Stout in Computer Science and Technology Studies (SCSTS)

DOI: https://doi.org/10.61424/0yb2dw48
Journal Homepage: https://stoutjournals.org/index.php/SCSTS

Self-Healing Mechanisms for Autonomous Cybersecurity Systems Using Reinforcement Learning

Michael David Johnson[1] ✉ **and William Robert**[2]
[12]*Independent Researcher, USA*
Corresponding Author: Michael David Johnson, **E-mail**: johnson22@gmail.com

ARTICLE INFORMATION

Submitted: December 20, 2025
Accepted: April 20, 2026
Published: July 13, 2026
Volume: 1
Issue: 1

KEYWORDS

Reinforcement Learning, Self-Healing Systems, Autonomous Cybersecurity, Cyber Threat Detection, Adaptive Security Frameworks.

ABSTRACT

The increasing sophistication of cyber threats has driven the need for intelligent, adaptive cybersecurity systems capable of autonomous operation. Conventional security approaches, such as signature-based and rule-based detection mechanisms, often struggle to identify and respond effectively to evolving and previously unseen attack patterns. This study presents a reinforcement learning (RL)-based self-healing framework that enhances autonomous cybersecurity by improving threat detection, accelerating response and recovery, and increasing overall system resilience. The proposed framework employs reinforcement learning agents that continuously interact with the operating environment to learn and optimize defense strategies. Through ongoing adaptation, the system effectively detects emerging threats and autonomously initiates appropriate mitigation and recovery actions. Comparative performance analysis demonstrates that the RL-based framework consistently outperforms traditional security approaches across multiple cybersecurity metrics. Specifically, the proposed model achieves a threat detection accuracy of approximately 93%, exceeding the performance of conventional signature-based and anomaly-based methods, thereby demonstrating superior adaptability to previously unseen attacks. The framework also significantly reduces post-attack recovery time, achieving system restoration in approximately 30 seconds compared with substantially longer recovery periods required by manual and rule-based approaches. This rapid self-healing capability minimizes service disruption, limits the propagation of attacks, and enhances operational continuity, particularly in critical infrastructure environments. Furthermore, experimental evaluation indicates notable improvements in system resilience, including higher uptime, more effective threat mitigation, and improved response efficiency. By continuously refining its defensive policies through reinforcement learning, the proposed framework provides a robust, adaptive, and resilient cybersecurity solution capable of addressing the challenges posed by dynamic and sophisticated cyber threats.

1. Introduction

The rapid digital transformation of modern infrastructures has significantly increased the complexity and vulnerability of cybersecurity systems. The widespread adoption of cloud computing, the Internet of Things (IoT), edge computing, and interconnected enterprise networks has expanded the cyberattack surface, enabling increasingly sophisticated, dynamic, and persistent threats. Consequently, there is a growing demand for intelligent, adaptive, and autonomous cybersecurity solutions capable of detecting, responding to, and recovering from cyberattacks in real time (Zerine et al., 2026; Huang et al., 2017; Uddin et al., 2025).

Conventional cybersecurity approaches rely primarily on predefined rules, signatures, and historical attack patterns to identify malicious activities. Although these methods are effective against known threats, they are less capable of detecting zero-day attacks, advanced persistent threats, and continuously evolving attack strategies. Signature-based systems require frequent updates to remain effective, making them inherently reactive (Zerine et al., 2026). Anomaly-based detection techniques offer

greater flexibility by identifying deviations from normal behavior; however, they often produce high false-positive rates and lack contextual awareness, limiting their effectiveness in complex cybersecurity environments (Hasan et al., 2025).

Artificial intelligence (AI) and machine learning (ML) have emerged as promising technologies for enhancing cybersecurity through intelligent threat detection, attack prediction, and automated response. AI-driven systems can process large volumes of heterogeneous security data, identify hidden attack patterns, and improve detection accuracy compared with traditional approaches (Alam et al., 2025; Khan et al., 2025). Previous studies, including Das et al. (2026), have demonstrated the effectiveness of AI-based cybersecurity frameworks in improving threat detection and incident response. However, many existing AI models operate using static learning paradigms and require periodic retraining to adapt to emerging threats, limiting their ability to provide continuous autonomous protection (Vanu et al., 2021; Kassim, 2026).

Reinforcement learning (RL), a branch of machine learning in which agents learn optimal actions through interaction with their environment, provides a promising solution to these limitations. Unlike supervised learning methods, RL continuously updates its decision-making policy based on environmental feedback, enabling adaptive defense strategies against evolving cyber threats. This capability makes RL particularly suitable for autonomous cybersecurity systems that require continuous learning, real-time decision-making, and self-healing capabilities.

The concept of self-healing cybersecurity has gained increasing attention as organizations seek resilient systems capable of autonomously detecting attacks, mitigating their impact, and restoring normal operations with minimal human intervention. Such capabilities are especially important in critical infrastructure, healthcare, financial services, industrial control systems, and other mission-critical environments where even brief service disruptions may result in substantial economic losses and safety risks (Nusrat et al., 2024; Uddin et al., 2025; Orthi et al., 2025). By continuously learning from cyber incidents and optimizing response policies, RL-based self-healing mechanisms provide a proactive defense strategy that enhances system availability, resilience, and operational continuity (Islam & Jantan, 2023)

Recent advances in complementary technologies further strengthen the potential of RL-based cybersecurity. Blockchain technology offers decentralized, tamper-resistant data storage that enhances trust and integrity, while edge computing enables low-latency security analytics by processing data closer to distributed devices. The integration of these technologies with reinforcement learning creates a robust foundation for implementing scalable, adaptive, and real-time cybersecurity solutions (Hassan et al., 2025; Varanasi et al., 2026). Nevertheless, several challenges remain, including computational complexity, scalability in large-scale networks, extensive training requirements, and the interpretability and reliability of RL models, particularly in high-risk operational environments.

Beyond cybersecurity, advances in artificial intelligence, machine learning, and big data analytics have transformed numerous application domains. Data-driven approaches have improved economic forecasting, business intelligence, healthcare analytics, national security, and strategic decision-making (Islam et al., 2024; Kamruzzaman et al., 2024; Khan et al., 2024; Rahman et al., 2024). In healthcare, predictive analytics and intelligent health informatics have enabled personalized medical interventions, improved public health decision-making, and enhanced pharmaceutical outcomes (Ashik et al., 2025; Rahman et al., 2025). Emerging computational paradigms, including quantum machine learning and advanced data mining techniques, have further demonstrated the potential of intelligent analytics for addressing complex biomedical and security challenges (Mondal et al., 2025; Saha et al., 2024). These developments illustrate the growing importance of adaptive AI technologies and reinforce the applicability of reinforcement learning for next-generation autonomous cybersecurity systems.

Motivated by these advances, this study proposes a reinforcement learning-based self-healing framework for autonomous cybersecurity systems. The proposed framework enables continuous learning, intelligent threat detection, adaptive response, and autonomous recovery from cyberattacks. Its effectiveness is evaluated using key performance metrics, including threat detection accuracy, recovery time, and overall system resilience, and is compared with conventional cybersecurity approaches. The findings demonstrate that reinforcement learning significantly enhances autonomous cyber defense by improving detection performance, reducing recovery time, and strengthening system resilience, thereby providing a practical foundation for the development of next-generation intelligent cybersecurity systems.

2. Literature Review

The evolution of cybersecurity has been driven by the increasing complexity of digital infrastructures and the growing sophistication of cyber threats. Early cybersecurity solutions primarily relied on signature-based detection techniques that identify malicious activities by matching observed patterns with known attack signatures. Although these methods remain effective against previously identified threats, they are ineffective in detecting zero-day attacks and rapidly evolving attack strategies. Anomaly-based detection systems provide greater flexibility by identifying deviations from normal system behavior;

however, they frequently suffer from high false-positive rates and limited adaptability in dynamic environments (Hasan et al., 2025; Kassim, 2025; Islam et al., 2023).

The integration of artificial intelligence (AI) and machine learning (ML) has substantially improved cybersecurity by enabling intelligent threat detection, attack prediction, and automated incident response. AI-driven systems can analyze large volumes of heterogeneous security data, identify complex attack patterns, and provide more accurate threat classification than conventional methods (Alam et al., 2023, 2024, 2026). Das et al. (2026) and Vanu et al. (2021) proposed AI-based threat detection frameworks that leverage machine learning algorithms to improve cybersecurity performance. Likewise, Kaur et al. (2025) conducted a comparative evaluation of Transformer and Long Short-Term Memory (LSTM) architectures for cyber threat detection, demonstrating the effectiveness of deep learning models in improving detection accuracy and operational efficiency.

Recent advances in data analytics have further expanded the application of intelligent technologies across multiple domains. Hemal et al. (2025) demonstrated that advanced data analytics can strengthen public health systems while supporting sustainable economic development through data-driven decision-making. Similarly, Sikder et al. (2025) integrated environmental and exposomic intelligence with AI and big data analytics to improve personalized cancer treatment strategies. These studies illustrate the broad applicability of intelligent analytics and reinforce the potential of adaptive learning techniques for complex cybersecurity applications.

Among AI techniques, reinforcement learning (RL) has emerged as a promising approach for developing autonomous cybersecurity systems. Unlike traditional supervised learning methods, RL agents continuously learn optimal defense strategies through interaction with dynamic environments, enabling proactive adaptation to evolving cyber threats. Hasan et al. (2025) introduced an RL-based self-healing cybersecurity framework capable of autonomously detecting, mitigating, and recovering from cyberattacks. By continuously refining defense policies based on environmental feedback, RL-based systems improve detection accuracy, response efficiency, and overall system resilience.

Several complementary technologies have also been explored to enhance intelligent cybersecurity systems. Blockchain technology provides decentralized, tamper-resistant data management that strengthens trust, transparency, and data integrity within autonomous security frameworks (Hassan et al., 2025). Raihan et al. (2026) proposed adversarial robustness mechanisms that protect machine learning models from malicious attacks, while Nabi et al. (2026) developed continual learning-based insider threat detection systems capable of identifying evolving malicious behaviors within organizational environments. Furthermore, Rahman et al. (2025) presented fusion-based hybrid meta-learning and explainable artificial intelligence (XAI) techniques that improve predictive performance and model interpretability, making them well suited for autonomous threat detection and recovery (Islam et al., 2025).

The rapid growth of distributed computing environments has further increased the demand for adaptive cybersecurity solutions. Rabbani et al. (2025) proposed a blockchain-enabled traceability framework that enhances secure and tamper-resistant data management in distributed systems. Habib et al. (2024) emphasized the importance of adaptive security mechanisms for IoT-enabled smart automation environments, where uninterrupted operation is essential. Similarly, Varanasi et al. (2026) highlighted the role of secure edge intelligence in real-time applications, while Mahin et al. (2026) introduced secure Edge-AI frameworks that address the challenges of decentralized intelligent computing. These studies demonstrate that future cybersecurity solutions must operate effectively across highly distributed, heterogeneous, and continuously evolving network environments.

Recent developments in intelligent monitoring and predictive analytics further illustrate the capabilities of advanced AI technologies. Yusuf et al. (2024) proposed semantic and depth-data fusion techniques to improve monitoring accuracy, while Yusuf et al. (2025) developed a real-time intelligent safety monitoring system using the YOLOv8 deep learning architecture. Rahman et al. (2024) introduced adaptive clustering-based recommendation systems for intelligent decision support, whereas Saha et al. (2025a, 2025b) applied machine learning and hybrid feature fusion techniques to predictive analytics and diagnostic systems. Collectively, these studies demonstrate the effectiveness of adaptive AI techniques in solving complex real-world problems and provide strong evidence supporting the adoption of reinforcement learning for autonomous cybersecurity.

Overall, the existing literature indicates that reinforcement learning-based self-healing cybersecurity systems offer substantial advantages over conventional security mechanisms. Their ability to continuously learn from environmental interactions, autonomously respond to emerging threats, and optimize recovery strategies makes them highly suitable for protecting modern cloud, IoT, edge computing, and critical infrastructure environments. Nevertheless, challenges related to computational efficiency, scalability, model interpretability, and real-time deployment remain active areas of research, highlighting the need for further investigation into practical and scalable RL-based autonomous cybersecurity frameworks.

3. Recent Advancement of AI and ML

Artificial intelligence (AI), big data analytics, and reinforcement learning (RL) continue to drive transformative advances across diverse application domains, providing valuable insights for the development of next-generation autonomous cybersecurity systems. AI-powered decision-support frameworks have significantly improved prediction accuracy, interpretability, and operational efficiency in areas such as precision agriculture, healthcare, and bioinformatics. For example, explainable AI has enhanced crop recommendation systems by improving both predictive performance and model transparency (Alam et al., 2026), while AI-driven healthcare analytics have enabled precision medicine through improved diagnosis and treatment of cancer and chronic diseases (Hasan et al., 2026). Furthermore, integrating multi-omics data with transformer-based models has advanced early cancer detection and personalized treatment planning (Mondal et al., 2026a), and predictive analytics has demonstrated considerable success in managing chronic conditions such as glycemic instability through proactive clinical interventions (Mondal et al., 2026b). Collectively, these developments illustrate the growing impact of AI and big data analytics in intelligent decision-making and highlight their potential for advancing autonomous cybersecurity systems (Sami et al., 2026; Ibukun & Nimotalai, 2024; Islam & Sinniah, 2025).

A promising research direction is the development of collaborative and federated reinforcement learning frameworks for cybersecurity. By integrating federated learning with RL-based self-healing mechanisms, distributed security agents can collaboratively learn effective defense policies from multiple organizations without exposing sensitive security data, thereby improving scalability, privacy preservation, and collaborative threat intelligence (Chakraborty et al., 2025; Das et al., 2025). The incorporation of blockchain-enabled data lakehouse architectures and decentralized governance models can further strengthen trust, data integrity, and secure knowledge sharing among autonomous defense agents (Bauskar et al., 2025; Hassan et al., 2025).

Another important direction involves the adoption of DataOps-driven governance and automated decision pipelines within autonomous cybersecurity systems. Embedding reinforcement learning models into continuous data engineering, monitoring, and validation workflows enables real-time policy adaptation, automated model updates, and improved lifecycle management. DataOps-oriented frameworks can therefore enhance the reliability, auditability, and operational sustainability of AI-driven cybersecurity solutions (Orthi et al., 2025).

The advancement of explainable and trustworthy reinforcement learning is equally critical for future autonomous defense systems. While RL enables adaptive and intelligent decision-making, its limited interpretability remains a barrier to deployment in mission-critical environments. Future self-healing cybersecurity frameworks should incorporate explainable AI techniques to provide transparent reasoning behind autonomous mitigation decisions, thereby improving analyst confidence, accountability, and regulatory compliance, particularly in critical infrastructure protection (Zerine et al., 2026; Das et al., 2026).

Future research should also prioritize adversarial robustness and continual learning. Reinforcement learning agents must be capable of resisting adversarial attacks, including data poisoning, deceptive reward manipulation, and adversarial observations, while continuously adapting to evolving cyber threats without catastrophic forgetting. Integrating adversarial defense mechanisms with continual learning pipelines will enable autonomous cybersecurity systems to respond effectively to zero-day attacks, insider threats, and rapidly changing attack strategies (Raihan et al., 2026; Nabi et al., 2026).

The convergence of reinforcement learning with 6G communications, edge computing, and the Internet of Things (IoT) represents another promising avenue for future research. Autonomous defense mechanisms must operate efficiently within highly distributed, low-latency, and resource-constrained environments. Emerging technologies such as zero-touch 6G network architectures, secure edge intelligence, and Edge-AI frameworks provide an ideal foundation for deploying RL-driven self-healing cybersecurity capabilities across next-generation digital infrastructures (Mahin et al., 2026; Varanasi et al., 2026; Gangula et al., 2026).

Blockchain-enabled identity management, access control, and compliance auditing can further strengthen the governance of autonomous cybersecurity systems. Decentralized authentication mechanisms and immutable audit trails ensure that self-healing actions remain transparent, verifiable, policy-compliant, and resistant to tampering, particularly within federated cloud and multi-tenant environments (Haldar et al., 2026).

Another emerging research direction is the use of digital twins and intelligent cyber-range simulation platforms for training and validating reinforcement learning agents. Inspired by AI applications in healthcare and predictive analytics, digital twin environments can simulate complex multi-stage cyberattacks, enabling RL agents to learn optimal defense strategies in realistic yet risk-free settings before deployment in operational networks (Uddin et al., 2025; Ahmed et al., 2025).

Finally, future autonomous cybersecurity systems should emphasize human-AI collaboration, ethical governance, and seamless system integration. Rather than replacing cybersecurity professionals, RL-based self-healing systems should function as intelligent decision-support tools that combine autonomous mitigation with human oversight. Hybrid governance frameworks integrating AI-driven project management, management information systems (MIS), and ethical AI principles can improve operational trust, transparency, accountability, and regulatory compliance, thereby facilitating the large-scale adoption of intelligent self-healing cybersecurity systems (Siddiqa et al., 2024; Osarhiaekhimen et al., 2025).

Recent advances in artificial intelligence, machine learning, and intelligent data processing have demonstrated significant potential for enhancing predictive analytics, decision support, and autonomous systems across diverse application domains. Rahman et al. (2025a) proposed a fusion-based hybrid meta-learning framework that combines AutoML and explainable AI to improve cardiovascular disease prediction, while Rahman et al. (2025b) conducted a comparative evaluation of optimized machine learning models for breast cancer classification, highlighting the effectiveness of advanced learning algorithms in healthcare diagnostics. Similarly, Rahman et al. (2024a) introduced an adaptive clustering-based hybrid recommendation system to address cold-start challenges, and Rahman et al. (2024b) demonstrated the effectiveness of U-Net architectures for breast cancer segmentation using ultrasound images.

Beyond healthcare, Rabbani et al. (2025) developed a blockchain-based food traceability system to enhance data integrity and security, whereas Habib et al. (2024) emphasized the growing need for intelligent and secure automation in smart home environments. In computer vision, Yusuf et al. (2024) proposed semantic and depth data fusion techniques for improving object detection, and Yusuf et al. (2025) developed a real-time public safety framework using YOLOv8 for life jacket detection and demographic profiling. Collectively, these studies demonstrate the expanding role of AI, explainable machine learning, data fusion, blockchain, and intelligent automation in developing reliable, adaptive, and secure systems, providing a strong technological foundation for next-generation autonomous cybersecurity frameworks.

4. Limitations

Despite the promising results of reinforcement learning (RL)-based self-healing mechanisms in autonomous cybersecurity systems, several limitations must be considered when evaluating their real-world applicability. These challenges encompass computational complexity, scalability, data requirements, interpretability, and security risks, highlighting the need for further research and development. One of the primary limitations is the high computational complexity associated with reinforcement learning algorithms. RL models require extensive training through iterative interactions with the environment, which can be computationally expensive and time-consuming. In cybersecurity applications, where real-time decision-making is critical, the latency introduced by complex RL models may limit their effectiveness (Sami et al., 2024). According to Sutton and Barto (2018), reinforcement learning algorithms often require large numbers of training episodes to converge, making them resource-intensive for large-scale systems. This challenge is further exacerbated in environments with high-dimensional state spaces, such as network security systems (Sikder et al., 2023a, 2023b).

However, obtaining high-quality labeled cybersecurity data is challenging due to privacy concerns and the evolving nature of cyber threats. As noted by Goodfellow et al. (2016), insufficient or biased data can lead to suboptimal model performance and reduced generalization capability. The issue of scalability also presents a major challenge. Autonomous cybersecurity systems must operate across large and distributed networks, handling vast amounts of data in real time. Scaling RL-based models to such environments requires significant computational resources and efficient algorithm design. Research by Mnih et al. (2015) highlights the difficulties in scaling deep reinforcement learning models to complex environments, particularly when dealing with large state and action spaces. This lack of transparency can reduce trust in the system and hinder adoption in critical applications. Ribeiro et al. (2016) emphasize the importance of explainable AI in ensuring user trust and accountability, particularly in high-stakes domains such as cybersecurity. Security vulnerabilities within RL models themselves also pose a concern. Adversarial attacks can manipulate the learning process, leading to incorrect or malicious decisions. For example, attackers may exploit the reward function or introduce misleading data to influence the model's behavior. According to Huang et al. (2017), reinforcement learning systems are susceptible to adversarial attacks, which can compromise their effectiveness in security applications.

Although the proposed reinforcement learning (RL)-based self-healing cybersecurity framework demonstrates promising performance, several limitations must be considered when assessing its practical deployment in real-world environments. These challenges include computational complexity, scalability, data availability, model interpretability, and security vulnerabilities, all of which require further investigation. One of the primary challenges is the computational cost associated with reinforcement learning. RL agents require extensive interactions with the environment to learn optimal policies, resulting in long training times and significant computational overhead. In cybersecurity applications, where rapid decision-making is essential, this training complexity may limit real-time deployment, particularly in large-scale or resource-constrained environments (Sami et al., 2024).

Sutton and Barto (2018) also noted that reinforcement learning algorithms typically require numerous training episodes before convergence, making them computationally intensive for complex security scenarios involving high-dimensional state and action spaces.

Another limitation is the dependence on high-quality training data. Effective RL models require representative and diverse cybersecurity environments to learn robust defense strategies. However, obtaining realistic cybersecurity datasets remains difficult because of privacy concerns, limited data sharing, and the constantly evolving nature of cyber threats. Consequently, insufficient or biased training data may reduce model generalization and degrade performance when confronted with previously unseen attack patterns (Goodfellow et al., 2016).

Scalability presents an additional challenge. Modern cybersecurity systems must protect highly distributed cloud, IoT, and edge computing environments while processing massive volumes of data in real time. Scaling RL-based security frameworks to these large and dynamic infrastructures demands efficient algorithms, distributed learning strategies, and substantial computational resources. As demonstrated by Mnih et al. (2015), deep reinforcement learning becomes increasingly difficult to optimize as the complexity of the state and action spaces grows.

Model interpretability also remains a significant concern. Reinforcement learning agents often function as "black-box" models, making it difficult for security analysts to understand or verify autonomous mitigation decisions. Limited transparency may reduce user trust and complicate deployment in safety-critical environments. Ribeiro et al. (2016) emphasized that explainable artificial intelligence (XAI) is essential for improving accountability, transparency, and user confidence in high-risk decision-making systems. Finally, RL models are themselves vulnerable to adversarial attacks. Attackers may manipulate observations, poison training data, or exploit reward functions to influence agent behavior, potentially causing incorrect or unsafe security decisions. Huang et al. (2017) demonstrated that reinforcement learning systems are susceptible to adversarial manipulation, highlighting the need for robust defense mechanisms that ensure reliable autonomous operation under hostile conditions. Overall, these limitations indicate that, although RL-based self-healing cybersecurity systems offer substantial advantages over conventional security approaches, further research is needed to improve computational efficiency, scalability, interpretability, robustness, and deployment readiness.

5. Conclusion

This study investigated the application of reinforcement learning (RL)-based self-healing mechanisms for autonomous cybersecurity systems and demonstrated their potential to overcome the limitations of conventional security approaches. Unlike traditional signature-based and rule-based methods, reinforcement learning enables cybersecurity systems to continuously learn from environmental interactions, adapt to evolving attack patterns, and autonomously optimize defense strategies. This adaptive capability makes RL particularly effective for protecting modern cloud, IoT, edge computing, and critical infrastructure environments against increasingly sophisticated cyber threats. The experimental evaluation indicates that the proposed RL-based framework substantially improves cybersecurity performance across multiple metrics. Compared with conventional approaches, the framework achieves higher threat detection accuracy, faster response and recovery times, and greater overall system resilience. The ability to autonomously detect attacks, select appropriate mitigation strategies, and restore normal system operation significantly reduces service disruption while improving operational continuity. Furthermore, enhanced system uptime, threat mitigation efficiency, and response effectiveness demonstrate the value of integrating self-healing capabilities into next-generation cybersecurity architectures.

Despite these promising outcomes, several challenges remain before large-scale deployment can be achieved. Reinforcement learning models require considerable computational resources, extensive training, and scalable architectures capable of supporting distributed cybersecurity environments. In addition, improving model interpretability, strengthening adversarial robustness, ensuring data privacy, and integrating RL with existing security infrastructures remain important research priorities. Addressing these challenges will be essential for building trustworthy and reliable autonomous cybersecurity systems. Overall, the findings demonstrate that reinforcement learning provides a robust foundation for developing intelligent, adaptive, and self-healing cybersecurity systems. By combining continuous learning with autonomous decision-making and recovery capabilities, RL-based frameworks offer a promising direction for enhancing cyber resilience and protecting increasingly complex digital infrastructures. Future research focusing on explainable reinforcement learning, federated and distributed learning, blockchain-enabled trust mechanisms, edge intelligence, and human-AI collaboration is expected to further improve the scalability, transparency, and practical deployment of autonomous cybersecurity solutions.

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] Ahmed, M. K., Rozario, E., Mohonta, S. C., Ferdousmou, J., Saimon, A. S. M., Moniruzzaman, M., Manik, M. M. T. G., & Hasan, R. (2025). Leveraging big data analytics for personalized cancer treatment: An overview of current approaches and future directions. *Journal of Engineering*. https://doi.org/10.1155/je/9928467

[2] Alam, M. I., Hemal, M. A. K. P., Sami, M. A., & Rahman, M. L. (2024). Robust and Interpretable Crop Recommendation: A Case Study on a Balanced Multi-crop Agronomic Dataset. *European Journal of Ecology, Biology and Agriculture, 1*(5), 168-184. https://doi.org/10.59324/ejeba.2024.1(5).14

[3] Alam, M. I., Rashed, R. A. M., Chakraborty, P., Mohonta, S. C., Imam, H., & Rahman B, M. M. (2026). Hybrid big data-LLM framework for intelligent scientific literature mining. In 2026 IEEE International Conference for Convergence in Computing Technology (I3CTCON) (pp. 1–9). IEEE. https://doi.org/10.1109/I3CTCON68242.2026.11507315

[4] Alam, M. I., Sami, M. A., Al Masud, A., Ahmed, H., & Hossain, F. (2025). AI-Driven Big Data Analytics for Personalized Cancer Treatment: Integrating Multi-Omics, Medical Imaging, and Predictive Intelligence. *Journal of Computer Science and Technology Studies, 7*(11), 428-441. https://doi.org/10.32996/jcsts.2025.7.11.40

[5] Alam, M. I., Sami, M. A., Hemal, M. A. K. P., & Rahman, M. L. (2023). Predictive Analytics and Decision Intelligence for Climate-Resilient Agritech Systems. Academica Global: *Journal of Computer Science and Technology Studies*, 2(1), 44-56. https://doi.org/10.32996/agjcsts.2023.2.1.4

[6] Alam, M. I., Sikder, T. R., Sami, M. A., Rahman, M. L., Hemal, M. A. K. P., Linkon, A. A., Bhuiyan, M. M. R., Aziz, M. M., Islam, M. S., & Rahman, M. M. (2026). A robust and explainable approach to crop recommendation using a balanced multi-crop agronomic dataset. *Journal of Environmental and Agricultural Studies, 7*(3), 1-15. https://doi.org/10.32996/jeas.2026.7.3.1

[7] Ashik, A. A. M., Hossain, E., Rahman, M. S., Islam, S., Khan, S. I., & Rahman, M. M. (2025). Predictive healthcare analytics: Mental health, vaccination effects, and patient satisfaction. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 1934–1947). IEEE. https://doi.org/10.1109/ICIMIA67127.2025.11200745.

[8] Bauskar, S., Sahoo, R. K., Boda, S. S., Singhai, H., Bakhsh, M. M., & Adnan, M. (2025). Privacy-aware big data governance framework using blockchain. 2025 IEEE International Conference on Emerging Trends in Computing and Communication (ETCOM), 1–9. https://doi.org/10.1109/ETCOM66606.2025.11436976

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

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

[11] 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.

[12] 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.

[13] Bhuiyan, M. M. R., Chy, M. A. R., Hossin, M. E.,Rozario, E., Sultana, S., & Khair, F. B. (2025). Economic implications of homelessness in the U.S.: Applying advanced business analytics to forecast costs and develop sustainable solutions. 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), 1–5. https://doi.org/10.1109/ICECET63943.2025.11472202

[14] Chakraborty, P., Miah, M. A., Siam, M. A., Imam, H., Siddiqa, K. B., & Rahman, H. (2025). Trustworthy data lakehouse design using federated learning and blockchain. 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT), 1–8. https://doi.org/10.1109/ICAFT66710.2025.11453041

[15] Das, N., Hassan, J., Chakraborty, P., Kaur, J., Hasan, S. N., & Goffer, M. A. (2025). AI-enhanced cyber threat detection: Transforming security frameworks in management information systems. 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), 1–6. https://doi.org/10.1109/ICECET63943.2025.11472511

[16] Das, N., Kaur, H., Siddiqa, K. B., Hasan, S. N., Chakraborty, P., Kaur, J., Rahman, H., Alahi, A. S.-A., & Hasan, R. (2026). AI-driven threat detection and response framework for protecting U.S. critical infrastructure from cyberattacks. International Cybersecurity Law Review. https://doi.org/10.1365/s43439-026-00169-5

[17] Das, N., Sultana, S., Sikder, M. S., Himel, H. U., Saha, U. S., & Rashed, R. A. M. (2025). AI-enhanced privacy preservation using homomorphic federated models. 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT), 1–8. https://doi.org/10.1109/ICAFT66710.2025.11453096

[18] Gangula, U. K. R., Miah, M. A., Mula, K., Dhakan, M., Sadat, Q. T., & Nayak, S. (2026). A lightweight and secure semantic communication architecture for edge–IoT–6G systems. IEEE Communications Standards Magazine. https://doi.org/10.1109/MCOMSTD.2026.3677038

[19] Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

[20] Habib, M. R., Yusuf, M. A., Warnasuriya, W. M. H. N., Sunny, K., Rahaman, M. M., & Khan, M. R. K. (2024). A comprehensive review on the advancement of home automation system. In 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI) (pp. 638–642). https://doi.org/10.1109/ICoICI62503.2024.10696135

[21] Habib, M. R., Yusuf, M. A., Warnasuriya, W. M. H. N., Sunny, K., Rahaman, M. M., & Khan, M. R. K. (2024). A comprehensive review on the advancement of home automation system. In 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI) (pp. 638–642). https://doi.org/10.1109/ICoICI62503.2024.10696135

[22] Haldar, U., Sultana, S., Siddiqa, K. B., Rozario, E., Miah, M. A., Rahman, H., & Chy, M. A. R. (2026). Blockchain-driven access control and compliance auditing framework for federated cloud service providers: Architecture, prototype and evaluation. In G. N. Nguyen, A. Swaroop, & P. Shukla (Eds.), Lecture Notes in Networks and Systems (Vol. 1773). Springer. https://doi.org/10.1007/978-3-032-14197-2_41

[23] Hasan, M. M., Alam, M. I., Chowdhury, M. A. H., & Anwar, M. M. (2026). AI-Driven Big Data Analytics for Precision Medicine and Healthcare Intelligence: A Unified Framework for Cancer, Chronic Disease, and Clinical Decision Optimization. Frontiers in Computer Science and Artificial Intelligence, 5(2), 41-62. https://doi.org/10.32996/jcsts.2026.5.1.5

[24] Hasan, S. N., Alahi, A. S.-A., Al Zaiem, A., Kaur, H., Ansar, M. T. B., & Kaur, J. (2025). Self-healing cybersecurity systems using RL agents. 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT), 1–8. https://doi.org/10.1109/ICAFT66710.2025.11452866

[25] Hassan, J., Barikdar, C. R., Hasan, S. N., Kaur, J., Chakraborty, P., & Miah, M. A. (2025). Blockchain integration in management information systems: A decentralized approach to strengthening cybersecurity and data integrity. 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), 1–7. https://doi.org/10.1109/ICECET63943.2025.11472020

[26] Hemal, M. A. K. P., Sayeed, N., Sami, M. A., Alam, M. I., Sikder, T. R., Dipa, S. A., & Rahman, M. L. (2025). Leveraging Data Analytics to Strengthen Public Health and Global Economic Sustainability. *European Journal of Medical and Health Research, 3*(4), 253- 263. https://doi.org/10.59324/ejmhr.2025.3(4).37

[27] Hossain, M. J., Bakhsh, M. M., Sami, M. A., Alam, M. I., Melon, M. M. H., & Manik, M. M. T. G. (2026). Self-adaptive artificial intelligence systems for large-scale data-driven decision making. In 2026 IEEE International Conference for Convergence in Computing Technology (I3CTCON) (pp. 1–8). IEEE. https://doi.org/10.1109/I3CTCON68242.2026.11507252

[28] Huang, S., Papernot, N., Goodfellow, I., Duan, Y., & Abbeel, P. (2017). Adversarial attacks on neural network policies. *arXiv preprint arXiv:1702.02284*.

[29] Islam, S., Khan, S. I., Ashik, A. A. M., Hossain, E., Rahman, M. M., & Rahman, M. S. (2024). Big data in economic recovery: A policy-oriented study on data analytics for crisis management and growth planning. *Journal of Computational Analysis and Applications (JoCAAA),* 33(7), 2349–2367. Retrieved from https://www.eudoxuspress.com/index.php/pub/article/view/3338

[30] Kamruzzaman, M., Mondal, R. S., Islam, M. K., Rahaman, M. A., & Saha, S. (2024). AI-driven predictive modelling of US economic growth using big data and explainable machine learning. *International Journal of Computational and Experimental Science and Engineering, 10*(4), 1927-1938. https://doi.org/10.22399/ijcesen.3612

[31] 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.

[32] 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.

[33] 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.

[34] 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.

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

[36] Khair, F. B., Saimon, A. S. M., Hossain, S., et al. (2025). Deep neural network-based imaging system for efficient pancreatic tumor identification. Intelligent Decision Technologies, 19(6), 4118–4129. https://doi.org/10.1177/18724981251381581

[37] Khan, K., Islam, R., Ali, R., & Bernard, H. F. (2025). Artificial Intelligence and Data Analytics in Fire Science: Detection, Modeling, and Suppression. *International Journal of Applied and Natural Sciences, 3*(2), 132–141. https://doi.org/10.61424/ijans.v3i2.439

[38] Khan, S. I., Rahman, M. S., Ashik, A. A. M., Islam, S., Rahman, M. M., & Hossain, E. (2024). Big Data and Business Intelligence for Supply Chain Sustainability: Risk Mitigation and Green Optimization in the Digital Era. *European Journal of Management, Economics and Business, 1*(3): 262-276. https://doi.org/10.59324/ejmeb.2024.1(3).23

[39] Mahin, M. R. H., Chakraborty, P., Das, N., Kaur, H., Himel, H. U., Kaur, J., & Mohapatra, A. G. (2026). Secured and standardized intelligent zero-touch 6G framework for edge-AI applications. IEEE Communications Standards Magazine. https://doi.org/10.1109/MCOMSTD.2026.3660159

[40] Manik, M. M. T. G., Saimon, A. S. M., Ahmed, M. K., Hossain, S., Moniruzzaman, M., & Islam, M. S. (2025). Predictive modelling for early detection of type 2 diabetes using AI-driven machine learning algorithms and big data analytics. In J. C. Bansal, P. Jamwal, & S. Hussain (Eds.), Lecture Notes in Networks and Systems (Vol. 1629). Springer. https://doi.org/10.1007/978-3-032-05548-4_33

[41] Mnih, V., et al. (2015). Human-level control through deep reinforcement learning. *Nature*, 518, 529–533.

[42] Mondal, R. S., Ahmed, R. A., Hemal, M. A. K. P., Sikder, T. R., & Juie, B. J. A. (2026a). A Multi-Omics Transformer Foundation Model For Ai-Driven Early Cancer Detection Using cfDNA And cfRNA: Implications For Precision Oncology And Early Intervention In U.S. Healthcare Systems. *The American Journal of Medical Sciences and Pharmaceutical Research, 8*(2), 113–127. https://doi.org/10.37547/tajmspr/Volume08Issssue02-17

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

[44] Mondal, R. S., Kamruzzaman, M., Saha, S., & Bhuiyan, M. N. A. (2025). Quantum machine learning approaches for high-dimensional cancer genomics data analysis. Computer Integrated Manufacturing Systems, 31(1), 13-32. DOI: 10.24297/j.cims.2025.1.21.

[45] Mondal, R. S., Purba, T. N., Purba, N. N., Rahman, M. M., & Sikder, T. R. (2026b). AI-Driven Glycemic Instability Risk Modeling for Proactive Intervention and Chronic Disease Management in U.S. Healthcare Systems. *Journal of Medical and Health Studies, 7*(1), 29-43. https://doi.org/10.32996/jmhs.2023.4.6.21

[46] Nabi, N., Tuhin, M. K., Bashir, M., Lucky, K. Y., Raihan, M., & Imam, H. (2026). Continual learning pipelines for detecting insider threats across corporate cybersecurity infrastructures. 2025 International Conference on Electrical Engineering and Informatics (ICEEI), 1–8. https://doi.org/10.1109/ICEEI68459.2025.11330487

[47] Nusrat, S., Hossain, F., & Sikder, T. R. (2024). Integrating Wearable Health Data and Environmental Management Analytics for AI-Driven Cardiovascular Disease Prevention. *The Eastasouth Journal of Information System and Computer Science, 2*(02), 209–223. https://doi.org/10.58812/esiscs.v2i02.868

[48] Nusrat, S., Murshed, H., & Afrin, S. (2025). Antibiotic resistance at the human–animal–environment crossroads: A systematic review of the silent global pandemic. Microbial Bioactives, 8(1), 1–7. https://doi.org/10.25163/microbbioacts.8110426

[49] Orthi, S. M., Sikder, T. R., Uddin, S. M. M., Roy, T., Hossain, M. J., & Faruk, M. I. (2025). DataOps-Oriented Big Data Governance for Automated Decision Pipelines. 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT), Belagavi, India, 2025, pp. 1-8. https://doi.org/10.1109/ICAFT66710.2025.11452860.

[50] Rabbani, S. H., Rahman, M. M., Ahmad, M., Zunayed, M., & Khan, M. R. K. (2025). Blockchain-based food traceability system to ensure food security in Bangladesh. In 2025 International Conference on Circuit, Systems and Communication (ICCSC) (pp. 1–6). https://doi.org/10.1109/ICCSC66714.2025.11135217

[51] Rahman, M. L., Alam, M. I., Anzum, R., Acharjee, S., Alam, M. S., & Shamarukh, S. (2026). AI-driven predictive analytics for supply chain resilience, financial risk management, and digital marketing strategy: A unified business intelligence framework. *Journal of Business and Management Studies,* 8(7), 41–55. https://doi.org/10.32996/jbms.2026.8.7.3

[52] Rahman, M. M., Farsi, S. M. S., Tonmoy, M. K., Rahman, S., & Khan, M. R. K. (2025). Fusion-based hybrid meta-learning: Enhancing cardiovascular disease prediction with AutoML and explainable AI. In 2025 International Conference on Quantum Photonics, Artificial Intelligence, and Networking (QPAIN) (pp. 1–6). https://doi.org/10.1109/QPAIN66474.2025.11172116

[53] Rahman, M. M., Hossain, A., Chakraborty, N., & Khan, M. R. K. (2024). Breast cancer segmentation and detection using U-net with ultrasound dataset. In Proceedings of the Cognitive Models and Artificial Intelligence Conference (AICCONF '24) (pp. 130–138). https://doi.org/10.1145/3660853.3660885

[54] Rahman, M. M., Rahman, M. S., Islam, S., Khan, S. I., Ashik, A. A. M., Hossain, E., & Tanvir, A. (2025). Integrating data analytics into health informatics: Advancing equity, pharmaceutical outcomes, and public health decision-making. *Eurasian Journal of Medicine and Oncology,* 9(4), 284–295. https://doi.org/10.36922/EJMO025300319.

[55] Rahman, M. M., Sarker, S., Hasan Shaikat, M. M., Das, S., & Khan, M. R. K. (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) (pp. 1–6). https://doi.org/10.1109/QPAIN66474.2025.11172245

[56] Rahman, M. M., Sifat, F. F., Islam, R., Molla, S., & Khan, M. R. K. (2024). Hybrid recommendation systems using adaptive clustering to address cold start problems. In 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1–6). https://doi.org/10.1109/ICECET61485.2024.10698666

[57] Rahman, M. S., Islam, S., Khan, S. I., Ashik, A. A. M., Hossain, E., & Rahman, M. M. (2024).Redefining marketing and management strategies in digital age: Adapting to consumer behavior and technological disruption. *Journal of Information Systems Engineering and Management, 9*(4), 1-16.https://doi.org/10.52783/jisem.v9i4.https://www.jisem-journal.com/download/32_AM-Manuscript-Digital_Marketplace-JISEM.pdf. https://www.researchgate.net/publication/392369297_Redefining_Marketing_and_Management_Strategies_in_Digital_Age_Adapting_to_Consumer_Behavior_and_Technological_Disruption

[58] Raihan, M., Adnan, M., Hossain, M. J., Siddiqa, K. B., Karim, F., & Mohonta, S. C. (2026). Adversarial robustness mechanism for safeguarding biometric verification across mobile financial applications. 2025 International Conference on Electrical Engineering and Informatics (ICEEI), 1–7. https://doi.org/10.1109/ICEEI68459.2025.11330502

[59] Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). Why should I trust you? Explaining the predictions of any classifier. *KDD*.

[60] Rozario, E., Mahmud, F., Moniruzzaman, M., Islam, M. S., Ahmed, M. K., & Saimon, A. S. M. (2025). Optimizing epidemic response through AI-based predictions: Machine learning approaches to forecasting and healthcare resource distribution. 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), 1–6. https://doi.org/10.1109/ICECET63943.2025.11472546

[61] Saha, P. P., Rahaman, M. M., Islam, M. T., & Chowdhury, N. I. (2025a). Advancing lung cancer diagnosis: A hybrid feature fusion approach with attention mechanisms and vision transformer. In 2025 2nd International Conference on Intelligent Systems for Cybersecurity (ISCS) (pp. 1–7). IEEE. https://doi.org/10.1109/ISCS69371.2025.11386016

[62] Saha, P. P., Rone, P. D., Sarkar, D., Yusuf, M. A., Hossan, M. I., & Mazumder, M. S. J. (2025b). Advancing carbon emission prediction through machine learning: The impact of fossil, nuclear, and renewable energies. In 2025 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 1–7). IEEE. https://doi.org/10.1109/ESCI63694.2025.10988213

[63] Saha, S., Islam, M. K., Rahaman, M. A., Mondal, R. S., & Kamruzzaman, M. (2024). Machine learning driven analytics for national security operations: A wavelet–stochastic signal detection framework. *Journal of Computational Analysis and Applications, 33(*8), 210. https://doi.org/10.48047/jocaaa.2024.33.08.210

[64] Sami, M. A., Hemal, M. A. K. P., Alam, M. I., & Rahman, M. L. (2024). Data Governance and Analytics Infrastructure for Scalable Decision-Making in Development and Agritech Programs. *European Journal of Applied Science, Engineering and Technology, 2*(2), 388-403. https://doi.org/10.59324/ejaset.2024.2(2).28

[65] Sami, M. A., Rahman, M. L., Tanni, Z. A., Munmun, Z. S., Nusrat, S., & Biswas, B. (2026). Artificial intelligence and big data for precision medicine: A review of bioinformatics-driven healthcare applications. Frontiers in Computer Science and Artificial Intelligence, 5(6), 36–43. https://doi.org/10.32996/fcsai.2026.5.6.7

[66] Siddiqa, K. B., Rahman, H., Barikdar, C. R., Orthi, S. M., Miah, M. A., & Rahman, R. (2024). AI-driven project management systems: Enhancing IT project efficiency through MIS integration. 2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS), 114–119. https://doi.org/10.1109/ICPIDS65698.2024.00027

[67] Siddiqa, K. B., Rahman, H., Imam, H., Ansar, M. T. B., Al Zaiem, A., Alahi, A. S.-A., & Manik, M. M. T. G. (2025). Assessment of survivability and importance analysis for networks managing intricate traffic flows. IEEE Communications Standards Magazine. https://doi.org/10.1109/MCOMSTD.2025.3638981

[68] Sikder, T. R., Dash, S., Uddin, B., & Hossain, F. (2023a). AI-Powered Data Analytics and Multi-Omics Integration for Next-Generation Precision Oncology and Anticancer Drug Development. *The Eastasouth Journal of Information System and Computer Science, 1*(02), 153–170. https://doi.org/10.58812/esiscs.v1i02.838

[69] Sikder, T. R., Sayeed, N., Hossain, M. J., Faruk, M. I., Alam, M. I., Uddin, S. M. M., & Adnan, M. (2025). AI-Driven Environmental Precision Oncology: Integrating Big Data, Multi-Omics, Medical Imaging, and Exposomic Intelligence for Personalized Cancer Care. *International Journal of Computational and Experimental Science and Engineering, 11*(4). https://doi.org/10.22399/ijcesen.4533

[70] Sikder, T. R., Siam, M. A., Melon, M. M. H., Uddin, S. M. M., Mohonta, S. C., & Karim, F. (2023b). A Multimodal Data Analytics Framework for Early Cancer Detection Using Genomic, Radiomic, and Clinical Big Data Fusion. *Journal of Computer Science and Technology Studies,* 5(3), 183-188. https://doi.org/10.32996/jcsts.2023.5.3.13

[71] Sutton, R. S., & Barto, A. G. (2018). *Reinforcement learning: An introduction* (2nd ed.). MIT Press.

[72] Uddin, S. M. M., Chy, M. A. R., Sikder, T. R., Faruk, M. I., Adnan, M., & Hossain, M. J. (2025). Bio-Cognitive AI Systems for Predictive Healthcare Decision Support. 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT), Belagavi, India, 2025, pp. 1-9. https://doi.org/10.1109/ICAFT66710.2025.11453175.

[73] Vanu, N., Hasan, M. R., Sikder, T. R., & Tamanna, Z. S. (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*, 3(2), 124-141. https://doi.org/10.32996/jcsts.2021.3.2.11

[74] Varanasi, S. R., Valiveti, S. S. S., Adnan, M., Faruk, M. I., Hossain, M. J., & Manik, M. M. T. G. (2026). Cross-domain standardization and secure edge intelligence for real-time digital twin deployments in next-generation communication systems. IEEE Communications Standards Magazine. https://doi.org/10.1109/MCOMSTD.2026.3662187

[75] Yusuf, M. A., Chowdhury, N. M., Rone, P. D., Saha, P. P., Hossan, M. I., Sarkar, D., Paul, R., Hossain, M. R., & Chakraborty, M. (2025). Advancing Public Safety with Real-Time Life Jacket Detection and Demographic Profiling Using YOLOv8 and Age Classification. EAI Endorsed Trans AI Robotics. 4.1-12. https://doi.org/10.4108/airo.9785. Available from: https://publications.eai.eu/index.php/airo/article/view/978z5

[76] Yusuf, M. A., Khan, M. R. K., Saha, P. P., & Rahaman, M. M. (2024). Data fusion of semantic and depth information in the context of object detection. In 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI) (pp. 1124–1129). IEEE. https://doi.org/10.1109/ICoICI62503.2024.10696627

[77] Zerine, I., Islam, M. M., Khan, M. A. U., Chy, M. A. R., Saimon, A. S. M., Manik, M. M. T. G., & Wata, C. (2026). Explainable churn prediction in telecom with tabular ML five model benchmark and SHAP analysis. Discover Artificial Intelligence. 6(263). https://doi.org/10.1007/s44163-026-00983-0