability, often incorporating privacy-preserving techniques such as federated learning, holomorphic encryption, and differential privacy to safeguard sensitive data.

Challenges and Future Considerations

Despite its transformative potential, AI-driven security systems face persistent challenges. Adversarial attacks (where malicious actors manipulate input data to deceive AI models) pose a serious threat to system reliability (Oseni et al., 2021). Additionally, AI deployment requires high-quality data, substantial computational resources, and skilled personnel, making implementation costly and technically demanding, particularly when integrating AI with legacy systems (Research Gate, 2023).

Emerging threats, including AI-powered phishing and automated social engineering, further complicate the security landscape. These developments underscore the risks associated with rapid AI deployment without adequate safeguards, potentially leading to privacy breaches and systemic vulnerabilities (Business Insider, 2025). Consequently, future security strategies must prioritize resilience, continuous auditing, and ethical governance alongside technological innovation.

Findings

The findings of this paper are derived from a qualitative, literature-based analysis of peer-reviewed research, policy documents, and institutional studies on the application of Artificial Intelligence in contemporary security systems. The analysis indicates that AI has fundamentally transformed security practices across both physical and digital domains by enhancing threat detection accuracy, analytical precision and real-time response capabilities. Through advanced machine learning algorithms and data-driven models, AI systems enable the early identification of anomalies and suspicious patterns, allowing potential threats to be addressed proactively before escalating into critical security incidents. This capability has strengthened overall system resilience, reduced dependence on reactive security measures, and improved operational robustness. The reviewed literature further demonstrates that AI plays a significant role in crisis detection and management by accelerating decision-making processes, enhancing situational awareness, and optimizing the allocation of security resources. By continuously learning from dynamic and heterogeneous data environments, AI-driven systems outperform traditional rule-based security frameworks that are constrained by static protocols and human cognitive limitations. As a result, security operations have increasingly shifted from reactive, post-incident responses to proactive and anticipatory models of threat management.

At the same time, the findings reveal several persistent challenges that limit the unrestricted or large-scale deployment of AI in security systems. A consistent concern across the literature relates to data privacy risks, algorithmic bias, and the limited transparency of AI decision-making processes. The opaque nature of many AI models raises critical issues of accountability and trust, particularly in high-stakes security contexts where decisions can have significant social, legal, and ethical consequences. In addition, the susceptibility of AI systems to adversarial attacks (where malicious actors deliberately manipulate inputs to deceive algorithms) emerges as a significant vulnerability, indicating that AI-enabled security systems may themselves become targets of sophisticated exploitation.

Overall, the findings suggest that while Artificial Intelligence has the potential to substantially enhance the effectiveness and adaptability of modern security systems, its success is not determined by technological capability alone. The literature consistently emphasizes that responsible governance, ethical safeguards, regulatory oversight, and sustained human involvement are essential to ensuring trustworthy and effective AI-driven security outcomes. Accordingly, AI should be understood not as a replacement for

human judgment, but as an augmentative tool that strengthens security capabilities when integrated within robust legal, ethical, and organizational frameworks.

Conclusion

Artificial intelligence is drastically altering the realm of security in both cyber and physical domains. It has the capability to process huge volumes of data within a very short time, identify minute issues, and advance itself through learning continuously. All these qualities combined make AI an indispensable element in the prevention of threats before they occur. It strengthens cyber security, elevates monitoring and enhances the efficiency of disaster response. The transition from simple reaction to threats to intelligent and predictive methods is a significant one. However, the transformation comes along with hurdles such as the moral challenges, privacy issues, biased algorithmic decisions, and the danger of being deceived by hackers. In order, to manage these concerns, it is required that we strengthen the technical barriers with lucid rules, ethical norms, and human supervision. The security future is dependent on collaboration among various sectors for the proper and safe utilization of AI. As the AI technology progresses, the question of how to incorporate it into security systems in a smart and equitable manner will determine the building of robust, adaptable, and trustworthy systems in a threat-laden world.

Recommendations

A thorough investigation of the influence of AI on the security area reveals that several ideas have popped up that are aimed at partially coping with the negative side of AI while at the same time reaping the beneficial ones. The first thing that comes to mind is that the policy makers and people in the security, technology, or other related industries should set a priority on building ethical guidelines that would be crystal clear and actually enforced so that AI in the security field will be controlled. Such regulations must address areas such as privacy, discrimination of one kind or another perpetrated by algorithms, and mistakes made by AI/people and thus, it is the public who will gradually come to trust the system.

The second idea is that AI's road to security should be bumpy but at least end-user friendly by investing more in the development of AI models that are the easiest to understand and at the same time the most transparent, which would facilitate human monitoring and decision-making. The third idea revolves around an even tighter collaboration among techies, security experts, philosophers, and lawyers to ensure that AI is deployed in an ethical and responsible manner. Fourth, security personnel should be given continuous training on using AI tools, recognizing their limitations, which would enhance their productivity as well as their ability to control the risks involved.

Finally, cutting-edge AI applications must undergo extensive assessments by skilled personnel on a routine basis to uncover potential vulnerabilities, stay updated with the attackers' tactics, and keep the ethical bar high. If these proposals are adhered to, the different stakeholders can resort to AI through the backdoor and with its light, maybe not always, but very frequently, they are going to be able to ensure security, thereby making it not only efficient but also just for the society in general.

References

AI Multiple. (2025). *Top 13 AI cyber security use cases with real examples*. https://aimultiple.com

Barredo Arrieta, A., Diaz-Rodriguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion, 58*, 82-115. https://doi.org/10.1016/j.inffus.2019.12.012

Berman, M., Bughin, J., Chui, M., Dobbs, R., Manyika, J., & Woetzel, J. (2019). The role of artificial intelligence in cyber security: Understanding the dynamics, impacts, and remediation. *Journal of Cyber Policy, 4*(2), 215-232. https://doi.org/10.1080/23738871.2019.1643210

Business Insider. (2025). *At Master Card, AI is helping to power fraud-detection systems*. https://www.businessinsider.com

Craw Security. (2025). *Artificial intelligence in cyber security: Trends and challenges*. https://www.crawsecurity.com

Crawford, K. (2024). *The atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.

Digital Defynd. (2025). *How HSBC uses artificial intelligence for fraud detection*. https://digitaldefynd.com

Ferrag, M. A., Maglaras, L., Janicke, H., Jiang, J., & Shu, L. (2023). AI-driven security: Redefining security information systems within digital governance. *International Journal of Research and Innovation in Social Science, 7*(3), 45-58.

Goud, M., Chinnegowda, P., & Kaul, S. (2024). Artificial intelligence in security systems: Applications and challenges. *International Journal of Cyber security and Digital Forensics, 13*(1), 1-14.

Jaggi, R., Temkar, S., Nakirekanti, M., & Bhatt, P. (2024). Machine learning approaches for modern cyber security threats. *Journal of Information Security and Applications, 76*, 103657. https://doi.org/10.1016/j.jisa.2023.103657

Mendes, R., & Rios, E. (2023). Artificial intelligence applications in cyber security: A systematic literature review aligned with the NIST framework. *Computers & Security, 124*, 102973. https://doi.org/10.1016/j.cose.2022.102973

Neupane, S., Ables, J., Anderson, W., Mittal, S., Rahimi, S., Banicescu, I., & Seale, M. (2022). Explainable intrusion detection systems (X-IDS): A survey of current methods, challenges, and opportunities. *ACM Computing Surveys, 55*(7), 1-38. https://doi.org/10.1145/3524496

Oseni, A., Moustafa, N., Janicke, H., Liu, P., Tari, Z., & Vasilakos, A. (2021). Security and privacy for artificial intelligence: Opportunities and challenges. *IEEE Access, 9*, 102537-102560. https://doi.org/10.1109/ACCESS.2021.3099069

Papanastasiou, Y. (2022). AI-driven security and its impact on governance and operational efficiency. *International Journal of Digital Governance, 4*(2), 89-105.

PwC. (2017). *Global state of information security survey*. Price water house Coopers.

Rahman, M., Hossain, M., Gony, M., & Rafy, M. (2022). Network anomaly detection using artificial intelligence techniques. *Journal of Network and Computer Applications, 198*, 103283. https://doi.org/10.1016/j.jnca.2021.103283

Research Gate. (2023). *Artificial intelligence and cyber security in the banking sector: Opportunities and risks*. https://www.researchgate.net

TechRadar Pro. (2025). *Redefining Sec Ops: The intelligent future of SIEM*. https://www.techradar.com

Zhang, Q., Yang, L. T., Chen, Z., & Li, P. (2022). A survey on explainable AI in security systems. *IEEE Transactions on Neural Networks and Learning Systems, 33*(11), 5895–5912. https://doi.org/10.1109/TNNLS.2021.3081548

Zhou, Y., & Jin, H. (2022). Theoretical foundations and models of AI-driven security in digital governance. *International Journal of Digital Governance, 4*(1), 21-38.