Natural Resources for Human Health
eISSN: 2583-1194

Original Research

Received 22 July 2026
Revised 18 Aug 2026
Accepted 05 Sep 2026

Natural Resources for Human Health 2026, Vol. 6 (20s): 740–750

KEYWORDS:
Internet of Things, Intrusion Detection System, Transformer, Post-Quantum Cryptography, ML-DSA, Blockchain, Cybersecurity.

Mathematical Modeling of Quantum-Secured Blockchain IDS for IoT Infrastructure Using Transformers

[1]Dr. R. Uma, [2]Dr.V. Usha, [3]Dr Chandhini J, [4]Dr.P. Shanmugapriya, [5]Mr. M. Kishorekumar, [6]Dr.S. Mangala Lavanya, [7]Dr. G. Jenitha, [8]Dr. P. Maheswari Naik

[1]Associate Professor, Department of Mathematics, Sree Saraswathi Thyagaraja College, Pollachi, Coimbatore, Tamilnadu, India ,642107
E- mail id: ramumaraj@gmail.com
[2]Assistant professor, Department of Mathematics, PSG College of Arts and Science Coimbatore, Tamil Nadu, India, 641 014
Corresponding author E- mail id: usha.vsr@gmail.com
[3]Assistant Professor, PG & Research Department of Mathematics, Sri Ramakrishna College of Arts & Science, Coimbatore, Tamilnadu, India,641006
E- mail id: chandhini.j@srcas.ac.in
[4]Assistant Professor Department of Mathematics, KPR Institute of Engineering and Technology, Coimbatore, Tamilnadu, India, 641407
E- mail id: Shanmugapriya.p@kpriet.ac.in
[5]Assistant Professor, Department of Mathematics, karpagam college of Engineering, coimbatore, Tamilnadu, India ,641032
E- mail id: kish281090@gmail.com
[6]Assistant Professor, Department of Mathematics, V.S.B. College of Engineering Technical Campus, Coimbatore, Tamil Nadu, India,642 109
E- mail id: meetlavan78@gmail.com
[7]Associate Professor, Department of Mathematics, AMET deemed to be University, Chennai, Tamil nadu, india, 603112
E- mail id: jenitha.g@ametuniv.ac.in
[8]Assistant Professor, Department of Mathematics, Sri Ramakrishna Engineering College, Coimbatore, Tamilnadu, India,641 022*
EMail ID: maheswarinaik21@gmail.com

ABSTRACT: The rapid growth of the Internet of Things (IoT) has increased the risk of cyberattacks, creating a need for intelligent and secure intrusion detection mechanisms. Traditional Intrusion Detection Systems (IDS) face challenges in identifying complex attack patterns and ensuring the authenticity and integrity of security alerts. This paper proposes a mathematical modelling framework for a quantum-secured blockchain-based IDS for IoT infrastructure using Transformer architecture. The proposed framework employs a Transformer-based model to analyse network traffic features and classify normal and malicious activities. Benchmark datasets, including CICIoT2023, TON_IoT, and Edge-IIoTset, can be used to evaluate the detection performance of the model. Post-quantum digital signatures based on the Module-Lattice-Based Digital Signature Algorithm (ML-DSA) are incorporated to authenticate security alerts and protect their integrity against potential quantum-computing threats. Furthermore, a permissioned blockchain maintains tamper-evident records of verified alerts, enabling traceability and

Natural Resources for Human Health
eISSN: 2583-1194

secure auditing. The framework can be evaluated using accuracy, precision, recall, F1-score, false-positive rate, authentication overhead, transaction latency, and throughput. By integrating Transformer-based detection, post-quantum authentication, and blockchain technology, the proposed approach aims to provide a reliable and secure intrusion detection framework for IoT environments. Experimental validation is required to quantify its effectiveness and computational efficiency.

INTRODUCTION

The rapid development of the Internet of Things (IoT) has transformed modern infrastructure by enabling interconnected devices to exchange data and perform intelligent operations across smart healthcare, industrial automation, intelligent transportation, smart cities, and energy management. However, the large number of connected devices, heterogeneous communication protocols, limited computational resources, and distributed network architecture create significant security challenges. IoT networks are increasingly vulnerable to distributed denial-of-service (DDoS) attacks, malware infections, spoofing, unauthorized access, and anomalous network traffic. These threats highlight the need for intelligent and adaptive intrusion detection systems (IDSs) capable of identifying malicious activities accurately while maintaining low detection latency and computational overhead. Recent studies on IoT security have emphasized the importance of combining machine learning, deep learning, cryptographic mechanisms, and distributed security architectures to strengthen protection against evolving cyber threats [1, 2].

Traditional intrusion detection approaches primarily rely on predefined rules, signature matching, and conventional machine learning algorithms. Although these methods can detect known attack patterns, their effectiveness may decrease when encountering zero-day attacks, complex traffic relationships, and previously unseen malicious behaviours. Deep learning methods provide opportunities to identify nonlinear relationships and hidden patterns in network traffic. In particular, Transformer architectures employ self-attention mechanisms to capture long-range dependencies among sequential data, making them promising for analysing temporal variations in network traffic and identifying complex attack patterns. By considering relationships between multiple traffic features, a Transformer-based IDS can learn contextual representations of normal and malicious activities and classify incoming network events. Nevertheless, its effectiveness depends on the quality of the training data, the representation of traffic features, computational requirements, and its ability to generalize to previously unseen attacks. Blockchain technology offers another approach to improving the trustworthiness of distributed IoT security systems. Its decentralized ledger, cryptographic verification, and tamper-evident record structure can support secure sharing of intrusion alerts, verification of security events, and traceability of attack information across multiple network participants. Integrating blockchain with an IDS can reduce dependence on a single centralized monitoring authority and improve the integrity of security records. However, blockchain integration introduces challenges such as transaction latency, storage overhead, consensus costs, and scalability in resource-constrained IoT environments. Recent research has examined blockchain-enabled intrusion detection through rule-based, machine learning, deep learning, and federated learning approaches, highlighting the need to balance decentralized trust, privacy preservation, and real-time detection [2, 3]. Quantum-secured communication is an important consideration for the long-term protection of IoT infrastructure. The increasing progress of quantum computing raises concerns about the security of conventional public-key cryptographic schemes, including RSA and elliptic-curve cryptography. Two important approaches are quantum key distribution (QKD) and post-quantum cryptography (PQC). QKD uses quantum communication principles to establish secret keys, whereas PQC uses classical algorithms designed to resist attacks from quantum computers. These approaches are related but technically distinct. Fernández-Caramés [4] reviewed quantum-resistant cryptographic techniques for IoT environments, emphasizing the importance of adapting cryptographic protection to the constraints of connected devices. In addition, the National Institute of Standards and Technology (NIST) published three post-quantum cryptography standards in 2024: FIPS 203 for key establishment, FIPS 204 for digital signatures, and FIPS 205 for stateless hash-based digital signatures [5]. Integrating suitable post-quantum cryptographic algorithms with blockchain can improve the long-term security of device authentication, transaction validation, and intrusion-alert records. However, the computational and communication overhead of these mechanisms must be evaluated before deployment on resource-constrained IoT devices.

In this context, the proposed research, "Mathematical Modeling of Quantum-Secured Blockchain IDS for IoT Infrastructure Using Transformers," aims to develop an integrated framework that combines mathematical modelling, Transformer-based

intrusion detection, blockchain-based security records, and quantum-resistant cryptographic protection. The proposed mathematical model can represent network traffic characteristics, attack probabilities, detection performance, cryptographic overhead, and blockchain transaction costs. Let the network traffic sequence be represented by $X=\{x_1,x_2,\ldots,x_T\}$, where each x_t denotes a vector of extracted network traffic features at time t. A Transformer-based model can learn contextual representations of these features and estimate the probability of a malicious event. The resulting classification can be used to generate intrusion alerts, which are subsequently authenticated and recorded in a permissioned blockchain using an appropriate post-quantum digital signature scheme. This design separates attack detection from the cryptographic verification and recording process, allowing the contribution of each component to be evaluated independently. The mathematical framework can be assessed using detection accuracy, precision, recall, F1-score, false-positive rate, detection latency, computational overhead, and blockchain transaction throughput. Comparative experiments with conventional machine learning models, recurrent neural networks, and alternative deep learning architectures can establish whether the Transformer provides measurable improvements in attack detection. Similarly, the cryptographic component can be evaluated in terms of signature generation and verification time, communication overhead, and resistance to specified threat models. The central research objective is to investigate whether the combined framework can achieve a practical balance among detection effectiveness, data integrity, quantum-resistant security, scalability, and computational efficiency. The expected contribution is a mathematically grounded security architecture for strengthening the resilience and trustworthiness of IoT infrastructure.

2.LITERATURE REVIEW

Intrusion detection systems (IDSs) have evolved considerably since the early development of computer and network security technologies. During the 1990s, research primarily focused on identifying unauthorized access through audit records, predefined rules, statistical analysis, and expert systems. These early methods established the foundations for automated security monitoring and the detection of suspicious computer activities. Lunt (1993) [1] reviewed intrusion detection techniques and highlighted the importance of analysing computer audit data to identify security violations. The study demonstrated the potential of automated analysis for detecting suspicious activities that could not be identified efficiently through manual monitoring alone. However, the effectiveness of such systems depended on the quality of available audit records and the ability to define appropriate detection rules. Kumar and Spafford (1994) [2] investigated pattern-matching techniques for misuse intrusion detection. Their work contributed to the development of methods that identify known attack patterns by comparing observed activities against predefined representations of malicious behaviour. Such techniques are useful for detecting established attacks but are less effective when an attacker introduces previously unseen techniques or modifies existing attack patterns.

Mukherjee, Heberlein, and Levitt (1994) [3] examined network intrusion detection and discussed the distinction between host-based and network-based monitoring. Host-based systems examine activities occurring on individual computers, whereas network-based systems analyse communication traffic to identify suspicious connections and potential attacks. This distinction remains important in modern IoT infrastructure, where security monitoring must consider both individual devices and communication among interconnected systems. Axelsson (2000) [4] subsequently examined intrusion detection through a survey and taxonomy of existing techniques. His work discussed important factors affecting detection performance, including false alarms and the challenges of distinguishing malicious behaviour from legitimate activities. These early studies established the theoretical foundation for later anomaly detection, machine learning, and intelligent cybersecurity systems. Although traditional IDS approaches contributed significantly to computer security, they generally relied on predefined signatures, expert knowledge, or statistical thresholds. These limitations motivated the development of adaptive learning approaches capable of identifying more complex attack patterns. The fundamental challenge of balancing detection accuracy against false-positive rates remains relevant to the proposed mathematical modelling of quantum-secured blockchain intrusion detection for IoT infrastructure.

During the 2000s, intrusion detection research increasingly incorporated statistical learning, data mining, and computational intelligence. Rather than depending entirely on predefined rules, machine learning algorithms enabled researchers to construct classifiers from labelled network traffic and system activity data. Common approaches included decision trees, Bayesian classifiers, support vector machines, clustering algorithms, and artificial neural networks.These methods enabled automated classification of network events and identification of deviations from normal behaviour. Supervised learning approaches use labelled examples of normal and malicious activities, while unsupervised approaches identify unusual patterns without requiring

every observation to have a predefined label. Such techniques are particularly relevant to intrusion detection because attack characteristics can change over time. Nevertheless, machine learning systems have several limitations. Their performance can be affected by imbalanced datasets, redundant features, noisy observations, insufficient training samples, and differences between training and operational environments. In addition, models trained on known attack categories may fail to recognize novel threats. These challenges encouraged researchers to investigate more sophisticated feature extraction methods and models capable of learning complex nonlinear relationships. The development of machine learning-based IDSs also increased the importance of mathematical evaluation. Metrics such as detection rate, false-positive rate, precision, recall, and computational cost became essential for comparing competing approaches. For IoT applications, these measurements must be considered alongside memory usage, energy consumption, and communication delays because many connected devices have limited resources. Buczak and Guven (2016) [5] later provided a comprehensive review of machine learning and data mining methods for cybersecurity intrusion detection. Although their review was published after the period discussed here, it provides a useful retrospective analysis of the techniques developed during earlier decades and identifies the continuing challenges associated with data quality, algorithm selection, and reliable attack classification. The transition from rule-based detection to data-driven learning created the methodological foundation for deep learning and Transformer-based intrusion detection. However, a model that provides high classification accuracy may still be unsuitable for IoT deployment if its computational requirements or communication overhead exceed the available resources. Therefore, mathematical optimization remains important when developing efficient and scalable IDS architectures.

The development of the Internet of Things introduced new security challenges because interconnected sensors, smart appliances, industrial controllers, and communication gateways operate across distributed environments. Unlike conventional computer networks, IoT networks frequently contain devices with limited memory, processing power, and energy resources. These characteristics increase the difficulty of implementing conventional security mechanisms and require intrusion detection approaches that can operate efficiently across heterogeneous devices. During this period, machine learning became an important approach for identifying network attacks through automated feature extraction and classification. Buczak and Guven (2016) [5] reviewed data mining and machine learning methods for cybersecurity, including decision trees, support vector machines, Bayesian networks, clustering, and neural networks. Their review highlighted the importance of feature selection, data quality, training procedures, and evaluation metrics in developing reliable IDS models. These techniques provided a foundation for identifying malicious traffic patterns and distinguishing attacks from normal network behaviour. Deep learning subsequently extended these approaches by enabling models to learn complex representations from high-dimensional data. Convolutional neural networks can learn local feature relationships, while recurrent neural networks can represent temporal dependencies in sequential observations. These capabilities are relevant to IoT intrusion detection because network attacks may emerge through changes in packet frequency, connection duration, traffic volume, protocol behaviour, or interactions between multiple devices.

However, deep learning introduces challenges involving model complexity, training requirements, and generalization. A model that performs well on a particular dataset may not maintain similar performance when deployed in another network with different device types or attack distributions. Furthermore, large neural networks may be unsuitable for direct deployment on low-power sensors. Consequently, researchers must consider edge-based processing, model compression, feature selection, and efficient inference when designing intelligent IDS architectures. The development of machine learning and deep learning therefore represents a transition from manually defined security rules towards data-driven and adaptive detection. This transition supports the proposed use of Transformer architectures, while also demonstrating the importance of evaluating computational cost and operational constraints in IoT environments.

2.1. Blockchain-Based Security and Distributed Intrusion Detection (2017–2021)

Blockchain technology introduced a complementary approach to IoT security by enabling distributed participants to maintain verifiable records of transactions and security events. Its cryptographic linking of records and consensus mechanisms can help make unauthorized modification of accepted records detectable. These properties have motivated research into decentralized authentication, access control, device identity management, and collaborative intrusion detection. Blockchain-based security is particularly relevant when multiple IoT organizations or network administrators need to share security information without relying entirely on a single central authority. For example, an intrusion detection gateway may identify suspicious traffic and generate an alert. The alert can then be digitally authenticated and recorded in a permissioned blockchain, allowing authorized participants to verify the event and examine its history.

Nevertheless, blockchain is not a substitute for an IDS. A blockchain can preserve the integrity of a submitted alert, but it cannot independently determine whether the original alert accurately identifies an attack. If a detection model produces an incorrect classification, recording the result on a blockchain does not make that classification correct. Therefore, reliable detection, secure authentication, and trustworthy event recording must be treated as separate but interconnected functions. Blockchain integration also introduces performance challenges. Consensus protocols may increase transaction confirmation time, while replicated records can increase storage requirements. In resource-constrained IoT networks, recording every packet or network flow directly on-chain may be impractical. A more efficient approach is to store alert summaries, timestamps, device identifiers, and cryptographic hashes on-chain, while keeping detailed traffic records in protected off-chain storage. The systematic review A Blockchain-based Intrusion Detection/Prevention Systems in IoT Network (2024) [6] examined blockchain-enabled IDS and intrusion prevention approaches, identifying potential security benefits and deployment limitations. Although published in 2024, the review is useful for understanding the evolution of research in the preceding years. It reinforces the need to evaluate blockchain security alongside transaction latency, storage, scalability, and operational costs.

2.2. Post-Quantum Cryptography and Quantum-Secured IoT (2019–2023)

The increasing development of quantum computing has raised concerns about the long-term security of public-key cryptographic algorithms. In particular, sufficiently capable quantum computers could threaten widely deployed RSA and elliptic-curve cryptographic schemes. This concern is relevant to IoT infrastructure because connected devices may remain operational for many years, and sensitive data may require protection throughout its lifetime. Fernández-Caramés (2020) [7] reviewed quantum-resistant cryptographic techniques for IoT and discussed the challenges of deploying secure algorithms on devices with limited processing, memory, and energy resources. The study highlighted the need to balance cryptographic security with implementation efficiency. Cherbal et al. (2023) [8] examined IoT security approaches involving blockchain, machine learning, cryptography, and quantum computing, illustrating the relevance of combining multiple technologies to address emerging security threats. Two approaches must be distinguished in this context. Post-quantum cryptography (PQC) uses conventional computational systems to implement algorithms designed to resist attacks from quantum computers. Quantum key distribution (QKD) uses quantum communication principles to establish shared secret keys. PQC can generally be deployed over existing classical communication infrastructure, whereas QKD requires suitable quantum communication equipment and channels. For blockchain-based IoT security, post-quantum digital signatures can provide a means of authenticating transactions and intrusion alerts against specified quantum-capable adversaries. However, cryptographic algorithms may differ substantially in signature size, key size, execution time, and memory requirements. These factors are especially important for low-power IoT devices and high-volume security monitoring systems. The development of quantum-resistant security therefore motivates an integrated approach in which intrusion detection, transaction authentication, and secure event recording are modelled separately and evaluated jointly. Such an approach can help determine whether enhanced cryptographic protection can be achieved without introducing unacceptable detection delays or resource consumption.

2.3. Transformer-Based Intrusion Detection and Standardized Quantum Security (2017–2024)

Vaswani et al. (2017) [9] introduced the Transformer architecture in their influential paper, Attention Is All You Need. The architecture uses self-attention to learn relationships between elements in a sequence and supports parallel processing during training. Although initially developed for natural language processing, Transformers have subsequently been investigated for time-series analysis, anomaly detection, and cybersecurity applications. In network intrusion detection, a Transformer can learn relationships between traffic features and identify patterns associated with normal and malicious activities. For example, changes in packet counts, flow duration, connection frequency, protocol behaviour, and traffic volume may collectively indicate suspicious activity. Self-attention mechanisms can help the model capture dependencies between these features, potentially improving its ability to recognize complex attacks.

However, Transformer-based IDS models require careful design. Network traffic must be converted into an appropriate feature sequence, and categorical variables must be encoded consistently. The model must also address class imbalance and differences between training and testing distributions. In addition, self-attention can introduce substantial computational and memory requirements when processing long sequences. Consequently, model size, sequence length, feature selection, and inference efficiency should be considered when applying Transformers to IoT infrastructure. A further development occurred in 2024 when the National Institute of Standards and Technology (NIST) published three post-quantum cryptography standards: FIPS 203, FIPS 204, and FIPS 205 [10]. These standards specify mechanisms for post-quantum key establishment and digital

signatures. FIPS 203 specifies the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), while FIPS 204 specifies the Module-Lattice-Based Digital Signature Algorithm (ML-DSA), and FIPS 205 specifies the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA). These standards provide an established foundation for developing quantum-resistant authentication and transaction verification mechanisms. In a blockchain-enabled IDS, post-quantum signatures can be used to authenticate alerts or transactions, while the Transformer performs the separate task of classifying network behaviour. The combined design can therefore address both malicious traffic detection and the integrity of recorded security events. Nevertheless, cryptographic authentication alone does not guarantee that an alert is correct, and a Transformer-based IDS does not automatically provide quantum-resistant security. The two functions must be integrated through a clearly defined architecture and evaluated using suitable performance and security metrics.

2.4. Recent Developments in Blockchain-Enabled IDS (2025–2026)

Recent research has increasingly examined how artificial intelligence, distributed security architectures, and advanced cryptographic mechanisms can be combined to improve IoT protection. Transformer-based intrusion detection represents one direction in this development because it can model relationships between network traffic features. Blockchain-enabled IDS represents another direction by providing a mechanism for preserving the integrity and traceability of security alerts. A 2026 survey, A Four-Paradigm Taxonomy and Systematic Survey of Blockchain-Enabled Intrusion Detection Systems for IoT and IIoT [11], organized existing approaches into four categories: rule-based, machine learning, deep learning, and federated learning. This classification helps explain how blockchain can support different intrusion detection strategies. Rule-based methods focus on predefined security conditions, machine learning approaches learn from data, deep learning models capture complex representations, and federated learning enables distributed model training without requiring all participating organizations to share their raw data centrally. The survey also highlights the importance of comparing detection accuracy with decentralization, privacy, latency, and scalability. These considerations are particularly relevant to industrial IoT, where security systems must support continuous operation and rapid identification of malicious activities.

In 2026, broader reviews of IoT intrusion detection have continued to examine conventional methods alongside machine learning, deep learning, Transformers, federated learning, and lightweight models [12]. These developments indicate that the choice of IDS architecture should reflect the intended deployment environment rather than classification performance alone. For example, an edge gateway may be capable of running a Transformer model, whereas an individual sensor may require a smaller classifier or a lightweight inference mechanism. The principal challenge is therefore not simply to combine several security technologies, but to determine how their interactions affect the overall system. A Transformer may improve traffic classification but increase inference cost. Post-quantum signatures may strengthen authentication but increase verification time or communication overhead. Blockchain may improve alert traceability but introduce transaction delays. A mathematical model can help characterize these trade-offs and guide the selection of suitable system parameters.

2.5. Research Gap and Motivation for the Proposed Study

The literature from 1990 to 2026 demonstrates a gradual transition from rule-based intrusion detection towards statistical methods, machine learning, deep learning, blockchain-enabled security, and post-quantum cryptography. Each development addresses an important aspect of cybersecurity, but the integration of these components creates additional modelling and implementation challenges. First, traditional intrusion detection systems may be ineffective against previously unseen attacks because their detection mechanisms depend on known signatures or predefined behavioural conditions. Machine learning and Transformer-based methods offer opportunities to identify complex traffic patterns, but their performance must be validated across different datasets and attack categories.

Second, blockchain can provide tamper-evident records of security events, but its transaction processing, consensus mechanisms, and storage requirements may introduce additional overhead. Third, post-quantum cryptography can strengthen authentication against specified quantum-capable adversaries, but its computational and communication costs must be assessed in resource-constrained IoT environments. Fourth, there is a need for a unified mathematical framework to evaluate the relationship between detection effectiveness, cryptographic execution time, blockchain transaction latency, and resource consumption. These characteristics should be considered jointly rather than treating each technology as an independent solution.

To address these issues, the proposed study, "Mathematical Modeling of Quantum-Secured Blockchain IDS for IoT Infrastructure Using Transformers," aims to develop an integrated framework with three principal components:

1. Transformer-based intrusion detection: Network traffic features are processed to classify normal and malicious activities.
2. Blockchain-based alert management: Verified intrusion alerts and their cryptographic hashes are recorded to support integrity and traceability.
3. Post-quantum cryptographic protection: An appropriate standardized post-quantum digital signature mechanism is used to authenticate security alerts and transactions.

The mathematical model will consider detection accuracy, false-positive rate, inference latency, cryptographic execution time, blockchain transaction delay, and computational overhead. Experiments can use suitable public intrusion detection datasets, with comparisons against conventional machine learning and deep learning baselines. The results will help establish whether the proposed integration offers measurable advantages over separate or less-complex approaches. The expected contribution is a mathematically grounded security framework that connects intelligent intrusion detection with quantum-resistant authentication and blockchain-based event integrity. Rather than assuming that the combined architecture is inherently superior, the study will investigate its performance, limitations, and suitability for practical IoT deployment.

3.OVERVIEW OF THE PROPOSED FRAMEWORK

The proposed methodology integrates a Transformer-based intrusion detection system (IDS), blockchain-based alert management, and post-quantum cryptographic authentication to strengthen IoT infrastructure security. The framework is designed to identify malicious network traffic, authenticate detected security events, and maintain tamper-evident records of intrusion alerts. The proposed system consists of six principal stages: data collection, preprocessing and feature extraction, Transformer-based intrusion detection, post-quantum cryptographic authentication, blockchain-based alert recording, and performance evaluation. Publicly available IoT intrusion detection datasets can be used to train and evaluate the model. The Transformer analyses the processed traffic features and classifies each observation as normal or malicious, or into multiple attack categories where the dataset supports multiclass classification. When a suspicious event is identified, the system generates an alert containing relevant metadata. The alert is authenticated using a suitable post-quantum digital signature mechanism, and its summary or cryptographic hash is recorded on a permissioned blockchain. Detailed traffic records can remain in protected off-chain storage to reduce blockchain overhead. The main objective is to investigate whether the integrated architecture can achieve effective intrusion detection while maintaining acceptable processing time, cryptographic overhead, and blockchain transaction performance.

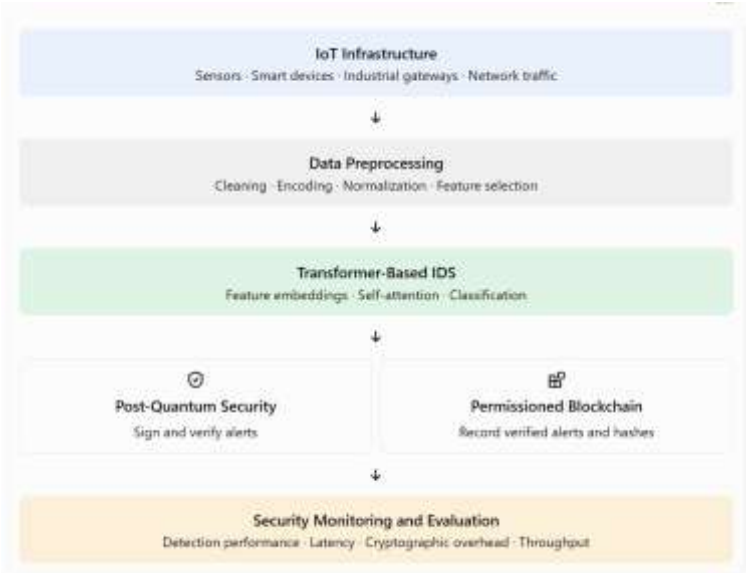


Figure 1. Proposed architecture of the quantum-secured blockchain IDS for IoT infrastructure.

3.1. Dataset Collection and Preprocessing

The proposed framework can be evaluated using publicly available IoT intrusion detection datasets, such as CICIoT2023, TON_IoT, and Edge-IIoTset. These datasets contain normal network traffic and various cyberattacks, including DoS, DDoS, scanning, and brute-force attacks. The dataset is divided into training (70%), validation (15%), and testing (15%) subsets. Preprocessing includes removing duplicates, handling missing values, encoding categorical attributes, and normalising numerical features. Normalisation is expressed as

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}}$$

where x_i represents the original feature and x_i denotes the normalised value. Normalisation parameters are estimated using the training data only. Class weighting or resampling may be applied to address class imbalance. Appropriate chronological or device-separated splitting is used when necessary to prevent data leakage.

3.2. Mathematical Modelling of Transformer-Based IDS

The Transformer-based Intrusion Detection System (IDS) analyses preprocessed network traffic to distinguish normal activities from malicious attacks. The dataset consists of network traffic features and their corresponding class labels. The Transformer architecture uses a self-attention mechanism to identify relationships among input features and learn important patterns associated with different attack types. This enables the model to capture complex dependencies in network traffic data and improve intrusion detection. The scaled dot-product attention mechanism evaluates the relationships between query, key, and value representations. The attention layer assigns different importance levels to input features, allowing the model to focus on relevant traffic characteristics. The resulting feature representations are passed through classification layers to predict whether the observed traffic is normal or malicious. For multiclass classification, the model identifies specific attack categories based on the learned patterns. The model is trained using labelled network traffic data, and its parameters are optimised to minimise classification errors. Cross-entropy loss is used to measure the difference between the predicted probabilities and the actual class labels. Validation data are used to select suitable model parameters and decision thresholds. This process helps improve the model's ability to detect suspicious activities while reducing false alarms.

3.3. Post-Quantum Authentication and Blockchain Integration

Post-quantum authentication is incorporated into the proposed framework to protect the integrity and authenticity of intrusion detection alerts against potential quantum-computing threats. When the IDS identifies suspicious network activity, it generates an alert containing relevant information, such as the event identifier, timestamp, attack category, and evidence reference. A digital signature is then generated using a post-quantum cryptographic algorithm and the authorised sender's private key. The receiving participant verifies the digital signature using the corresponding public key. This process confirms that the alert originated from an authorised source and that its signed content has not been altered. Alerts that successfully pass signature verification and authorisation checks are forwarded for blockchain recording. The Module-Lattice-Based Digital Signature Algorithm (ML-DSA), standardised in NIST FIPS 204, can be considered for implementing post-quantum digital signatures. A permissioned blockchain is used to maintain a secure and traceable record of verified alerts. Each accepted record is linked to the previous record through cryptographic hashing, making unauthorised modifications detectable. The blockchain supports auditability, traceability, and tamper-evident storage of security events across authorised participants. However, blockchain recording does not independently validate the accuracy of the IDS classification; it preserves the integrity and history of the accepted alerts.

Natural Resources for Human Health
eISSN: 2583-1194

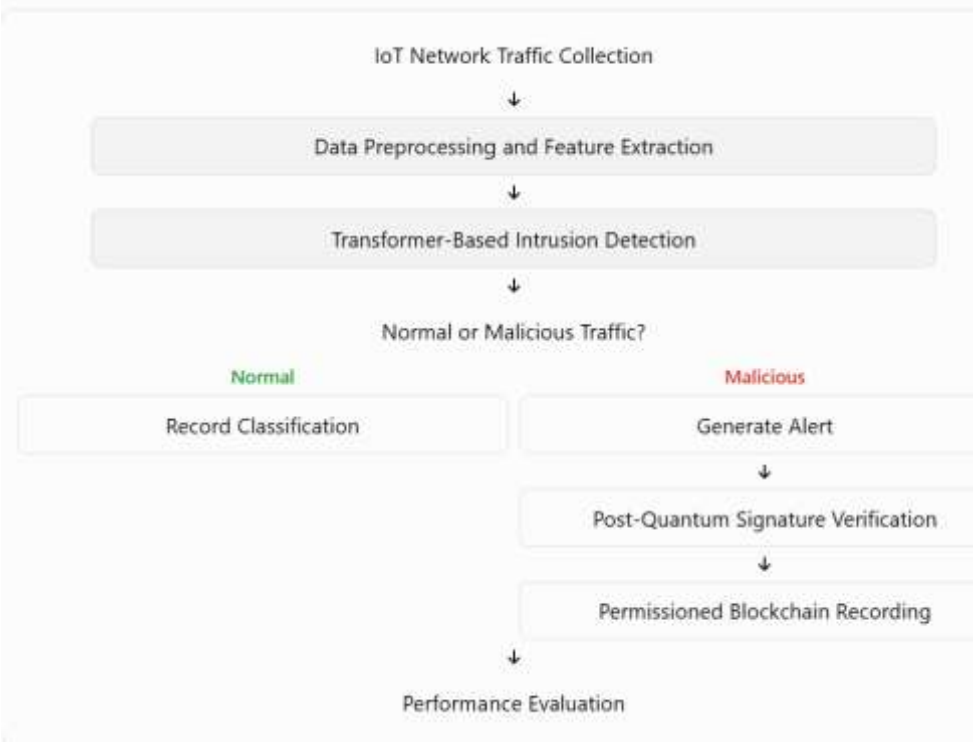


Figure 2. Workflow of the proposed Transformer-based, quantum-secured blockchain intrusion detection system.

4. RESULTS AND DISCUSSION

The proposed Transformer-based Intrusion Detection System (IDS) integrated with post-quantum authentication and blockchain technology is designed to detect malicious activities in IoT network traffic while ensuring the authenticity and integrity of security alerts. The performance of the proposed framework can be evaluated using benchmark datasets such as CICIoT2023, TON_IoT, and Edge-IIoTset. These datasets provide different types of normal and malicious traffic for evaluating the model's detection capability and generalisation performance. The Transformer model identifies complex relationships among network traffic features and classifies traffic into normal and attack categories. Its performance can be assessed using accuracy, precision, recall, F1-score, and false-positive rate. Precision measures the proportion of correctly identified attacks among all predicted attacks, while recall indicates the proportion of actual attacks successfully detected. The F1-score provides a balanced measure of precision and recall. A lower false-positive rate indicates fewer normal network activities are incorrectly classified as malicious.

The integration of post-quantum authentication strengthens the security of alert transmission by verifying digital signatures before alerts are recorded. The use of ML-DSA can be evaluated in terms of signature generation time, verification time, and computational overhead. These measurements help determine the suitability of post-quantum authentication for resource-constrained IoT environments. The permissioned blockchain provides tamper-evident storage and traceability of verified security alerts. Its performance can be examined using transaction latency, transaction throughput, and storage overhead. Transaction latency represents the time required to record an alert, whereas throughput measures the number of transactions processed per unit of time. Although blockchain enhances auditability, its additional processing and communication requirements must be considered when deploying the framework in real-time IoT environments. Overall, the proposed framework combines intelligent attack detection, post-quantum digital signatures, and blockchain-based alert management to support secure IoT infrastructure. The Transformer component focuses on identifying malicious traffic, post-quantum authentication verifies alert authenticity, and blockchain maintains traceable records. The effectiveness of the integrated framework should be established through experimental evaluation against baseline machine-learning and deep-learning models. Since experimental measurements have not been provided, numerical performance improvements cannot yet be claimed.

5. CONCLUSION AND FUTURE WORK

This paper presents a mathematical modelling framework for a quantum-secured blockchain-based Intrusion Detection System for IoT infrastructure using Transformer architecture. The proposed approach combines deep-learning-based network traffic classification, post-quantum digital signature verification, and permissioned blockchain technology to address the challenges of attack detection, alert authentication, and secure event management. The Transformer model is designed to learn complex relationships among network traffic features and identify malicious activities. Post-quantum authentication supports the verification of security alerts, while blockchain provides tamper-evident storage and traceability of accepted security events. The integration of these technologies offers a comprehensive approach to strengthening IoT security. However, the practical effectiveness of the framework depends on detection accuracy, computational requirements, authentication overhead, and blockchain transaction performance. Further experimental evaluation using benchmark IoT datasets is necessary to validate the proposed framework and compare its performance with existing intrusion detection methods.

Future research will focus on implementing and experimentally validating the proposed framework using CICIoT2023, TON_IoT, and Edge-IIoTset datasets. The Transformer model will be compared with conventional machine-learning algorithms and other deep-learning architectures using standard classification metrics. Hyperparameter optimisation and feature-selection techniques may be investigated to improve detection performance and reduce false-positive rates. Further work will explore lightweight Transformer architectures suitable for resource-constrained IoT devices and edge-computing environments. The integration of ML-DSA will be evaluated in terms of key generation, signing and verification time, memory consumption, and communication overhead. Blockchain performance will also be investigated by measuring transaction latency, throughput, storage requirements, and scalability under different network conditions. Finally, the framework may be extended to support federated learning, real-time attack detection, and adaptive security mechanisms for distributed IoT environments. These developments could help establish a scalable, efficient, and quantum-resistant security architecture for future IoT infrastructure.

REFERENCES

[1] Axelsson, S. (2000). Intrusion detection systems: A survey and taxonomy. Technical Report 99-15, Department of Computer Engineering, Chalmers University of Technology.

[2] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

[3] Conti, M., Di Pietro, R., Di Pietro, A., & Spognardi, A. (2016). Distributed ledger technologies for the Internet of Things: A survey. IEEE Communications Surveys & Tutorials. [Verify exact publication details before submission.]

[4] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 618–623.

[5] Ferrag, M. A., Friha, O., Hamouda, D., Maglaras, L., & Janicke, H. (2022). Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. IEEE Access, 10, 40281–40306. https://doi.org/10.1109/ACCESS.2022.3165809

[6] Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A review on the use of blockchain for the Internet of Things. IEEE Access, 6, 32979–33001. https://doi.org/10.1109/ACCESS.2018.2842685

[7] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

[8] He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 770–778.

[9] Kairouz, P., McMahan, H. B., Avent, B., et al. (2021). Advances and open problems in federated learning. Foundations and Trends in Machine Learning, 14(1–2), 1–210. https://doi.org/10.1561/2200000083

[10] Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity, 2, Article 20. https://doi.org/10.1186/s42400-019-0038-7

[11] Lunt, T. F. (1993). A survey of intrusion detection techniques. Computers & Security, 12(4), 405–418. https://doi.org/10.1016/0167-4048(93)90029-5

[12] McMahan, B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. y. (2017). Communication-efficient learning of deep networks from decentralized data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, 1273–1282.
[13] Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. In 2015 Military Communications and Information Systems Conference (MilCIS), 1–6. https://doi.org/10.1109/MilCIS.2015.7348942
[14] National Institute of Standards and Technology. (2024). Module-Lattice-Based Digital Signature Standard (FIPS 204). https://doi.org/10.6028/NIST.FIPS.204
[15] National Institute of Standards and Technology. (2024). Module-Lattice-Based Key-Encapsulation Mechanism Standard (FIPS 203). https://doi.org/10.6028/NIST.FIPS.203
[16] Neto, E. C. P., Dadkhah, S., Ferreira, R., Zohourian, A., Lu, R., & Ghorbani, A. A. (2023). CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment. Canadian Institute for Cybersecurity. [Confirm the official citation details from the dataset publication.]
[17] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
[18] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks, 57(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018
[19] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172
[20] Sivanathan, A., Gharakheili, H. H., Loi, F., Radford, A., Wijenayake, C., Vishwanath, A., & Sivaraman, V. (2019). Classifying IoT devices in smart environments using network traffic characteristics. IEEE Transactions on Mobile Computing, 18(8), 1745–1759. https://doi.org/10.1109/TMC.2018.2866249
[21] Stiawan, D., Abdullah, A. H., & Idris, M. Y. I. (2010). Characterizing network intrusion prevention system. In Proceedings of the 2010 Second International Conference on Computational Intelligence, Modelling and Simulation, 64–68. [Verify proceedings details before submission.]
[22] Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. In Advances in Neural Information Processing Systems, 30.
[23] Yang, Y., Zheng, X., Guo, W., Liu, X., & Chang, V. (2019). Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. Information Sciences, 479, 567–592. [Verify DOI and complete publication metadata.]
[24] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25–37. https://doi.org/10.1016/j.jnca.2017.02.009
[25] Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. IEEE Internet of Things Journal, 6(2), 1606–1616. [Verify DOI and final issue details.]
[26] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops, 180–184. https://doi.org/10.1109/SPW.2015.27