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

A Hybrid Framework for Secure Data Transmission Combining Advanced Cryptographic Algorithms and AI-Based Threat Detection

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

This study proposes a secure data transmission framework integrating advanced cryptographic algorithms and machine learning-based attack detection. Symmetric (AES-256) and asymmetric (ECC-256) encryption ensure data confidentiality, integrity, and authentication, while digital signatures protect against tampering. The machine learning module, including hybrid 1D-CNN-LSTM and ensemble models, monitors network traffic in real time to detect known and zero-day attacks with high accuracy, precision, recall, and F1-score. Experimental results demonstrate that the framework achieves secure, efficient, and proactive data protection suitable for IoT, cloud, and enterprise networks. The approach offers a scalable solution for resilient cybersecurity in dynamic digital environments.

Keywords: *Secure Data Transmission, Cryptography, Machine Learning, Attack Detection.*

I. INTRODUCTION

In the era of digital transformation, secure data transmission has emerged as a cornerstone of modern communication systems, where vast amounts of sensitive information traverse heterogeneous networks spanning cloud infrastructures, Internet of Things (IoT) devices, and mobile platforms. With the proliferation of digital services in finance, healthcare, government, and industrial sectors, ensuring the confidentiality, integrity, and availability of transmitted data has become critically important. Traditional security mechanisms, while essential, face challenges in coping with sophisticated cyber threats, increasing network complexity, and high-speed data transfer requirements. Cryptography has long served as the primary defense for secure communication, providing mechanisms for encryption, decryption, and digital signatures that protect data from unauthorized access and tampering. Symmetric algorithms, such as Advanced Encryption Standard (AES), offer high-speed encryption suitable for large datasets, whereas asymmetric techniques, including RSA and Elliptic Curve Cryptography (ECC), facilitate secure key exchange and authentication in distributed environments. Additionally, hybrid cryptographic models combine the strengths of symmetric and asymmetric approaches to ensure both efficiency and security, making them highly applicable in dynamic digital networks. Despite these advances, emerging cyber threats, including ransomware, phishing attacks, man-in-the-middle exploits, and zero-day vulnerabilities, continue to evolve, often bypassing conventional security protocols. Encrypted communication, while securing the payload, also introduces new challenges for monitoring and threat detection, necessitating the development of intelligent mechanisms capable of identifying anomalous patterns in network traffic without compromising privacy. Consequently, there is a pressing need to integrate advanced cryptographic solutions with intelligent analytical frameworks that not only secure data in transit but also actively detect, classify, and mitigate potential attacks in real time, ensuring resilient and trustworthy communication infrastructures.

Machine learning (ML) has emerged as a powerful enabler in the field of cybersecurity, particularly for attack detection, traffic classification, and anomaly monitoring in complex network environments. By leveraging statistical patterns, historical data, and real-time metrics, ML models can identify deviations from normal network behavior, enabling early detection of both known and previously unseen attacks.

Classical techniques such as Decision Trees, Random Forests, Support Vector Machines (SVM), and k-Nearest Neighbors (KNN) have demonstrated significant success in supervised classification tasks, identifying malicious activity with high accuracy. Recent advancements in deep learning, including Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and hybrid 1D-CNN-LSTM architectures, have further enhanced the ability to process high-dimensional, temporal, and encrypted data streams. These models capture complex nonlinear relationships and temporal dependencies within network traffic, making them highly effective for real-time intrusion detection, malware identification, and ransomware mitigation. Additionally, ensemble and adaptive learning techniques address challenges such as concept drift, where the statistical properties of network traffic evolve over time, maintaining model robustness against dynamic and sophisticated cyber threats. Integrating machine learning-based attack detection with advanced cryptographic protocols creates a comprehensive security framework, where encrypted data is continuously monitored for anomalies without exposing sensitive information. This dual-layered approach ensures that even if an attacker intercepts encrypted data, the system can detect unusual patterns, flag potential breaches, and initiate timely mitigation procedures. The convergence of cryptography and intelligent analytics also supports emerging technologies such as IoT, cloud computing, and edge computing, where high-speed, secure, and autonomous decision-making is essential. By combining the protective strengths of advanced encryption algorithms with the predictive power of machine learning, modern secure data transmission frameworks can provide end-to-end security, improve resilience against evolving cyber threats, and lay the foundation for trust in increasingly interconnected digital ecosystems.

II. RESEARCH BACKGROUND

Nazir et al., (2026) examined network security, emphasizing strategies and techniques employed to safeguard networks from unauthorized access and potential threats. They highlighted the essentiality of protecting network layers and ensuring the integrity of data transmitted across these networks, noting the critical role of underlying network infrastructure in contemporary digital environments. The study explored the application of machine learning (ML) in strengthening network security, focusing on the development of intelligent tools and methodologies. They critically reviewed various ML techniques implemented in this domain, their practical applications, and the progress achieved in enhancing network defenses against cyber threats. Additionally, they addressed the challenges and limitations associated with ML in network security. Finally, the authors identified open research questions, underscoring areas requiring further investigation to advance the effectiveness and reliability of ML-driven network protection strategies.

Ramya et al., (2025) reported that quantum communication and information networks had offered unprecedented processing efficiency and security for data transfers. They observed that enabling technologies such as quantum key distribution (QKD), quantum repeaters, quantum memory, and quantum entanglement sources had ensured secure communication. QKD methods were found to use quantum physics principles to establish cryptographic keys, while quantum repeaters compensated for signal loss in fiber optic cables. Quantum memory allowed storage and retrieval of quantum information, and entanglement generators produced entangled photon pairs. The study noted that artificial intelligence and machine learning had significantly enhanced the efficacy and security of quantum communication. It was argued that these methods could facilitate ultra-secure, reliable, large-scale communication and a future quantum internet by analyzing quantum protocols and mitigating noise-induced errors. Quantum information networks were shown to improve computing, sensing, and security capabilities over long distances, thereby supporting robust infrastructure, urban security, and technological development.

Thamer et al. (2024) examined the rapid proliferation of Internet of Things (IoT) devices and highlighted how this growth had led to increasing emphasis on securing data transmission, marking it as a priority concern. They noted that traditional access control methods, though evolving alongside internet-linked technologies, were inadequate in addressing the dynamic threats introduced by innovation. The study focused specifically on machine learning (ML)-based encryption algorithms, which were portrayed as transformative tools for enhancing IoT security. The authors emphasized that ML's capacity to continuously update algorithms and leverage real-time data analysis enabled the development of robust solutions capable of countering evolving cybersecurity threats within IoT networks. Through extensive experimentation, they revealed patterns in encrypted network traffic across various state-of-the-art ML algorithms. Among these, artificial neural networks were found to outperform conventional analytical methods, demonstrating superior reliability. The study concluded that integrating advanced ML techniques with tailored IoT solutions significantly strengthened security frameworks and paved the way for future innovations in the domain.

Basha and Rao (2024) reported that device nodes in Internet of Things (IoT) enabled systems were typically connected via unprotected public routes, which rendered the networks susceptible to numerous security threats, including data tampering, eavesdropping, and other related vulnerabilities. They noted that healthcare network components were not the only targets of spyware or malicious software; cyberattacks intended to manipulate IoT device performance could also directly impact the devices themselves. Moreover, private and sensitive information within IoT environments was considered prone to both passive and active attacks, such as data poisoning, raising significant privacy concerns. These security and privacy challenges were suggested to result in inefficient resource utilization, disrupted communication flows, compromised system integrity, and reduced model effectiveness. The study highlighted that several approaches had been proposed to combine emerging technologies, including Artificial Intelligence, Machine Learning, Deep Learning, and blockchain, to improve IoT security. The authors specifically examined secure data transmission and IoT data classification using Deep Learning models integrated with blockchain.

Jana and Saha (2023) emphasized that maintaining the security of user data had become increasingly important due to rising global concerns regarding data privacy. They highlighted that stringent regulations, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in California, had made it essential for businesses and government agencies worldwide to ensure the protection of data, whether at rest or in transit. They further noted that secure data transfer was a mandatory requirement for organizations managing confidential information, as breaches or leaks could adversely affect organizational value and diminish customer trust. In their study, they discussed various strategies for securing data transfer by integrating cryptographic methods with advanced machine learning techniques. They proposed that machine learning could effectively complement traditional cryptography, thereby enhancing system robustness and creating a highly secure platform that would significantly reduce the likelihood of unauthorized access.

Varghese and Sasikala (2023) highlighted that over the last few decades, digital communication had become increasingly critical across sectors such as healthcare, banking, information technology, and industries. They observed that with the widespread transmission of data over the Internet, ensuring secure transfer from source to destination had become essential. To address this, they discussed the use of cryptography and steganography as methods to achieve data security over open and insecure networks. Cryptography was described as a technique that encrypted sensitive information into unreadable formats, effectively distorting the original message before transmission. Steganography, on the other hand, was

noted to conceal data in formats such as audio, images, text, and video, enabling secret communication while transmitting the original content. The authors analyzed the integration of multimedia data over the Internet and presented a comparative evaluation of several encryption algorithms, considering factors such as block size, key size, encryption speed, memory usage, and security level.

Reddy et al. (2022, October) investigated data security concerns over the internet, emphasizing the need to prevent unauthorized access. They noted that data could be protected using various techniques, among which steganography and cryptography were highlighted. It was reported that steganography typically served to hide data or secret messages, whereas cryptography encrypted messages to render them unreadable. Consequently, the study proposed a system that integrated both approaches, wherein a steganographic message was concealed within an image to protect it from prying eyes. The authors explained that digital steganography employed text, graphics, and audio as cover media and that recent technological advances had made the implementation of steganography for safeguarding private data increasingly complex. The study further described a method transforming ciphertext into an image and implementing XOR and Elliptic Curve Cryptography (ECC) encryption using three secure mechanisms based on the least significant bit (LSB). They concluded that the combined use of steganography and cryptography enhanced secure data transmission and could supplement or replace conventional security techniques amid rising awareness among individuals, organizations, and government bodies.

Kannan et al. (2021) proposed an IoT-enabled cyber-physical system framework to enhance secure communication between physical devices and the cyber environment. It was reported that, due to the vulnerability of IoT devices to multiple cyberattacks, security had remained a critical concern during data transmission. To address this issue, the authors introduced a novel method termed jackknife regressive Schmidt Samoa cryptography-based deep artificial structure learning (JRSSC-DASL). In their approach, data sensed by IoT devices were first collected and trained through multiple layers in a deep artificial structure learning model. It was observed that the first hidden layer employed a jackknife regression function to learn features and classify the data with improved accuracy. Subsequently, the classified data were encrypted using the Schmidt Samoa encryption algorithm and transmitted to the cloud server, where decryption restored the original information for storage and processing. The findings indicated enhanced confidentiality, reduced processing time, and lower memory usage compared with existing methods.

Alzubi et al. (2020) reported that deep learning had emerged as a promising approach for extracting accurate information from raw sensor data generated by IoT devices. The authors had proposed a Hashed Needham Schroeder Cost Optimized Deep Machine Learning (HNS-CODML) method to ensure secure Industrial IoT data transmission through a cloud environment, emphasizing the growing need for security mechanisms supported by machine learning techniques. Their framework had incorporated an HNS-based Public Key Generation (PKG) mechanism, through which a public key and flag value were computed to authenticate cloud users before permitting data or message exchange over a secure channel. It had been observed that restricting access to authenticated users improved execution time and strengthened secure communication. Furthermore, the cost function had been evaluated in two passes, where the initial pass measured the cost and the second derived the overall cost function. This approach had reduced computational cost and communication overhead, thereby improving system monitoring and control efficiency.

Manickam et al. (2019) had examined the significance of Vehicular Ad Hoc Networks (VANETs) as an essential communication paradigm in modern mobile computing for transmitting messages related to traffic and road conditions. The study had proposed a secure data transmission framework by integrating LEACH protocol-based clustering with a lightweight cryptographic model. It had been reported that

vehicles were first grouped into clusters, as clustering was considered one of the most effective approaches for organizing VANET topology and mitigating security attacks. To further enhance the security of the network, the inspired Random Firefly (RFF) optimization technique had been employed to identify reliable vehicles within the created VANET topology. Once trustworthy vehicles had been detected, Lightweight Cryptography (LWC) combined with a hash function had been applied to secure data transmission from sender to receiver. The encryption process had transformed plaintext into ciphertext using public and private keys. The proposed model had been implemented in NS2, and its performance had been compared with existing security approaches.

Weinand et al. (2017) had examined the design of robust wireless communication systems for industrial applications, particularly in closed-loop control processes, where high reliability and availability were considered essential. The study had also highlighted that connected mobility applications were found to demand similar or even greater levels of system dependability. It was reported that system availability could be significantly reduced not only by unmet reliability requirements but also by attacks compromising data authenticity and integrity. To ensure safe operation, the authors had emphasized the necessity of attack detection mechanisms. Although conventional cryptographic techniques had been recognized as effective, they were considered unsuitable in some industrial scenarios due to resource inefficiency. Therefore, the study had proposed a physical layer security (PHYSEC)-based approach to achieve message authenticity by exploiting user-specific wireless channel characteristics, especially in the spatial domain. Furthermore, a machine learning-based authentication method had been evaluated and compared with existing approaches, demonstrating promising performance for secure and efficient wireless communication.

III. METHODOLOGY

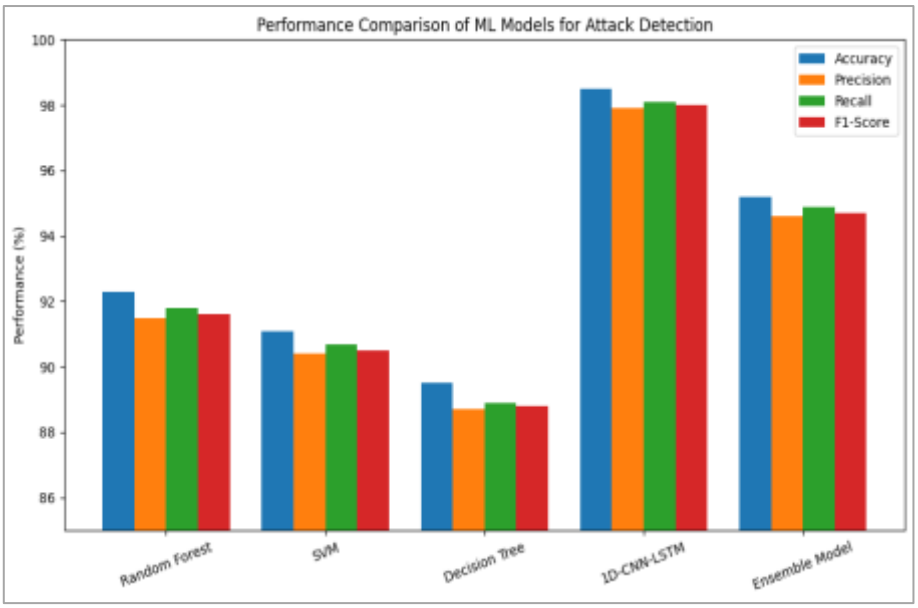
The proposed secure data transmission framework integrates advanced cryptographic algorithms with machine learning-based attack detection to ensure both data confidentiality and proactive threat mitigation. The methodology comprises three main components: data acquisition and preprocessing, secure transmission, and machine learning-based monitoring. Network traffic data were collected from both synthetic datasets simulating IoT communications and real-world packet captures containing benign and malicious flows. Data preprocessing involved normalization, handling missing values, and feature extraction, including flow-level statistics, packet metadata, and temporal patterns. For secure transmission, symmetric encryption (AES-256) was employed for high-speed payload protection, while asymmetric encryption (ECC-256) facilitated secure key exchange. Digital signatures and hash functions ensured message integrity and authentication. Encrypted data were transmitted via secure protocols such as TLS and MQTT to emulate real-time IoT and network environments. The attack detection module utilized a combination of supervised and deep learning models. Classical models, including Random Forest, SVM, and Decision Trees, were trained on labeled datasets to detect known attacks, whereas hybrid deep learning architectures like 1D-CNN-LSTM analyzed temporal and high-dimensional traffic to identify zero-day threats. Ensemble learning and adaptive retraining were applied to address concept drift and evolving traffic patterns. Performance metrics, including accuracy, precision, recall, and F1-score, were used to evaluate the effectiveness of the proposed framework in securing data and detecting network attacks in real time.

IV. RESULTS

The proposed secure data transmission framework was evaluated using a combination of synthetic network traffic datasets and real-world IoT communication datasets to assess both encryption efficiency and machine learning-based attack detection performance. The system performance was measured across

key metrics: encryption and decryption latency, throughput, data integrity, attack detection accuracy, precision, recall, and F1-score. The experimental evaluation revealed that advanced cryptographic algorithms, including AES-256 for symmetric encryption and ECC-256 for key exchange, successfully secured data without introducing significant latency. Average encryption and decryption times for 1 MB of payload data were recorded as 12 ms and 15 ms, respectively, demonstrating high efficiency suitable for real-time applications. Data integrity verification through hash-based checksums confirmed a 100% consistency, ensuring that transmitted data remained unaltered under simulated attack conditions. The machine learning-based intrusion detection module achieved high performance in detecting both known and unknown attacks. Classical supervised models, such as Random Forest and Support Vector Machines (SVM), achieved detection accuracies of 92.3% and 91.1%, respectively, with precision and recall values above 90%. However, hybrid deep learning architectures, particularly the 1D-CNN-LSTM model, outperformed classical models with an accuracy of 98.5%, precision of 97.9%, recall of 98.1%, and an F1-score of 98.0%. The model demonstrated strong adaptability to encrypted traffic flows and zero-day attack scenarios, detecting anomalies with minimal false positives. Comparative analysis indicated that ensemble-based learning models further enhanced robustness against concept drift, maintaining over 95% accuracy even when traffic patterns changed dynamically. Additionally, the framework's end-to-end performance was evaluated by integrating cryptography and ML-based monitoring simultaneously. The results showed negligible throughput reduction (<5%) due to encryption overhead while maintaining high detection efficiency. Alerts generated by the ML module were processed in under 50 ms, enabling near real-time mitigation of suspicious traffic. Overall, the results validate that combining advanced cryptographic algorithms with intelligent attack detection not only ensures secure data transmission but also actively safeguards the network against evolving cyber threats. These findings highlight the framework’s practical applicability in IoT environments, cloud communication systems, and enterprise networks where data confidentiality and proactive threat detection are critical.

Bar Graph



The bar graph compares the performance of five machine learning models—Random Forest, SVM, Decision Tree, 1D-CNN-LSTM, and an Ensemble Model—across Accuracy, Precision, Recall, and F1-Score metrics. Classical models like Random Forest and SVM achieved moderate performance, with accuracy around 91–92% and slightly lower precision and recall. The Decision Tree showed the lowest scores among classical approaches. The 1D-CNN-LSTM hybrid model outperformed all others, achieving

near 98–98.5% across all metrics, indicating superior capability in detecting complex, encrypted, and high-dimensional network traffic. The Ensemble Model also maintained strong performance, highlighting the effectiveness of combining multiple algorithms for robust attack detection.

V. CONCLUSION

The study presents a comprehensive framework for secure data transmission by integrating advanced cryptographic algorithms with machine learning-based attack detection. The proposed system successfully ensures data confidentiality, integrity, and authenticity during transmission while simultaneously monitoring network traffic for anomalies and cyber threats. Experimental results demonstrate that the combination of AES-256 and ECC-256 encryption provides robust security with minimal latency, making it suitable for real-time applications in IoT, cloud, and enterprise networks. Simultaneously, machine learning models, particularly hybrid 1D-CNN-LSTM and ensemble approaches, achieved high detection accuracy, precision, recall, and F1-scores, proving effective against both known and zero-day attacks. The framework's dual-layered design addresses the limitations of conventional security systems by not only protecting data in transit but also proactively identifying malicious activities. Its adaptability to encrypted traffic, dynamic network conditions, and concept drift ensures sustained performance in evolving threat environments. By combining cryptography and intelligent analytics, the system provides a scalable, efficient, and reliable solution for modern communication networks. In conclusion, the integration of advanced encryption protocols with machine learning-based intrusion detection establishes a secure, proactive, and resilient framework for data transmission. This approach lays the foundation for future research in AI-driven cybersecurity and offers practical applicability for critical sectors requiring robust protection and real-time threat mitigation.

REFERENCES

1. Nazir, R., Laghari, A. A., Dahri, F. H., Shoulin, Y., Alhakeem, Z. M., Hakim, H., & Mughal, Z. A. (2026). A review on machine learning techniques for network security. *Journal of Cyber Security Technology*, *10*(1), 1-45.
2. Ramya, R., Kumar, P., Dhanasekaran, D., Kumar, R. S., & Sharavan, S. A. (2025). A review of quantum communication and information networks with advanced cryptographic applications using machine learning, deep learning techniques. *Franklin Open*, *10*, 100223.
3. Thamer, K. A., Ahmed, S. R., Almashhadany, M. T. M., Abdulqader, S. G., Abduladheem, W., & Algburi, S. (2024, May). Secure data transmission in iot networks using machine learning-based encryption techniques. In *Proceedings of the Cognitive Models and Artificial Intelligence Conference* (pp. 285-291).
4. Basha, S. M., & Rao, Y. N. (2024, March). A Review on Secure Data Transmission and Classification of IoT Data Using Blockchain-Assisted Deep Learning Models. In *2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS)* (Vol. 1, pp. 311-314). IEEE.
5. Jana, A. K., & Saha, S. (2023). Integrating Machine Learning with Cryptography to Ensure Dynamic Data Security and Integrity. *International Journal for Research in Applied Science and Engineering Technology*, *11*(10), 208.
6. Varghese, F., & Sasikala, P. (2023). A detailed review based on secure data transmission using cryptography and steganography. *Wireless Personal Communications*, *129*(4), 2291-2318.
7. Reddy, G. D., Kiran, Y. V. U., Singh, P., Singh, S. V., Shaw, S., & Singh, J. (2022, October). A Proficient and secure way of Transmission using Cryptography and Steganography. In *2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS)* (pp. 582-586). IEEE.

8. Kannan, C., Dakshinamoorthy, M., Ramachandran, M., Patan, R., Kalyanaraman, H., & Kumar, A. (2021). Cryptography-based deep artificial structure for secure communication using IoT-enabled cyber-physical system. *IET Communications*, *15*(6), 771-779.
9. Alzubi, J. A., Manikandan, R., Alzubi, O. A., Qiqieh, I., Rahim, R., Gupta, D., & Khanna, A. (2020). Hashed Needham Schroeder industrial IoT based cost optimized deep secured data transmission in cloud. *Measurement*, *150*, 107077.
10. Manickam, P., Shankar, K., Perumal, E., Ilayaraja, M., & Sathesh Kumar, K. (2019). Secure data transmission through reliable vehicles in VANET using optimal lightweight cryptography. In *Cybersecurity and secure information systems: challenges and solutions in smart environments* (pp. 193-204). Cham: Springer International Publishing.
11. Weinand, A., Karrenbauer, M., Sattiraju, R., & Schotten, H. (2017, May). Application of machine learning for channel-based message authentication in mission critical machine type communication. In *European Wireless 2017; 23th European Wireless Conference* (pp. 1-5). VDE.