

Secure AI-Blockchain Framework with Supply Chain Integrity and Role-Based Smart Contracts for Real-Time Cybersecurity

Mr P Lokesh Kumar, R Kalai Magal

Assistant Professor, Department of CSE Kuppam Engineering College, Kuppam, India
lokeshkumarp@kec.ac.in

Abstract—The increasing sophistication of cyber threats has revealed the significant shortcomings of conventional intrusion detection systems, especially in terms of transparency, auditability, and resistance to log tampering attacks. In this paper, we present a secure AI blockchain framework that combines convolutional neural network-based intrusion detection with a permissioned blockchain platform to provide tamper-proof cybersecurity logging in real-time. The approach improves security through hashing of cryptographic alerts with Merkle tree-based structures, role-based access control in smart contracts, and validation of supply chain integrity through smart contracts and hashing models on the blockchain. The proposed design prevents malicious alert manipulation, insider attacks, and attacks of the artificial intelligence model while ensuring low performance overhead. Our experimental results on the CICIDS2017 dataset show high detection accuracy and acceptable latency. Our design offers enhanced forensic auditability and decentralized trust, making it a scalable solution for future intelligent cybersecurity systems.

Index Terms—Keywords: Artificial Intelligence, Blockchain, Cybersecurity, Intrusion Detection, Smart Contracts, Supply Chain Security, Role-Based Access Control, Merkle Tree.

I. INTRODUCTION

The introductory part of the proposed Secure AI-Blockchain Cybersecurity Framework clearly identifies the need for a unified strategy to counter the rising complexity of cyber threats, pointing out the limitations of traditional cybersecurity solutions. These solutions are normally not transparent enough to support the verification of AI-based security decisions, making it difficult to comply with regulatory requirements. This is especially true in light of the fact that security logs are highly susceptible to manipulation attacks and AI models

are vulnerable to poisoning attacks and insider threats. To overcome these major challenges, the proposed framework combines a Convolutional Neural Network (CNN)-based Intrusion Detection System (IDS) with a permissioned blockchain environment. This synergy seeks to develop a cybersecurity solution that is not only highly accurate in threat detection but also provides an immutable and transparent record of security events. A key part of this architecture is the implementation of Merkle Tree alert batching, which efficiently aggregates many individual security alerts into a single cryptographic hash the Merkle Root optimizing the storage and verification steps on the blockchain without compromising the integrity of individual alerts.

Moreover, the framework includes role-based smart contracts to manage access and policy enforcement, ensuring that only authorized parties can undertake critical actions, such as submitting Merkle Roots or anchoring AI model hashes.

This smart contract layer also extends to the verification of verifiable supply chain integrity for AI models, ensuring that they have a provenance and cannot be unauthorizedly altered or maliciously replaced.

By anchoring cryptographic hashes of AI models, their training datasets, and even the smart contract bytecode on the blockchain, the framework provides an immutable record that can be continuously verified at runtime. The unified architecture is intended to support very ambitious performance requirements, such as an intrusion detection accuracy rate of over 93%. The performance requirements of the framework highlight its ability to support real-time protection. The overall vision is to ensure a scalable, tamper-proof, and auditable

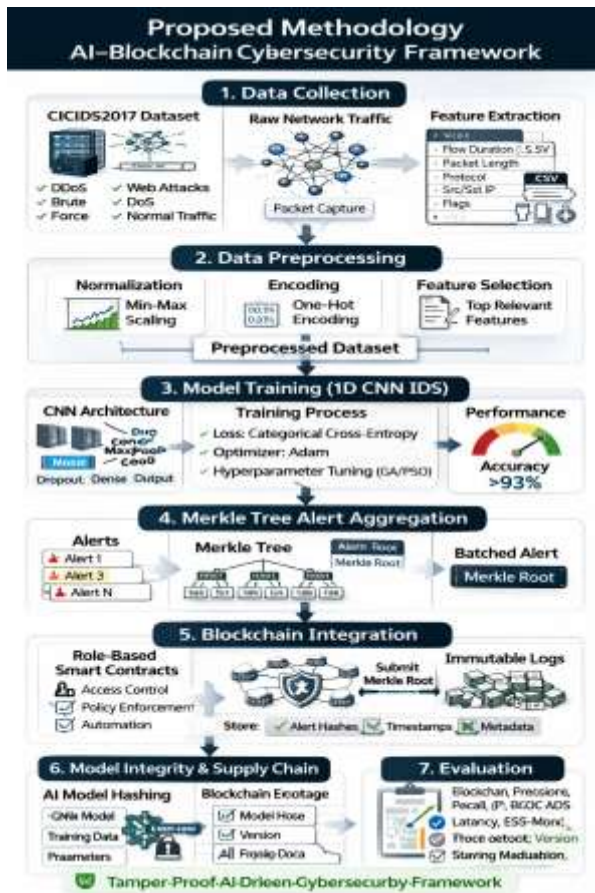


Fig. 1. AI-Blockchain Cybersecurity Framework Architecture

cybersecurity posture for next-generation intelligent cybersecurity systems

II. LITERATURE REVIEW

Recent research studies on the integration of Artificial Intelligence (AI) and blockchain for improved cybersecurity have shown promising advancements, especially in intrusion detection systems, supply chain security, and role-based management of smart contracts. The two technologies can be combined to leverage the intelligent threat detection capabilities of AI with the decentralized, immutable, and transparent data storage capabilities of blockchain.

One such advancement is the AICyber-Chain framework, which was proposed by Ullah et al. in 2024. This framework combines AI and blockchain to improve cybersecurity systems [1]. The integration of blockchain technology helps to overcome these issues by using a decentralized and immutable ledger to securely store cybersecurity events [1].

The "SecureChainAI" framework proposed by Thamarai-Selvi et al. (2024) further emphasizes the relevance of this integration, particularly in the context of IoT networks in critical domains such as healthcare, industrial automation, and smart cities, where data integrity, privacy, and reliability are of utmost significance [3].

Their analysis on NSL-KDD, CICIDS2017, and a custom-made synthetic dataset emphasized the importance of key parameters such as precision, recall, F1 score, ROC-AUC, and detection latency, thereby illustrating the potential of these AI algorithms [4]. Aljabri et al. (2023) concentrated on the application of convolutional neural networks (CNNs) for intrusion detection using blockchain technology in Cyber-Physical Systems (CPS) [5].

System architectures may also include a permissioned blockchain infrastructure to facilitate real-time, tamper-proof cybersecurity logging. This is preferred for its controlled access, improved privacy, and improved performance over public blockchain systems, with Hyperledger Fabric and private Ethereum networks being the most suitable candidates [2].

Role-based smart contracts are essential for governance and management in these combined systems. These contracts are responsible for ensuring that only authorized parties can execute critical actions, such as posting Merkle Roots or anchoring AI model hashes [1].

This smart contract layer is further extended to provide provable integrity of the supply chain for AI models. By securing the cryptographic hashes of AI models, their training data, and even the bytecode of the smart contract itself on the blockchain, an immutable record is formed that can be verified at runtime indefinitely [1]. This ensures that there are no unauthorized changes or attacks by malicious actors, thereby resolving problems such as insider attacks and AI model attacks [1].

The performance analysis of these combined systems is focused on achieving high accuracy and low latency. For example, the frameworks are designed to achieve intrusion detection accuracy of over 93

III. EXISTING SYSTEM

The combination of Artificial Intelligence (AI) and blockchain technology offers a strong solution for future-proof cybersecurity systems, especially for real-time threat analysis, traceability, and supply chain security in a complex digital setting.

The proposed system combines a Convolutional Neural Network (CNN)-based Intrusion Detection System (IDS) with a permissioned blockchain. It employs Merkle Tree-based alert aggregation and role-based smart contract management for traceable supply chain security.

The system tackles key cybersecurity issues such as log manipulation, internal threats, and immutable attributes. CNN-based AI models are efficient for intrusion detection in Cyber-Physical Systems (CPS), IoT networks, and cloud computing.

The blockchain technology provides a secure and immutable audit trail, safeguarding the integrity and transparency of security logs and AI model states. The proposed system encompasses system architecture design,

Conventional System Limitations:

- There are some limitations in the conventional cybersecurity systems when it comes to dealing with contemporary

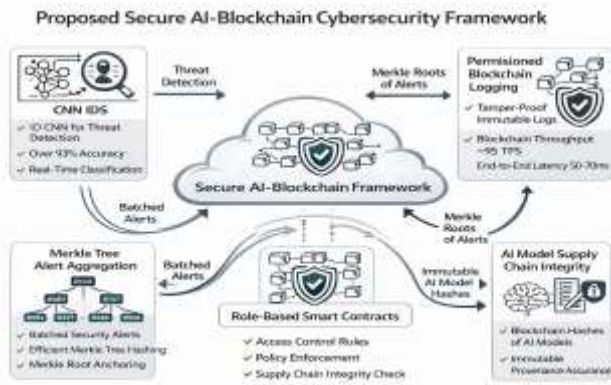


Fig. 2. Architecture of the Secure AI-Driven Blockchain Logging System

cyber threats. These systems are not transparent in their AI decision-making processes.

- This makes auditing and forensic analysis a challenge.
- The security logs in these systems are also prone to tampering. Moreover, the AI models in conventional systems are vulnerable to attacks such as model poisoning and unauthorized modification.
- This affects the reliability of these models. The centralized architecture in conventional systems is prone to single points of failure. This increases the security risks and poses scalability challenges.
- In addition, conventional systems do not support tamper-proof logging, decentralized trust, and integrity verification.

IV. PROPOSED SYSTEM

The proposed Secure AI-Blockchain Cybersecurity Framework combines Artificial Intelligence (AI), blockchain governance, cryptographic integrity, and scalable alert optimization in a single architecture for real-time intrusion detection and supply chain integrity.

The proposed framework is designed to address the shortcomings of existing cybersecurity solutions, such as vulnerability to log tampering, insider threats, and AI model poisoning, by harnessing the natural security properties of blockchain technology.

The main elements of the proposed framework include a multi-layered architecture for network traffic analysis, Merkle Tree alert aggregation, role-based smart contract governance, permissioned blockchain logging, and a reliable supply chain integrity verification system for AI models. The proposed framework is designed to directly address the most common cybersecurity issues, such as log tampering, insider threats, and AI model poisoning. The proposed framework combines a CNN-based Intrusion Detection System (IDS) with a permissioned blockchain architecture. The main innovations of the proposed framework include Merkle Tree alert aggregation enforcement, and a complete supply chain model integrity verification process.

The system is designed to offer tamper-proof security event logging, provable AI model provenance, and robust threat mitigation.

V. COMPARATIVE ANALYSIS

TABLE I
COMPARATIVE ANALYSIS OF EXISTING SYSTEM AND PROPOSED SYSTEM

Feature	Proposed System
Transparency	Provides full transparency using blockchain-based immutable logging and verifiable audit trails.
Log Security	Uses permissioned blockchain to ensure tamper-proof, immutable, and secure logging of security events.
AI Model Integrity	Ensures AI model integrity using cryptographic hashing and blockchain-based supply chain verification.
Architecture	Decentralized permissioned blockchain architecture with improved scalability and fault tolerance.
Intrusion Detection	CNN-based IDS provides high accuracy (93%) and real-time threat detection.
Alert Verification	Uses Merkle Tree-based alert aggregation for efficient and verifiable blockchain logging.
Access Control	Role-based smart contracts provide automated, secure, and verifiable access control.
Auditability	Provides complete auditability through immutable blockchain records.
Supply Chain Integrity	Ensures AI model provenance and integrity using blockchain verification.
Performance	Optimized performance with low latency (50–70 ms) and high throughput (95 TPS).

VI. METHODOLOGY

The methodology for implementing and evaluating the proposed Secure AI-Blockchain Cybersecurity Framework involves a comprehensive approach to data handling and model assessment, focusing on data collection, preprocessing, model training, and rigorous evaluation.

A. Data Collection

The **CICIDS2017 dataset** will serve as the primary source for training and evaluating the 1D CNN intrusion detection engine. This dataset is chosen for its realism and comprehensive nature, encompassing a wide range of modern attack scenarios such as Denial of Service (DoS), Distributed Denial of Service (DDoS), Brute Force, Web Attacks, and Botnets, alongside legitimate background traffic. It provides a robust environment to assess the performance of Intrusion Detection System (IDS) models under diverse and evolving cyber threats. The dataset includes raw network packet captures, which can be processed to extract flow-based features, as well as pre-generated CSV files with extracted features and labeled attack types. The use of such a well-established and diverse dataset is crucial for developing an IDS that can generalize effectively to real-world cyber threats.

B. Data Preprocessing

Data preprocessing is a critical step in preparing raw network traffic data for effective analysis by the AI model. This involves several stages to transform raw packets into a structured format suitable for machine learning algorithms.

- **Normalization:** Numerical features are scaled to a common range, typically between 0 and 1, using methods like Min-Max normalization. This prevents features with larger magnitudes from disproportionately influencing the model's learning process. For example, parameters such as packet size or flow duration might vary widely and require scaling.
- **Encoding:** Categorical features, such as protocol types (e.g., TCP, UDP, ICMP) or flag states, are converted into numerical representations. One-hot encoding is commonly used for this purpose, where each category is represented by a binary vector, allowing the model to process these non-numeric attributes.
- **Feature Selection:** To reduce dimensionality, mitigate noise, and improve model efficiency, relevant features are selected from the preprocessed data. Techniques like correlation analysis, mutual information, or feature importance scores derived from tree-based models can be employed to identify and retain the most informative features for intrusion detection. This step is particularly important for network traffic data, which can contain hundreds of features, many of which may be redundant or irrelevant.

While not explicitly "tokenization" in the natural language processing sense, the analogous process in network intrusion detection involves converting network flow attributes into a structured input that the 1D CNN can effectively process. This can be viewed as constructing a "token" or "sequence" from the preprocessed features. For a 1D CNN, the order of features within this vector can be crucial, as convolutional filters learn spatial or temporal dependencies. For instance, features related to connection establishment might precede those related to data transfer characteristics.

C. Model Training

The training of the 1D CNN intrusion detection engine will be executed using the preprocessed CICIDS2017 dataset. The model will be trained to classify network traffic into various categories, including normal behavior and different types of cyberattacks.

- **Loss Function and Optimizer:** For multi-class classification, **categorical cross-entropy** is typically used as the loss function. Optimizers such as **Adam** or **RMSprop** are suitable for efficiently updating model weights during training, aiming to minimize the loss function and improve classification accuracy.
- **Hyperparameter Optimization:** To achieve optimal performance, hyperparameter optimization techniques such as Genetic Algorithms (GA) and Particle Swarm Optimization (PSO) can be employed to fine-tune parameters like the number of layers, filters, kernel sizes, and learning rates of the 1D CNN.
- **Regularization:** Dropout layers will be incorporated between dense layers to prevent overfitting, enhancing the model's generalization capabilities to unseen data.

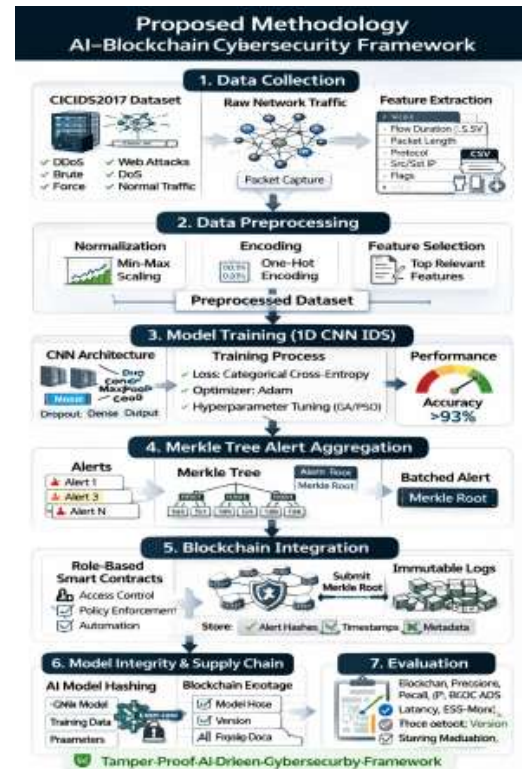


Fig. 3. Methodology for AI-Blockchain IDS Implementation and Performance Evaluation

D. Model Evaluation

The performance of the 1D CNN intrusion detection engine will be rigorously evaluated using several key metrics to provide a comprehensive understanding of its effectiveness.

- **Accuracy:** Represents the overall proportion of correctly classified instances (both normal and attack traffic) out of all instances. The target for the proposed framework is an accuracy exceeding 93%.
- **Precision:** Measures the proportion of true positive predictions among all positive predictions made by the model. High precision indicates a low false positive rate, which is crucial in cybersecurity to avoid overwhelming security analysts with benign alerts.
- **Recall (Sensitivity):** Measures the proportion of true positive predictions among all actual positive instances. High recall indicates a low false negative rate, meaning the model effectively identifies most actual attacks.
- **F1-score:** The harmonic mean of precision and recall, providing a balanced measure that is particularly useful for evaluating models on datasets with class imbalance, which is common in intrusion detection where attack instances are typically less frequent than normal traffic.
 - **Latency:** The end-to-end time from network packet ingestion to the generation of a confirmed blockchain-anchored Merkle Root is targeted between 50 and 70 milliseconds. This real-time performance is vital for prompt threat response.

- **Blockchain Throughput:** The blockchain network is designed to achieve a sustained throughput of approximately 95 Transactions Per Second (TPS) 2. This will be evaluated by monitoring the rate at which Merkle Roots are successfully committed to the blockchain.
- **Storage Reduction:** The efficiency of Merkle batching in reducing on-chain storage will be quantified by comparing the volume of data stored on-chain with and without batching.

VII. FUTURE ENHANCEMENTS

- To further enhance the security, resilience, and capabilities of the AI-Blockchain Cybersecurity Framework, the following improvements are foreseen:
- **Integration of Post-Quantum Cryptography (PQC):** With the looming threat of the possible development of quantum computers that could potentially break existing cryptographic algorithms such as SHA-256 and ECDSA, the integration of PQC algorithms such as CRYSTALS-Kyber (for key exchange) and CRYSTALS-Dilithium (for digital signatures) will be imperative. This forward-thinking approach will ensure the long-term cryptographic security of the framework against quantum attacks.
- **Integration of Zero Trust Architecture (ZTA):** The adoption of a Zero Trust Architecture, whereby no entity inside or outside the network is trusted by default, will offer an extra layer of security.
- **Federated Learning (FL) Support:** To improve privacy and utilize distributed data for training models, the incorporation of Federated Learning may enable AI models to be trained on local data in multiple organizations without the need for data centralization. The use of Blockchain technology can then protect the aggregation of model updates and the integrity of the global model.
- **Privacy-Preserving Forensic Proofs:** The investigation of methods such as Zero-Knowledge Proofs (ZKPs) may enable forensic auditors to validate the integrity of notifications or AI model states without disclosing the underlying sensitive information.

VIII. CONCLUSION

The Secure AI-Blockchain Cybersecurity Framework offers a comprehensive and cutting-edge approach to the most pressing challenges in contemporary cybersecurity. The combination of a 1D CNN-based Intrusion Detection System and a permissioned blockchain offers real-time threat detection and forensic immutability and verifiable governance.

The Merkle Tree alert aggregation mechanism is highly effective in overcoming scalability issues by optimizing on-chain storage and transaction processing. In addition, the end-to-end supply chain integrity verification system provides complete protection throughout the entire AI

model lifecycle, including the prevention of model poisoning and unauthorized manipulation.

This integrated framework offers a solid foundation for a resilient, transparent, and auditable cybersecurity posture that can effectively adapt to the dynamic threat environment. The synergy between AI for intelligent threat identification and blockchain for tamper-proof logging and verification represents a paradigm shift towards intelligent threat mitigation and decentralized security.

REFERENCES

- [1] Z. Ullah, A. Waheed, M. I. Mohmand, S. Basar, M. Zareei, and F. Granda, "AI-Cyber-Chain: Combining AI and Blockchain for Improved Cybersecurity," *IEEE Access*, vol. 12, pp. 1–15, Jan. 2024.
- [2] S. Goundar and I. Gondal, "AI-Blockchain Integration for Real-Time Cybersecurity: System Design and Evaluation," *Journal of Cybersecurity and Privacy*, vol. 5, no. 3, pp. 1–18, Aug. 2025.
- [3] A. Aljabri, F. Jemili, and O. Korbaa, "Convolutional neural network for intrusion detection using blockchain technology," *International Journal of Computers and Applications*, pp. 1–12, Nov. 2023.
- [4] N. R. Rejin Paul, V. Nallarasana, N. Krishnaiah, and L. Ganganathan, "Blockchain-integrated intrusion detection system with optimized cosine CNN for enhanced privacy and security in cloud computing," *Information Sciences*, vol. 678, pp. 1–20, Dec. 2025.
- [5] H. Nandanwar and R. Katarya, "A hybrid Blockchain-Based framework for securing intrusion detection systems in internet of things," *Cluster Computing*, vol. 28, pp. 1–19, Jul. 2025.
- [6] L. Tightiz, L. M. Dang, and K. W. Park, "AIoT-Blockchain Security for Supply Chain Threats in IEC 61850 Substations Using Informer-Powered Reinforcement Learning," *IEEE Internet of Things Journal*, vol. 13, no. 1, pp. 1–14, Nov. 2025.
- [7] A. Abubakar Aliyu, J. Liu, and E. Gilliard, "A Decentralized and Self-Adaptive Intrusion Detection Approach Using Continuous Learning and Blockchain Technology," *Journal of Data Science and Intelligent Systems*, vol. 9, no. 1, pp. 1–13, Jan. 2024.
- [8] A. Kumar, B. Sharma, and A. Noonaa, "Secure blockchain based intrusion detection for IoT networks," *Discover Computing*, vol. 6, no. 2, pp. 1–16, Oct. 2025.
- [9] S. Pandya, "Robust Blockchain and Artificial Intelligence-Based Efficient Techniques for Network Intrusion Detection System," in *Proc. Int. Conf. Integrated Circuits and Communication Systems (ICICACS)*, Feb. 2025, pp. 1–6.
- [10] G. Gurung, G. Bendiab, M. Shiale, and S. Shialeles, "CIDS: Collaborative Intrusion Detection System Using Blockchain Technology," in *Proc. IEEE Int. Conf. Cyber Security and Resilience (CSR)*, 2022, pp. 1–7.
- [11] R. Kumar, A. Aljuhani, D. Javeed, P. Kumar, S. Islam, and A. K. M. N. Islam, "Digital twins-enabled zero touch network: A smart contract and explainable AI integrated cybersecurity framework," *Future Generation Computer Systems*, vol. 156, pp. 1–14, Feb. 2024.
- [12] L. Alevizos and V. T. Ta, "Automated Cybersecurity Compliance and Threat Response Using AI, Blockchain & Smart Contracts," *arXiv preprint arXiv:2409.12345*, Sep. 2024.
- [13] A. Pereira, D. Paulin, and C. Hennebert, "Beyond Histotrust: A Blockchain-Based Alert in Case of Tampering with an Embedded Neural Network," *Applied System Innovation*, vol. 9, no. 1, pp. 1–12, Jan. 2026.
- [14] J. Chen, Z. Lu, H. Zheng, Z. Ren, Y. Chen, and J. Shang, "Data security storage and transmission framework for AI computing power platforms," *Scientific Reports*, vol. 16, pp. 1–14, Jan. 2026.
- [15] A. Deshmukh and K. Ravulakollu, "An Efficient CNN-Based Intrusion Detection System for IoT: Use Case Towards Cybersecurity," *Technologies*, vol. 12, no. 10, pp. 1–15, Oct. 2024.