Vol 6, Issue 3, March 2026 www.ijesti.com E-ISSN: 2582-9734
International Journal of Engineering, Science, Technology and Innovation (IJESTI)

Integrating Machine Learning with Cryptography for Enhanced Secure Data Transmission in Modern Networks

Dewanshu Kumar
M. Tech. in Computer Science Engineering, CBS Group of Institutions, Jhajjar, Haryana.

Amreesh Kumar Yadav
A.P CSE Department, CBS Group of Institutions, Jhajjar, Haryana.

ABSTRACT

Secure data transmission is essential in modern communication systems, especially with the rise of cloud computing, IoT, vehicular networks, and distributed infrastructures. Traditional cryptographic methods are inadequate in addressing evolving cyber threats such as quantum decryption and persistent attacks. To enhance security, integrating machine learning (ML) with cryptography offers adaptive systems capable of real-time threat detection and intrusion management. Studies highlight innovations in vehicular, cloud, and IoT environments, such as hybrid encryption models and ML-driven anomaly detection, which improve data security and system efficiency. This approach is increasingly vital in protecting sensitive data across diverse platforms and emerging technologies.

Keywords: *Secure Transmission, Cryptography, Machine Learning, Cloud Computing, IoT.*

I. INTRODUCTION

Secure data transmission has become a fundamental requirement in modern communication systems due to the rapid expansion of cloud computing, Internet of Things (IoT), vehicular networks, and distributed digital infrastructures. As data exchange increases across heterogeneous environments, ensuring confidentiality, integrity, and availability of information has become increasingly complex. Traditional cryptographic mechanisms alone are no longer sufficient to counter evolving cyber threats such as advanced persistent attacks, quantum decryption risks, and intelligent intrusion attempts. As a result, researchers have shifted toward integrating advanced cryptographic algorithms with machine learning (ML)-based attack detection frameworks to build adaptive and intelligent security systems. Recent advancements in vehicular cloud environments demonstrate the growing need for robust secure transmission frameworks. Joseph et al. (2026) highlighted the vulnerabilities in Vehicle-to-Vehicle (V2V) communication within Vehicular Ad-hoc Networks (VANETs), proposing a hybrid framework combining federated learning and quantum key cryptography to enhance data security. Their study emphasized that integrating machine learning with cryptographic key management significantly improves intrusion detection and communication reliability in dynamic vehicular systems. Similarly, the emergence of quantum computing has introduced new security challenges to classical encryption systems. Temara et al. (2025) emphasized that traditional cryptographic protocols are highly susceptible to quantum attacks such as those enabled by Shor's algorithm. To address this, they proposed an ML-enhanced cryptographic framework incorporating neural networks and reinforcement learning for anomaly detection and adaptive key management. Their findings demonstrated that machine learning can dynamically strengthen encryption systems against quantum-based threats. In cloud computing environments, security concerns remain a major barrier to adoption. KVK et al. (2025) developed a deep learning-based cryptographic transformation model using SqueezeNet and optimization techniques to identify sensitive data before encryption. This hybrid approach significantly improved cloud data security and system efficiency. Similarly, Thabit et al. (2023) reviewed multiple machine learning-based lightweight cryptographic approaches, emphasizing their importance in improving scalability and reducing computational overhead

in cloud security systems. In IoT and healthcare systems, secure data transmission is even more critical due to the sensitivity of personal and medical data. Ranjan and Kumar (2024) proposed a blockchain-integrated hybrid encryption model using deep learning and optimization algorithms for secure IoT-based medical data transmission. Their results indicated improved privacy protection and resistance to unauthorized access. Additionally, Bokhari et al. (2019) introduced a sensitivity-based encryption framework using K-nearest neighbors (KNN), demonstrating that adaptive encryption enhances efficiency and reduces processing overhead. Earlier research also laid the foundation for secure transmission systems. Vimal et al. (2020) introduced a Markov decision-based security model combined with AES encryption for cognitive radio networks, improving both energy efficiency and security. Manikandan and Masilamani (2018) explored reversible data hiding techniques using machine learning for secure medical image transmission, showing that data embedding and recovery can be efficiently achieved without compromising integrity. Furthermore, Dubey et al. (2022) and Ch et al. (2021) emphasized the role of cloud cryptography and blockchain-based machine learning systems in mitigating data leakage and enhancing IoT security. These studies collectively demonstrate that integrating ML with cryptographic systems enables real-time threat detection, adaptive encryption, and intelligent security management.

II. RESEARCH BACKGROUND

Joseph et al. (2026) investigated Vehicle Ad-hoc Networks (VANETs) in the context of cloud security during Vehicle-to-Vehicle (V2V) communication. They highlighted that the automotive industry had recently transformed wireless network communication by integrating vehicles into the digital ecosystem. The study emphasized that vehicle-based cloud computing facilitated multiple communication types, including Vehicle-to-Vehicle, Vehicle-to-Infrastructure, and Vehicle-to-Device, where vehicles exchanged information using sensing capabilities. It was noted that secure communication had remained a major challenge in V2V interactions. To address this, they introduced a model termed Light Gradient-Boosting Machine Optimized Federated-Based Quantum Key Cryptography. Data were collected from GPS records, vehicle safety messages, and transmission logs, which were preprocessed via a base station to enhance quality and detection. The Optimized Boruta with Light Gradient Boosting Machine model was applied for classifying data as attacked or attack-free. Federated-Based Quantum Key Cryptography was employed for secure cloud access, and experimental results demonstrated superior performance with high accuracy, efficiency, and security metrics compared to previous approaches.

Temara et al., (2025) examined the emerging risks posed by quantum computing to traditional cryptographic protocols, which were considered vulnerable to quantum decryption methods such as Shor's algorithm. They proposed an innovative cryptographic framework that integrated machine learning (ML) techniques to enhance data security in the quantum computing era. Their approach employed ML-driven anomaly detection, adaptive key management, and predictive analytics to develop a flexible and resilient cryptographic defense. The anomaly detection module was reported to use neural networks to identify potential quantum-based decryption attempts, while reinforcement learning was applied to optimize key generation and distribution in response to detected threats. Experimental results indicated that the ML-augmented framework significantly improved anomaly detection accuracy and reduced vulnerability to quantum decryption by dynamically adjusting cryptographic parameters. Their findings highlighted the potential of machine learning to strengthen cryptographic systems and make them adaptable to advanced quantum computing threats.

KVK et al. (2025) investigated the increasing adoption of cloud computing, highlighting its significance in the information technology industry due to its capacity to manage diverse data and information systems efficiently. They noted that the exponential growth of software applications had substantially increased

the volume of available data, prompting many companies and industries to store information on the cloud. However, they observed that customer adoption remained limited due to persistent security and privacy concerns. To address this issue, they proposed a novel approach combining a deep learning algorithm with a lightweight cryptographic transformation model to enhance cloud data security. The methodology involved two stages: sensitive data selection and data protection. Initially, sensitive information was identified using the SqueezeNet deep learning model, whose hyperparameters were optimized via the Rat Optimization Algorithm (ROA). Subsequently, the selected data were encrypted using the Lightweight Transformation Model (LWTM) before cloud storage. Experimental outcomes demonstrated that the proposed method improved security over existing cloud standards, achieving an average processing period of 1.53 and an average throughput of 190.08 kb/s.

Ranjan and Kumar (2024) investigated the growing significance of e-health, particularly following the advent of the Internet of Things (IoT), and highlighted the complexities associated with maintaining patient privacy due to the sensitivity of medical data. They noted that patient health information was frequently stored in cloud environments, limiting users' control over their own data. To address these privacy and security concerns, they described a framework where medical data collected from IoT sensors embedded in patients was transmitted to Personal Digital Assistants (PDAs) for further processing. A hybrid encryption algorithm was employed to secure data during transmission, after which the encrypted reports were stored in the cloud under controlled access and encryption mechanisms. They further emphasized the integration of blockchain technology to enhance secure data transmission and reduce the risk of breaches. The study also reported that encryption and decryption keys were generated using a hybrid deep learning model (LSTM and CNN), with the optimal key selection facilitated by the Self-Improved Lion Optimization Algorithm (SI-LA), resulting in improved efficiency and robustness compared to existing techniques.

Thabit et al. (2023) examined cloud computing (CC) as a paradigm that enabled on-demand access to network resources, including data storage and processing, without requiring direct administration by users. They highlighted that CC initially emerged as a combination of public and private data centers, offering clients a unified platform over the Internet. The study indicated that CC had transformed the technological landscape due to its performance, accessibility, low cost, and other advantages. However, the exponential growth of cloud services had necessitated robust data security mechanisms. The authors reported that comprehensive security policies, organizational security culture, and cloud-specific solutions were employed to maintain data protection. They reviewed various techniques for securing cloud communications, emphasizing the role of encryption algorithms. Current research, as discussed, focused on lightweight cryptography, genetics-based cryptography, and machine learning (ML) approaches, including supervised, unsupervised, semi-supervised, and reinforcement learning, to mitigate security threats. Finally, they outlined potential directions for future research in cloud security.

Dubey et al. (2022) investigated cloud cryptography, describing it as a form of cryptography implemented on cloud-based systems, which allowed encryption services to be provided as software in a more accessible and cost-effective manner. They reported that cloud cryptographic services were typically offered as managed services by hosting providers, though dedicated parties could also provide such services while assuming the associated costs and liabilities. The study highlighted that cloud encryption served to protect data stored within the cloud, addressing the widespread problem of data leakage in distributed systems where information was simultaneously transferred and distributed across multiple systems. Dubey et al. further noted that, in addition to the security measures deployed by cloud infrastructure, intrusion detection systems (IDS) and firewalls were also employed to enhance protection. They explained that various mechanisms were utilized within cloud cryptography to add layers of security, aiming to prevent unauthorized access, hacking, or malware impact on sensitive data.

Ch et al. (2021) had examined the growing significance of the Internet of Things (IoT) in enabling automated monitoring, remote handling, and adaptive system responses without human intervention. The authors had highlighted that the rapid expansion of IoT devices across diverse applications had intensified concerns regarding user security and privacy, particularly due to the increasing frequency of cyber-attacks. It had been reported that blockchain technology emerged as an advanced solution for securing IoT environments by facilitating safe digital transactions, distributed ledger access, and intelligent contracts without relying on intermediaries. The study had further indicated that machine learning algorithms were employed to analyze large and complex datasets for identifying and predicting vulnerabilities in IoT-based systems. In this context, the researchers had proposed a Machine Learning based Data Security Model with Blockchain (MLDSMB) for secure IoT data transmission. Their findings had suggested that the proposed model achieved higher levels of secure data transmission compared to traditional methods.

Vimal et al. (2020) reported that cognitive radio networks had been recognized as a promising technology for allocating unused spectrum resources to unlicensed secondary users when licensed primary users were not utilizing them. The authors explained that the CR network had adopted a reactive security policy to improve energy monitoring while operating over primary channels. It was observed that maintaining secure data communication with moderate energy consumption had remained a major challenge, as intruders frequently attacked the network to deplete the energy levels of both primary and secondary users. To address this issue, a discrete-time partially observed Markov decision process had been employed as the core security framework. The study further indicated that private key encryption had been integrated with sensing outcomes, while the Eclat algorithm had been utilized for energy detection and Byzantine attack prediction. In addition, AES-based encryption had been applied to secure communication, and simulation results had demonstrated improved energy efficiency and enhanced network security.

Bokhari et al. (2019) had examined the importance of securing data during transmission in cloud computing environments, where users store and access information remotely over the Internet. The authors had observed that not all user data possess the same degree of sensitivity, and therefore a uniform encryption strategy may not be efficient. To address this issue, they had proposed a sensitivity-based security framework in which the K-nearest neighbors (KNN) algorithm was employed to classify data as either normally sensitive or highly sensitive. Based on this classification, different encryption mechanisms had been applied. For user authentication, a one-time password (OTP) mechanism had been incorporated. Data categorized as normally sensitive had been protected using AES-192 encryption. In contrast, highly sensitive data had been secured through AES-256, while the AES key had been encrypted using RSA. Additionally, a hash-based message authentication code (HMAC) had been appended to ensure message integrity and authenticity during cloud data transmission.

Manikandan and Masilamani (2018) had examined reversible data hiding (RDH) as an emerging information security technique for secure digital data transmission, particularly in telemedicine applications. They had highlighted that the rapid advancement of communication technologies and medical robotics had increased the need for secure transmission of medical images and electronic patient records (EPR). The study had emphasized that RDH schemes could be employed not only for authenticating medical images and ownership information but also for embedding EPR data into encrypted medical images before transmission. The receiver, according to their findings, had been able to extract the embedded EPR data and recover the original image successfully. The authors had proposed a novel RDH scheme in which EPR data had been embedded during the image encryption process using a block-wise image encryption method. A significant contribution of the study had been the application of support vector machine (SVM)-based classification for data extraction and image recovery. Experimental results on OsiriX medical images had indicated improved embedding rate and reduced bit error rate.

III. KEY FINDINGS FROM STUDY

Author(s)	Year	Methodology	Key Contribution	Findings
Joseph et al.	2026	Federated learning + Quantum cryptography + Light GBM	Secure V2V communication in VANETs	High accuracy intrusion detection and secure transmission
Temara et al.	2025	Neural networks + Reinforcement learning	ML-based quantum-resistant cryptography	Improved anomaly detection and adaptive security
KVK et al.	2025	SqueezeNet + ROA + Lightweight cryptography	Sensitive data classification and encryption	Improved cloud security and throughput
Ranjan & Kumar	2024	Deep learning + Blockchain + Hybrid encryption	Secure IoT medical data transmission	Enhanced privacy and reduced data breach risk
Thabit et al.	2023	ML + Lightweight cryptography review	Cloud security frameworks	Identified scalable ML-based security models
Dubey et al.	2022	Cloud cryptography systems	Data leakage prevention in cloud	Improved encryption-based protection
Ch et al.	2021	ML + Blockchain for IoT	Secure IoT data transmission model	Higher security and reduced vulnerability
Vimal et al.	2020	Markov model + AES encryption	Cognitive radio network security	Improved energy efficiency and security
Bokhari et al.	2019	KNN + AES + RSA + OTP	Sensitivity-based encryption system	Efficient adaptive encryption mechanism
Manikandan & Masilamani	2018	SVM + Reversible data hiding	Secure medical image transmission	Better embedding and data recovery

IV. CONCLUSION

The reviewed literature clearly demonstrates that secure data transmission frameworks have evolved significantly from traditional encryption methods to intelligent hybrid systems combining machine learning and advanced cryptographic techniques. Across domains such as cloud computing, IoT, vehicular networks, and healthcare systems, researchers have consistently highlighted the limitations of static encryption models in handling modern cyber threats. Machine learning has proven highly effective in enhancing intrusion detection, anomaly recognition, and adaptive security response mechanisms. Additionally, the integration of blockchain, quantum cryptography, and lightweight encryption techniques has significantly improved data confidentiality, integrity, and system scalability. Overall, the convergence of cryptography and machine learning represents a transformative approach to building next-generation secure communication systems.

V. FUTURE SCOPE

- Development of fully autonomous AI-driven cryptographic systems for real-time threat prevention.
- Integration of post-quantum cryptography with deep learning models for quantum-resilient security.

- Lightweight ML-cryptographic frameworks for edge and IoT devices with limited computational power.
- Federated learning-based decentralized security systems for privacy-preserving data transmission.
- Enhanced blockchain-ML hybrid models for secure multi-domain communication networks.
- Real-time adaptive encryption algorithms using reinforcement learning for dynamic threat environments.
- Scalable intrusion detection systems using large language models and advanced deep neural networks.

REFERENCES

1. Joseph, A. J., Asaletha, R., Manoj, V. J., & Nishanth, R. (2026). Machine Learning-Based Intrusion Detection and Quantum Cryptography in Vehicular Networks. *International Journal of Robust and Nonlinear Control*, *36*(1), 341-359.
2. Temara, S., Bhagyalakshmi, L., Suman, S. K., Shakunthala, M., Chitra, N. T., & Golla, K. (2025, February). Cryptography innovations for securing data in the quantum computing era: Integrating machine learning for enhanced security. In *2025 International Conference on Computer, Electrical & Communication Engineering (ICCECE)* (pp. 1-6). IEEE.
3. KVK, C., & Lokeswara Reddy, V. (2025). A novel deep learning technique with cryptographic transformation for enhancing data security in cloud environments. *Multimedia Tools and Applications*, *84*(8), 5149-5173.
4. Ranjan, A. K., & Kumar, P. (2024). Ensuring the privacy and security of IoT-medical data: a hybrid deep learning-based encryption and blockchain-enabled transmission. *Multimedia Tools and Applications*, *83*(33), 79067-79092.
5. Thabit, F., Can, O., Wani, R. U. Z., Qasem, M. A., Thorat, S. B., & Alkhzaimi, H. A. (2023). Data security techniques in cloud computing based on machine learning algorithms and cryptographic algorithms: Lightweight algorithms and genetics algorithms. *Concurrency and Computation: Practice and Experience*, *35*(21), e7691.
6. Dubey, H. A. R. S. H. I. T., Kumar, S. U. D. H. A. K. A. R., & Chhabra, A. N. U. R. E. E. T. (2022). Cyber security model to secure data transmission using cloud cryptography. *Cyber Secur. Insights Mag*, *2*, 9-12.
7. Ch, S. C., Puli, S., & Santhi, M. V. B. T. (2021, August). Machine Learning Based Data Security Model Using Blockchain for Secure Data Transmission in IoT. In *2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC)* (pp. 1521-1527). IEEE.
8. Vimal, S., Kalaivani, L., Kaliappan, M., Suresh, A., Gao, X. Z., & Varatharajan, R. (2020). Development of secured data transmission using machine learning-based discrete-time partially observed Markov model and energy optimization in cognitive radio networks. *Neural Computing and Applications*, *32*(1), 151-161.
9. Bokhari, M. U., Shallal, Q. M., & Tamandani, Y. K. (2019). Reducing the required time and power for data encryption and decryption using K-NN machine learning. *IETE Journal of Research*, *65*(2), 227-235.
10. Manikandan, V. M., & Masilamani, V. (2018). Reversible data hiding scheme during encryption using machine learning. *Procedia computer science*, *133*, 348-356.