OPEN ACCESS
World Journal of Multidisciplinary Studies
ISSN (Online): 3049-0855 | Vol. 3, No. 5, May. 2026
Website: https://wasrpublication.com/index.php/wjms

A Systematic Survey of AI-Enhanced Cybersecurity in Saudi Arabia: Strategic Trends and Future Directions

Mohamed Geaiger*

Department of Management Information System, College of Business and Economics, Qassim University, Buraydah, Saudi Arabia.

Received: 14/02/2026 | Accepted: 19/04/2026 | Published: 26/05/2026

Abstract: Artificial intelligence (AI) has become a foundational component of modern cybersecurity systems, particularly in nations undergoing rapid digital transformation. This paper presents a condensed survey of AI-driven cybersecurity research and implementations in Saudi Arabia during the current mid-decade period. Through a meta-analysis of a substantial body of academic literature, this research delineates primary AI methodologies, industry implementations, and nascent obstacles. Findings show accelerated adoption of machine learning, deep learning, and hybrid models across critical sectors including healthcare, banking, cloud infrastructure, and smart cities. Key application areas include intrusion detection, malware analysis, fraud prevention, anomaly detection, and predictive threat intelligence. Despite significant progress, challenges persist in data quality, algorithmic bias, explainability, and infrastructure limitations. The paper concludes by outlining future research opportunities in federated learning, explainable AI, and sector-tailored security frameworks aligned with Saudi Vision 2030.

Keywords: Artificial Intelligence, Cybersecurity, Machine Learning, Intrusion Detection Systems, Saudi Vision 2030.

I. Introduction

Saudi Arabia's digital transformation under Vision 2030 has elevated cybersecurity to a national priority [3]. As cyber threats grow in sophistication—ranging from advanced persistent threats (APTs) to zero-day exploits—traditional rule-based defenses have become insufficient [4], [10], [27]. AI-driven cybersecurity systems offer predictive, adaptive, and automated capabilities that align with the Kingdom's expanding digital ecosystem. Over the contemporary five-year horizon, Saudi Arabia has experienced rapid adoption of AI-powered security solutions across healthcare, banking, government services, and cloud infrastructure [12], [19].This paper integrates findings from numerous peer-reviewed studies to provide a comprehensive overview of AI applications in Saudi cybersecurity, highlighting trends, challenges, and future directions [1], [2], [3]. It focuses on key AI techniques, application domains, institutional initiatives, challenges, and future research opportunities [2]. By synthesizing findings from different research work, it aims to provide insights for researchers, practitioners, and policymakers regarding the evolving landscape of AI-driven cybersecurity in the country.

II. Background

The evolution of cybersecurity threats within Saudi Arabia has shifted toward highly sophisticated methodologies, including stealth, automation, and polymorphism, which frequently bypass traditional signature-based detection systems [8], [11], [27]. Modern attackers are increasingly utilizing artificial intelligence to automate reconnaissance and exploit vulnerabilities, necessitating a transition toward intelligent, self-learning defense mechanisms [4], [18]. The theoretical foundation of AI-driven cybersecurity in the Kingdom relies on a combination of supervised, unsupervised, semi-supervised, and deep learning models designed for anomaly detection, pattern recognition, and predictive analytics to forecast attacks using historical data. Central to this shift is the Saudi Vision 2030 initiative, which prioritizes a secure digital transformation [3]. Under this mandate, the National Cybersecurity Authority (NCA) has established critical frameworks for AI adoption and data governance, effectively accelerating national investment in research, infrastructure, and workforce development to counter emerging threats.

III. Related Work

Recent scholarly efforts have extensively explored the integration of Artificial Intelligence (AI) within the Saudi Arabian cybersecurity landscape, reflecting a national strategic focus on secure digital transformation. While these studies provide valuable insights into sector-specific implementations, they are often limited by critical factors that this survey seeks to address:

1. Critical Infrastructure Protection: Research has examined the transition from traditional signature-based systems to AI-powered Intrusion Detection Systems (IDS) capable of identifying advanced persistent threats (APTs) and zero-day exploits [8], [11], [27]. However, much of this work remains focused on theoretical performance, frequently failing to account for the real-world computational costs that exceed the capabilities of many Saudi organizations.
2. Healthcare Security: Studies have developed deep learning models to protect Electronic Health Records (EHRs) and enhance insider-threat detection [1]. While technically robust, these models are often criticized for their lack of "explainability," making it difficult for medical practitioners to trust automated security

***Corresponding Author**

Mohamed Geaiger*

decisions and complicating compliance with strict national data-protection requirements.

3. Financial Fraud Mitigation: Literature highlights the leadership of Saudi banks in adopting machine learning for real-time fraud detection [2]. Nevertheless, existing research often overlooks the inherent risk of algorithmic bias, where models trained on imbalanced datasets may produce inaccurate or unfair security outcomes.
4. Smart Cities and IoT: Emerging research focuses on securing smart city systems and IoT devices within the Kingdom's expanding digital infrastructure [3],[28]. A significant gap in this area is the lack of standardized, sector-specific security frameworks, leading to fragmented implementations that struggle to adapt to the rapidly evolving threat landscape.
5. Technical Advancements: Contributions have proposed integrated approaches combining machine learning and deep learning—such as CNNs, LSTMs, and Transformers—to improve detection accuracy [22],[12]. Despite high accuracy in laboratory settings, these studies frequently suffer from a scarcity of high-quality, labeled local datasets, which limits the practical applicability of the models.
6. Based on the systematic survey of AI-driven cybersecurity in Saudi Arabia (2022–2026), the following table compares the Strengths (Strong points) and Weaknesses (Weak points) of the current landscape.

Table 1: Comparing the Strengths and Weaknesses of current models

7. Feature	***8. Strengths (Strong Points)***	***9. Weaknesses (Weak Points)***
Detection & Response [15],[23]	Proactive Defense: AI systems achieve up to 95% detection accuracy, identifying Advanced Persistent Threats (APTs) and zero-day exploits that traditional systems miss.	False Positives: High sensitivity in anomaly detection can lead to "alert fatigue," where security teams are overwhelmed by non-threatening flags.
Automation [2]	Operational Efficiency: Automated Incident Response (AIR) has reduced threat resolution times by approximately 50%, with SOCs automating over 70% of routine tasks.	Over-reliance on Automation: Excessive trust in automated systems can lead to "automation bias," where human oversight misses subtle logic-based attacks that AI fails to categorize.
Strategic Framework [1],[2],[3],[5]	National Alignment: Strong integration with Saudi Vision 2030 and NCA frameworks provides a clear regulatory and investment roadmap for AI adoption.	Regulatory Lag: The rapid pace of AI evolution sometimes outstrips the development of specific governance policies, particularly in emerging areas like Generative AI.
Technological Implementation [7],[22],[24],[6],[8]	Advanced Techniques: Widespread use of Deep Learning (CNNs, LSTMs) and hybrid models across healthcare, banking, and smart cities (e.g., NEOM).	Infrastructure Costs: High computational and energy requirements for training advanced deep learning models exceed the budget and hardware limits of smaller organizations.
Data & Privacy [2], [5]	Centralized Intelligence: Effective use of "Threat Lakes" to aggregate national-level data for predictive analytics and pattern recognition.	Data Quality & Sovereignty: Challenges with imbalanced datasets and strict data-sovereignty laws can limit the training of robust, localized AI models.
Human Capital [2]	Upskilling Initiatives: Massive government-led training programs (SDAIA/NCA) are rapidly closing the technical gap for thousands of professionals.	Specialized Talent Gap: Despite training efforts, there remains a critical shortage of high-level experts in niche subfields like Explainable AI (XAI) and Adversarial Machine Learning.
Security Architecture [4], [15]	Zero Trust Integration: Over 60% of large businesses have successfully integrated AI-driven Zero Trust Architecture (ZTA) to secure remote and cloud environments.	Explainability (Black Box): The lack of transparency in deep learning decision-making makes it difficult to audit security actions in highly regulated sectors like banking.

Summary of Analysis

The strengths of the Saudi landscape are primarily driven by strong institutional leadership and high-performance automation, which have positioned the Kingdom as a global leader in cybersecurity indices table 1. Conversely, the weaknesses are rooted in technical transparency and resource barriers, highlighting a need for future focus on Explainable AI (XAI) and Federated Learning to ensure a more inclusive and trustworthy security ecosystem.

IV. Methodology

We utilized multiple digital repositories, including Google Scholar, ArXiv, and various SciSpace search tools, to conduct a systematic review of existing research. From a comprehensive

initial pool of candidates, we selected a curated sample of unique papers focusing on AI-driven cybersecurity in Saudi Arabia. Our analytical approach adhered to a rigorous four-phase protocol: assessing relevance, applying thematic codes, performing a comparative analysis, and synthesizing the final findings.

V. Results and Discussion

1. A. Sector-Specific Implementations
    a. Healthcare: Deep learning models enhance insider-threat detection and secure electronic health records. Major challenges include legacy system integration and strict data-protection requirements [1].
    b. Banking and Financial Services: Saudi banks lead in AI adoption for identity verification and fraud prevention. Barriers include infrastructure limitations and algorithmic bias concerns [2].
    c. Cloud and Digital Infrastructure: AI-powered anomaly detection and IDS support secure cloud migration and compliance with data-sovereignty regulations [3].
2. B. AI Techniques Used in Saudi Cybersecurity
    a. Machine Learning: SVM, Random Forest, and Decision Trees are utilized for traffic classification, while KMeans and PCA are employed for anomaly detection [4], [12].
    b. Deep Learning: CNNs are applied for malware classification, LSTM/RNNs for sequential log analysis, and Transformers for NLP-based threat intelligence [1], [11], [14], [22], [28].
    c. Hybrid and Optimization Models: Combining ML and DL improves accuracy, while genetic algorithms and Flamingo Search optimize model performance [9], [22].
3. C. Application Areas AI-powered Intrusion Detection Systems (IDS) outperform traditional systems in detecting APTs and zero-day attacks. Malware detection is enhanced through CNN-based classification and behavioral analysis. For proactive defense, predictive analytics and automated threat hunting enable advanced detection. Real-time fraud detection and anomaly detection are widely applied across financial and network environments [5], [6], [7], [8], [28], [29], [30]. Finally, AI is critical in securing smart city systems and IoT devices within Saudi Arabia's smart infrastructure.

VI. Challenges

Significant infrastructure limitations exist, as high computational requirements for deep learning models often exceed the capabilities of some Saudi organizations. Data quality and availability issues, including imbalanced datasets and privacy concerns, continue to hinder model performance. Furthermore, algorithmic bias and a lack of explainability in deep learning models complicate regulatory compliance in critical sectors like banking and healthcare.

VII. Future Work

Future research will focus on federated learning to enable collaborative model training without sharing sensitive data. The advancement of Explainable AI (XAI) is essential for regulatory compliance and building stakeholder trust [17], [20], [27]. There is a growing need for sector-specific AI security frameworks tailored for healthcare, banking, and smart cities. Additionally, the development of adaptive and autonomous security systems will focus on self-learning mechanisms capable of real-time adaptation to emerging threats.

VIII. Conclusion

AI has become a cornerstone of Saudi Arabia's cybersecurity transformation. During this intensive period of digital evolution, significant progress was made in deploying machine learning, deep learning, and hybrid models across critical sectors. While challenges persist—particularly in data quality, explainability, and infrastructure—the trajectory is strongly aligned with Vision 2030. Future research should focus on federated learning, explainable AI, and sector-specific frameworks to ensure secure, resilient, and trustworthy digital ecosystems.

References

1. Aljaramiz, A., et al. (2025). Deep learning-driven cybersecurity threat detection and mitigation in Saudi Arabia healthcare system. In *Proceedings of ITIKD 2025*. IEEE. https://doi.org/10.1109/ITIKD63574.2025.11004975
2. Eskandarany, A. (2024). Adoption of artificial intelligence and machine learning in banking systems: A qualitative survey of board of directors. *Frontiers in Artificial Intelligence*. https://doi.org/10.3389/frai.2024.1440051
3. Kayani, M. (2024). *AI driven cloud security and anomaly detection in Saudi Arabia: A strategic enabler of Vision 2030 digital transformation (Revised version–updated after peer review)*.
4. Thallam, R. (2024). AI-powered cybersecurity: How machine learning is redefining threat detection and prevention. *Indian Scientific Journal of Research in Engineering and Management*. https://doi.org/10.55041/IJSREM40041
5. Intrusion detection for softwarized networks with semi-supervised federated learning. (2022). In *ICC 2022 – IEEE International Conference on Communications*. IEEE. https://doi.org/10.1109/ICC45855.2022.9839042
6. Alsamir, A., et al. (2024). Anomaly-based intrusion detection systems using machine learning. *Journal of Cybersecurity and Information Management, 14*(1). https://doi.org/10.54216/jcim.140102
7. Jin, Y. (2024). Machine learning and big data analytics for cyber security intrusion detection. In *Proceedings of ICCASIT 2024*. IEEE. https://doi.org/10.1109/ICCASIT62299.2024.10828110
8. Alshahrani, H., et al. (2022). Adversarial attacks against supervised machine learning based network intrusion detection systems. *PLOS ONE*. https://doi.org/10.1371/journal.pone.0275971
9. Alajmi, M., et al. (2023). Automated threat detection using flamingo search algorithm with optimal deep learning on cyber-physical system environment. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3332213
10. Rahman, M., et al. (2025). Application of artificial intelligence in detecting and mitigating cyber threats.

International Research Journal of Innovations in Engineering and Technology, 9(1). https://doi.org/10.47001/irjiet/2025.901003

11. Alzahrani, A., et al. (2022). Detecting the presence of malware and identifying the type of cyber attack using deep learning and VGG-16 techniques. *Electronics, 11*(22), 3665. https://doi.org/10.3390/electronics11223665
12. Chen, X., et al. (2024). Threat detection driven by artificial intelligence: Enhancing cybersecurity with machine learning algorithms. *World Journal of Innovation and Modern Technology, 7*(6). https://doi.org/10.53469/wjimt.2024.07(06).09
13. Patel, R. (2023). Leveraging AI and machine learning for cyber threat analysis. *Journal of Artificial Intelligence in Cloud Computing, 2*. https://doi.org/10.47363/JAICC/2023(2)e205
14. Moamin, M., et al. (2025). Artificial intelligence in malware and network intrusion detection: A comprehensive survey of techniques, datasets, challenges, and future directions. *Bangladesh Journal of Artificial Intelligence*. https://doi.org/10.58496/bjai/2025/008
15. Pujari, S. (2025). AI-powered cybersecurity: A unified approach to protecting enterprise, cloud, and SaaS applications. *International Research Journal of Advanced Engineering and Hub*. https://doi.org/10.47392/IRJAEH.2025.0445
16. Zhang, L. (2025). Research progress on network security threat detection and defense technology based on artificial intelligence. *Applied and Computational Engineering*. https://doi.org/10.54254/2755-2721/2025.tj23838
17. Talati, M. (2024). Enhancing cybersecurity and privacy using artificial intelligence: Trends and future directions of research. *International Journal of Innovative Research in Science, Engineering and Technology, 13*(1). https://doi.org/10.15680/IJIRSET.2024.1301007
18. Uzoka, F., et al. (2024). Applying artificial intelligence in cybersecurity to enhance threat detection, response, and risk management. *Computer Science and IT Research Journal, 5*(10). https://doi.org/10.51594/csitrj.v5i10.1677
19. Nnaka, C., et al. (2025). AI-powered threat detection: Opportunities and limitations in modern cyber defense. *World Journal of Advanced Research and Reviews, 27*(2). https://doi.org/10.30574/wjarr.2025.27.2.2854
20. Thapaliya, S. (2025). Artificial intelligence and cybersecurity: Pioneering next-generation protection strategies. *SADGAMAYA, 2*(1). https://doi.org/10.3126/sadgamaya.v2i1.80334
21. Polinati, R. (2025). AI and deep learning-powered threat intelligence and automated response mechanisms. In *Proceedings of ICSCDS 2025*. IEEE. https://doi.org/10.1109/ICSCDS65426.2025.11167069
22. Nguyen, T., et al. (2023). Using machine learning and deep learning to improve anomaly attack. *Journal of Southwest Jiaotong University, 58*(4). https://doi.org/10.35741/issn.0258-2724.58.4.40
23. Vashishth, P., et al. (2025). AI-driven threat detection and incident response. In *Advances in Computational Intelligence and Robotics Book Series*. https://doi.org/10.4018/979-8-3373-2115-8.ch003
24. Parihar, R. (2025). Investigating the impact of artificial intelligence on cybersecurity threat detection and response mechanisms. *International Journal of Innovative Science and Research Technology*. https://doi.org/10.38124/IJISRT/24NOV1610
25. Kaur, P., et al. (2025). AI-powered threat detection. *NBE Nnuraicr, 5*. https://doi.org/10.58532/nbennuraicr5
26. Sankaram, S., et al. (2024). A comprehensive review of artificial intelligence applications in enhancing cybersecurity threat detection and response mechanisms. *Journal of Business Economics and Digital Product Management, 3*(5). https://doi.org/10.62304/jbedpm.v3i05.180
27. Olafuyi, A. (2023). Artificial intelligence in cybersecurity: Enhancing threat detection and mitigation. *International Journal of Scientific and Research Publications, 13*(12). https://doi.org/10.29322/IJSRP.13.12.2023.p14419
28. Schmitt, J. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. *Social Science Research Network*. https://doi.org/10.2139/ssrn.4397870
29. Gupta, R., et al. (2023). *Machine learning in finance: Risk management, trading, and fraud detection*. Zenodo. https://doi.org/10.5281/zenodo.8167962
30. Cyber security using machine learning techniques. (2023). *Advances in Computer Science Research*. https://doi.org/10.2991/978-94-6463-136-4_59