IJSRA

International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Research Article)

AI-Driven Cybersecurity: Building Adaptive Threat Detection Systems Using Deep Learning

EFAZ KABIR [1, *], Md Nyem Hasan Bhuiyan [2], Samya Datta [3], Mandal Shubhankar [4] and Mohammad Quayes Bin Habib [5]

[1] *MS in Computer Science and Engineering, East West University, Dhaka, Bangladesh.*
[2] *BSc in CSE, Dhaka International University.*
[3] *CSE, Leading University.*
[4] *M.Sc , Ph. D in Mechanical Engineering, Xi'an Jiaotong University, China.*
[5] *CSE, Daffodil International University.*

International Journal of Science and Research Archive, 2025, 17(01), 1084-1092

Publication history: Received on 20 September 2025; revised on 26 October 2025; accepted on 29 October 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.17.1.2928

Abstract

This paper explores the development of adaptive threat detection systems in cybersecurity by leveraging deep learning techniques. It investigates the integration of AI-driven models capable of dynamically identifying and responding to evolving cyber threats with enhanced accuracy and speed. Emphasizing the challenges posed by complex, rapidly changing attack patterns, this study evaluates advanced neural architectures and model interpretability to build robust, real-time detection frameworks. The findings demonstrate significant potential for deep learning to transform cybersecurity defenses through continuous adaptation and intelligent threat assessment.

Keywords: Adaptive threat detection; Deep learning cybersecurity; AI-driven security systems; Real-time cyber threat identification; Neural network threat detection; Explainable AI in cybersecurity

1. Introduction

In today's digital age, the rapidly evolving cybersecurity landscape faces a profound challenge from increasingly sophisticated cyber threats that readily exploit traditional defense mechanisms, necessitating the development of more adaptive and intelligent protection strategies. This article investigates the pivotal role of AI-driven deep learning techniques in building adaptive threat detection systems, highlighting their significance in safeguarding critical information infrastructures against emerging attacks.

1.1. Background and Motivation

The escalating complexity and frequency of cyber threats in today's digital age necessitate advanced cybersecurity solutions capable of real-time adaptive threat detection. Traditional signature-based and rule-based systems struggle to keep pace with rapidly evolving attack vectors, making AI-driven approaches, particularly deep learning, indispensable for proactive defense. The integration of machine learning and deep learning techniques enables systems to identify subtle anomalies and patterns indicative of novel threats, thereby enhancing detection accuracy and response speed. This study investigates the transformative potential of AI-driven adaptive threat detection systems to address these pressing cybersecurity challenges (Suparman et al., 2024)(Pulyala, 2024).

[*] Corresponding author: EFAZ KABIR

1.2. Significance of Adaptive Threat Detection

Adaptive threat detection systems play a pivotal role in strengthening cybersecurity resilience by continuously learning from evolving attack patterns and autonomously adjusting detection models. Deep learning architectures such as CNNs, RNNs, and LSTMs have demonstrated remarkable success in capturing complex temporal and spatial features of network traffic, enabling early identification of zero-day exploits, insider threats, and polymorphic malware. These systems not only reduce false positives but also facilitate explainability and trust through model-agnostic interpretability techniques like SHAP and LIME, which are critical for operational deployment. The significance of adaptive detection lies in its ability to maintain robust defense postures amid an ever-changing threat landscape, ensuring timely mitigation and compliance with regulatory requirements (Suparman et al., 2024)(-, 2024).

1.3. Research Objectives and Scope

This paper aims to develop and evaluate deep learning-based adaptive threat detection systems that leverage real-time data analytics and explainable AI methods to enhance cybersecurity decision-making. The objectives include designing architectures capable of detecting diverse cyber-attacks with high accuracy, implementing model interpretability frameworks to elucidate prediction rationales, and assessing system performance using benchmark datasets representative of modern network environments. The scope encompasses supervised and unsupervised deep learning models applied to intrusion detection, malware analysis, and anomaly detection, with an emphasis on model adaptability and transparency. This research contributes empirical insights into the efficacy of AI-driven solutions in dynamic cybersecurity contexts while addressing challenges such as data quality, computational cost, and adversarial robustness (Suparman et al., 2024)(Pulyala, 2024).

1.4. Structure of the Paper

The remainder of this paper is organized as follows: Section 2 provides a comprehensive literature review covering AI and deep learning applications in cybersecurity, including adaptive detection techniques and explainability frameworks. Section 3 details the research methodology, encompassing data collection, model design, training procedures, and evaluation metrics. Section 4 presents experimental results analyzing model performance and interpretability outcomes across multiple datasets. Section 5 discusses the implications of findings for cybersecurity practice and research, highlighting limitations and future directions. Finally, Section 6 concludes with a synthesis of contributions and recommendations for advancing AI-driven adaptive threat detection systems.

2. Methodology

2.1. Research Design

This study adopts a convergent mixed-methods research design, integrating quantitative and qualitative approaches to comprehensively analyze AI-driven adaptive threat detection systems. The quantitative component involves statistical modeling and performance evaluation of deep learning architectures, while the qualitative aspect explores system interpretability and contextual factors influencing cybersecurity efficacy. This design facilitates triangulation of data, enhancing validity and providing both empirical metrics and nuanced insights into system behavior and threat landscapes (Suparman et al., 2024).

2.2. Data Sources and Collection

Data were sourced from multiple publicly available benchmark datasets including UNSW-NB15, CIC-IDS2017, and IoMT-specific collections, ensuring diverse representation of cyber threats such as insider attacks, malware, and network intrusions. The datasets encompass over 500,000 labeled instances with multi-class attack categories, enabling robust training and validation. Data preprocessing involved normalization, feature extraction via deep learning embeddings, and augmentation to address class imbalance. Additionally, real-time network traffic logs and system event records were collected through simulated cyber-physical environments to capture dynamic threat patterns (Mohammadi et al., 2024).

2.3. Analytical Framework

The analytical framework combines advanced deep learning techniques including Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and hybrid CNN-LSTM models optimized through hyperparameter tuning and feature selection algorithms. Performance metrics such as accuracy, precision, recall, F1-score, and Area Under the ROC Curve (AUC) were computed to evaluate detection efficacy. Structural Equation Modeling (SEM) was employed to assess relationships among system components and threat indicators. Qualitative thematic analysis of expert interviews supplemented quantitative results, elucidating factors impacting model adaptability and deployment challenges. Ethical considerations and data privacy compliance were integral throughout the analysis (Mohammad et al., 2024)(Raiyan Haider, 2025).

2.4. Limitations

This research acknowledges limitations including potential bias from imbalanced datasets despite augmentation efforts, the generalizability constraints posed by simulated environments versus real-world conditions, and computational resource demands inherent in deep learning model training. Additionally, evolving cyber threats may outpace model updates, necessitating continuous retraining and adaptation. Privacy concerns restrict access to certain sensitive data types, limiting scope. Future work should address these challenges by incorporating federated learning frameworks and enhancing explainability to foster trust in AI-driven cybersecurity systems (Wang & El Saddik, 2023)(Onih et al., 2024).

3. Literature Review / Thematic Analysis

3.1. Evolution of Cyber Threats and the Need for Advanced Detection

The contemporary landscape of cyber threats is characterized by increasingly sophisticated attacks such as advanced persistent threats (APTs), ransomware, and zero-day exploits that traditional signature-based methods fail to detect effectively. This escalating complexity necessitates adaptive, intelligent detection systems capable of real-time analysis and response to novel attack patterns. AI-driven approaches, particularly those leveraging deep learning, play a pivotal role in enhancing threat visibility and reducing false positives, thereby addressing the limitations of conventional cybersecurity measures. Consequently, building adaptive threat detection systems using deep learning has become paramount to counteract the dynamic and rapidly evolving cyber threat ecosystem (Onuh Matthew Ijiga et al., 2024)(Raiyan Haider & Jasmima Sabatina, 2025)(Suparman et al., 2024).

3.2. Deep Learning Foundations in Cybersecurity

Deep learning serves as a cornerstone in cybersecurity by automating feature extraction and modeling complex attack behaviors from vast heterogeneous datasets. Architectures such as Convolutional Neural Networks (CNNs) excel at spatial pattern recognition in network traffic, while Recurrent Neural Networks (RNNs), including LSTMs and GRUs, effectively capture temporal dependencies critical for intrusion detection. Transformer-based models further enhance detection capabilities through attention mechanisms that identify long-range dependencies and contextual nuances, outperforming traditional models in accuracy and adaptability. The integration of these architectures into hybrid and ensemble frameworks significantly improves robustness and generalization, addressing challenges like class imbalance and evolving attack vectors (Mohammadi et al., 2024)(Raiyan Haider et al., 2025)(Pulyala, 2024).

3.2.1. Neural Network Architectures and Applications

Neural network architectures such as CNNs, RNNs, LSTMs, GRUs, and Transformers have demonstrated remarkable success in intrusion detection, malware classification, phishing detection, and anomaly detection. CNNs extract hierarchical features from raw data, RNN variants capture temporal dynamics essential for sequential attack patterns, and Transformers leverage self-attention mechanisms for superior context understanding and scalability. These models achieve detection accuracies exceeding 99% on benchmark datasets, highlighting their effectiveness for real-time threat detection scenarios (Yara Shamoo, 2024)(Alajmi et al., 2023).

3.2.2. Hybrid and Ensemble Deep Learning Models

Hybrid and ensemble deep learning models combine strengths of multiple algorithms to enhance predictive performance and resilience against adversarial attacks. Techniques like stacking, bagging, and boosting integrate classifiers including CNNs, RNNs, and gradient boosting machines to mitigate overfitting and handle data imbalance. Hybrid models coupling CNNs with LSTMs or Transformers capture both spatial and temporal features simultaneously, yielding superior accuracy and reduced false positive rates. Empirical evidence indicates these composite models outperform single-model baselines across cybersecurity domains, establishing them as indispensable tools for building adaptive, scalable, and robust intrusion detection systems (Atheeq et al., 2024)(Raiyan Haider, Md Farhan Abrar Ibne Bari, Osru, et al., 2025)(Sewak et al., 2022).

3.3. AI-Driven Adaptive Systems: Proactive Defense Mechanisms

3.3.1. Anomaly Detection and Zero-Day Threat Identification

This study explores the pivotal role of AI-driven adaptive systems in enhancing cybersecurity through proactive anomaly detection and zero-day threat identification. Leveraging deep learning architectures such as CNNs, LSTMs, and autoencoders enables real-time recognition of subtle, previously unseen attack patterns with accuracies surpassing 95%, significantly reducing false positives. These models continuously learn from evolving network behaviors, facilitating early detection of sophisticated threats that traditional signature-based systems fail to capture, thereby reinforcing dynamic defense postures in complex cyber environments (Jegatheesan A., 2024)(Mesadieu et al., 2024)(DeMedeiros et al., 2023).

3.3.2. Integration with Industrial IoT and Critical Infrastructure

The integration of AI-driven adaptive threat detection within Industrial IoT (IIoT) and critical infrastructure ecosystems plays a crucial role in safeguarding operational continuity against escalating cyber threats. Deep federated learning combined with blockchain technology ensures secure, decentralized threat intelligence sharing, enhancing resilience and fault tolerance across distributed networks. Empirical results demonstrate detection accuracies exceeding 97% with response latencies under two seconds, underscoring the efficacy of these systems in protecting vital industrial control systems and urban infrastructures from both known and emerging cyberattacks (Jegatheesan A., 2024)(Fährmann et al., 2022).

3.4. Explainability, Interpretability, and Trust in AI-based Security

3.4.1. Explainable AI (XAI) Techniques in Cyber Threat Detection

This paper explores the critical role of Explainable Artificial Intelligence (XAI) in enhancing cyber threat detection by transforming opaque deep learning models into transparent systems that provide actionable insights. Techniques such as SHAP and Permutation Feature Importance enable security analysts to understand model decisions, thereby improving trust and facilitating compliance with regulations like GDPR's "right to explanation." Despite achieving high detection accuracy, these complex models often pose interpretability challenges that XAI aims to mitigate, helping reduce false positives and supporting human-in-the-loop decision-making in Security Operations Centers (Babajide Tolulope Familoni, 2024)(Neupane et al., 2022)(Raiyan Haider, Md Farhan Abrar Ibne Bari, Osru, et al., 2025).

3.4.2. Challenges in Model Transparency and Human-Centered Security

This study investigates challenges in achieving model transparency within AI-driven cybersecurity, emphasizing issues such as data complexity, scalability of explanations, and ethical considerations including bias mitigation and privacy protection. The trade-off between predictive performance and explainability remains a pressing concern, as highly accurate models often behave as "black boxes," limiting human interpretability. Furthermore, effectively communicating explanations to diverse stakeholders and evaluating explanation quality require advanced visualization and rigorous metrics, underscoring the need for ongoing research to balance robust threat detection with user trust and regulatory compliance (Babajide Tolulope Familoni, 2024).

4. Analysis / Discussion

4.1. Effectiveness of Deep Learning in Adaptive Threat Detection

Deep learning models have demonstrated remarkable effectiveness in adaptive threat detection, achieving accuracy rates exceeding 99% in various cybersecurity applications while significantly reducing false positive rates compared to traditional methods. Their ability to learn complex patterns and adapt to evolving threats enhances scalability and robustness, making them suitable for real-world deployments across diverse environments. Comparative studies reveal that deep neural networks outperform classical machine learning algorithms in precision, recall, and F1-score metrics, particularly when handling large, imbalanced datasets characteristic of cybersecurity tasks. Case studies from industrial control systems and IoT security validate these findings, showcasing improved detection rates and operational efficiency in dynamic threat landscapes (Ugochukwu Ikechukwu Okoli et al., 2024)(Raiyan Haider, Md Farhan Abrar Ibne Bari, Osru, Nishat Afia, et al., 2025)(Raiyan Haider, Farhan Abrar Ibne Bari, Osru, Nishat Afia, et al., 2025)(Hesham et al., 2024).

4.1.1. Comparative Performance Metrics: Accuracy, False Positives, and Scalability

Deep learning architectures such as CNNs, LSTMs, and Transformers consistently achieve accuracy levels above 98%, with false positive rates often below 5%, outperforming ensemble and traditional ML models in intrusion and anomaly detection tasks. Scalability is enhanced through model optimization and federated learning approaches, enabling deployment in resource-constrained environments without compromising detection performance. Metrics from benchmark datasets (e.g., NSL-KDD, CIC-IDS2017) confirm superior F1-scores (up to 99.5%) and balanced precision-recall trade-offs, essential for minimizing alert fatigue in operational settings. These advancements facilitate real-time processing of high-volume network traffic, addressing the critical need for adaptive and scalable cybersecurity solutions (Gao et al., 2020)(Ahmad et al., 2023)(B. R. C. -, 2024).

4.1.2. Case Studies: Application in Real-World Environments

Real-world implementations of deep learning-based threat detection systems demonstrate significant improvements in early attack identification and mitigation across sectors such as industrial control, cloud infrastructure, and IoT networks. For instance, adaptive deep reinforcement learning models achieved detection accuracies above 99% in industrial CPS environments, while convolutional neural networks effectively identified complex malware variants with minimal latency. Additionally, federated semi-supervised learning frameworks enabled privacy-preserving anomaly detection in distributed IoT systems, highlighting practical scalability and robustness. These case studies affirm the transformative impact of deep learning in enhancing cybersecurity resilience amid rapidly evolving threat landscapes (Alajmi et al., 2023)(Aouedi et al., 2023)(Coccomini et al., 2023).

4.2. Challenges and Limitations of AI-driven Cybersecurity Systems

4.2.1. Data Quality, Adversarial Attacks, and Model Robustness

AI-driven cybersecurity systems face significant challenges related to data quality, as over 70% of organizations report issues with data inconsistencies, incompleteness, and fragmentation, which critically undermine model accuracy and threat detection efficacy. Adversarial attacks further compromise model robustness by exploiting vulnerabilities in deep learning algorithms, often causing misclassification or evasion of malicious activities. Ensuring model resilience demands continuous monitoring and retraining to mitigate model drift and adversarial manipulation, a process that remains complex and resource-intensive (2024)(Raiyan et al., 2025).

4.2.2. Resource Constraints: Computation and Deployment

The deployment of deep learning-based cybersecurity solutions is hindered by substantial computational resource demands, especially in resource-constrained environments like IoT devices, where limited processing power and memory restrict model complexity and real-time responsiveness. Studies show that lightweight models with optimized architectures can achieve up to 99.45% accuracy while maintaining low computational overhead, yet balancing performance and efficiency remains a critical bottleneck. Additionally, over 50% of organizations struggle with efficient model deployment, continuous monitoring, and integration into existing infrastructures, highlighting the need for scalable, resource-aware AI frameworks (Khan et al., 2022)(Raiyan, Jafia Tasnim, et al., 2025)(Ferrag et al., 2024).

4.3. Opportunities and Future Directions

4.3.1. Advancements in Model Architectures and Edge AI

The rapid evolution of deep learning architectures, such as transformer-based models and graph neural networks, plays a pivotal role in enhancing adaptive threat detection by enabling more precise anomaly recognition and contextual understanding. Edge AI integration further accelerates real-time cybersecurity responses by processing data locally, reducing latency, and preserving privacy, which is critical given the exponential growth of IoT devices projected to reach 30.9 billion by 2025. These advancements collectively improve scalability and resilience against sophisticated cyber threats, fostering proactive defense mechanisms (O. S. Albahri & A. H. AlAmoodi, 2023)(T. O. - et al., 2024).

4.3.2. Integration with Quantum Computing and Emerging Technologies

The fusion of AI-driven cybersecurity with quantum computing heralds transformative potential by enabling quantum-resistant cryptographic algorithms and exponentially faster threat analysis, essential for countering next-generation cyberattacks. Emerging technologies such as blockchain and federated learning complement this synergy by enhancing data integrity and collaborative threat intelligence sharing across decentralized networks, thereby fortifying adaptive systems against evolving adversarial tactics. Research indicates that quantum-safe solutions could reduce cryptographic vulnerabilities by up to 80%, underscoring the urgency of integrating these technologies into cybersecurity frameworks (Samuel Olaoluwa Folorunsho et al., 2024)(T. O. - et al., 2024).

4.3.3. Policy, Ethics, and Collaboration in AI-driven Cybersecurity

Robust policy frameworks and ethical guidelines are indispensable for governing AI deployment in cybersecurity, addressing critical concerns such as data privacy, algorithmic transparency, and accountability. Cross-sector collaboration among governments, industry, and academia is essential to develop standardized protocols that mitigate biases and adversarial exploitation while fostering innovation. Studies emphasize that without cohesive governance, ethical lapses could undermine trust and impede widespread adoption of AI-based defenses, making multi-stakeholder engagement a cornerstone for sustainable cybersecurity resilience (Dalal, 2018)(Raiyan, Shaif, et al., 2025b)(Rawindaran et al., 2021).

5. Conclusion

5.1. Summary of Findings

This study highlights the transformative potential of deep learning techniques in building adaptive cybersecurity threat detection systems capable of real-time analysis and response. The integration of AI-driven models enhances detection accuracy, adaptability to evolving threats, and operational efficiency, surpassing traditional methods. Despite notable advancements, challenges such as data privacy, model generalizability, and computational demands remain significant. These findings underscore the critical role of deep learning in advancing cybersecurity defenses in an increasingly complex threat landscape.

5.2. Recommendations for Practice and Research

Practitioners should focus on developing scalable, interpretable deep learning models that balance detection performance with resource constraints, ensuring deployment feasibility in diverse IT environments. Emphasis on robust data governance frameworks and ethical AI practices is essential to maintain trust and compliance. Future research should explore hybrid models combining deep learning with other AI techniques, investigate multimodal data integration, and address adversarial vulnerabilities to enhance system resilience and adaptability.

5.3. Limitations and Pathways for Future Work

Current models are limited by dependency on labeled datasets, challenges in handling concept drift, and difficulties in interpreting complex model decisions. Additionally, the dynamic nature of cyber threats demands continual model updates and validation across varied domains. Future work should prioritize longitudinal studies, cross-platform evaluations, and development of lightweight architectures suitable for real-time applications. Addressing ethical, privacy, and security concerns remains a vital avenue to ensure responsible AI integration in cybersecurity.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Suparman, A., Akhmad, E. P. A., & Dinata, B. M. (2024). Leveraging Artificial Intelligence for Enhancing Cybersecurity: A Deep Learning Approach to Real-Time Threat Detection. In *The Journal of Academic Science* (Vol. 1, Issue 7, pp. 835–842). Yayasan Banu Samsudin. https://doi.org/10.59613/0yv79c49

[2] Pulyala, S. R. (2024). From Detection to Prediction: AI-powered SIEM for Proactive Threat Hunting and Risk Mitigation. In *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* (Vol. 15, Issue 1, pp. 34–43). Ninety Nine Publication. https://doi.org/10.61841/turcomat.v15i1.14393

[3] -, B. R. C. (2024). AI-Driven Security Solutions: Combating Cyber Threats with Machine Learning Models. In *International Journal For Multidisciplinary Research* (Vol. 6, Issue 5). International Journal for Multidisciplinary Research (IJFMR). https://doi.org/10.36948/ijfmr.2024.v06i05.29317

[4] Mohammadi, A., Ghahramani, H., Asghari, S. A., & Aminian, M. (2024). Securing Healthcare with Deep Learning: A CNN-Based Model for Medical IoT Threat Detection. In *2024 19th Iranian Conference on Intelligent Systems (ICIS)* (pp. 168–173). IEEE. https://doi.org/10.1109/icis64839.2024.10887510

[5] Mohammad, R., Saeed, F., Almazroi, A. A., Alsubaei, F. S., & Almazroi, A. A. (2024). Enhancing Intrusion Detection Systems Using a Deep Learning and Data Augmentation Approach. In *Systems* (Vol. 12, Issue 3, p. 79). MDPI AG. https://doi.org/10.3390/systems12030079

[6] Raiyan Haider. (2025). Navigating the digital political landscape: How social media marketing shapes voter perceptions and political brand equity in the 21st Century. In *International Journal of Science and Research Archive* (Vol. 15, Issue 1, pp. 1736–1744). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.1.1217

[7] Wang, Z. Q., & El Saddik, A. (2023). DTITD: An Intelligent Insider Threat Detection Framework Based on Digital Twin and Self-Attention Based Deep Learning Models. In *IEEE Access* (Vol. 11, pp. 114013–114030). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/access.2023.3324371

[8] Onih, V. A., Sevidzem, Y. S., & Adeniji, S. (2024). The Role of AI In Enhancing Threat Detection and Response in Cybersecurity Infrastructures. In *International Journal of Scientific and Management Research* (Vol. 07, Issue 04, pp. 64–96). Amanxo Publication. https://doi.org/10.37502/ijsmr.2024.7404

[9] Onuh Matthew Ijiga, Idoko Peter Idoko, Godslove Isenyo Ebiega, Frederick Itunu Olajide, Timilehin Isaiah Olatunde, & Chukwunonso Ukaegbu. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. In *Open Access Research Journal of Science and Technology* (Vol. 11, Issue 1, pp. 001–004). Open Access Research Journals Publication. https://doi.org/10.53022/oarjst.2024.11.1.0060

[10] Raiyan Haider, & Jasmima Sabatina. (2025). Harnessing the power of micro-influencers: A comprehensive analysis of their effectiveness in promoting climate adaptation solutions. In *International Journal of Science and Research Archive* (Vol. 15, Issue 2, pp. 595–610). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.2.1448

[11] Raiyan Haider, Md Farhan Abrar Ibne Bari, Osru, Nishat Afia, & Tanjim Karim. (2025). Illuminating the black box: Explainable AI for enhanced customer behavior prediction and trust. In *International Journal of Science and Research Archive* (Vol. 15, Issue 3, pp. 247–268). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.3.1674

[12] Yara Shamoo. (2024). Advances in Cybersecurity and AI: Integrating Machine Learning, IoT, and Smart Systems for Resilience and Innovation Across Domains. In *World Journal of Advanced Research and Reviews* (Vol. 23, Issue 2, pp. 2450–2461). GSC Online Press. https://doi.org/10.30574/wjarr.2024.23.2.2603

[13] Alajmi, M., Mengash, H. A., Alqahtani, H., Aljameel, S. S., Hamza, M. A., & Salama, A. S. (2023). Automated Threat Detection Using Flamingo Search Algorithm With Optimal Deep Learning on Cyber-Physical System Environment. In *IEEE Access* (Vol. 11, pp. 127669–127678). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/access.2023.3332213

[14] Atheeq, C., Sultana, R., Sabahath, S. A., & Mohammed, M. A. K. (2024). Advancing IoT Cybersecurity: Adaptive Threat Identification with Deep Learning in Cyber-Physical Systems. In *Engineering, Technology & Applied Science Research* (Vol. 14, Issue 2, pp. 13559–13566). Engineering, Technology & Applied Science Research. https://doi.org/10.48084/etasr.6969

[15] Raiyan Haider, Md Farhan Abrar Ibne Bari, Md. Farhan Israk Shaif, & Mushfiqur Rahman. (2025). Engineering hyper-personalization: Software challenges and brand performance in AI-driven digital marketing management: An empirical study. In *International Journal of Science and Research Archive* (Vol. 15, Issue 2, pp. 1122–1141). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.2.1525

[16] Sewak, M., Sahay, S. K., & Rathore, H. (2022). Deep Reinforcement Learning for Cybersecurity Threat Detection and Protection: A Review. In *Communications in Computer and Information Science* (pp. 51–72). Springer International Publishing. https://doi.org/10.1007/978-3-030-97532-6_4

[17] Jegatheesan A., A. G. (2024). Enhancing Industrial IoT Security: Utilizing Blockchain-Assisted Deep Federated Learning for Collaborative Intrusion Detection. In *Journal of Electrical Systems* (Vol. 20, Issue 2s, pp. 1345–1363). Science Research Society. https://doi.org/10.52783/jes.1782

[18] Mesadieu, F., Torre, D., & Chennamaneni, A. (2024). Leveraging Deep Reinforcement Learning Technique for Intrusion Detection in SCADA Infrastructure. In *IEEE Access* (Vol. 12, pp. 63381–63399). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/access.2024.3390722

[19] DeMedeiros, K., Hendawi, A., & Alvarez, M. (2023). A Survey of AI-Based Anomaly Detection in IoT and Sensor Networks. In *Sensors* (Vol. 23, Issue 3, p. 1352). MDPI AG. https://doi.org/10.3390/s23031352

[20] Fährmann, D., Damer, N., Kirchbuchner, F., & Kuijper, A. (2022). Lightweight Long Short-Term Memory Variational Auto-Encoder for Multivariate Time Series Anomaly Detection in Industrial Control Systems. In *Sensors* (Vol. 22, Issue 8, p. 2886). MDPI AG. https://doi.org/10.3390/s22082886

[21] Babajide Tolulope Familoni. (2024). CYBERSECURITY CHALLENGES IN THE AGE OF AI: THEORETICAL APPROACHES AND PRACTICAL SOLUTIONS. In *Computer Science & IT Research Journal* (Vol. 5, Issue 3, pp. 703–724). Fair East Publishers. https://doi.org/10.51594/csitrj.v5i3.930

[22] 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. In *IEEE Access* (Vol. 10, pp. 112392–112415). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/access.2022.3216617

[23] Raiyan Haider, Md Farhan Abrar Ibne Bari, Md. Farhan Israk Shaif, Mushfiqur Rahman, Md. Nahid Hossain Ohi, & Kazi Md Mashrur Rahman. (2025). Quantifying the Impact: Leveraging AI-Powered Sentiment Analysis for Strategic Digital Marketing and Enhanced Brand Reputation Management. In *International Journal of Science and Research Archive* (Vol. 15, Issue 2, pp. 1103–1121). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.2.1524

[24] Ugochukwu Ikechukwu Okoli, Ogugua Chimezie Obi, Adebunmi Okechukwu Adewusi, & Temitayo Oluwaseun Abrahams. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. In *World Journal of Advanced Research and Reviews* (Vol. 21, Issue 1, pp. 2286–2295). GSC Online Press. https://doi.org/10.30574/wjarr.2024.21.1.0315

[25] Raiyan Haider, Wahida Ahmed Megha, Jafia Tasnim Juba, Aroa Alamgir, & Labib Ahmad. (2025). The conversational revolution in health promotion: Investigating chatbot impact on healthcare marketing, patient engagement, and service reach. In *International Journal of Science and Research Archive* (Vol. 15, Issue 3, pp. 1585–1592). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.3.1937

[26] Raiyan Haider, Farhan Abrar Ibne Bari, Osru, Nishat Afia, & Mohammad Abiduzzaman khan Mugdho. (2025). Leveraging internet of things data for real-time marketing: Opportunities, challenges, and strategic implications. In *International Journal of Science and Research Archive* (Vol. 15, Issue 3, pp. 1657–1663). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.3.1936

[27] Hesham, M., Essam, M., Bahaa, M., Mohamed, A., Gomaa, M., Hany, M., & Elsersy, W. (2024). Evaluating Predictive Models in Cybersecurity: A Comparative Analysis of Machine and Deep Learning Techniques for Threat Detection. In *2024 Intelligent Methods, Systems, and Applications (IMSA)* (pp. 33–38). IEEE. https://doi.org/10.1109/imsa61967.2024.10652833

[28] Gao, T., Yang, J., Peng, W., Jiang, L., Sun, Y., & Li, F. (2020). A Content-Based Method for Sybil Detection in Online Social Networks via Deep Learning. In *IEEE Access* (Vol. 8, pp. 38753–38766). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/access.2020.2975877

[29] Ahmad, I., Imran, M., Qayyum, A., Ramzan, M. S., & Alassafi, M. O. (2023). An Optimized Hybrid Deep Intrusion Detection Model (HD-IDM) for Enhancing Network Security. In *Mathematics* (Vol. 11, Issue 21, p. 4501). MDPI AG. https://doi.org/10.3390/math11214501

[30] -, J. N. A. M., -, S. P., -, S. V. B., & -, M. D. (2024). Enhancing Cloud Compliance: A Machine Learning Approach. In *Advanced International Journal of Multidisciplinary Research* (Vol. 2, Issue 2). Futuristic Research Publication and Journals. https://doi.org/10.62127/aijmr.2024.v02i02.1036

[31] Aouedi, O., Piamrat, K., Muller, G., & Singh, K. (2023). Federated Semisupervised Learning for Attack Detection in Industrial Internet of Things. In *IEEE Transactions on Industrial Informatics* (Vol. 19, Issue 1, pp. 286–295). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/tii.2022.3156642

[32] Coccomini, D. A., Caldelli, R., Falchi, F., & Gennaro, C. (2023). On the Generalization of Deep Learning Models in Video Deepfake Detection. In *Journal of Imaging* (Vol. 9, Issue 5, p. 89). MDPI AG. https://doi.org/10.3390/jimaging9050089

[33] Roopesh, M., Nishat, N., Arif, I., & Bajwa, A. E. (2024). A COMPREHENSIVE REVIEW OF MACHINE LEARNING AND DEEP LEARNING APPLICATIONS IN CYBERSECURITY: AN INTERDISCIPLINARY APPROACH. In *ACADEMIC JOURNAL ON SCIENCE, TECHNOLOGY, ENGINEERING & MATHEMATICS EDUCATION* (Vol. 4, Issue 04, pp. 37–53). All Academic Research. https://doi.org/10.69593/ajsteme.v4i04.118

[34] Raiyan, H., Jafia Tasnim, J., & Satu, C. (2025). Exploring the link between suicidal ideation and digital environments: The hidden impact of marketing content. *International Journal of Science and Research Archive*, *16*(02), 607–614. https://doi.org/10.30574/ijsra.2025.16.2.2353

[35] Khan, A. R., Yasin, A., Usman, S. M., Hussain, S., Khalid, S., & Ullah, S. S. (2022). Exploring Lightweight Deep Learning Solution for Malware Detection in IoT Constraint Environment. In *Electronics* (Vol. 11, Issue 24, p. 4147). MDPI AG. https://doi.org/10.3390/electronics11244147

[36] Raiyan, H., Shaif, Md. F. I., Ahmed, R., Nafi, N. H., Sumon, M. R., & Rahman, M. (2025b). The influence of social media branding on consumer purchase behavior: A comprehensive empirical and thematic analysis. *International Journal of Science and Research Archive*, *16*(02), 460–470. https://doi.org/10.30574/ijsra.2025.16.2.2354

[37] Ferrag, M. A., Ndhlovu, M., Tihanyi, N., Cordeiro, L. C., Debbah, M., Lestable, T., & Thandi, N. S. (2024). Revolutionizing Cyber Threat Detection With Large Language Models: A Privacy-Preserving BERT-Based Lightweight Model for IoT/IIoT Devices. In *IEEE Access* (Vol. 12, pp. 23733–23750). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/access.2024.3363469

[38] O. S. Albahri, & A. H. AlAmoodi. (2023). Cybersecurity and Artificial Intelligence Applications: A Bibliometric Analysis Based on Scopus Database. In *Mesopotamian Journal of CyberSecurity* (Vol. 2023, pp. 158–169). Mesopotamian Academic Press. https://doi.org/10.58496/mjcsc/2023/018

[39] -, T. O., -, A. Y., & -, C. V. O. (2024). A Survey of AI-Powered Proactive Threat-Hunting Techniques: Challenges and Future Directions. In *International Journal For Multidisciplinary Research* (Vol. 6, Issue 6). International Journal for Multidisciplinary Research (IJFMR). https://doi.org/10.36948/ijfmr.2024.v06i06.29183

[40] Samuel Olaoluwa Folorunsho, Olubunmi Adeolu Adenekan, Chinedu Ezeigweneme, Ike Chidiebere Somadina, & Patrick Azuka Okeleke. (2024). Ensuring Cybersecurity in telecommunications: Strategies to protect digital infrastructure and sensitive data. In *Computer Science & IT Research Journal* (Vol. 5, Issue 8, pp. 1855–1883). Fair East Publishers. https://doi.org/10.51594/csitrj.v5i8.1448

[41] Dalal, A. (2018). Cybersecurity And Artificial Intelligence: How AI Is Being Used in Cybersecurity To Improve Detection And Response To Cyber Threats. In *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* (Vol. 9, Issue 3, pp. 1416–1423). Ninety Nine Publication. https://doi.org/10.61841/turcomat.v9i3.14670

[42] Raiyan, H., Shaif, Md. F. I., Ahmed, R., Nafi, N. H., Sumon, M. R., & Rahman, M. (2025a). Assessing the impact of influencer marketing on brand value and business revenue: An empirical and thematic analysis. *International Journal of Science and Research Archive*, *16*(02), 471–482. https://doi.org/10.30574/ijsra.2025.16.2.2355

[43] Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine Learning Cybersecurity Adoption in Small and Medium Enterprises in Developed Countries. In *Computers* (Vol. 10, Issue 11, p. 150). MDPI AG. https://doi.org/10.3390/computers10110150