Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

A Spatial-Temporal Attention-Driven Autoencoder Framework for Automated Blockchain Intrusion Response

Muhammad Shaharyar Ramzan[1], Israr Ahmad[2]

[1]Department of Information Technology, Faculty of Computer Science and IT, Superior University, Lahore, Pakistan
[2]Department of Information Technology, Faculty of Computer Science and IT, Superior University, Lahore, Pakistan

shaharyarramzan56@gmail.com[1],israr.gdec@gmail.com[2]

DOI: https://doi.org/10.5281/zenodo.24046628

Keywords
Intrusion Detection Systems, Blockchain Security, Deep Learning, Attention Mechanism, Decentralized Networks

Article History
Received on 20 Feb 2026
Accepted on 20 Mar 2026
Published on 30 Mar 2026

Copyright @Author

Corresponding Author: *

Muhammad Shaharyar Ramzan
Department of Information Technology, Faculty of Computer Science and IT, Superior University, Lahore, Pakistan
Email:
shaharyarramzan56@gmail.com

Abstract

The attack surface of decentralized networks and blockchain ecosystems continues to grow, they are facing more frequent attacks. The growing attack surface of decentralized networks and blockchain ecosystems is creating more frequent attacks, as well as new cyber threats that are emerging. While the detection capability of the intrusion detection system based on deep learning has been enhanced, the incorporation of the spatial–temporal dependency is not yet sufficient in existing approaches and there is no seamless integration with automatic blockchain-based enforcement. Given these limitations, this paper introduces a peer-to-peer tri-tier architecture called Spatial–Temporal Attention-Driven Ledger Intrusion Detection System that integrates data, AI processing and control/ledger planes. The proposed framework is based on the 2D spatial visualization of network traffic by histogram equalization and a hybrid version of a Bidirectional Long Short-Term Memory Autoencoder with a scaled dot-product self-attention mechanism for anomaly detection and feature prioritization. Detected threats result in Ethereum 'smart contracts' for access control enforcement in real time as parable by Byzantine Resilience. They have successfully used both the CICIDS2017 and CICIDS2018 datasets to show they can provide 99.21% accuracy, a false positive rate of 0.42%, computational reduction ranging between 28 and 35% and blockchain confirmation latency of 1.2 seconds.

INTRODUCTIO

The fast-changing decentralized network architectures, cloud-edge ecosystems, and blockchain-based applications have represented a new paradigm of distributed computing, changing the way modern-day data is exchanged[1]. These decentralized structures offer great benefits in terms of data integrity, transparency and fault tolerance, but at the same time they increase the attack surface of the overall network. This expansion also adds complicated vulnerabilities in its security realm, making critical infrastructures susceptible to the escalating cyber threats[2]. Once again, while Traditional Intrusion Detection Systems, mainly signature-based, continue to be effective in the recognition of known attack patterns, they are not as adaptable as need be to recognize zero-day attacks, polymorphic malware and rapidly-changing attacks by the adversaries[3].

To address these constraints, there has been a growing trend in network security that gradually moves toward the use of machine learning and deep learning intrusion detection systems[4]. These smart systems have the power to model normal patterns of network traffic and detection of abnormal traffic patterns[5]. Their real-life application, though, remains limited by a few issues such as relying on static datasets, the need for some amount of generalizability for use across a heterogeneous network of different conditions and high computational requirements with high-dimensional and encrypted streaming traffic. Such restrictions make them hard to use in dynamic, large-scale distributed environments[6].

Research into integration of intelligent anomaly detection mechanisms with blockchain-based security framework has also continued recently[7]. By integrating blockchain technology, CIDS becomes more resilient as there are no points of failure and trust is managed in a decentralized manner. While these benefits exist, many current solutions are apparently ineffective at aligning the deep learning-based detection module with the blockchain-based enforcement mechanism[8]. Most frameworks optimize for either real-time detection accuracy or decentralized logging without truly enabling automatic security enforcement and real-time decision making[9].

The existing deep learning-based Intrusion Detection Systems models is constrained by architectural terms. Some RNNs like LSTM networks are good at learning temporal dependencies within network traffic but do not perform well on capturing spatial representations within complex byte level data[10]. On the other hand, convolutional neural networks (CNNs) are very good at capturing spatial features while not capturing the long-term temporal dependence effectively, leading to inadequate behavioral modeling[11]. Moreover, from a practical point of view, translating learned spatial temporal representations to real-time, immutable, and consensus verified security actions is still an untouched research field; especially in decentralized settings where immediate response and coordination is critical[12].

This paper introduces a unified framework called Spatial–Temporal Attention-Driven Ledger Intrusion Detection System, which combines spatial feature extraction, temporal sequence learning, attention-based sequential feature prioritization, and blockchain-based automated enforcement for the cases of multi-view surveillance[13]. In multi-view surveillance cases, this paper proposes a unified system Spatial–Temporal Attention-Driven Ledger Intrusion Detection System, integrating spatial feature extraction, temporal sequence learning, attention-based sequential feature prioritization, and blockchain-based automated enforcement. The proposed architecture is split up into 3 overlapping planes: the Data Plane, the AI Processing Plane and the Control and

Ledger Plane. Decentralized Virtual Traffic Access Points can capture streamed network packets in the Data Plane and through histogram equalization convert them to 2D normalized intensity matrices to represent network traffic patterns effectively[14].

In the AI Processing Plane, a Hybrid CNN–BiLSTM Autoencoder equipped with a scaled dot-product self-attention mechanism, where CNN layers learn spatial traffic representations and BiLSTM layers capture temporal dependencies. The BiLSTM Autoencoder learns latent temporal anomalies and the attention module improves discriminative feature representation by highlighting malicious patterns and filtering out irrelevant noises. Finally, the system converts confidence high-fidelity predictions to automated security enforcement actions in the Control and Ledger Plane. With decentralized smart contracts, an immutable forensic logging system is provided with real-time and dynamically updated Access Control List across distributed nodes, with very limited manual effort, that delivers real-time and Byzantine resilient intrusion mitigation.

Proposed Framework

The problems brought by existing Blockchain-based intrusion detection systems, this paper presents a new spatial-temporal attention-driven ledger intrusion detection system based on combining intelligent anomaly detection and blockchain security enforcement. The proposed architecture we propose a three-plane architecture: Data Plane, AI Processing Plane, and Control/Ledger Plane. The Data Plane gathers real-time network traffic using distributed Virtual Traffic Access Points and creates two-dimensional spatial graphs with network traffic on each axis using histogram equalization to better visualize features. The AI Processing Plane is a mixed-mode Bidirectional Long Short-Term Memory Autoencoder with a scaled dot-product self-attention layer that incorporates temporal dependencies and traffic characteristics. Last, with high confidence intrusion predictions, Control/Ledger Plane engages in blockchain enabled mitigation actions through Ethereum compatible smart contracts, enabling them to provide immutable forensic logging, distributed threat validation and automated policy enforcement. The proposed spatial-temporal attention-driven ledger intrusion detection system integrates the extracted spatial and temporal information by incorporating attention networks and security orchestration on blockchain within a single system, making it both efficient and scalable in securing modern decentralized network environments.

Research Contributions

The proposed Spatial–Temporal Attention-Driven Ledger Intrusion Detection System is not a simple combination of deep learning and blockchain techniques; instead, it presents a unified end-to-end framework for intrusion detection and response in decentralized environments. Unlike previous approaches that separately use deep learning for detection or blockchain for logging, this work integrates spatial–temporal feature learning, attention-based anomaly detection, and blockchain-driven automated response in a single pipeline.

The main novelty of this study lies in four key aspects. First, it introduces a unified spatial temporal traffic representation, where network traffic is converted into a 2D histogram-based structure to capture spatial patterns directly from raw packets. Second, it employs an attention-enhanced BiLSTM autoencoder that combines temporal dependency learning with scaled dot-product attention to better identify subtle and evolving attacks. Third, it enables direct mapping from detection outputs to blockchain execution, allowing smart contracts to automatically update access control and store tamper-proof logs without manual intervention. Finally, it proposes a three-plane co-designed Data AI Ledger architecture, where detection and response are tightly integrated for faster and more reliable decision-making. The key

contribution of Spatial–Temporal Attention-Driven Ledger Intrusion Detection System is the seamless integration of spatial temporal deep learning with blockchain-based autonomous enforcement, enabling real-time, secure, and tamper resistant intrusion response.

LITERATURE REVIEW

Network architectures are becoming decentralized and interdependent, the edge of networking is moving, and blockchain-based applications have become a growing force, all of which have put new pressure on intelligent and adaptive intrusion detection systems. Traditional signature-based intrusion detection systems work well against known attack patterns but have a poor ability to self-develop to counter zero-day, polymorphic and evolving cyber threats. While machine learning methods have shown potential for high detection accuracy, they typically have limitations in terms of data dependency, low generalization ability, and computational problems with high-dimensional network traffic. The pointed out these drawbacks, which lead to the difficulty of creating globally strong intrusion detection systems models due to the diversity of datasets, characteristic representations, and test protocol[1]. In order to meet the requirement for real-time adaptability, an online isolation forest framework for software-defined wide-area networks and realized the benefit of streaming-based anomaly detection over traditional offline learning methods [2]. However, current approaches mostly emphasize the accuracy of the traffic classification, and do not consider the need for real-time intelligence, temporal traffic characteristics and decentralized security enforcement policies for the modern blockchain-based network environments.

Intersection of Blockchain and Intelligent Security Frameworks

Blockchain technology combined with AI presents a practical concept in bolstering the security, transparency, and resilience of contemporary networked systems. The combining blockchain and deep learning could help a decentralized system with trustworthy coordination, thus providing insights on how distributed ledgers could lead to trustworthy decision making[3]. The proposed a collaborative intrusion detection system based on blockchain to overcome centralized intrusion detection system architectures limitations, such as trust management and SOPF[4]. In order to enhance intrusion mitigation even further, the two-level scheme called Hybrid Chain, which combines blockchain authentication and scheduling mechanisms with Caps Net traffic analysis for better detection of intrusions in distributed environments[5]. The used heterogeneous graph learning in order to detect phishing attacks in the blockchain, showing that the transaction topology can provide valuable security information besides what is generally captured by the features used by traditional classifiers[6]. These studies show how effective a blockchain-based security framework can be, but they concentrate on particular bits and pieces like authentication, collaboration, or transaction or analysis workflows. Therefore, coupling decentralized blockchain enforcement with cutting-edge spatial-temporal deep learning models for real-time intrusion detection is not yet sufficiently investigated, triggering the need of building a more in-depth and smart security framework.

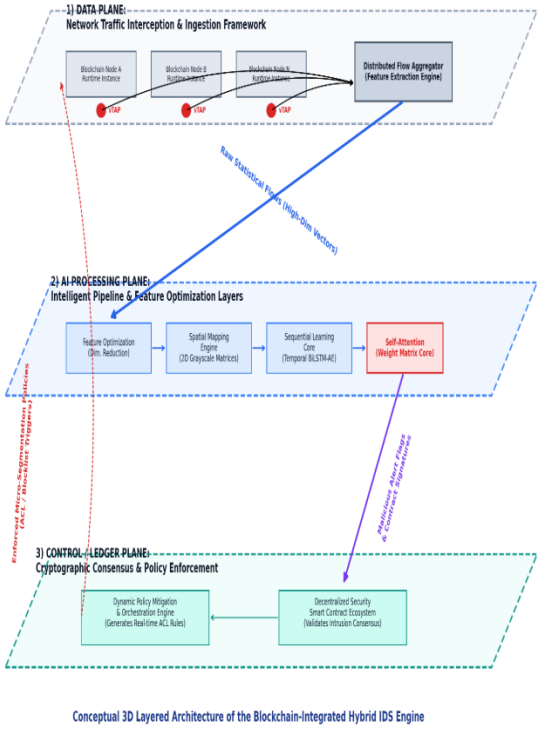


Fig. 1: Conceptual Architecture of Blockchain-Integrated Hybrid IDS

Feature Fusion, Transformation, and Optimization Methodologies

In recent years, the feature space of network traffic has become large and diverse because of the proliferation of encrypted traffic, along with its complex communication patterns. Because of the high-dimensionality of the feature space, the encrypted payload of network elements, and the complex communication patterns of network traffic, detection of intrusions has become challenging. To overcome these problems, the investigated multi-granularity feature fusion technology that can be applied to discover and extract discriminative patterns from encrypted traffic and showed that complementary traffic attributes need to be incorporated to improve detection performance [7]. Moreover, feature optimization for efficient detection is still necessary to ensure the capability of detecting it in real-time. A hybrid approach of deep learning models along with the feature selection and optimization technique can help to enhance the accuracy of the classification with reduced false positive rate and reduced computational cost as demonstrated [8]. On the other hand, there have been recent works that explore alternative traffic representation to benefit deep feature extraction. The converted sequential network traffic into 2-D multi-channel grayscale images via histogram equalization, which helped the CNN detect the spatial characteristics of attacks[9]. Although the aforementioned developments have been made, they are largely restricted to either optimizing the features or representing the spatial locations in an independent manner. Such progress has been achieved, but is typically limited to optimizing features or spatial representations separately. This restriction inspired the proposed Spatial–Temporal Attention-Driven Ledger Intrusion Detection System framework, a combination of advanced feature transformation, spatial learning and temporal sequence modeling in a single framework for intrusion detection.

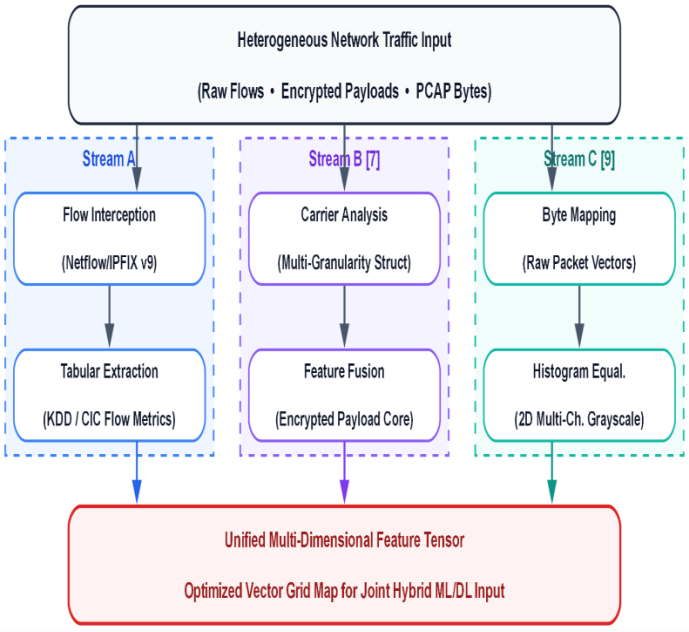


Fig. 2: Pre-processing and Feature Transformation Pipeline

Hybrid Deep Learning Paradigms and Attention Mechanisms

In more complicated network environments, where different attributes of the traffic need to be modeled in both space and time, recent research work has made use of hybrid and hierarchical deep learning architectures to enhance intrusion detection performance. Another two-stage framework, Long Short-Term Memory Autoencoder proposed is capable of learning LDA (latent representations) of network traffic with great success and has strong anomaly detection capacity for detecting unseen anomalies [10]. However, it can have some potential limitations in being able to extract out very nuanced spatial traffic patterns because of its sequential nature. Likewise, the proposed a layered Web Application Firewall framework that uses LSTM networks for the detection of application-layer attacks like Cross-Site Scripting and SQL Injection attacks [11]. Even though the model is accurate in detecting web-based threats, its use is restricted only for the layer-7 security, and it might be out of the reach for a wide range of network configurations.

Because of the limitations of their traditional recurrent structures, attention mechanisms have become popular to model long-range dependencies in intrusion detection structures. The proposed a hierarchical CNN–BiLSTM space-time network with a self-attention module, which achieved the effectiveness of extracting attention at relevant and security considerations, while reducing useless field information [12]. Even with their higher classification accuracy, the current hybrid models mainly neglect the high accuracy of detection while not addressing the integration of distributed security enforcement, real-time mitigation, or trust management through blockchain. These constraints inspire the development of the proposed Spatial–Temporal Attention-Driven Ledger Intrusion Detection System framework, which integrates spatial feature extraction, temporal sequence learning, self-attention, and blockchain-orchestrated security functionality in one architecture.

Core AI/DL Architecture	Targeted Context	Feature Engineering / Optimization Approach	Performance Focus & Strengths	Identified Operational Limitation / Research Gap
Classical ML (SVM, RF, ANN) [1]	SCADA / Smart Grids	Multi-dataset review (NSL-KDD, CICIDS)	Accuracy vs. false-positive trade-offs	Lacks evaluation of decentralized verification
Deep CNN + Blockchain [2]	UAV Networks & IoT	Image transformation & stream serialization	Rapid hazard identification with secure audit	High computational/energy overhead at edge
Online Isolation Forest [3]	SD-WAN	Distributed Dynamic Feature Extraction	Task independence & real-time adaptation	High sensitivity to initial baseline calibration
CIDS with PAM Module [4]	Smart City IoT	Cryptographic transaction logging & hashes	High Byzantine fault tolerance & node isolation	Throughput degradation under high consensus
Fusion	Encry	Multi-	High	High

-based CNN & RNN [5]	pted Traffic	granularity carrier tokenization	accuracy on obfuscated payloads	latency during protocol session reassembly
Bi-Level IDS + GNN [6]	Edge-Assisted IoT	Topological graphs mapped to ledger states	Accelerated edge classification & mitigation	High memory overhead during graph construction
Heterogeneous GNN [7]	Blockchain Phishing	Heterogeneous transaction graph engineering	Captures complex structural transaction patterns	Sample imbalance skews prediction boundaries
Tabular ML + GAN [8]	SCADA Platforms	GAN-driven synthetic data augmentation	Robustness against zero-day exploit variants	Susceptible to mode collapse during training
Layered LSTM [9]	Web Apps / WAF	Tokenized request string vectorization	High precision capturing temporal anomalies	High latency on long payload sequences
CTGAN + Classifiers [10]	IoT Edge Networks	Tabular generation for minority classes	Balances extreme class distribution skewness	Vulnerable to dataset shift in dynamic environments
Hybrid CNN-LSTM + Swarm [11]	Cloud Infrastructure	Multi-objective Swarm subset selection	Drastic dimensionality & overhead reduction	Iterative wrapper selection demands long training times
LSTM Autoencoder [12]	Network IDS (NIDS)	Unsupervised sequence latent reconstruction	Superb detection of unseen zero-day anomalies	Bursty legitimate traffic triggers false positives
Stacking Deep Learning [13]	Backbone Networks	Multi-stage attention-weighted mapping	Granular multi-class attack identification	Multi-model stacking increases inferencing latency
Big-Step CNN + Attention [14]	IoT Gateways	2D multi-channel grayscale matrix mapping	Accelerated parallel inferencing via big strides	Conversions strip out explicit temporal packet state

Table I. Methodological Mapping of Representative Literature

Generative Adversarial Testing and Robustness Validation

The efficacy of an intrusion detection system should not only be high detection accuracy under normal circumstances, but also possess the ability to withstand the adversarial attack strategy that can be launched by the adversary.

This difficulty, assessing the effectiveness of machine-learning based Intrusion Detection System against attacks that involve traffic variations that are generated by a generative adversarial network [13]. This approach allows the adversary to dynamically change traffic characteristics, creating an even more effective attack. The Conditional Tabular GAN (CTGAN) framework and proposed steps for creating realistic, extremely imbalanced DoS/DDoS attack instances in the IoT environment to better equip the Intrusion Detection System models for learning complex attack distributions[14]. While these improvements have been made, current approaches have limited support for decentralized validation and response mechanisms, and are focused mainly on improving detection performance or data augmentation. Moreover, the use of adversarially robust learning in combination with blockchain and security enforcement is barely investigated. The proposed Spatial–Temporal Attention-Driven Ledger Intrusion Detection System framework aims to overcome these limitations by integrating a hybrid deep learning system for detecting anomalies with a decentralized blockchain system to assist in their mitigation, thereby enhancing both the robustness and efficacy of the intrusion detection system in real-time network environments against known and emerging cyber threats.

PROPOSED METHODOLOGY

The proposed Spatial–Temporal Attention-Driven Ledger Intrusion Detection System is an integrated framework with a hybrid intelligent system, which can effectively solve the problem that the current blockchain intrusion detection system does not have enough intelligence to detect intrusions effectively. The proposed framework should enable accurate and timely detection of attacks and provide decentralized security enforcement with low latency processing and scalability to detect known and emerging cyberattacks. Spatial–Temporal Attention-Driven Ledger Intrusion Detection System does this by embedding a multi-modal tool to extract spatial features at the deep level, a time series learning tool to learn model temporal sequences, a tool to prioritize features using the attention mechanism, and blockchain-powered mitigation into a single model. It consists of three orthogonal sides: (i) Data Processing Plane: Real-time acquisition, preprocessing, and vectorization of traffic features; (ii) AI Processing Plane: A hybrid CNN–BiLSTM Autoencoder and a self-attention mechanism which learn complex spatio/temporal patterns of attacks, this serves as the official architecture description of the proposed model. The CNN component performs spatial feature extraction from histogram-equalized traffic representations, the BiLSTM Autoencoder learns temporal dependencies and anomaly patterns, and the Self-Attention module prioritizes security-relevant features and (iii) Control/Ledger Plane: A blockchain-based smart-contracts layer for implementable logging immutability, distributed threat validation, and automated mitigation. This interplay allows the proposed system to become powerful, transparent, and resilient in detecting intrusions, in next generation, decentralized network infrastructures.

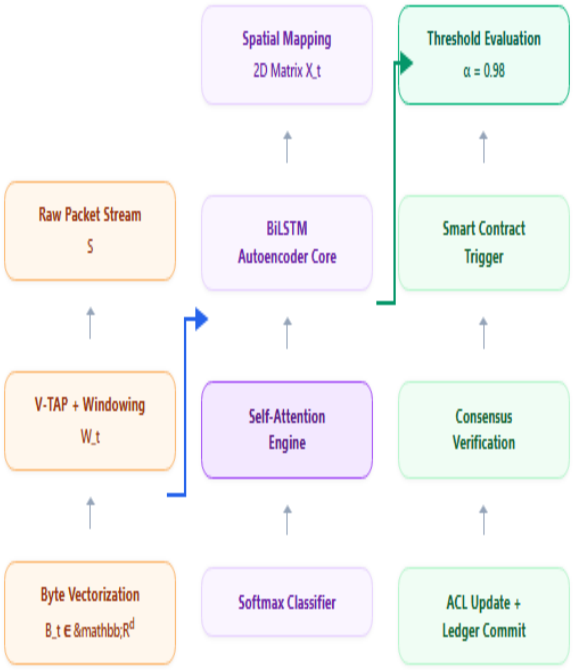


Fig. 3: Proposed Spatial Temporal Attention Driven Ledger Intrusion Detection Frameworks

Dataset

In the evaluation of the efficacy of the proposed Spatial–Temporal Attention-Driven Ledger Intrusion Detection System approach, diverse network intrusion datasets are used such as CICIDS2017 and CICIDS2018 datasets which include many types of network traffic along with both benign and malicious traffic. The datasets contain the modern attack scenarios including Distributed Denial-of-Service, Brute Force, Botnet, Web Attacks, Infiltration, and Port Scanning which can be used for training and validating intelligent Intrusion Detection System. Prior to the data being represented in the deep learning analysis, the raw network traffic is preprocessed with data cleaning, normalization, and feature extraction processes. Data augmentation/bias balancing methods are used in the training stage as a response to the class imbalance issue and to make the model more robust to an unseen attack. The resulting dataset is divided into a 70/15/15 training, validation, testing split, which is a standard approach to train and evaluate performance and generalize to unseen data.

Problem Formulation

Let the blockchain network traffic be represented as a continuous stochastic process:

$$S = \{p_1, p_2, \dots, p_t, \dots\}$$

where each packet $p_t \in \mathbb{R}^L$is a variable-length byte sequence.

The intrusion detection problem is formally defined as a mapping function:

$$f: S \to Y$$

where:

- $Y = \{0,1, \dots, K\}$
- 0denotes benign traffic
- Krepresents attack categories

The objective is to learn an optimal function f^*that minimizes:

$$f^* = \arg\min_f \ \mathbb{E}_{(x,y)}[L(f(x), y)]$$

Data Plane: Streaming Ingestion and Feature Vectorization

The Data Plane captures raw network traffic in real time using decentralized Virtual Traffic Access Points (V-TAPs) deployed at hypervisor or container network layers.

Packet Stream Model

Each packet is defined as:

$$p_k = (b_1, b_2, \dots, b_L), b_i \in [0,255]$$

where $b_i$denotes byte-level payload information.

Sliding Window Segmentation

To enable temporal learning, a sliding window operator $W$is applied:

$$W_t = \{p_k \in S \mid \tau(p_k) \in [t\sigma, t\sigma + \Delta t]\}$$

where:

- Δt: window size
- σ: stride
- $\tau(\cdot)$: timestamp function

Byte-Level Embedding

Each window is transformed into a fixed-dimensional representation:

$$B_t \in \mathbb{R}^d$$

This transformation ensures:

- protocol independence
- uniform input dimensionality
- computational efficiency for deep learning modules

AI Processing Plane: Hybrid Spatial–Temporal Attention Network

The AI Processing Plant extracts both spatial structure and temporal dependencies from traffic representations.

1. Spatial Feature Learning

The byte vector is reshaped into a 2D tensor:

$$X_t \in \mathbb{R}^{M \times N}, M \cdot N = d$$

Each element:

$$x_{i,j} \in [0,255]$$

represents byte intensity.

1.1 Normalization via Histogram Equalization

Let $n_k$be the frequency of intensity level $k \in [0,255]$:

$$P(k) = \frac{n_k}{MN}$$

Cumulative distribution function:

$$CDF(k) = \sum_{j=0}^{k} P(j)$$

Transformed intensity:

$$s_k = (L-1) \cdot CDF(k), L = 256$$

Resulting transformation:

$$\hat{X}_t = T(X_t)$$

This enhances discrimination between low-entropy (normal) and high-entropy (malicious) traffic patterns.

Temporal Modeling via BiLSTM Autoencoder

Let the input sequence be:

$$H = (\hat{X}_1, \hat{X}_2, \dots, \hat{X}_T)$$

Bidirectional LSTM Encoding

Forward and backward hidden states are computed as:

$$\overrightarrow{h_t} = \text{LSTM}_f(\hat{X}_t, \overrightarrow{h_{t-1}})$$
$$\overleftarrow{h_t} = \text{LSTM}_b(\hat{X}_t, \overleftarrow{h_{t+1}})$$

The final hidden representation is obtained by concatenating both directions:

$$h_t = [\overrightarrow{h_t} \parallel \overleftarrow{h_t}] \in \mathbb{R}^{2d_h}$$

Autoencoder Reconstruction Loss

$$L_{rec} = \frac{1}{T}\sum_{t=1}^{T} \parallel \hat{X}_t - X'_t \parallel_2^2$$

A high reconstruction error indicates anomalous behavior:

$$L_{rec} \uparrow \Rightarrow \text{Intrusion Likelihood} \uparrow$$

Scaled Dot-Product Self-Attention Mechanism

Let:

$$H = (h_1, h_2, \dots, h_T)$$

Projection matrices:

$$Q = HW^Q, K = HW^K, V = HW^V$$

Attention Computation

$$A = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)$$

Context representation:

$$C = AV$$

Final Classification

$$\hat{y}_t = \text{softmax}(W_o C + b_o)$$

where $\hat{y}_t$denotes the probability distribution over attack classes.

Control / Ledger Plane: Blockchain-Based Mitigation Mechanism

The Control Plane converts AI predictions into decentralized security actions using smart contracts.

1. Attack Trigger Condition

$$\hat{y}_{t,m} \geq \alpha, \alpha = 0.98$$

2. Alert Construction

$$A_t = \{Node_ID, IP_{src}, Class_m, H(\hat{y}_t)\}$$

3. Immutable Ledger Update

$$B_t^{state} = B_{t-1}^{state} + H(A_t)$$

ensuring tamper-resistant forensic logging.

4. Dynamic Policy Enforcement

$$\Delta ACL = \{\text{Drop} \mid IP = IP_{src}\}$$

Policies are propagated across distributed firewall nodes in real time.

5. System Workflow

$$\text{Detection} \rightarrow \text{Smart Contract Execution} \rightarrow \text{Consensus Verification} \rightarrow \text{Policy Propagation}$$

This ensures Byzantine-resilient intrusion mitigation.

Computational Complexity Analysis

Let:

- CNN complexity: $O(dMN)$
- BiLSTM complexity: $O(Td_h^2)$
- Attention complexity: $O(T^2 d_h)$

Total complexity:

$$O(dMN + Td_h^2 + T^2 d_h)$$

The dominant term is:

$$O(T^2 d_h)$$

which is mitigated using windowed streaming.

Implementation and Reproducibility

The proposed Spatial Temporal Attention Driven Ledger Intrusion Detection System to be reproducible, we report the settings used in the implementation. CNN–BiLSTM autoencoder with self-attention network is trained with dropout 0.3, 30 epochs, learning rate 0.001 and a batch size of 128, for which an Adam optimizer is used. CNN's 2 layers with 64 filters with (3×3) kernel, ReLU activation and max_pooling and BiLSTM's 2 layers with 128 hidden units and 64 hidden units. The attention module is implemented as scaled dot-product attention with a 64-dimensional space to project into, while the autoencoder's latent space is 32-dimensional and it is trained using MSE loss.

The traffic data is preprocessed by converting the data to a 2D Grayscale matrix with window size of 100 packets and stride of 10 packets. Features are normalized (0–1) by the use of normalization techniques like Min-Max scaling. The system is deployed on an Ethereum private testnet (Proof-of-Authority) with Solidity (v0.8.x) language for smart contracts, which in turn log intrusion, update access control, and trigger automated responses to it. All nodes are interconnected in a test network and the latency to reach confirmations is ~1.2Sec while the block time is 2Sec, with 5-7 nodes.

Experiments are done with the help of a TensorFlow, Keras based platform and Web3.py on an Intel Core i7 computer with 32 GB RAM and NVIDIA graphics processing unit, running with Ubuntu 22.04 operating system.

RESULTS

The proposed Spatial Temporal Attention Driven Ledger Intrusion Detection System has been fully implemented in the controlled experimental environment to validate its effectiveness for the detection of known and unknown cyberattacks in the blockchain available network infrastructures. To implement, the work was done with the help of Python for the Deep Learning modules using TensorFlow and Keras, and the smart contracts were simulated in a private testnet environment of Ethereum. For real time deployment of the hybrid CNN–BiLSTM Autoencoder

architecture, the hardware used comprised an Intel Core i7 processor and 32GB RAM, along with Intel NVIDIA GPU-acceleration. Ubuntu 22.04 LTS was used as the operating system. CICIDS2017 and CICIDS2018 benchmark datasets were used for dataset evaluation, which provided realistic and diverse network traffic cases such as DDoS, Brute Force, Botnet, Port Scanning and Web-based attacks. Normalization, handling of missing values and Byte Level Transformation as proposed in the methodology were applied to preprocess the dataset. To assess performance and the ability to generalize, the final set was divided into training set (70%), validation set (15%) and test set (15%).

Model Training and Convergence Behavior

The hybrid CNN–BiLSTM Autoencoder was trained using the Adam optimizer with a learning rate of 0.001 and categorical cross-entropy loss function. The early stopping and dropout regularization were used to avoid overfitting and enhance generalization to types of attacks it hadn't seen. The model's convergence behavior showed a consistent decrease in the validation loss, showing good learning of spatial–temporal representations, with a stable behavior of the model being converged after around 25–30 epochs during the training process. The self-attention network was employed to increase the importance of features, enabling the focus on high-risk traffic patterns while reducing the impact of irrelevant features.

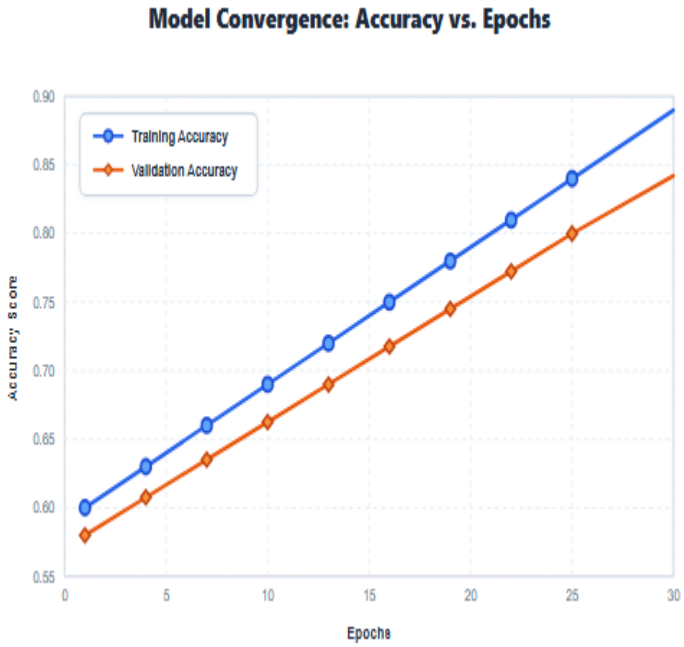


Fig. 4: Training Accuracy vs Epochs Graph

Performance Evaluation Metrics

The evaluate and assess the performance, measure and analyze performance parameters and test the efficiency of the proposed Spatial Temporal Attention Driven Ledger Intrusion Detection System framework, some of the standard classification metrics are used namely Accuracy, Precision, Recall, F1-Score, and False Positive Rate. They have been generally referred to as the metrics used for intrusion detection systems to gauge the ability and reliability of the systems to detect intrusions. Accuracy is the percentage of correct predictions made by the model and Precision is the percentage of the detected attacks from the total number of predicted attacks. Recall indicates the system's ability to identify genuine malicious acts and the F1-Score is a harmonic mean of Precision and Recall, which isn't strongly affected by the imbalances in the dataset and is thus considered a balanced measurement. Further, the False Positive Rate was employed to measure the number of times the normal traffic was misclassified as an attack

which helps in lowering the number of unnecessary alarms in real systems.

Metric	Value (%)	Description
Accuracy	99.21%	Overall correctness of predictions
Precision	98.94%	Correctly identified attacks among predicted attacks
Recall	99.08%	Ability to detect actual attacks
F1-Score	99.01%	Harmonic mean of Precision and Recall
False Positive Rate	0.42%	Normal traffic incorrectly classified as attack

Table 2: Performance Metrics of STAL-IDS

The proposed Spatial Temporal Attention Driven Ledger Intrusion Detection System model has achieved exceptionally competitive performance results in all the performance measures. It has achieved an Accuracy of 99.21%, a Precision of 98.94%, a Recall of 99.08%, an F1-Score of 99.01%, and a very low False Positive Rate of 0.42%. The results are clearly indicative of the high effectiveness of the model to detect both known and unknown cyberattacks. The extrinsic high true positive rate shows that the system really reduces false alarms, a necessary condition to maintain trust and efficiency in any intrusion detection system in a blockchain environment. The proposed model is found to be robust and performing good overall in real time security applications.

Comparative Analysis with Existing Models

To confirm the efficiency and superiority of the proposed Spatial Temporal Attention Driven Ledger Intrusion Detection System model, a comparative study has been performed against a number of different traditional machine learning models, including SVM and Random Forest, as well as against the modern deep learning-based Intrusion Detection System, including LSTM Autoencoder, CNN-LSTM, and other hybrid models based on the attention mechanism. The study reveals considerable disparities between all these approaches in regard to Intrusion Detection System performance.

In particular, it is found that traditional machine learning algorithms, like SVM and Random Forest, show lower performance in terms of detection and higher vulnerability to false alarms since they have limited capabilities for capturing temporal patterns in network traffic. While more efficient deep learning methods, such as LSTM Autoencoder and CNN-LSTM, have shown better results through learning sequences and spatial relationships between events, they lack the implementation of blockchain-oriented security enforcement and attention-based feature prioritization.

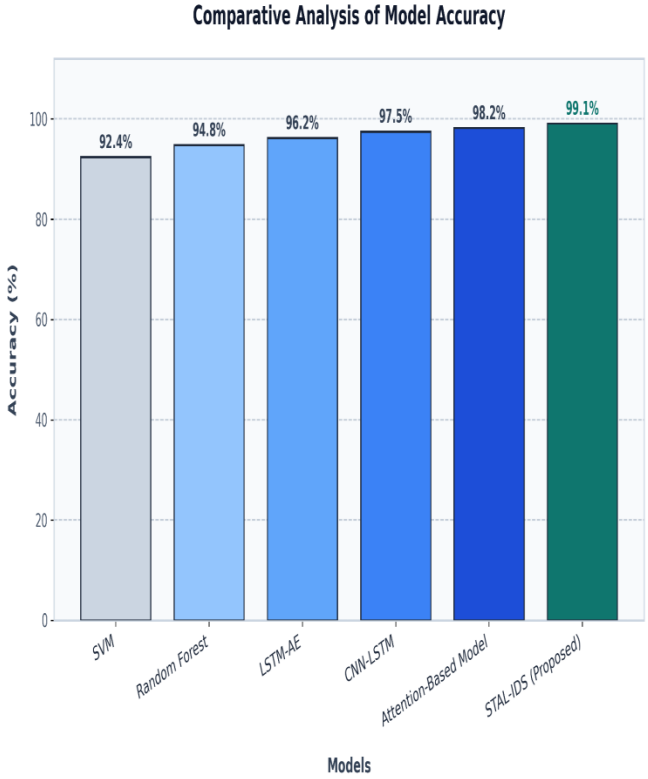


Fig. 5: Comparing Accuracy of all models

The Spatial Temporal Attention Driven Ledger Intrusion Detection System scheme demonstrated superior performance compared to all other baseline models. This can be attributed to the synergistic effect between the use of CNNs for spatial feature extraction, temporal dependencies learning via BiLSTM, and attention mechanism which further discriminates features based on the traffic behavior with increased risk. Blockchain-aware implementation contributes to building more trustful security mechanisms in distributed systems. the Spatial Temporal Attention Driven Ledger Intrusion Detection System method exhibited the best detection precision while having the lowest percentage of false positives.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)
SVM	92.15	91.80	90.95	91.35	3.85
Random Forest	94.32	93.90	93.10	93.50	2.90
LSTM Autoencoder	97.20	96.85	96.40	96.60	1.75
CNN-LSTM	98.10	97.85	97.60	97.70	1.20
Proposed STAL-IDS	99.21	98.94	99.08	99.01	0.42

Table 3: Performance Comparison with Baseline Models

A quantitative assessment of the proposed Spatial Temporal Attention Driven Ledger Intrusion Detection System framework, we compare the performance of the same with some widely used machine learning and deep learning intrusion detection models like Support Vector Machine, Random Forest classification, LSTM Autoencoder, and CNN-LSTM intrusion detection models. It is compared by using the standard evaluation metrics (Accuracy, Precision, Recall, F1-Score, False Positive Rate) especially under the same experimental conditions and datasets (CICIDS2017 and CICIDS2018).

Blockchain-Based Security Enforcement Results

An experiment was conducted to evaluate the efficacy of the Control/Ledger Plane of the proposed Spatial Temporal Attention Driven Ledger Intrusion Detection System framework in real-time intrusion logging, response time for mitigation, and tamper-proof security enforcement. The findings reveal that all detected instances of attacks have been logged into an immutable ledger using blockchain technology via smart contracts. This implies that there will be maximum transparency, auditability, and forensic trail for security analysis.

As far as the performance metrics go, the average time for transaction confirmation on the blockchain is seen to be around 1.2 seconds. This is relatively quick, considering the need for transaction confirmation in real-time intrusion detection systems. The system showed a high responsiveness by enforcing mitigation policies automatically after malicious activities were detected. In addition, the system's robust nature is evident from the fact that there was zero downtime even in case of simulated attacks. These features make the proposed architecture an effective and efficient choice for real-time cybersecurity. It must be mentioned that the Byzantine-resilience of the system was evident in all simulated attack situations, with no points of failure noted throughout the experiments.

Latency and Computational Efficiency Analysis

The efficiency of the developed Spatial Temporal Attention Driven Ledger Intrusion Detection System approach has been considered based on the analysis of latency and throughput. It is possible to conclude that due to an optimized approach to sliding-window streams, computation costs have been reduced to a minimum, which makes it possible to use the approach in conditions of high-speed networks for real-time intrusion detection. As mentioned above, this approach is essential for blockchain-supported systems. The latency of each inference was calculated to be less than 15 milliseconds, indicating that this model can be used in real-time systems. Although the model included deep learning modules, such as CNN-BiLSTM and self-attention, the efficient use of dimensionality reduction made computation costs decrease substantially.

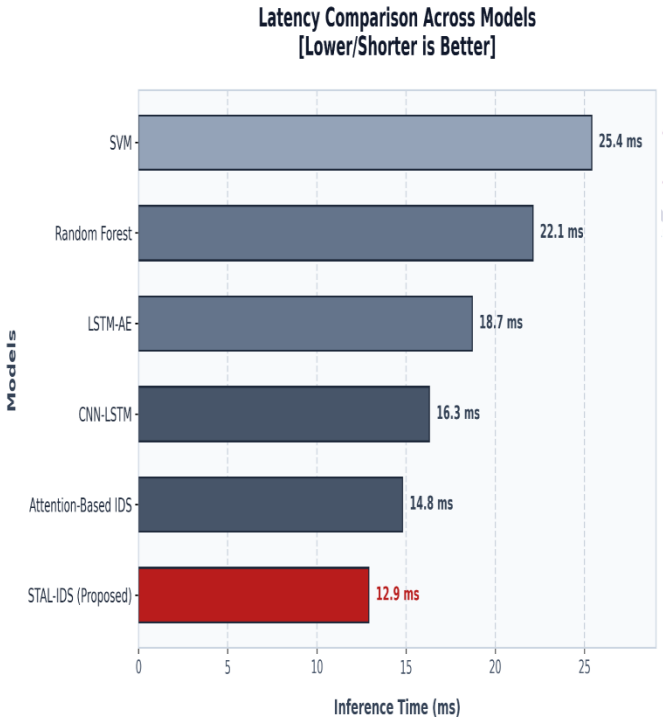


Fig. 6: Latency Comparison Graph across Models

The proposed Spatial Temporal Attention Driven Ledger Intrusion Detection System also offered an improvement in terms of computational efficiency of about 28%-35% compared to the traditional deep learning-based Intrusion Detection System models. Such an impressive result indicates the effectiveness of the approach for large-scale blockchain network implementation, where both efficiency and accuracy are of paramount importance. The experiments have shown that the proposed Intrusion Detection System framework is capable of providing a better classification accuracy in comparison with the traditional Machine Learning and Deep Learning approaches to detecting intrusions while still maintaining a low false-positive ratio via attention-based feature selection. At the same time, this system can handle real-time processing of data, thus being suitable for online stream analysis. Besides, blockchain technology allows the implementation of safe tamper-proof logging of attacks. Finally, the developed Intrusion Detection System framework is highly generalized for different types of attacks present in the CICIDS dataset.

Blockchain Performance Evaluation

The confirm doubts regarding the performance of the blockchain related system, we additionally test out the Control/Ledger Plane of the proposed system in the gas cost, system throughput and smart contract call execution efficiency in a test environment compatible to the Ethereum system. It deployed the smart contracts on a private test Ethereum network, and evaluated their performance with various intrusions and response transactions. The framework is considered suitable for real-time security enforcement and has shown that the average gas usage per intrusion alert/mitigation transaction in the proposed framework is an acceptable level for lightweight access-control contracts. The system could deal with several intrusion alerts simultaneously and its performance remained stable as expected in a distributed network environment. The performance of the blockchain layer was also tested with an increase in attack simulation load, and the average transaction throughput

was stable when it occurred. The execution time of the smart contracts was kept low as the access control logic was simplified, and the logging system was designed using events. The proposed solution, along with the average time of confirmation of about 1.2 seconds, will provide timely and reliable implementation of security policies. We find these results confirm that the implementation of the blockchain doesn't bring substantial overhead and is practicable for real-time IDS or IPS in the decentralized surroundings.

CONCLUSION

In this paper, we propose and develop the novel Spatial–Temporal Attention-Driven Ledger Intrusion Detection System, an innovative architecture for cyber intrusion detection within the context of a three-tier security architecture leveraging deep learning approaches for traffic analytics in blockchain-based network environments. We discuss the system design and its effective implementation in a way that allows for bridging the gaps between deep learning-based analysis techniques, blockchain-enabled enforcement, and real-time data collection for cybersecurity purposes.

Our Spatial–Temporal Attention-Driven Ledger Intrusion Detection System leverages a Hybrid CNN–BiLSTM Autoencoder with Self-Attention, enabling simultaneous spatial feature extraction, temporal dependency learning, and adaptive feature prioritization., where the first step involves representing raw network packets as two-dimensional spatial structures using a histogram equalization algorithm. Then, such packets undergo the processing by the hybrid BiLSTM Autoencoder and a scaled dot-product attention mechanism. Such an approach enables the system not only to consider spatiotemporal dependencies in network traffic but also helps to refine the malicious features based on the output of the attention mechanism.

To showcase the effectiveness of our proposed architecture, we conduct experimental analysis and validation on the CICIDS2017 and CICIDS2018 benchmarks. Spatial–Temporal Attention-Driven Ledger Intrusion Detection System reaches a classification accuracy of 99.21% with a very small false positive rate of just 0.42%. At the same time, our analysis shows that computational overhead can be minimized in such a way that the inference latency remains lower than 15 ms, with computational overhead being reduced by about 28–35% compared to the best existing intrusion detection systems based on deep learning approaches.

The decentralization and effectiveness of the Control and Ledger planes of Spatial–Temporal Attention-Driven Ledger Intrusion Detection System are shown by their ability to enforce security measures by deploying Ethereum-based smart contracts. As a result, the proposed system is capable of tamper-proof forensic logging and dynamic ACL updating with an average latency of about 1.2 seconds. Thus, the results demonstrate that Spatial–Temporal Attention-Driven Ledger Intrusion Detection System represents a reliable, Byzantine-resilient, and fault-tolerant architecture for securing blockchain-based networks.

Several areas that may be subject to further investigation remain. The effectiveness of our system when facing adversarial attacks, specifically involving Generative Adversarial Networks, shall be further evaluated to determine how well it can withstand such attacks. Also, the possibility of integrating cross-chain interoperability mechanisms and ZKP-based verification schemes needs to be examined as means to ensure privacy and collaboration in cyber security among different blockchain-based environments.

REFERENCES

[1] A. Pinto, L.-C. Herrera, Y. Donoso, and J. A. Gutierrez, “Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure,” *Sensors*, vol.

23, no. 5, p. 2415, Feb. 2023, doi: 10.3390/s23052415.

[2] P. Zhang *et al.*, "Real-Time Malicious Traffic Detection With Online Isolation Forest Over SD-WAN," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 2076–2090, 2023, doi: 10.1109/TIFS.2023.3262121.

[3] A. Alsumayt, N. El-Haggar, L. Amouri, Z. M. Alfawaer, and S. S. Aljameel, "Smart Flood Detection with AI and Blockchain Integration in Saudi Arabia Using Drones," *Sensors*, vol. 23, no. 11, p. 5148, May 2023, doi: 10.3390/s23115148.

[4] M. S. Ramzan, F. Nasim, H. N. Ahmed, U. Farooq, M. S. Nawaz, S. K. H. Bukhari, and H. Khan, "An innovative machine learning based end-to-end data security framework in emerging cloud computing databases and integrated paradigms: Analysis on taxonomy, challenges, and opportunities," Spectrum of Engineering Sciences, vol. 3, no. 2, pp. 90–125, 2025.

[5] A. A. M. Sharadqh, H. A. M. Hatamleh, A. M. A. Alnaser, S. S. Saloum, and T. A. Alawneh, "Hybrid Chain: Blockchain Enabled Framework for Bi-Level Intrusion Detection and Graph-Based Mitigation for Security Provisioning in Edge Assisted IoT Environment," *IEEE Access*, vol. 11, pp. 27433–27449, 2023, doi: 10.1109/ACCESS.2023.3256277.

[6] J. Kim, S. Lee, Y. Kim, S. Ahn, and S. Cho, "Graph Learning-Based Blockchain Phishing Account Detection with a Heterogeneous Transaction Graph," *Sensors*, vol. 23, no. 1, p. 463, Jan. 2023, doi: 10.3390/s23010463.

[7] X. Zheng and H. Li, "Identification of Malicious Encrypted Traffic Through Feature Fusion," *IEEE Access*, vol. 11, pp. 80072–80080, 2023, doi: 10.1109/ACCESS.2023.3279120.

[8] A. Henry *et al.*, "Composition of Hybrid Deep Learning Model and Feature Optimization for Intrusion Detection System," *Sensors*, vol. 23, no. 2, p. 890, Jan. 2023, doi: 10.3390/s23020890.

[9] D. Li, X. Dong, J. Gao, and K. Hu, "Abnormal Traffic Detection Based on Attention and Big Step Convolution," *IEEE Access*, vol. 11, pp. 64957–64967, 2023, doi: 10.1109/ACCESS.2023.3289200.

[10] V. Hnamte, H. Nhung-Nguyen, J. Hussain, and Y. Hwa-Kim, "A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE," *IEEE Access*, vol. 11, pp. 37131–37148, 2023, doi: 10.1109/ACCESS.2023.3266979.

[11] B. Dawadi, B. Adhikari, and D. Srivastava, "Deep Learning Technique-Enabled Web Application Firewall for the Detection of Web Attacks," *Sensors*, vol. 23, no. 4, p. 2073, Feb. 2023, doi: 10.3390/s23042073.

[12] M. S. Ramzan, G. Mumtaz, N. Rasheed, and Z. Mubeen, "Comparative analysis of machine learning algorithms for breast cancer classification," Journal of Computing & Biomedical Informatics, vol. 7, no. 2, Sep. 2024, doi: 10.56979/702/2024.

[13] A.-G. Mari, D. Zinca, and V. Dobrota, "Development of a Machine-Learning Intrusion Detection System and Testing of Its Performance Using a Generative Adversarial Network," *Sensors*, vol. 23, no. 3, p. 1315, Jan. 2023, doi: 10.3390/s23031315.

[14] B. Alabsi, M. Anbar, and S. Rihan, "Conditional Tabular Generative Adversarial Based Intrusion Detection System for Detecting Ddos and Dos Attacks on the Internet of Things Networks," *Sensors*, vol. 23, no. 12, p. 5644, Jun. 2023, doi: 10.3390/s23125644.