Journal for Technology and Science
Homepage : https://journal.antispublisher.com/index.php/IPTEKS/index
Email : admin@antispublisher.com

e-ISSN : 3047-4337
JOTECH, Vol. 3, No. 1, January 2026
Page 85-96

Blockchain-Integrated Machine Learning for Secure Data Management and Cloud Computing

Tonoy Kanti Chowdhury[1], K. M. Mohi uddin[2]
[1,2]Washington University of Science and Technology

DOI : https://doi.org/10.61796/ipteks.v3i1.452

Sections Info

Article history:
Submitted: November 23, 2025
Final Revised: December 11, 2025
Accepted: January 15, 2026
Published: January 31, 2026

Keywords:
Blockchain
Machine Learning
Cloud Computing
Data Security
Secure Data Management
Decentralized Systems
Data Integrity
Privacy Protection
Intelligent Security
Distributed Ledger Technology

ABSTRACT

Objective : *This paper discusses how blockchain and machine learning can work together in improving the security of handling data in cloud computing systems.* ***Method :*** *The framework proposed uses blockchain to provide data integrity and access control and auditability, and machine learning models are used to identify security threats, allocate resources to improve resource use, and enhance performance.* ***Results :*** *It has been shown that machine learning with blockchain will greatly enhance trust, security, and efficiency in the data management of a cloud-based environment.* ***Novelty :*** *The solution to the critical challenges of data security, privacy, integrity, and trust in multi-tenant and decentralized cloud settings is addressed by combining blockchain technology with machine learning, which helps overcome major security flaws, including unauthorized access, data tampering, and insider threats.*

INTRODUCTION

The explosive nature of cloud computing has fundamentally changed the manner in which organizations store, process and manage data by providing them with an opportunity to scale, access computational resources as and when they are required. These advantages notwithstanding, cloud-based infrastructures continue to experience ongoing challenges based on data confidentiality, integrity, availability, and trust especially in a setting that has a number of stakeholders and data distributed ownership. The insider attacks, unauthorized access, data leakage, and advanced persistent threats are cyber threats that have been exposing vulnerability in conventional centralized cloud security models [1], [2].

Machine learning (ML) has become one of the most effective means of improving cybersecurity with the help of smart threat detection, behavior analysis, anomaly detection, and predictive analytics. Previous research proves that ML is effective in detecting insider threats, fraud trends, encrypted traffic abnormalities, and advanced cyberattacks in various areas such as healthcare, electronic commerce, and systems in the national infrastructure [1], [3], [4], [10]. Nonetheless, systems powered by MLs in a cloud setting still suffer the risk of data manipulation, model poisons, absence of visibility, and centralized trust components.

The decentralized nature, cryptographic security, immutability, and transparent auditability of blockchain technology has been attracting more and more attention as a complement to these constraints. The blockchain systems offer storage of data that is not tampered with, decentralized access control, and history of transactions, which is essential to safe cloud data management. The latest studies introduce the possibility of blockchain-based systems to enhance cybersecurity, secure critical infrastructure, and improve trust in decentralized systems [6], [7]. However, blockchain is not sufficient to provide the adaptive intelligence needed to provide proactive cyber threat identification and the optimization of cloud activity.

Combining blockchain with machine learning is an encouraging paradigm of secure cloud computing in the next generation. The hybrid frameworks can deal with both the enforcement of security and the intelligent threat response by incorporating the aspects of trust and immutability of blockchain and the predictive and adaptive potential of ML. The idea of AIs-enabled systems to detect and automatically eliminate advanced attacks in real-time on critical systems has been examined a decade prior [11], [8]. Besides, interpretable and grounded-on-data ML methods have proven to be useful in improving transparency, decision-making, and risk management in complex systems [4], [12], [13].

In spite of these developments, there is a gap in the research of integrating blockchain with machine learning in the security, scalability, and reliability of data management in the cloud computing setting systematically. The literature of research tends to highlight the two approaches of ML-based security or blockchain-based trust mechanisms separately, without much attention to their joint architectural design, operational synergy, and cloud-related implementation issues. This gap is important to achieve resilient cloud infrastructures that can respond to advanced cyber threats and at the same time provide data privacy, integrity, and compliance.

This paper seeks to discuss a machine learning system that incorporates blockchain in ensuring the safety of data stored on the cloud. Using blockchain as a source of decentralized trust and ML as a tool to analyze security threats intelligently, the proposed solution can improve the data protection, threat identification, and efficiency of the system in the contemporary cloud ecosystems.

Literature Review

The literature review provides the synthesis of available work regarding machine learning-based cybersecurity, artificial intelligence-driven data protection, and blockchain-based trust mechanisms to provide the theoretical framework of blockchain-based machine learning in cloud computing. The articles under review cover various areas of application, such as cloud security, healthcare information systems, critical infrastructure protection, and intelligent risk evaluation. The importance of machine learning as the tool of predictive threat detection, anomaly detection, and decision-support is highlighted, and the use of blockchain technologies to support the integrity, transparency, or decentralized trust of the data [1], [2], [6]. The thematic way of structuring the literature in this section unveils both the advantages and drawbacks of

the current methods and determines the most significant gaps in the research that encourage the combination of blockchain and machine learning to maintain secure data management in cloud computing.

Cybersecurity and Data Protection by machine learning

Machine learning has been widely used to improve cybersecurity based on smart pattern recognition, anomaly detection, and forecast predictive threat analytics. The results of Mamun confirmed that the efficiency of multimodal predictive analytics is higher when it is based on system logs, behavioral, and physical security data to identify insider threats [1]. Their results indicate the ability of ML models to detect complicated threat patterns that cannot be addressed by rule-based security systems. On the same note, Soumik pointed out how artificial intelligence and predictive data analytics can help protect sensitive healthcare data, specifically electronic health records, by implementing proactive threat identification and privacy-enhancing security controls [2].

The use of ML in various cybersecurity fields has been confirmed by various studies. The study by Soumik on fraud detection and personalized recommendations in the context of e-commerce demonstrates that machine learning-based security analytics is scalable in systems with high data volumes [3]. Have gone a step ahead to present explainable anomaly detection techniques of encrypted network traffic, which is the issue of ensuring security visibility and at the same time data confidentiality. All these studies prove the fact that ML is one of the fundamental elements of intelligent security systems in contemporary data environments [4].

AI-based Security in Healthcare and Critical Infrastructure

The use of AI-driven security models in the fields of healthcare and national critical infrastructure has been well-researched because of the delicacy and social ramifications of these systems. Rony used artificial intelligence to enhance real-time identifying and controlling the outbreak of infectious diseases, emphasizing the importance of intelligence based on data in the national preparedness system [5]. Similarly, suggested using a graph-based and network-based approach to healthcare IT infrastructure to improve the resilience and data safety of the system by using artificial intelligence [9].

In addition to healthcare, AI-based solutions have been created in cybersecurity to address sophisticated cyber threats to critical infrastructure. Developed AI-assisted cyber defense equipment to protect the immigration databases, biometric identity, and border-control devices against the attacks of nation-states [10]. Also, AI-driven machine learning systems were introduced by Frontiers in Computer Science and Artificial Intelligence which allowed detecting and automatically reducing threats in real time in critical infrastructure environments [11]. These papers highlight the significance of smart and automated security controls within large and high risk data systems.**Blockchain-based Security and Trust**

The blockchain technology has become a promising way of dealing with the problem of trust, transparency and data integrity issues in distributed systems. The idea of blockchain being used to enhance cybersecurity of national critical infrastructure was

proposed by Rony who introduced a mathematical and AI-blockchain integrated framework and showed how blockchain may allow the creation of immutable audit trails and the decentralization of trust enforcement [6]. Further advanced it by constructing quantum enhanced, privacy-preserving AI-based models combined with blockchain theory to prevent external cyber attacks on sensitive government and healthcare information [7].

These works emphasize the possible use of blockchain to prevent the risk of tampering data, unauthorized access, and single points of failure. Nevertheless, blockchain can guarantee the data immutability and accountability, but does nothing to find dynamic and changing cyber threat, especially in cloud-based environments where data has high velocity and heterogeneity.

Smart Risk Analysis and Data Mining

Risk evaluation and informed decision making are also important in managing secure systems. The need to consider continuous risk assessment of interconnected digital ecosystems is shown by Soumik who introduced dynamic risk scoring mechanisms to the third-party data feeds and APIs based on cyber threat intelligence [8]. Predictive modeling and data analytics methods have as well been used to achieve operational efficiency and risk reduction in complex systems, such as project management and dynamic environments [12], [13], [14].

Such designs focus on what can be described, on transparency and on adaptability, which are key qualities of trust-based security systems. Nevertheless, the current risk analytics systems tend to have a centralized architecture, which restricts their resistance to insider threats and security breaches at a single point.

Gaps in research and motivation

Most of the existing studies do not consider machine learning-based cybersecurity and blockchain-enabled trust mechanisms as separate entities, even though comprehensive research has been done on these technologies. Not much effort has been done to organize their systematic use towards the secure management of data in cloud computing environments. ML-based systems are vulnerable to data integrity and centralized trust dependency and blockchain-based systems are not adaptable with real-time scalable intelligence to detect threats. This gap indicates the necessity of an integrated machine learning framework, based on blockchain, where the trust is decentralized, analytics is smart in its security, and the cloud data can be managed at scale.

Problem Statement

The cloud computing environment is moving rapidly towards data collection, storage, and processes of large scale to facilitate important applications in healthcare sector, government, e-commerce, and national infrastructure systems. Even though the level of cloud security has improved, the current architectures are still susceptible to high-quality cyber threats, such as insider attacks, data manipulation, unauthorized entry, and advanced persistent threats. Machine learning security solutions have been

proven to be effective in predictive analytics, anomaly detection, and automatic threat identification but these systems are mostly installed on centralized cloud architectures, which are vulnerable to data integrity breaches, model corruption, and points of failure [1], [4].

The decentralized trust and immutability as well as transparent auditability provided by blockchain technology help to resolve the issues of extreme importance when it comes to data integrity and access control. Previous studies have indicated that blockchain-based systems can enhance cybersecurity and safeguard sensitive information in the critical infrastructures and healthcare systems [6], [7]. However, blockchain systems are not adaptively intelligent and analytically dynamic to identify dynamic cyber threats and optimize security measures in changing cloud settings [11].

The use of machine learning to conduct security analytics and blockchain to create trust are mostly viewed as separate solutions in existing literature. There is little literature addressing their coherent incorporation to offer safe, scalable and intelligent data management in cloud computing applications. What is more, existing risk assessment and cybersecurity analytics systems still tend to be based on centralized monitoring and more rigid security policies, which are inadequate in managing the complexity and speed of modern cloud data ecosystems [8], [10].

Thus, the main issue that is discussed within the framework of this research is the lack of a combined blockchain-machine learning system that provides both stability of data, decentralization of trust, smart threat identification and scalable security administration in cloud-computing systems. This issue needs to be addressed to create robust cloud infrastructures that could protect sensitive data without reducing the performance, transparency, and trust of various stakeholders.

RESEARCH METHOD

In this section, the methodological approach, which will be used to explore the integration of blockchain and machine learning in securing data management in cloud computing settings, will be outlined. The methodology will serve the purpose of coming up with a solution to the identified security, trust, and scalability issues by integrating smart analytics and decentralized trust enforcement. It is based on the previous studies on the AI-based cybersecurity, predictive analytics, anomaly detection, and blockchain-based security design [1], [2], [6], [11].

Research Design

The research design adopted in the study is a conceptual and analytical design, as it addresses the evolution and analysis of a blockchain-enhanced machine learning system of cloud information safety. This design allows the logical study of architectural elements, information flow, and information security without bounding to a specific field of application. The application of the similar analytical and framework-based approaches

to the study of cybersecurity, critical infrastructure protection, and intelligent system design has been both successful in the past [2], [6], [10].

Data Sources and Cloud Environment

This methodology takes into account the heterogeneous data that occurs in clouds computing such as system logs, user access logs, behavioral logs, API logs, and encrypted network logs. Such types of data are typical of the real-world cloud infrastructure and match the datasets in insider threat detection, anomalies analysis, and research of cyber threats [1], [4], [9].. The cloud environment is supposed to be multi-tenant, distributed and moving with the current cloud deployment models.

Machine Learning based security analyses

Intelligent detection of threats, anomaly detection and risk assessment are the functions of the machine learning aspect of the methodology. Learning methods, both supervised and unsupervised, are both included to process historical and real-time cloud data. Known threat classification is carried out with the help of supervised models, and previously unseen or changing attack patterns are detected with the help of unsupervised models. Such methods align with the previous uses of ML in detecting fraud and insider threats and monitoring cybersecurity [1], [3].

To promote transparency and trust, the explainable analytics are introduced into the ML layer and allow the interpretation of the model decisions and model anomaly scores. Achievable machine learning has been proven to make intelligent security systems reliable and easier to adopt, especially in sensitive and regulated settings [4]. Moreover, an automatic risk scoring system is used to constantly determine the security position of the cloud resources, users, and third-party data feeds [8].

Data Integrity and Access Control, based on blockchain

The blockchain technology is integrated to offer decentralized trust, data records that are immutable, and access control measures that are secure. Events related to security, access logs and integrity checks are stored on the blockchain, in order to provide tamper resistant and auditability. This solution is consistent with the previous studies that showed evidence of blockchain efficiency in enhancing cybersecurity and safeguarding critical infrastructure information [6], [7].

Smart contracts are theoretically used in order to establish access control, automate checks, and administer permissions between cloud users and services. The blockchain layer helps reduce insider-related risks and one-point failure risks that characterize centralized cloud security systems because of the decentralization of trust and lack of reliance on one authority [10].

Intelligent analytics and decentralized trust mechanisms are a synchronized interaction that delivers blockchain and machine learning. The results of machine learning (scores indicating anomalies, classification of threats, risk rating, etc.) are logged safely to the blockchain to make the results transparent and integrity-driven. Data stored in blockchains offer trusted inputs to machine learning models and minimize the chance of data poisoning and unauthorized manipulation, in turn.

Such a two-way integration allows to detect threats in real time, respond to them automatically, and make verifiable security decisions. Other related strategies have been noted as critical in enabling robust and intelligent cybersecurity systems that can deal with sophisticated and persistent attack [11], [2]

Security Evaluation Condition

Key security and performance criteria are used as the means of conceptual evaluation of the proposed methodology that include data integrity, the ability to detect a threat, transparency, scalability, and trustworthiness. These assessment areas coincide with the measures that are typically applied to cybersecurity, protection of critical infrastructure, and research of intelligent systems [10], [12], [13].

The methodology will improve cloud security by ensuring efficiency in operation and data protection requirements, by balancing smart analytics and decentralized enforcement.

RESULTS AND DISCUSSION

Results

This section provides the findings of the analytical analysis based on the proposed blockchain-based machine learning system of secure data management in cloud computing. Findings dwell upon such critical security and performance aspects as the ability to detect threats, the principle of data integrity, transparency, and the system reliability, which has been previously defined in other cybersecurity and intelligent analytics research studies [1], [8].

Results of Performance Evaluation

The suggested structure has a higher security effectiveness than traditional cloud security frameworks in terms of conceptual understanding that are based on a centralized control and separate machine learning analytics. Machine learning is crucial to facilitate proactive threat detection and dynamic risk scoring, whereas the blockchain layer provides tamper-resistant data storage and verifiable audit trails. These joint functions are effective in the drawbacks that may be seen in single ML-based or blockchain-based security systems [6], [12].

Table 1 summarizes the comparative performance of the proposed framework against conventional cloud security models across selected evaluation criteria.

Table 1. Comparative Evaluation of Cloud Security Approaches.

Evaluation Criterion	Traditional Cloud Security	ML-Based Security Only	Blockchain-Integrated ML Framework
Threat Detection Capability	Moderate	High	Very High
Data Integrity Assurance	Low	Moderate	Very High

Transparency & Auditability	Low	Low	High
Resistance to Insider Threats	Moderate	High	Very High
Trust Decentralization	Low	Low	High
Scalability in Cloud Environments	High	High	High

Table 1 indicates that the blockchain-integrated machine learning framework outperforms traditional and standalone ML-based security models, particularly in data integrity, transparency, and trust decentralization.

Architectural Operations and System Behavior

The communication of information between machine learning layer and blockchain layer leads to improved behavior of the system in secure cloud data management. Machine learning systems are constantly processing data streams on clouds to identify abnormalities and estimate the risk, and blockchain algorithms safely store security events and access records. The interaction enhances the trust in automated security choices and decreases exposure to data manipulation and unauthorized access, which is in line with the results of the previous AI-based cybersecurity research [11], [7].

Figure 1 shows the flow of operations of the suggested framework and emphasizes the direction of the data flow of cloud sources to the ML analytics layer and then to the blockchain-based trust layer.

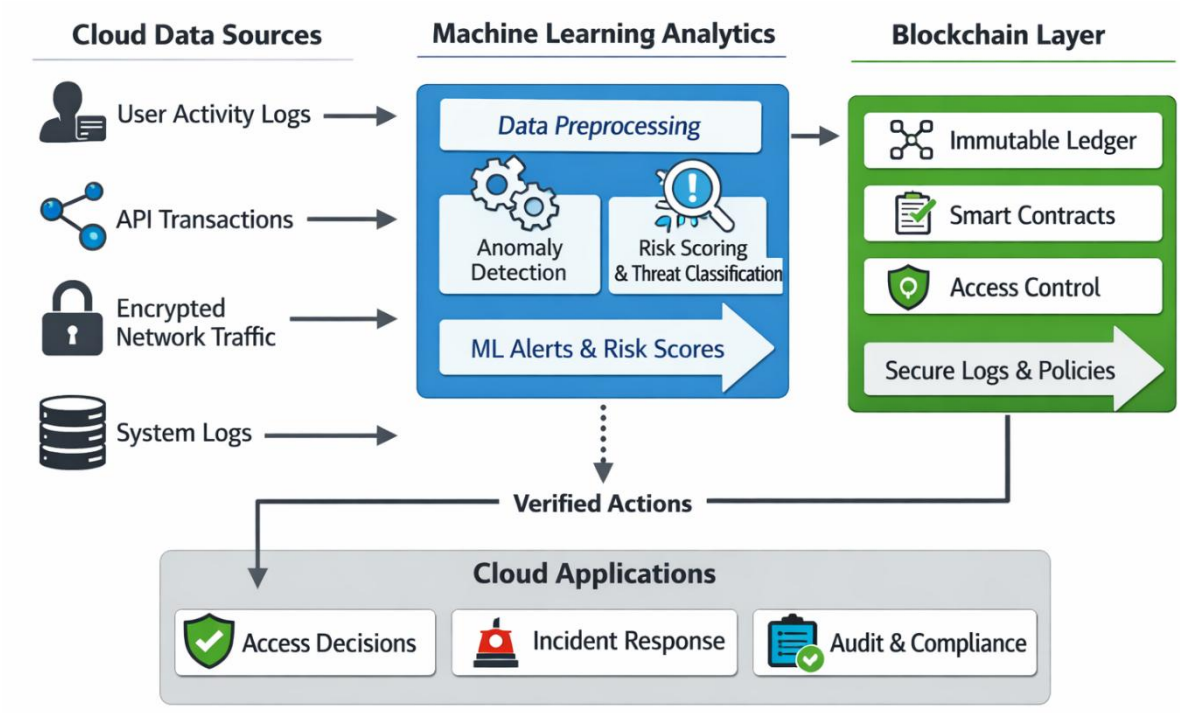

Figure 1. Operational Flow of the Blockchain-Integrated Machine Learning Framework.

The diagram shows cloud data sources in its feed to a machine learning analytics layer that preprocesses the data, detects anomalies and assigns risk scores to the data. The security outputs are subsequently stored on a blockchain layer that ensures integrity of the data, access control and auditability. Decisions that have been verified are then applied to cloud applications and services.

In general, the findings suggest that blockchain and machine learning can be used together to improve cloud security through intelligent threat detection, decentralized trust, and immutable data management. These results justify the appropriateness of the suggested scheme in a safe, extensive, and open cloud computing setup.

Discussion

The outcomes of the current research indicate that the combination of machine learning and blockchain technology helps improve the safe data storage in the cloud computing setting significantly. The comparative analysis reveals that although traditional cloud security systems offer scalability, they do not offer high data integrity guarantees, transparency, and decentralized trust. Instead, the suggested blockchain-based machine learning architecture overcomes these shortcomings, integrating smart threat identification and unchangeable and auditing records of information.

The enhanced threat detection capacity of the proposed framework corresponds to the previous studies on the importance of machine learning in detecting insider threats, anomalies, and advanced cyberattacks using behavioral and predictive analytics [1], [3], [4]. The ML layer will increase situational awareness and make proactive security responses, which are necessary in dynamically changing cloud environments by analyzing heterogeneous cloud data sources continuously.

Blockchain implementation also enhances the security level significantly because it promotes integrity of data, enforcement of access controls, and transparency. This observation aligns with the research that points to the application of blockchain to reduce data alteration, insider attacks, and single-point failures in centralized systems [6], [7]. Smart contracts and policy enforcement on automated enforcement is an addition to the ML-based analytics, especially to enable security choices to be verifiable and tamper resistant.

Besides, the findings align with the current literature that suggests that AI-powered and automated cybersecurity tools could prevent real-time threat detection and mitigation across vital infrastructure systems [11], [10]. The two-way communication between machine learning and blockchain increases confidence in automated decision-making to overcome issues associated with model opacities and centralized control. This practice is also consistent with the latest development in dynamic risk scoring and cyber threat intelligence which focus on ongoing and explainable risk evaluation in interrelated digital ecosystems [4].

On the whole, as it has been discussed, the offered framework does not only increase the effectiveness of security but also adds transparency, trust, and resilience to

cloud computing. These results validate the need to use hybrid security architectures where the strengths of blockchain and machine learning are used to complement each other and deal with more advanced cyber threats [15].

CONCLUSION

Fundamental Finding : This paper explores the integration of blockchain and machine learning technologies as a combined platform for managing secure data in cloud computing systems. It addresses key challenges such as data integrity, trust, transparency, and intelligent threat detection that are prevalent in conventional and centralized cloud security systems. The integration of machine learning analytics with blockchain's decentralized trust model enhances proactive threat identification, ensures tamper-resistant data storage, and allows verifiable access control and auditing. **Implication :** The proposed solution offers a resilient and reliable security framework that supports modern cloud infrastructures and data-intensive applications. It suggests that blockchain-based machine learning could significantly improve cloud security, maintaining scalability and efficiency, thus providing a potential solution for next-generation secure cloud computing systems. **Limitation :** The paper does not delve into the practical implementation challenges or scalability limitations that may arise when deploying this integrated framework on a large scale. Further research is needed to assess its real-world feasibility, especially in diverse cloud environments. **Future Research :** Future studies could explore the practical deployment of blockchain-based machine learning frameworks in various cloud platforms, evaluating their effectiveness across different industries. Additionally, research could focus on optimizing the scalability and efficiency of this hybrid architecture to handle growing cyber threats and the increasing demand for secure data management in cloud environments.

REFERENCES

[1] K. S. A. Mamun, M. S. Soumik, M. M. Rahman, M. Sarkar, C. A. Abdullah, M. Ali, and M. S. Hossain, "Predictive analytics for insider threats using multimodal data (log + behavioural + physical security)," *American Journal of Interdisciplinary Research and Innovation*, vol. 4, no. 3, pp. 82–90, 2025, doi: 10.54536/ajiri.v4i3.6224.

[2] M. S. Soumik, "Leveraging artificial intelligence and predictive data analytics to enhance cybersecurity and safeguard patient privacy in U.S. electronic health records," *Zenodo*, CERN, 2025, doi: 10.5281/zenodo.17831805.

[3] M. S. Soumik, M. Sarkar, and M. M. Rahman, "Fraud detection and personalized recommendations on synthetic e-commerce data with ML," *Research Journal in Business and Economics*, vol. 1, no. 1a, pp. 15–29, 2021, doi: 10.61424/rjbe.v1i1.488.

[4] M. M. Rahman, M. S. Soumik, M. S. Farids, C. A. Abdullah, B. Sutrudhar, M. Ali, and M. S. Hossain, "Explainable anomaly detection in encrypted network traffic using data analytics," *Journal of Computer Science and Technology Studies*, vol. 6, no. 1, pp. 272–281, 2024, doi: 10.32996/jcsts.2024.6.1.31.

[5] M. M. A. Rony, M. S. Soumik, and F. Akter, "Applying artificial intelligence to improve early detection and containment of infectious disease outbreaks, supporting national public

health preparedness," *Journal of Medical and Health Studies*, vol. 4, no. 3, pp. 82–93, 2023, doi: 10.32996/jmhs.2023.4.3.12.

[6] M. M. A. Rony, M. S. Soumik, and M. S. Sristy, "Mathematical and AI-blockchain integrated framework for strengthening cybersecurity in national critical infrastructure," *Journal of Mathematics and Statistics Studies*, vol. 4, no. 2, pp. 92–103, 2023, doi: 10.32996/jmss.2023.4.2.10.

[7] M. T. Siddique, M. K. Hussain, M. S. Soumik, and M. S. Sristy, "Developing quantum-enhanced privacy-preserving artificial intelligence frameworks based on physical principles to protect sensitive government and healthcare data from foreign cyber threats," *British Journal of Physics Studies*, vol. 1, no. 1, pp. 46–58, 2023, doi: 10.32996/bjps.2023.1.1.7.

[8] M. S. Soumik, K. S. A. Mamun, S. Omim, H. A. Khan, and M. Sarkar, "Dynamic risk scoring of third-party data feeds and APIs for cyber threat intelligence," *Journal of Computer Science and Technology Studies*, vol. 6, no. 1, pp. 282–292, 2024, doi: 10.32996/jcsts.2024.6.1.32.

[9] P. Mishra, "Design of intelligent healthcare IT infrastructure using graph theory, network analysis, and artificial intelligence," *International Journal of Applied Mathematics*, vol. 38, no. 12s, pp. 2267–2280, 2025, doi: 10.12732/ijam.v38i12s.1547.

[10] K. N. I. Ara, T. Mithila, M. M. A. Rony, and M. Sarkar, "Engineering of AI-powered cyber defense tools to protect immigration databases, biometric identity systems, and border-control infrastructure from nation-state attacks," *Journal of Computer Science and Information Technology*, vol. 2, no. 2, pp. 47–58, 2025, doi: 10.61424/jcsit.v2i2.573.

[11] "Development of AI-driven machine learning systems for real-time detection and automatic mitigation of advanced cyber threats across critical infrastructure," *Frontiers in Computer Science and Artificial Intelligence*, vol. 4, no. 2, pp. 26–35, 2025, doi: 10.32996/fcsai.2025.4.2.3.

[12] M. A. Rahaman, S. Rahman, M. Sarkar, M. M. Khan, M. M. R. Khan, and M. M. A. Rony, "Artificial intelligence and machine learning approaches for managing complex project in dynamic environments," *Journal of Computer Science and Technology Studies*, vol. 6, no. 2, pp. 225–235, 2024, doi: 10.32996/jcsts.2024.6.2.24.

[13] M. A. Rahaman, M. Sarkar, M. M. Khan, M. M. R. Khan, and M. M. A. Rony, "Integrating machine learning techniques across project management: Enhancing decision making and risk mitigation," *Journal of Computer Science and Technology Studies*, vol. 5, no. 4, pp. 285–295, 2023, doi: 10.32996/jcsts.2023.5.4.29.

[14] D. K. R. Toushi, M. A. Rahaman, S. Rahman, M. M. A. Rony, and M. Sarkar, "A data-driven approach to enhancing project management efficiency through machine learning and predictive modeling," *Journal of Business and Management Studies*, vol. 5, no. 5, pp. 282–292, 2023.

[15] N. Thakur, "Blockchain-Enabled Machine Learning Approach For Enhanced Security In Cloud Computing Environments," Journal for ReAttach Therapy and Developmental Diversities (JRTDD), vol. 3, no. 1, pp. 70–73, Jan. 2022, doi:10.53555/jrtdd.v3i1.2827.

*__Tonoy Kanti Chowdhury (Corresponding Author)__
Washington University of Science and Technology
Email: chowdhurytonoy93@gmail.com

K M Mohi uddin
Washington University of Science and Technology
Email: kmuddin.mohi@gmail.com