Stout in Computer Science and Technology Studies (SCSTS)

DOI: https://doi.org/10.61424/0m9p0s77
Journal Homepage: https://stoutjournals.org/index.php/SCSTS

Cybersecurity Techniques for Enhancing the Security of Internet of Things (IoT)-Based Systems

Dakota Ryan[1] ✉ **and Riley Quinn Morgan**[2]
[12]*McGill University, Canada*
Corresponding Author: Dakota Ryan, **E-mail**: ryan22@gmail.com

ARTICLE INFORMATION

Submitted: June 20, 2025
Accepted: May 15, 2026
Published: July 13, 2026
Volume: 1
Issue: 1

KEYWORDS

Malware, data breaches, device hijacking, cybersecurity techniques

ABSTRACT

The rapid expansion of Internet of Things (IoT)-based systems across critical sectors has significantly improved connectivity, automation, and operational efficiency while simultaneously introducing complex cybersecurity challenges. The increasing number of interconnected devices, heterogeneous communication protocols, and resource-constrained architectures have created vulnerabilities that are frequently exploited through malware, distributed denial-of-service (DDoS) attacks, unauthorized access, data breaches, and device hijacking. This review examines contemporary cybersecurity techniques designed to strengthen the security and resilience of IoT-based systems. It explores key security mechanisms, including encryption, authentication and authorization protocols, blockchain technology, intrusion detection and prevention systems, artificial intelligence and machine learning-based threat detection, secure firmware updates, network segmentation, and zero-trust security models. The review further discusses the major security challenges associated with IoT environments, such as scalability, interoperability, privacy protection, and limited computational resources. Evidence from recent studies indicates that a layered and adaptive cybersecurity framework integrating conventional security controls with intelligent threat detection provides more effective protection than isolated security solutions. The study concludes that strengthening IoT security requires continuous risk assessment, secure-by-design principles, regulatory compliance, and the adoption of emerging technologies capable of responding to evolving cyber threats. These findings provide valuable insights for researchers, cybersecurity professionals, policymakers, and system developers seeking to improve the security, reliability, and resilience of IoT-based infrastructures.

1. Introduction

1.1 The Letter

The rapid expansion of the Internet of Things (IoT) has revolutionized modern digital ecosystems by enabling seamless connectivity among billions of devices across healthcare, smart cities, industrial automation, agriculture, transportation, and smart manufacturing. This unprecedented growth has significantly improved automation, operational efficiency, and data-driven decision-making. However, the increasing number of interconnected devices has also expanded the cyberattack surface, exposing IoT systems to numerous security and privacy threats. The heterogeneous, distributed, and resource-constrained nature of IoT devices makes them particularly vulnerable to cyberattacks such as malware, eavesdropping, spoofing, data manipulation, distributed denial-of-service (DDoS) attacks, and unauthorized access [1,2]. Moreover, the limited computational capability, memory, and energy resources of many IoT devices restrict the implementation of conventional cryptographic and security mechanisms, making the protection of data confidentiality, integrity, and availability a critical challenge for modern IoT deployments [3–5].

To address these challenges, artificial intelligence (AI) and machine learning (ML) have emerged as key enabling technologies for intelligent cybersecurity. Machine learning-based intrusion detection systems (IDS) continuously analyze network traffic, identify anomalous behavioral patterns, and automatically adapt to evolving attack strategies, thereby significantly improving threat detection and response capabilities [6,7]. Recent advances in deep learning have further enhanced intrusion detection performance. Hybrid architectures combining Convolutional Neural Networks (CNNs) and Gated Recurrent Units (GRUs) have achieved detection accuracies exceeding 99%, demonstrating the effectiveness of integrating spatial and temporal feature learning for sophisticated cyberattack detection [8]. Furthermore, Rahman et al. [9] introduced a fusion-based hybrid meta-learning framework integrated with explainable artificial intelligence (XAI), significantly improving predictive threat detection and decision transparency in intelligent surveillance environments. Rahman et al. [10] further demonstrated that AI-driven predictive analytics strengthen cybersecurity resilience through integrated business intelligence frameworks, while Alam et al. [11] proposed a hybrid big data and large language model (LLM) framework for intelligent threat intelligence and automated knowledge discovery. Similarly, Hossain et al. [12] developed self-adaptive AI systems capable of continuous learning and autonomous optimization, enabling large-scale cybersecurity operations through intelligent real-time responses. Collectively, these studies demonstrate that integrating AI-driven learning mechanisms into IoT security architectures substantially improves threat detection, adaptive defense, and automated incident response.

Blockchain technology has also emerged as a fundamental component of secure IoT infrastructures by providing decentralized trust management, immutable audit trails, and tamper-resistant data storage. Unlike centralized architectures, blockchain eliminates single points of failure while ensuring transparency, traceability, and secure information sharing across distributed IoT networks [13,14]. Rabbani et al. [15] demonstrated the effectiveness of blockchain-enabled traceability systems for securing distributed communication environments, while Hassan et al. [16] showed that blockchain integration significantly enhances cybersecurity and data integrity in management information systems. Similarly, Bauskar et al. [17] proposed a blockchain-enabled big data governance framework that improves privacy protection, regulatory compliance, and secure data management in large-scale distributed systems. Complementing blockchain technologies, edge and fog computing enable localized processing of security-sensitive data, reducing communication latency and supporting real-time intrusion detection without relying exclusively on centralized cloud infrastructures [18,19]. Habib et al. [20] further emphasized the importance of secure communication protocols, intelligent monitoring, and adaptive protection mechanisms for IoT-enabled smart home automation systems, highlighting the critical role of edge-layer security in resource-constrained environments.

Figure 1 illustrates the proposed multi-layer cybersecurity architecture for IoT-based systems, which integrates complementary security mechanisms across four interconnected layers. At the device layer, lightweight encryption, authentication protocols, and secure firmware update mechanisms protect resource-constrained IoT devices [3,21]. The network layer incorporates intrusion detection systems and secure communication protocols to monitor traffic, identify malicious activities, and mitigate network-based attacks, including DDoS incidents [2,22]. The edge and fog layer provided AI-driven anomaly detection, real-time threat analysis, and intelligent response mechanisms with minimal latency, enabling rapid mitigation of emerging cyber threats [18,23]. Finally, the cloud and application layer integrated blockchain-enabled data integrity, advanced analytics, and long-term threat intelligence to support scalable security management and predictive cyber defense [13,14,24]. Unlike conventional single-layer security models that address isolated vulnerabilities, this integrated architecture combines lightweight cryptography, machine learning, edge intelligence, and decentralized data governance to provide comprehensive end-to-end protection for modern IoT ecosystems. Recent studies employing transformer-based intrusion detection models and continual learning frameworks further validate the effectiveness of adaptive, AI-driven security architectures for detecting sophisticated and continuously evolving cyber threats [25,26].

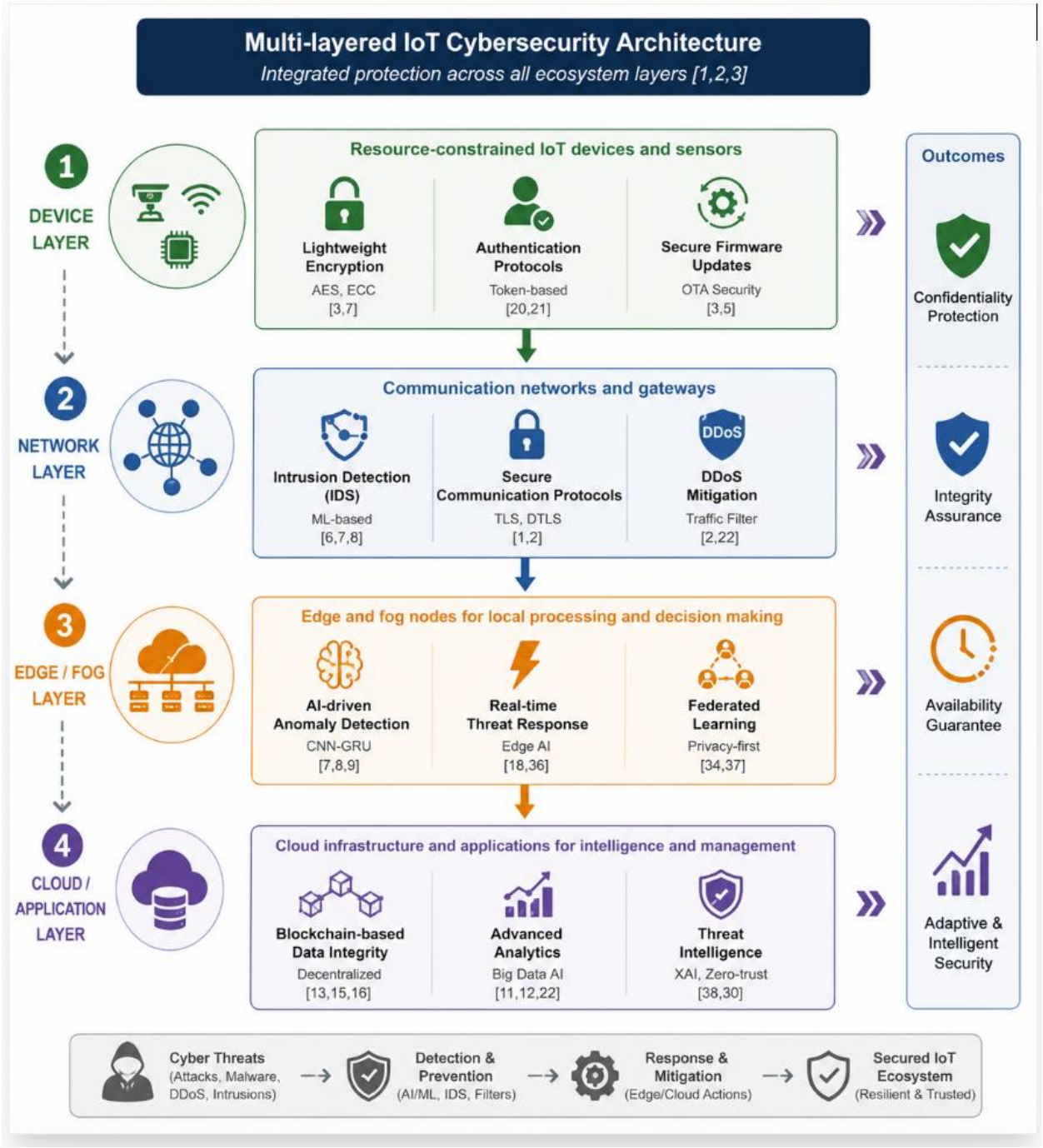

Figure 1. Proposed Multi-Layer Cybersecurity Framework for IoT-Based Systems

Despite significant progress, several challenges continue to limit the widespread deployment of advanced IoT cybersecurity solutions. Ensuring scalability across billions of heterogeneous devices remains a major concern because current AI and blockchain frameworks often require computational resources beyond the capabilities of resource-constrained IoT devices [11,12,27]. The diversity of communication protocols, hardware platforms, and vendor-specific implementations also creates interoperability challenges that hinder the development of unified security frameworks [28,29]. Furthermore, AI-based security models depend heavily on large, representative datasets and remain susceptible to adversarial attacks that can manipulate model behavior and reduce detection accuracy [30,31]. Blockchain consensus mechanisms, particularly Proof-of-Work (PoW), impose considerable computational and energy overhead, limiting their applicability in lightweight IoT environments, while more efficient consensus protocols have yet to achieve widespread standardization [13,32]. In addition, many proposed cybersecurity frameworks have been evaluated primarily through simulation studies rather than real-world deployments, limiting their demonstrated effectiveness under practical operational conditions [33,34]. Recent studies suggest that DataOps-based

governance frameworks can improve system integration, automation, and lifecycle management [35], whereas bio-cognitive AI systems provide promising mechanisms for adaptive, resource-aware cybersecurity in constrained IoT environments [36].

Future research should focus on developing intelligent, scalable, and trustworthy cybersecurity frameworks capable of addressing these limitations. Federated learning represents a promising direction by enabling distributed model training without exposing sensitive local data, thereby improving privacy, scalability, and collaborative threat intelligence across heterogeneous IoT networks [4,37]. The integration of explainable artificial intelligence (XAI) will enhance model transparency, interpretability, and user trust while supporting regulatory compliance and security auditing [30,38]. Hybrid frameworks that combine blockchain, edge intelligence, and AI-driven analytics can simultaneously improve data integrity, reduce communication latency, and enable decentralized decision-making across distributed IoT infrastructures [13,18]. Zero-trust security architectures, which continuously authenticate users and devices regardless of network location, provide another effective strategy for mitigating insider threats and unauthorized access [1,2]. Moreover, emerging technologies such as 6G communications and semantic networking will enable ultra-low-latency, intelligent, and context-aware cybersecurity services for next-generation IoT ecosystems [39]. The successful application of AI-driven analytics across healthcare, precision medicine, socio-economic forecasting, and scientific knowledge discovery further demonstrates the potential of adaptive, multidimensional learning frameworks for strengthening future IoT cybersecurity systems [40–44].

Overall, protecting IoT-based systems requires a comprehensive and adaptive cybersecurity framework that simultaneously addresses vulnerabilities across the device, network, edge, and cloud layers. The integration of machine learning-based intrusion detection, blockchain-enabled trust management, edge intelligence, and advanced cloud analytics provides a robust foundation for securing increasingly complex IoT ecosystems. Although challenges related to scalability, interoperability, energy efficiency, explainability, and real-world deployment remain, emerging technologies such as federated learning, explainable AI, zero-trust security, and 6G-enabled networking offer promising pathways toward intelligent, resilient, and future-proof IoT cybersecurity infrastructures [45–52].

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers
Artificial Intelligence (AI) Use Disclosure: The authors declare that no artificial intelligence tools were used in the preparation of this manuscript.

References

[1] Ahakonye LAC, et al. (2024) Blockchain-enabled IoT security frameworks. Sensors. 2024;24(10):3111.
[2] Alaba FA, Othman M, Hashem IAT, Alotaibi F. (2017) Internet of Things security: A survey. *Journal of Network and Computer Applications*. 2017;88:10–28.
[3] Alam MI, Hemal MAKP, Sami MA, Rahman ML. (2024) Robust and Interpretable Crop Recommendation. European Journal of Ecology, Biology and Agriculture. 2024;1(5):168–184. https://doi.org/10.59324/ejeba.2024.1(5).14
[4] Alam MI, Rashed RAM, Chakraborty P, Mohonta SC, Imam H, Rahman Bhuiyan MM. (2026) Hybrid big data-LLM framework for intelligent scientific literature mining. In 2026 IEEE I3CTCON, 1–9. https://doi.org/10.1109/I3CTCON68242.2026.11507315
[5] Alam MI, Sami MA, Al Masud A, Ahmed H, Hossain F. (2025) AI-Driven Big Data Analytics for Personalized Cancer Treatment. *Journal of Computer Science and Technology Studies*. 2025;7(11):428–441. https://doi.org/10.32996/jcsts.2025.7.11.40
[6] Alam MI, Sami MA, Hemal MAKP, Rahman ML. (2023) Predictive Analytics and Decision Intelligence for Climate-Resilient Agritech Systems. 2023;2(1):44–56. https://doi.org/10.32996/agjcsts.2023.2.1.4
[7] Alam MI, Sikder TR, Sami MA, Rahman ML, et al. (2026) A robust and explainable approach to crop recommendation. *Journal of Environmental and Agricultural Studies*. 2026;7(3):1–15. https://doi.org/10.32996/jeas.2026.7.3.1
[8] Bauskar S, Sahoo RK, Boda SS, Singhai H, Bakhsh MM, Adnan M. (2025) Privacy-aware big data governance framework using blockchain. 2025 IEEE ETCOM, 1–9. https://doi.org/10.1109/ETCOM66606.2025.11436976
[9] Bhuiyan MNA, Kamruzzaman M, Saha S, Siddiki MS, Mondal RS. (2025) Role of data analysis and integration of artificial intelligence. *Journal of Business and Management Studies*. 2025;7(4):379–388. https://doi.org/10.32996/jbms.2025.7.4.20.26
[10] Buczak AL, Guven E. (2016) Machine learning for intrusion detection. IEEE Communications Surveys. 2016;18(2):1153–1176.
[11] Conti M, et al. (2018) Security and privacy in IoT. IEEE Communications Surveys. 2018;20(4):3416–3452.
[12] Das K, et al. (2026) AI-driven intrusion detection in IoT systems. Future Internet. 2026;18(2):145–162.
[13] Habib MR, Yusuf MA, Warnasuriya WMHN, Sunny K, Rahaman MM, Khan MRK. (2024) A comprehensive review on the advancement of home automation system. In 2024 ICoICI, 638–642. https://doi.org/10.1109/ICoICI62503.2024.10696135
[14] Hasan MM, Alam MI, Chowdhury MAH, Anwar MM. (2026) AI-Driven Big Data Analytics for Precision Medicine and Healthcare Intelligence. Frontiers in Computer Science and Artificial Intelligence. 2026;5(2):41–62. https://doi.org/10.32996/jcsts.2026.5.1.5
[15] Hassan J, Barikdar CR, Hasan SN, Kaur J, Chakraborty P, Miah MA. (2025) Blockchain integration in management information systems. 2025 5th ICECET, 1–7. https://doi.org/10.1109/ICECET63943.2025.11472020

[16] Hemal MAKP, Sayeed N, Sami MA, Alam MI, Sikder TR, Dipa SA, Rahman ML. (2025) Leveraging Data Analytics to Strengthen Public Health and Global Economic Sustainability. *European Journal of Medical and Health Research*. 2025;3(4):253–263. https://doi.org/10.59324/ejmhr.2025.3(4).37

[17] Hossain MJ, Bakhsh MM, Sami MA, Alam MI, Melon MMH, Manik MMTG. (2026) Self-adaptive artificial intelligence systems for large-scale data-driven decision making. In 2026 IEEE I3CTCON, 1–8. https://doi.org/10.1109/I3CTCON68242.2026.11507252

[18] Ibukun, K., & Nimotalai, K. O. (2024). A Comparative Analysis of the Cost-Effectiveness of Universal Health Coverage (UHC) Financing Models and Their Policy Implications in Low-and Middle-Income Countries. *Journal of Medical Science, Biology, and Chemistry*, *1*(1), 37-45.

[19] Islam, A., & Jantan, A. H. B. (2023). The mediation effect of affective organizational commitment on the relationship between HRM practices and turnover intention in the RMG industry. *Research Journal in Business and Economics*, *1*(1), 24-38.

[20] Islam, A., Jantan, A. H. B., Khalifa, G. S., Islam, A., Islam, B., & Hossian, A. (2023). Effects of Decision Making and Work-life Balance on Productivity of Female Employees in the RMG Industry of Bangladesh. The Mediating Role of Work Motivation. *Research Journal in Business and Economics*, *1*(1), 48-59.

[21] Islam, M. A., & Sinniah, S. (2025). Exploring customer relationship management factors, customer trust, and innovation capacity: A quantitative study on customer retention. *Accountancy Business and the Public Interest*, *41*(10), 12-29.

[22] Islam, M. A., Islam, M. A., Amin, M. B., Hossain, M. M., Hassan, M. S., Afrin, S., & Oláh, J. (2025). Enhancing academic's performance: Exploring the interaction of innovative work behavior, intrinsic motivation, and self-efficacy in public universities. *Social Sciences & Humanities Open*, *12*, 102210.

[23] Kamruzzaman M, Mondal RS, Islam MK, Rahaman MA, Saha S. (2024) AI-driven predictive modelling of US economic growth. *International Journal of Computational and Experimental Science and Engineering*. 2024;10(4):1927–1938. https://doi.org/10.22399/ijcesen.3612

[24] Kamruzzaman M, Saha S, Siddiki MS, Mondal RS, Bhuiyan MNA. (2025) Applications of artificial intelligence in small and medium scale business. *Journal of Business and Management Studies.* 2025;7(4):314–325. https://doi.org/10.32996/jbms.2025.7.4.20.21

[25] Kassim, N. O. (2025). Community-Driven Behavioral Intelligence Framework Strengthening US Public Health Systems, Violence Prevention, and Nationwide Community Resilience Initiatives.

[26] Kassim, N. O. (2026). Assessing Mental Health Awareness and Stigma in Hartford, Connecticut, USA. *Annals of Innovation in Medicine*, *4*(1).

[27] Kaur J, Prabha M, Samiun M, Hasan SN, Hasan R, Esa H, et al. (2025) Comparative analysis of transformer and LSTM architectures for cybersecurity threat detection. EAI Endorsed Transactions on AI and Robotics. 2025;4. https://publications.eai.eu/index.php/airo/article/view/9759

[28] Kshetri N. (2018) Blockchain's role in cybersecurity. Computer. 2018;51(9):68–72.

[29] Mondal RS, Ahmed RA, Hemal MAKP, Sikder TR, Juie BJA. (2026) A Multi-Omics Transformer Foundation Model For AI-Driven Early Cancer Detection. *The American Journal of Medical Sciences and Pharmaceutical Research*. 2026;8(2):113–127. https://doi.org/10.37547/tajmspr/Volume08Issue02-17

[30] Mondal RS, Bhuiyan MNA, Kamruzzaman M, Saha S, Siddiki MS. (2025) A comparative analysis of tools for data mining and big data mining. *Journal of Business and Management Studies.* 2025;7(4):232–242. https://doi.org/10.32996/jbms.2025.7.4.14

[31] Mondal RS, Kamruzzaman M, Saha S, Bhuiyan MNA. (2025) Quantum machine learning approaches for high-dimensional cancer genomics data analysis. Computer Integrated Manufacturing Systems. 2025;31(1):13–32. https://doi.org/10.24297/j.cims.2025.1.21

[32] Mondal RS, Purba TN, Purba NN, Rahman MM, Sikder TR. (2026) AI-Driven Glycemic Instability Risk Modeling. *Journal of Medical and Health Studies. 2026*;7(1):29–43. https://doi.org/10.32996/jmhs.2023.4.6.21

[33] Nabi N, Tuhin MK, Bashir M, Lucky KY, Raihan M, Imam H. (2025) Continual learning pipelines for detecting insider threats. 2025 ICEEI, 1–8. https://doi.org/10.1109/ICEEI68459.2025.11330487

[34] Nusrat S, Hossain F, Sikder TR. (2024) Integrating Wearable Health Data and Environmental Management Analytics. The *Eastasouth Journal of Information System and Computer Science*. 2024;2(02):209–223. https://doi.org/10.58812/esiscs.v2i02.868

[35] Orthi SM, Sikder TR, Uddin SMM, Roy T, Hossain MJ, Faruk MI. (2025) DataOps-Oriented Big Data Governance for Automated Decision Pipelines. 2025 1st ICAFT, 1–8. https://doi.org/10.1109/ICAFT66710.2025.11452860

[36] Orthi SM, Sikder TR, Uddin SMM, Roy T, Hossain MJ, Faruk MI. (2025) DataOps-Oriented Big Data Governance for Automated Decision Pipelines. 2025 1st ICAFT, 1–8. https://doi.org/10.1109/ICAFT66710.2025.11452860

[37] Osarhiaekhimen, G., Oge, S. O., Oyeniyi, T., Ifezuoke, N. F., Emesobum, M., Olamiju, J. O., ... & Aja, L. (2025). Psychosocial Predictors of Drug Use Disorders among Secondary School Adolescents in Abuja, Nigeria: The Role of Emotional Neglect, Family Dysfunction, and Parental Substance Abuse. *F1000Research*, *14*, 1415

[38] Qaddos A, et al. (2024) Hybrid deep learning IDS. Scientific Reports. 2024;14:72049.

[39] Rabbani SH, Rahman MM, Ahmad M, Zunayed M, Khan MRK. (2025) Blockchain-based food traceability system to ensure food security in Bangladesh. In 2025 ICCSC, 1–6. https://doi.org/10.1109/ICCSC66714.2025.11135217

[40] Rahman ML, Alam MI, Anzum R, Acharjee S, Alam MS, Shamarukh S. (2026) AI-driven predictive analytics for supply chain resilience, financial risk management, and digital marketing strategy. *Journal of Business and Management Studies.* 2026;8(7):41–55. https://doi.org/10.32996/jbms.2026.8.7.3

[41] Rahman MM, Sarker S, Hasan Shaikat MM, Das S, Khan MRK. (2025) Machine learning for breast cancer classification: A comparative study of grid search-optimized SVM, random forest, and XGBoost. In 2025 International Conference on Quantum Photonics, Artificial Intelligence, and Networking (QPAIN), 1–6. https://doi.org/10.1109/QPAIN66474.2025.11172245

[42] Rahman MM, Sifat FF, Islam R, Molla S, Khan MRK. (2024) Hybrid recommendation systems using adaptive clustering. In 2024 ICECET, 1–6. https://doi.org/10.1109/ICECET61485.2024.10698666

[43] Saha PP, Rahaman MM, Islam MT, Chowdhury NI. (2025) Advancing lung cancer diagnosis: A hybrid feature fusion approach. In 2025 2nd ISCS, 1–7. https://doi.org/10.1109/ISCS69371.2025.11386016

[44] Saha PP, Rone PD, Sarkar D, Yusuf MA, Hossan MI, Mazumder MSJ. (2025) Advancing carbon emission prediction through machine learning. In 2025 ESCI, 1–7. https://doi.org/10.1109/ESCI63694.2025.10988213

[45] Saha S, Islam MK, Rahaman MA, Mondal RS, Kamruzzaman M. (2024) Machine learning driven analytics for national security operations. *Journal of Computational Analysis and Applications.* 2024;33(8):210. https://doi.org/10.48047/jocaaa.2024.33.08.210
[46] Saha S, Siddiki MS, Mondal RS, Bhuiyan MNA, Kamruzzaman M. (2025) Risk assessment of cyber security in the banking sector. *Journal of Business and Management Studies. 2025*;7(4):208–218. https://doi.org/10.32996/jbms.2025.7.4.12
[47] Sami MA, Hemal MAKP, Alam MI, Rahman ML. (2024) Data Governance and Analytics Infrastructure for Scalable Decision-Making. *European Journal of Applied Science, Engineering and Technology.* 2024;2(2):388–403. https://doi.org/10.59324/ejaset.2024.2(2).28
[48] Sami MA, Rahman ML, Tanni ZA, Munmun ZS, Nusrat S, Biswas B. Artificial intelligence and big data for precision medicine. Frontiers in Computer Science and Artificial Intelligence. 2026;5(6):36–43. https://doi.org/10.32996/fcsai.2026.5.6.7
[49] Shi W, et al. (2016) Edge computing overview. *IEEE Internet of Things Journal*. 2016;3(5):637–646.
[50] Sicari S, et al. (2015) IoT security challenges. Computer Networks. 2015;76:146–164.
[51] Siddiki MS, Mondal RS, Bhuiyan MNA, Kamruzzaman M, Saha S. (2025) Assessment the knowledge, attitudes, education, and practices toward artificial intelligence. *Journal of Business and Management Studies. 2025*;7(5):106–116. https://doi.org/10.32996/jbms.2025.7.5.9
[52] Sikder TR, Dash S, Uddin B, Hossain F. (2023) AI-Powered Data Analytics and Multi-Omics Integration for Next-Generation Precision Oncology. *The Eastasouth Journal of Information System and Computer Science. 2023*;1(02):153–170. https://doi.org/10.58812/esiscs.v1i02.838
[53] Sikder TR, Sayeed N, Hossain MJ, Faruk MI, Alam MI, Uddin SMM, Adnan M. (2025) AI-Driven Environmental Precision Oncology. *International Journal of Computational and Experimental Science and Engineering*. 2025;11(4). https://doi.org/10.22399/ijcesen.4533
[54] Sikder TR, Siam MA, Melon MMH, Uddin SMM, Mohonta SC, Karim F. A (2023) Multimodal Data Analytics Framework for Early Cancer Detection. *Journal of Computer Science and Technology Studies.* 2023;5(3):183–188. https://doi.org/10.32996/jcsts.2023.5.3.13
[55] Uddin SMM, Chy MAR, Sikder TR, Faruk MI, Adnan M, Hossain MJ. (2025) Bio-Cognitive AI Systems for Predictive Healthcare Decision Support. 2025 1st ICAFT, 1–9. https://doi.org/10.1109/ICAFT66710.2025.11453175
[56] Vanu N, Hasan MR, Sikder TR, Tamanna ZS. (2021) AI-Driven Big Data Analytics for Precision Medicine: A Unified Framework Integrating Molecular Data Intelligence, Wearable Health Systems, and Predictive Modeling. *Journal of Computer Science and Technology Studies. 2021*;3(2):124–141. https://doi.org/10.32996/jcsts.2021.3.2.11
[57] Xu X, et al. (2021) Blockchain architectures. Springer; 2021.
[58] Yang Q, et al. (2019) Federated learning. ACM Transactions on Intelligent Systems. 2019.
[59] Yusuf MA, Chowdhury NM, Rone PD, et al. (2025) Advancing Public Safety with Real-Time Life Jacket Detection Using YOLOv8. EAI Endorsed Transactions on AI and Robotics. 2025;4:1–12. https://doi.org/10.4108/airo.9785
[60] Yusuf MA, Khan MRK, Saha PP, Rahaman MM. (2024) Data fusion of semantic and depth information in the context of object detection. In 2024 ICoICI, 1124–1129. https://doi.org/10.1109/ICoICI62503.2024.10696627