



BLOCKCHAIN-DRIVEN TRANSFORMER-BASED INTRUSION DETECTION AND ACCESS CONTROL SYSTEM (BDL-IDACS)

C. Ramya*¹, A. Suphalakshmi²

¹Research Scholar, Department of Computer Science and Engineering, Takshashila University, Ongur, Tindivanam, Villupuram (Dt), Tamilnadu, India.

¹Assistant Professor, Department of Information Technology, Mailam Engineering College, Mailam, Villupuram (Dt), Tamilnadu, India.

²Professor, Department of Computer Science and Engineering, Takshashila University, Ongur, Tindivanam, Villupuram (Dt), Tamilnadu, India.

¹<https://orcid.org/0009-0001-7860-7035>^{ID}, ²<https://orcid.org/0000-0001-6149-9878>^{ID}

Email: *ramyajitesh82@gmail.com, suphaprabhu@gmail.com

ARTICLE INFO

Article History

Received: February 10, 2026

Reviewed: June 6, 2026

Accepted: July 6, 2026

Published: July 31, 2026

Keywords:

Intrusion Detection System (IDS),
Blockchain-Assisted Security, Deep
Learning,

Attention Models, Fully
Homomorphic Encryption,
Smart Contracts,
Cyber Attack Detection,
Cloud-IoT Security.

ABSTRACT

The increasing complexity of cyber threats across IoT-cloud infrastructures necessitates the use of innovative, flexible, and confidentiality-preserving prevention techniques. The Blockchain-Assisted Hybrid Attention-Based Intrusion Detection and Access Control System (BHA-IDACS) is presented in this paper. The primary detection module employs an Adaptive Spatio-Temporal Representation Architecture-Self-Attention and Intersample Attention Transformer (Astra-SAINT) to precisely detect evolving intrusion tendencies. A heron optimization algorithm (HOA) is utilized for tuning the model thereby improving accuracy of detection and convergence. Fully Homomorphic Encryption (FHE) maintains the security of data and storage of encrypted data in unsecured cloud and blockchain circumstances. On a Consortium Blockchain, all encrypted transactions and audit trails are maintained by a Proof-of-Stake Authority (PoSA) consensus method. Additionally, based on user behavior and trust level, Smart Contract-Based Dynamic Access Control independently enforces permission and authentication regulations. The suggested model provides better precision, recall, F1-score, F2-score, specificity, and Cohen's Kappa values in addition to a mean accuracy of 99.16%. Furthermore, statistical analysis using confidence intervals and low standard deviation values demonstrates that Astra-SAINT is reliable and consistent across all validation folds. These results demonstrate the efficacy of the suggested Astra-SAINT framework as a scalable and dependable intrusion detection method for protecting IoT environments of the next decade.



Copyright ©2026 by authors and Galileo Institute of Technology and Education of the Amazon (ITEGAM). This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

I. INTRODUCTION

The coordination of limited resource-intensive IoT devices with cloud-based services has made ensuring security in IoT-cloud ecosystems a significant research challenge [1]. Since they are unable to adequately handle the adaptability, heterogeneity, and dynamic attack behaviors present in IoT networks, standard security solutions are typically inadequate [2]. Therefore, in order to detect advanced cyber threats in IoT cloud systems accurately and promptly, adaptive and data-driven security measures are becoming more and more necessary [3]. Due to their reliance on static rules, predetermined signatures, and centralized control structures, traditional IDS and access control systems are completely unsuitable for contemporary IoT scenarios [4]. These techniques are unable to deal with the dynamic nature of IoT traffic and are inadequate to recognize novel or evolving attack patterns. Furthermore, centralized security architectures' low scalability and single points of failure severely restrict their effectiveness in massive implementations [5]. As a result, scalable, intelligent, and adaptive security systems that are resistant to possible threats and capable of learning intricate traffic patterns are becoming more and more necessary [6]. The potential of deep learning (DL) powered IDS to identify and extract high-level information from huge volumes of network traffic data has received a lot of interest [7]. While recurrent and convolutional neural network-based models have shown promising outcomes, they often fail to grasp the intricate feature interactions and long-term temporal correlations present in Internet of Things traffic [8]. More recently, it has been shown that transformer and attention-based designs are better at simulating global contextual relationships [9]. Despite these developments, a significant research problem is still obtaining dependable detection performance in the face of extremely unbalanced data, changing attack techniques, and real-time restrictions.

IoT-cloud infrastructures must guarantee data privacy, integrity, and trust management in addition to detection accuracy [10], [11]. Sensitive information is frequently included in IoT data, and traditional encryption methods necessitate data decryption before analysis, raising the possibility of data leakage in untrusted environments. Furthermore, because user behavior and trust levels are constantly changing in IoT systems, static access control solutions are inadequate [12]. Blockchain and other decentralized technologies have shown promise as safe data management and auditability solutions; nevertheless, it is still unclear how to effectively integrate them with intelligent security methods while maintaining scalability and privacy [13]. Inspired by these difficulties, this work investigates intelligent intrusion detection, privacy-preserving processing of information, decentralized trust management, and dynamic access control within one integrated structure in order to address the shortcomings of current IoT security solutions. The ultimate goal is to ensure safe and scalable operation in next-generation IoT-cloud systems while improving detection accuracy, reliability, and consistency.

1.1 MAJOR CONTRIBUTION

- To assure reliable, secure, and scalable IoT-cloud security, a novel Blockchain-Assisted Hybrid Attention-Based Intrusion Detection and Access Control System (BHA-IDACS) is proposed.
- An advanced Astra-SAINT is developed to capture intricate temporal traffic patterns and inter-feature correlations in order to accurately identify new IoT attacks.
- FHE enables safe analysis of encrypted IoT data, while a Consortium Blockchain with PoSA consensus guarantees data integrity, auditability, and scalability.
- Throughout validation folds, standard deviation analysis and confidence intervals are used in the study's comprehensive statistical evaluation. The Astra-SAINT model's narrow confidence range and low variation demonstrate its stability, dependability, and generalizability.

Section 2 provides the related work, section 3 defines the proposed methodology framework, section 4 defines the result and discussion and section 5 ends with conclusion and future scope.

II. RELATED WORK

In order to improve IDS in IoT and cyber-physical contexts, a lot of research has been done recently on combining blockchain technology with deep learning (DL) methods. The major goals of these investigations are to promote decentralized security monitoring, preserve data integrity, and improve detection performance. While blockchain technology is used to guarantee safe, tamper-resistant data storage and ongoing verification, a variety of deep learning architectures, including convolutional neural networks (CNNs), recurrent neural networks (RNNs), bidirectional long short-term memory (BiLSTM) networks, and attention-based transformer models, have been used to successfully capture complex network traffic characteristics. However, issues with scalability, adaptation to new attack patterns, privacy protection, and computing complexity still hamper current systems. A comparative analysis of representative studies is given in Table 1, which summarizes their goals, main contributions, benefits, and drawbacks.

Table 1: Comparative Analysis of Blockchain-Enabled IDS models.

Reference	Methods Used	Goal	Key Contributions	Merits	Demerits
Saravanan et al. (2024) [14]	Blockchain + Optimized RNN	Secure IoT intrusion detection	Introduced an optimized RNN integrated with blockchain for attack detection	Improved detection accuracy and secure data logging	Limited handling of complex spatio-temporal dependencies
Aljabri et al. (2024) [15]	CNN + Blockchain	Network intrusion detection	Combined CNN-based feature learning with blockchain for integrity	Efficient feature extraction and decentralized storage	CNN struggles with long-term temporal patterns
Mansour (2022) [16]	AI Optimization + Deep Learning + Blockchain	CPS intrusion detection	Applied AI-based optimization to enhance deep learning IDS performance	High accuracy and blockchain-backed trust	High computational cost and limited privacy discussion
Saveetha & Maragatham (2022) [17]	Deep Learning + Blockchain	IoT attack detection	Designed a blockchain-enabled deep learning IDS framework	Secure and reliable attack detection	Static access control and lack of adaptability
Mbaya et al. (2023) [18]	Federated Learning + BiLSTM + Blockchain	Privacy-aware distributed IDS	Proposed a federated IDS with blockchain and BiLSTM	Preserves data privacy and supports distributed learning	Communication overhead and model convergence complexity
Alkhonaini et al. (2025) [19]	Sandpiper Optimization + Hybrid DL + Blockchain	IoT intrusion detection	Used Sandpiper optimization to tune hybrid DL models	Enhanced accuracy and optimized learning	Increased training complexity and resource demand
Ali et al. (2025) [20]	Blockchain Encryption + Optimized Attention Transformer	Secure medical IoT IDS	Developed an attention-based adversarial transformer with blockchain	Strong privacy preservation and high detection accuracy	Domain-specific design and higher computational overhead

Source: Authors, (2026).

Even though previous research shows how well DL and blockchain work together for intrusion detection, there are still a number of obvious drawbacks. A number of current approaches rely on single-level feature representations, which limits their capacity to describe the intricate inter-sample correlations and spatiotemporal relationships prevalent in IoT network data. While optimization techniques can improve detection speed, they often result in significant processing cost, which restricts scalability and makes real-time implementation difficult. Furthermore, many blockchain-based solutions fall short in meeting the needs for dynamic access control and privacy-preserving processes, even while they offer data integrity and traceability. These difficulties highlight the necessity for more advanced attention-based, blockchain-enabled IDS and highlight the significance of an overall structure that can concurrently achieve high detection accuracy with realistic deployment efficiency.

III. PROPOSED METHODOLOGY

The RT-IoT2022 dataset is used by the proposed Blockchain-Driven Transformer-Based Intrusion Detection and Access Control System (BDL-IDACS) and it is shown in Figure 1. This dataset comprises real-time IoT network traffic that includes both hostile and benign activities, such as different cyberattacks. To produce high-quality representations of IoT traffic flows, the dataset first undergoes through extensive preprocessing, which includes removing noise and outliers, imputing missing values, normalizing features, and removing redundant properties. The Astra-SAINT transformer model uses self-attention, intersample attention, and spatiotemporal learning and the Heron optimization algorithm is used to tune the hyperparameters of the model to improve detection performance and convergence efficiency. Fully Homomorphic Encryption (FHE) is used to safeguard IoT traffic features and detection results in order to guarantee data privacy. The consortium blockchain, which is controlled by a Proof-of-Stake Authority consensus method, then stores all encrypted records, forecasts, and access logs. Lastly, smart contract-based dynamic access control provides a privacy-preserving security framework for IoT-cloud infrastructures by autonomously enforcing authentication and authorization decisions based on user behavior and trust level while producing real-time alerts for detected intrusions.

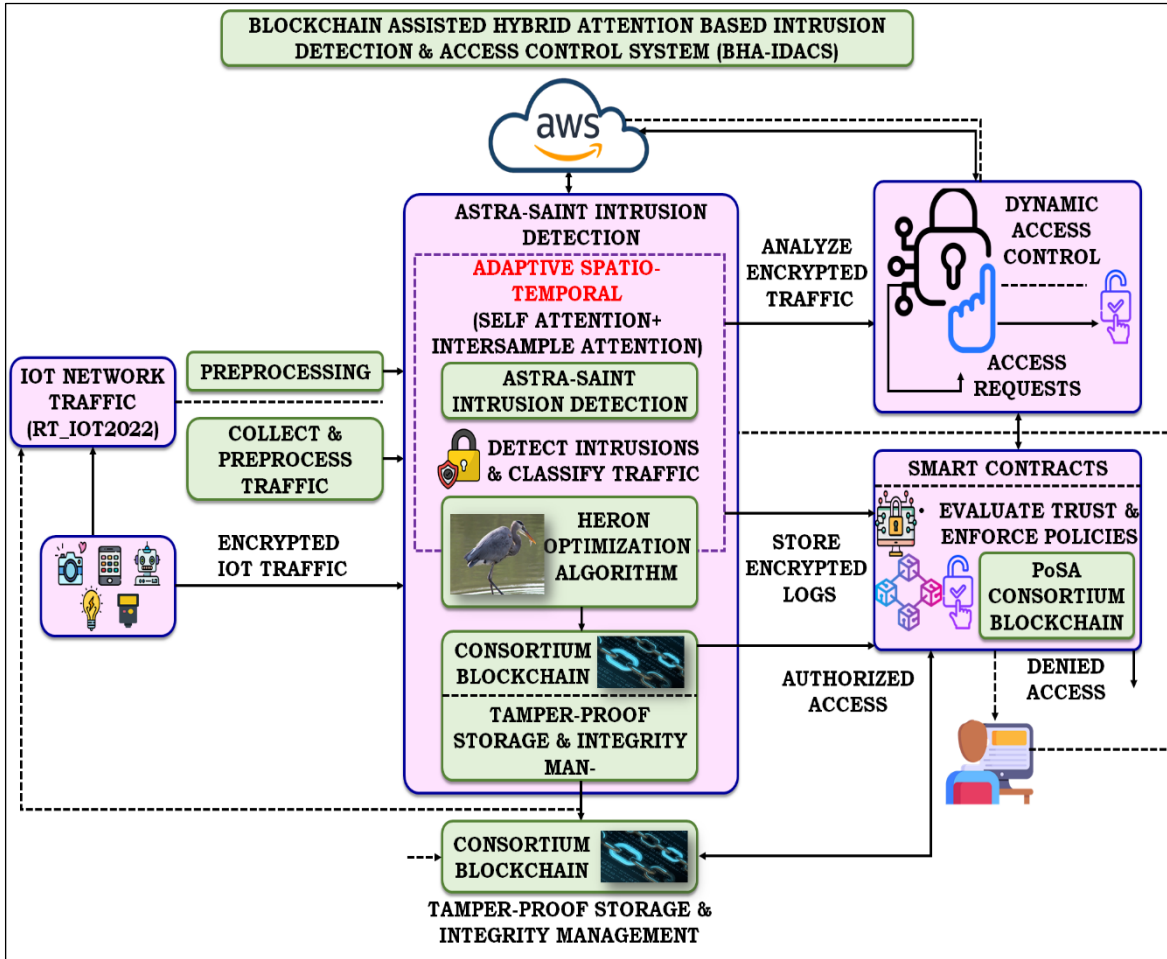


Figure 1: Overall proposed framework.
Source: Authors, (2026).

III.1 STAGE I: RT-IOT2022 DATA ACQUISITION AND PREPROCESSING

The collection and preparation of IoT network traffic obtained from the RT-IoT2022 dataset constitute the first phase of the proposed BDL-IDACS system. Let's use a multivariate feature matrix to convey the dataset:

$$X = \{x_{i,j}\} \in \mathbb{R}^{N \times D} \quad (1)$$

Where D is the number of retrieved traffic features and N is the total number of network flow instances. Every instance is associated with a real-time IoT communication record that has been classified as either normal or falling under a certain threat category. Direct use of the raw dataset might seriously impair learning performance due to the heterogeneous nature of IoT traffic as well as the existence of noise, missing values, and skewed feature distributions. In order to solve this problem, aberrant data that substantially differ from typical traffic behavior are first eliminated by outlier detection. The standardized score (z-score) of an instance i is calculated for a given feature j as:

$$z_{i,j} = \frac{x_{i,j} - \mu_j}{\sigma_j} \quad (2)$$

Where μ_j and σ_j stand for the j^{th} feature's mean and standard deviation, respectively. When τ is a predetermined threshold and which satisfy $|z_{i,j}| > \tau$ are considered outliers and eliminated from further examination. In order to maintain data accuracy, missing values in the dataset are filled by employing statistical imputation after outlier removal. Mean-based imputation is used for each missing feature value $x_{i,j}^{miss}$ as:

$$x_{i,j}^{miss} = \frac{1}{N_j} \sum_{i=1}^{N_j} x_{i,j} \quad (3)$$

Where the number of non-missing observations for feature j is represented by N_j . Feature normalization is then carried out to prevent high-magnitude features from dominating during model training and to guarantee consistent scaling across all traffic attributes. The use of min-max normalization is described as:

$$\hat{x}_{i,j} = \frac{x_{i,j} - \min(x_j)}{\max(x_j) - \min(x_j)} \quad (4)$$

where $\min(x_j)$ and $\max(x_j)$ represent the j^{th} feature's minimum and maximum values, respectively. All feature values are mapped into the interval $[0, 1]$ via this transformation.

To find replicated or poorly informative features, correlation analysis and exploratory data analysis are also carried out. A reduced feature matrix is produced by eliminating highly correlated characteristics in order to minimize multicollinearity and reduce dimensionality.

$$X' \in \mathbb{R}^{N \times d}, d < D \quad (5)$$

The raw RT-IoT2022 traffic data is converted into a structured, noise-reduced, and normalized representation by various preprocessing steps, maintaining important IoT communications behavioral traits. In order to effectively understand spatiotemporal attack patterns, this revised dataset provides a solid basis for later transformer-based intrusion detection.

III.2 STAGE II: ASTRA-SAINT TRANSFORMER WITH ADAPTIVE SPATIO-TEMPORAL REPRESENTATION

III.2.1 Input Embedding and Temporal Encoding

IoT network traffic statistics show substantial temporal relationships and varied feature distributions as the consequence of constantly changing attack and communication patterns. Astra-SAINT starts by extending each preprocessed traffic instance into a dense latent space that facilitates attention-based learning in order to guarantee that such complicated properties are efficiently captured. Let $\mathbf{x}_{t,i} \in \mathbb{R}^d$ represent the i^{th} traffic incident detected at time index t . An embedding vector is mapped to this instance via a learnable embedding function $E(\cdot)$ and its mathematical expression is given below:

$$\mathbf{e}_{t,i} = E(\mathbf{x}_{t,i}) \quad (6)$$

Here, $\mathbf{e}_{t,i} \in \mathbb{R}^{d_e}$ defines the embedded representation and d_e describes the embedding dimension respectively. Temporal ordering must be maintained since intrusion patterns frequently appear as progressive departures over time. This is accomplished by adding a temporal positional encoding vector, $\mathbf{p}_t \in \mathbb{R}^{d_e}$ to the embedded input and its expression is given below:

$$\tilde{\mathbf{e}}_{t,i} = \mathbf{e}_{t,i} + \mathbf{p}_t \quad (7)$$

In this formulation, the relative temporal position of the traffic instance within the traffic stream is encoded by $\mathbf{p}_t$, and the time-aware embedding is represented by $\tilde{\mathbf{e}}_{t,i}$. Because of this temporal enrichment, the model can distinguish between identical traffic patterns that happen at different times.

III.2.2 Adaptive Spatio-Temporal Representation Learning

Not all temporal and spatial variables are equally important for intrusion detection, even when temporal encoding maintains ordering. While certain attributes could be superfluous or noisy, others might have powerful attack signatures. Astra-SAINT introduces an adaptive spatio-temporal gating system that dynamically controls feature relevance in order to rectify this imbalance. This method calculates a gating vector and its expression is given below:

$$\mathbf{g}_{t,i} = \sigma(\mathbf{W}_g \tilde{\mathbf{e}}_{t,i} + \mathbf{b}_g) \quad (8)$$

Where $\mathbf{W}_g$ and $\mathbf{b}_g$ specifies the learnable parameters, and $\sigma(\cdot)$ denotes the sigmoid activation function. Next, element-wise modulation yields the gated spatio-temporal representation and it is given below:

$$\mathbf{z}_{t,i} = \mathbf{g}_{t,i} \odot \tilde{\mathbf{e}}_{t,i} \quad (9)$$

In this case, element-wise multiplication is represented by $\odot$ and the adaptively weighted spatiotemporal embedding is denoted by $\mathbf{z}_{t,i}$. By reducing irrelevant variations and selectively amplifying informative aspects linked to anomalous traffic behavior, this technique improves robustness against malicious and changing intruders.

III.2.3 Self-Attention for Spatial Feature Dependency Modeling

A multi-head self-attention system then processes the gated embeddings to identify spatial correlations between characteristics in each traffic occurrence. For tabular IoT data, self-attention allows the model to establish correlations between traffic aspects rather than depending on predefined locality assumptions. The query, key, and value vectors are calculated for every $\mathbf{z}_{t,i}$ and it is defined below:

$$\mathbf{Q}_{t,i} = \mathbf{W}_Q \mathbf{z}_{t,i}, \quad \mathbf{K}_{t,i} = \mathbf{W}_K \mathbf{z}_{t,i}, \quad \mathbf{V}_{t,i} = \mathbf{W}_V \mathbf{z}_{t,i} \quad (10)$$

The learnable projection matrices are stated as $\mathbf{W}_Q, \mathbf{W}_K, \mathbf{W}_V$ and d_k represents the dimensionality of the key and query vectors. Scaled dot-product attention is used to calculate the self-attention output and it is defined below:

$$\text{SA}(\mathbf{z}_{t,i}) = \text{softmax} \left(\frac{\mathbf{Q}_{t,i} \mathbf{K}_{t,i}^T}{\sqrt{d_k}} \right) \mathbf{V}_{t,i} \quad (11)$$

In this case, the self-attention function is denoted by $\text{SA}(\cdot)$, and the gradient magnitude is stabilized throughout training by the scaling factor $\sqrt{d_k}$. Layer normalization and residual connections are used to maintain information flow and enhance optimization stability:

$$\mathbf{h}_{t,i}^{(1)} = \text{LayerNorm}(\mathbf{z}_{t,i} + \text{SA}(\mathbf{z}_{t,i})) \quad (12)$$

A position-wise feed-forward network is used to further improve the obtained representation:

$$\mathbf{h}_{t,i}^{(SA)} = \text{LayerNorm}(\mathbf{h}_{t,i}^{(1)} + \text{FFN}(\mathbf{h}_{t,i}^{(1)})) \quad (13)$$

Here, $\text{FFN}(\cdot)$ signifies a two-layer feed-forward network with nonlinear activation, and $\mathbf{h}_{t,i}^{(SA)}$ denotes the spatially enriched representation.

III.2.4 Intersample Attention for Contextual and Temporal Dependency Modeling

Intrusion behavior in IoT networks frequently results from correlations across various traffic flows, even while self-attention captures feature-level interactions. Astra-SAINT uses an intersample attention mechanism that functions across traffic instances within the same temporal window in order to describe such contextual dependencies. Let $\mathbf{H}_t = [\mathbf{h}_{t,1}^{(SA)}, \mathbf{h}_{t,2}^{(SA)}, \dots, \mathbf{h}_{t,b}^{(SA)}]$ defines the batch level feature matrix. Here, b describes the batch size. Therefore, the mathematical computation of intersample attention is defined using below equation:

$$\text{IA}(\mathbf{H}_t) = \text{softmax} \left(\frac{\mathbf{Q}_t \mathbf{K}_t^T}{\sqrt{d_k}} \right) \mathbf{V}_t \quad (14)$$

Here, $\mathbf{Q}_t = \mathbf{W}_Q^{(I)} \mathbf{H}_t$, $\mathbf{K}_t = \mathbf{W}_K^{(I)} \mathbf{H}_t$, and $\mathbf{V}_t = \mathbf{W}_V^{(I)} \mathbf{H}_t$. The intersample projection matrices are stated as $\mathbf{W}_Q^{(I)}, \mathbf{W}_K^{(I)}, \mathbf{W}_V^{(I)}$ respectively. With the aid of residual normalization, the output of intersample is integrated and its mathematical formulation is given below. Alos, it is followed by feed-forward refinement.

$$\mathbf{h}_{t,i}^{(2)} = \text{LayerNorm}(\mathbf{h}_{t,i}^{(SA)} + \text{IA}(\mathbf{H}_t)_i) \quad (15)$$

$$\mathbf{r}_{t,i} = \text{LayerNorm}(\mathbf{h}_{t,i}^{(2)} + \text{FFN}(\mathbf{h}_{t,i}^{(2)})) \quad (16)$$

The ultimate contextual representation of the i^{th} traffic instance is denoted by $\mathbf{r}_{t,i}$ which incorporates both feature-level and inter-flow dependencies.

III.2.5 Contextual Spatio-Temporal Representation Output

The model gradually improves traffic representations by stacking L_X Astra-SAINT layers, enabling the capturing of higher-order spatiotemporal interactions. The expression for the total Astra-SAINT transition is given below:

$$\{\mathbf{r}_{t,i}\}_{i=1}^b = S(\{E(\mathbf{x}_{t,i})\}_{i=1}^b), \quad (17)$$

Where the composite Astra-SAINT mapping is shown by $S(\cdot)$. Under dynamic network conditions, these contextualized representations enable precise discrimination between benign and malicious IoT data by serving as the foundation for further intrusion categorization.

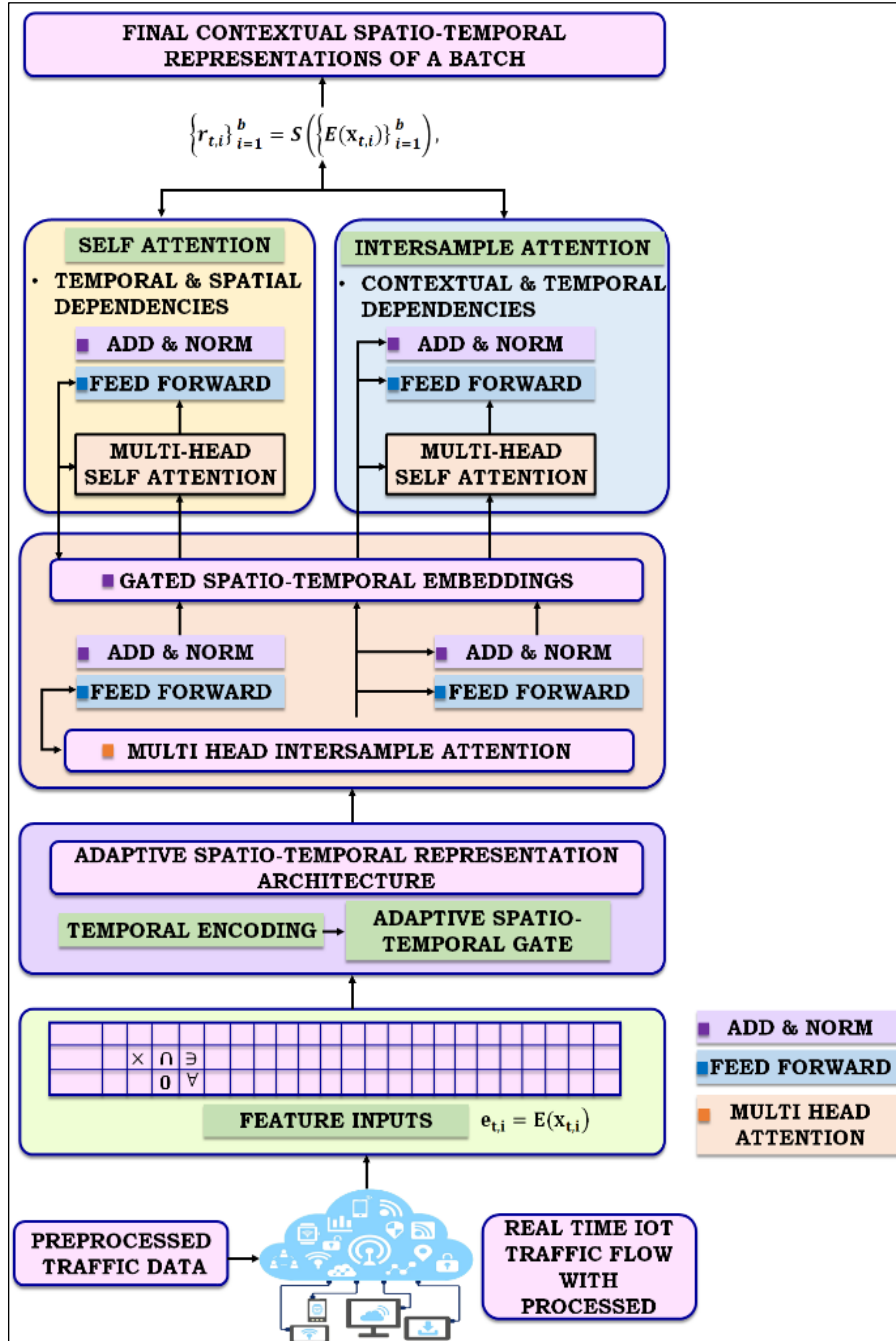


Figure 2: Architecture of Astra-SAINT Transformer.
Source: Authors, (2026).

The block-wise architecture of the suggested Astra-SAINT model is shown in Figure 2. A batch of embedded IoT traffic samples that have undergone preprocessing and feature embedding are fed into the architecture. The Astra processes these embedded inputs first. It uses temporal encoding to maintain linear dependencies and an adaptive spatio-temporal gating mechanism to dynamically highlight important temporal and spatial features of network traffic. The stacked Astra-SAINT encoder layers consisting of two complimentary attention blocks and receive the corrected embeddings. The self-attention block captures intra-sample dependencies and makes it possible to extract discriminative spatial and temporal feature interactions. In order to recognize integrated and spread attack behaviors frequently seen in IoT environments, the intersample attention block simultaneously acts across samples within the same batch to learn contextual correlations among data flows. The learnt representations are gradually enhanced by regularly stacking this self-attention and intersample attention modules. The architecture's ultimate output is a collection of contextualized spatio-temporal representations for the batch, which are used for precise intrusion classification.

III.3 STAGE III: HERON OPTIMIZATION-BASED MODEL PARAMETER TUNING

While adaptive spatiotemporal dependability and contextual relationships in IoT traffic are efficiently captured by the Astra-SAINT architecture, its ability to perform is highly dependent on the ideal configuration of model parameters, such as regularization coefficients, learning rates, and attention weights. Conventional gradient-based optimization may prematurely converge to inadequate solutions because of the dynamic nature of intrusion data and the nonconvex nature of deep transformer loss landscapes.

The suggested framework incorporates a nature-inspired Heron Optimization Algorithm (HOA) to improve convergence stability and detection accuracy in order to get over this limitation.

III.3.1 Solution Representation and Fitness Evaluation

A collection of trainable Astra-SAINT parameters and hyperparameters is represented by each potential solution in the heron population. Therefore, the initialization process is defined below:

$$\theta_k = \{\theta_{k,1}, \theta_{k,2}, \dots, \theta_{k,n}\} \quad (18)$$

Here, k^{th} defines the candidate parameter vector and n defines the total number of selected parameters for optimization. A fitness function generated from the intrusion detection objective is used to assess the quality of each potential solution:

$$\mathcal{F}(\theta_k) = \alpha \cdot \mathcal{L}_{\text{cls}} + \beta \cdot \text{FPR} \quad (19)$$

Here, the classification loss of the network model is stated as $\mathcal{L}_{\text{cls}}$, false positive rate is defined as FPR, the weighting coefficients are stated as α, β . The optimizer is encouraged by this formulation to reduce both redundant security alarms and misclassification.

III.3.2 Heron-Inspired Position Update Mechanism

Heron's search behavior is demonstrated by adaptive positional updates that are impacted by both environmental exploration and the current best solution. As a result, each potential solution's position is updated as

$$\theta_k^{(t+1)} = \theta_k^{(t)} + \lambda_1 \cdot r_1 \cdot (\theta_{\text{best}} - \theta_k^{(t)}) + \lambda_2 \cdot r_2 \cdot (\theta_{\text{rand}} - \theta_k^{(t)}) \quad (20)$$

At iteration t , the parameter vector is stated as $\theta_k^{(t)}$, the best solution is defined as θ_{best} , the randomly selected candidate solution is stated as θ_{rand} , $r_1, r_2 \in (0,1)$ specifies the random vectors, λ_1, λ_2 control exploitation and exploration consecutively.

III.3.3 Integration with Astra-SAINT Training

By periodically adjusting certain parameters depending on fitness feedback, the heron optimization mechanism works in combination with Astra-SAINT training. Upon the satisfaction of the termination condition, the optimized parameter set is defined below:

$$\theta^* = \arg \min_{\theta_k} \mathcal{F}(\theta_k) \quad (21)$$

By including Heron optimization, the model achieves improved convergence behavior, fewer false alarms, and greater generalization across different IoT attack scenarios.

III.4 STAGE IV: BLOCKCHAIN-ASSISTED PRIVACY PRESERVATION AND SMART CONTRACT-BASED DYNAMIC ACCESS CONTROL

After using Heron optimization to optimize the Astra-SAINT model parameters, the IDS produces precise and extremely reliable predictions on the behavior of IoT networks. However, in actual IoT-cloud systems, merely detecting intrusions is insufficient. To allay these worries, the proposed solution includes a blockchain-assisted security layer, autonomous access control, and privacy-preserving encryption.

III.4.1 Fully Homomorphic Encryption for End-to-End Data Confidentiality

Sensitive information is encrypted using FHE before being stored or transmitted across the IoT-cloud infrastructure. For the i^{th} traffic event at time t , let $y_{t,i}$ represent the contextual representation. The ciphertext that has been encrypted is recovered as follows:

$$\mathbf{c}_{t,i} = \mathcal{E}_{pk}(\mathbf{y}_{t,i}) \quad (22)$$

The encryption using the public key pk is represented by $\mathcal{E}_{pk}(\cdot)$. In this case, pk is shared across authorized entities, and $\mathbf{c}_{t,i}$ is the encrypted output. The mathematical expression of decryption process is defined below:

$$\mathbf{y}_{t,i} = \mathcal{D}_{sk}(\mathbf{c}_{t,i}) \quad (23)$$

The decryption using the secret key sk is defined as $\mathcal{D}_{sk}(\cdot)$. This method ensures that cloud servers or blockchain validators cannot infer sensitive intrusion information from preserved ciphertexts.

III.4.2 Consortium Blockchain for Secure and Immutable Storage

Stake-based validation and authority-controlled participation are combined in the Proof-of-Stake Authority (PoSA) consensus process that powers the blockchain. Timestamps, validator signatures, encrypted data payloads, and a cryptographic hash connecting it to the preceding block are all included in each block. The k^{th} block is denoted by B_k , which is defined as:

$$B_k = \langle H(B_{k-1}), \mathcal{C}_k, T_k, \Sigma_k \rangle \quad (24)$$

Here, the hash of the prior block is stated as $H(B_{k-1})$, T_k specifies the timestamp, $\mathcal{C}_k$ describes the set of encrypted ciphertexts and the validator's digital signature is stated as Σ_k .

III.4.3 Smart Contract–Based Dynamic Access Control

The suggested system uses smart contracts to independently implement dynamic access control rules in order to get around this limitation. Self-executing programs termed smart contracts are implemented on the blockchain and assess access requests using contextual trust metrics and pre-established security guidelines. Let T_j stand for its trust score which is based on past behavior, intrusion alarms, and policy compliance, and let U_j represent an entity requesting access to intrusion data or system resources. Access choices are made as follows:

$$\text{Access}(U_j) = \begin{cases} \text{Granted,} & \text{if } T_j \geq \tau, \\ \text{Denied,} & \text{otherwise,} \end{cases} \quad (25)$$

Where τ is a pre-established trust threshold. Here, adaptive and context-aware permission is ensured by dynamically updating T_j based on the results of real-time intrusion detection. The final step guarantees that intrusion detection results are not only accurate but also safe, reliable, and useful by integrating consortium blockchain technology, smart contract-based dynamic access control, and fully homomorphic encryption. The HOA layer and the improved Astra-SAINT detection module are seamlessly integrated with this stage. The blockchain and encryption processes use the optimized predictions as inputs, and smart contracts respond instantly to detection results. Consequently, a closed-loop security architecture combining decentralized trust enforcement and intelligent intrusion detection is achieved by the proposed BDL-IDACS framework.

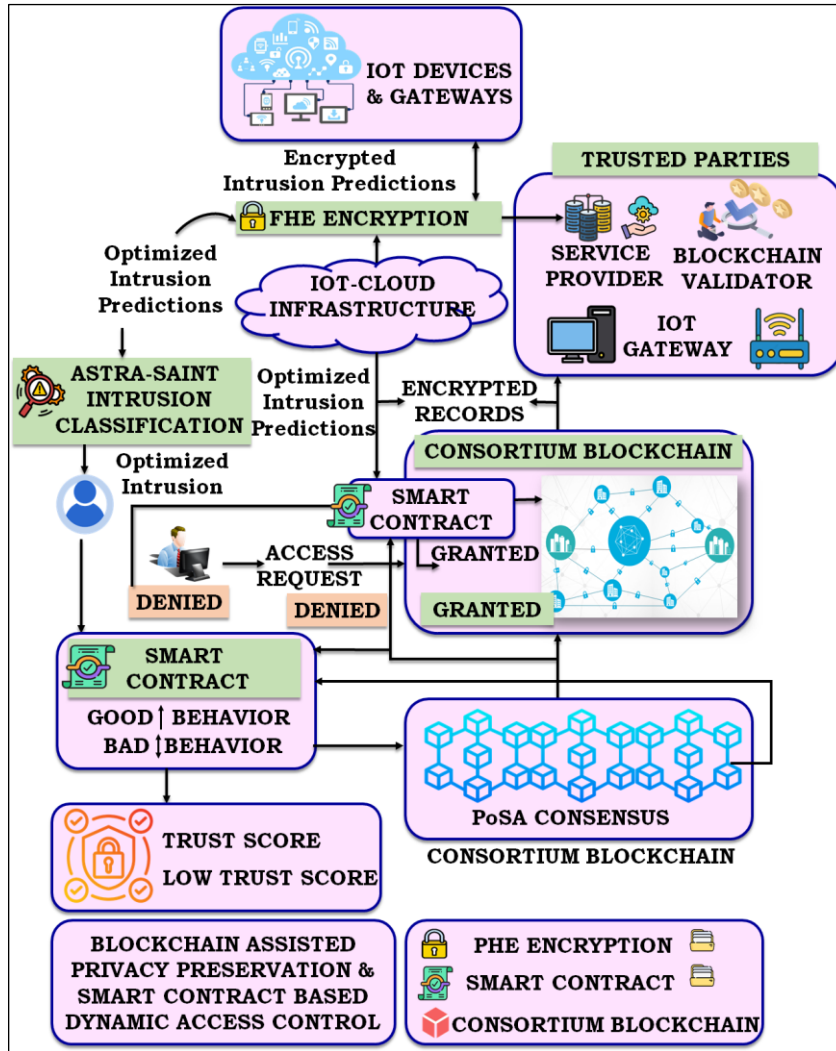


Figure 3: Blockchain-assisted privacy preservation framework.
Source: Authors, (2026).

The blockchain-assisted privacy preservation and smart contract-based dynamic access control stage is shown in figure 3. Data generated by IoT devices and gateways is first sent to the IoT-cloud infrastructure, where FHE is used to encrypt intrusion records and prediction outputs to guarantee data confidentiality throughout the course of storage and processing. By analysing the encrypted data, the Astra-SAINT intrusion classification algorithm generates optimal intrusion predictions without disclosing sensitive raw data. After that, these encrypted prediction records are sent to a consortium blockchain network, where reliable entities like IoT gateways, blockchain validators, and service providers contribute to the upkeep of a decentralized, impenetrable ledger. Smart contracts assess user or application access requests and automatically implement access control policies based on past trust scores and anticipated intrusion behavior.

The choice is permanently recorded on the blockchain, and the smart contract dynamically allows or rejects access based on whether the observed behavior is deemed evil or positive. A unified and thorough method for intelligent, secure, and privacy-preserving intrusion detection in IoT-cloud contexts is created by the proposed BDL-IDACS architecture.

IV. RESULT AND DISCUSSION

IV.1 DATASET DESCRIPTION AND EXPERIMENTAL CONFIGURATION

The proposed BDL-IDACS system is evaluated experimentally using the RT-IoT2022 dataset, a publicly available benchmark dataset from the UCI Machine Learning Repository designed for real-time IDS in IoT applications. There are 85 attributes in each of the collection's 123,117 network traffic samples that capture different protocol-level, flow-based, and statistical traits common to both benign and malicious IoT activities. These characteristics make it possible to describe intricate spatiotemporal attack behaviors in dynamic IoT-cloud infrastructures. A 5-fold cross-validation technique is divided into five mutually exclusive subsets and the model is iteratively trained and verified across all folds, is used to guarantee reliable and objective performance evaluation. For the suggested intrusion detection and access control system, this validation technique reduces overfitting, improves generalization capacity, and yields statistically reliable performance estimates.

IV.2 OUTLIER ANALYSIS OF KEY NETWORK TRAFFIC FEATURES IN RT-IOT2022

The outlier distribution of a few network traffic characteristics from the RT-IoT2022 dataset is shown in figure 4, emphasizing the extreme values and distributional skewness present in actual IoT traffic. Overall, this figure emphasizes the significance to handle outliers robustly during the preprocessing phase because, if ignored, these severe variances can negatively impact learning stability and skew intrusion classification models. The implementation of normalization and outlier-aware feature preprocessing before training the Astra-SAINT intrusion detection system is justified by the observed distributions.

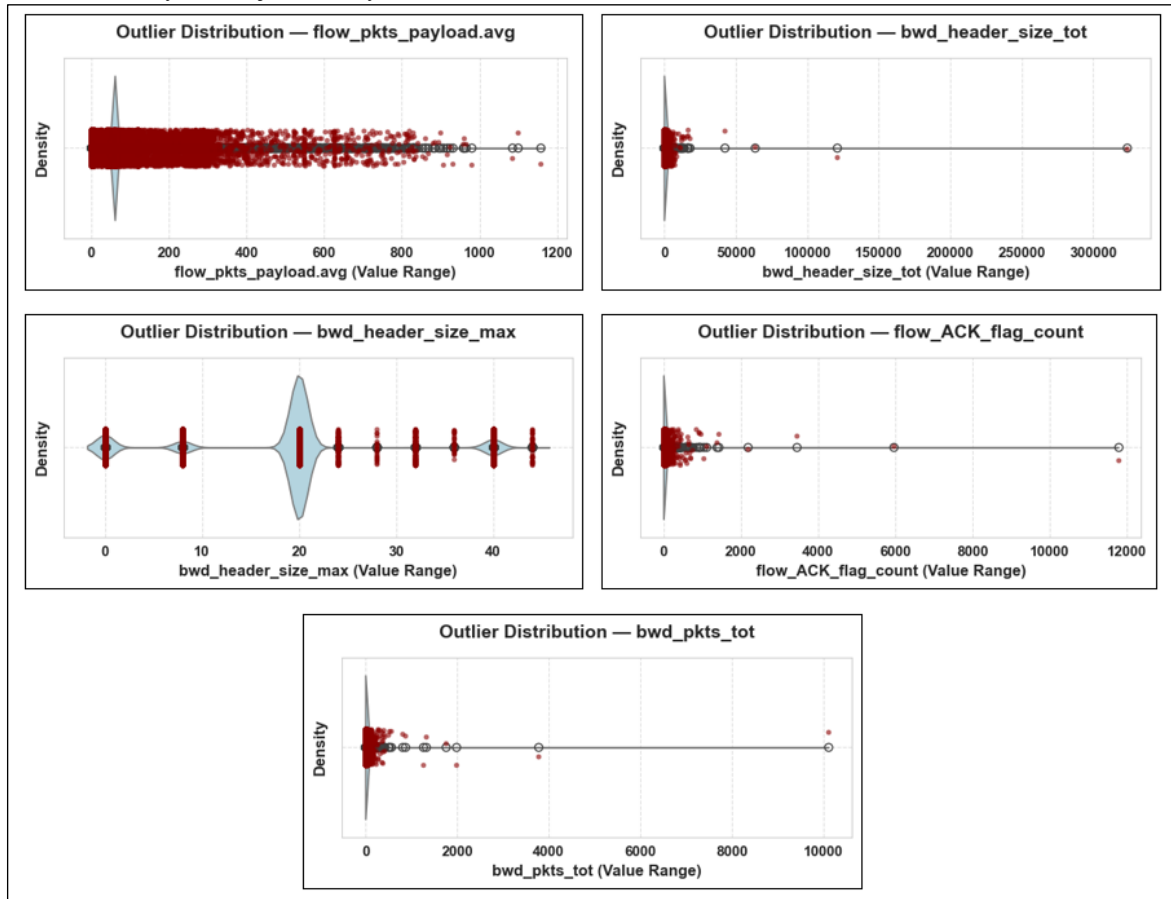


Figure 4: Outlier Distribution of Representative Traffic Features in the RT-IoT2022 Dataset.

Source: Authors, (2026).

IV.3 ATTACK AND PROTOCOL DISTRIBUTION CHARACTERISTICS OF THE RT-IOT2022 DATASET

A thorough examination of attack-type and protocol distributions is shown in figure 5. Denial-of-Service (DoS) attacks make up the majority of malicious samples are highly prevalent according to the attack distribution research. The protocol distribution analysis also shows that TCP traffic predominates in the dataset with ICMP traffic appearing only infrequently and UDP traffic making up a less significant rather than considerable percentage. The requirement for IDS models that can learn consistent and discriminative representations across majority and minority traffic classes is highlighted by this protocol imbalance. Overall, the figure emphasizes the difficulties faced by class imbalance and protocol diversity in IoT intrusion detection, highlighting the significance of attention-based modeling and strong training techniques within the suggested BDL-IDACS framework.

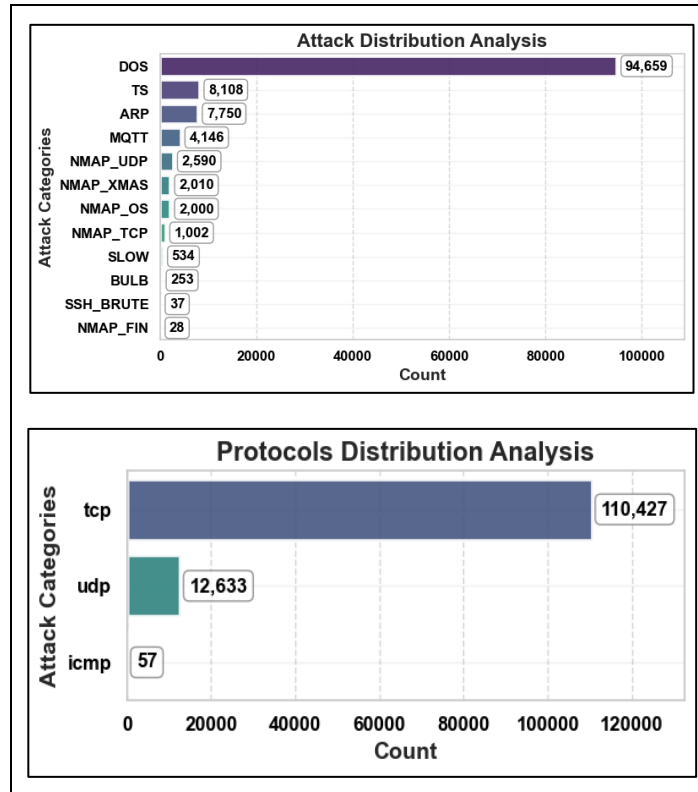


Figure 5: Attack-Type and Protocol Distribution Analysis of the RT-IoT2022 Dataset.
Source: Authors, (2026).

IV.4 CROSS-FOLD ACCURACY AND LOSS COMPARISON BETWEEN STAR-RNN AND PROPOSED ASTRA-SAINT MODELS

Using 5-fold cross-validation, Figure 6 compares the learning behavior of the basic STAR-RNN and the suggested Astra-SAINT transformer model. STAR-RNN's accuracy fluctuations over initial training epochs exhibit observable variation across various folds, with abrupt drops in validation accuracy and consequent rises in validation loss. This indicates that the model is sensitive to data partitioning and possesses limited generalization capability under some folds. As opposed to this, the Astra-SAINT model exhibits more consistent convergence patterns, much lower training loss values, and consistently achieves good training and validation accuracy across the majority of folds. Additionally, the model is robust to class imbalance and temporal unpredictability in IoT traffic, as evidenced by the small effect of moderate fluctuations in validation loss on overall accuracy. Overall, the figure 6 validates the efficacy of transformer-based attention mechanisms for IoT intrusion detection by showing that Astra-SAINT outperforms the STAR-RNN baseline in terms of convergence stability, prediction reliability, and cross-fold generalization.

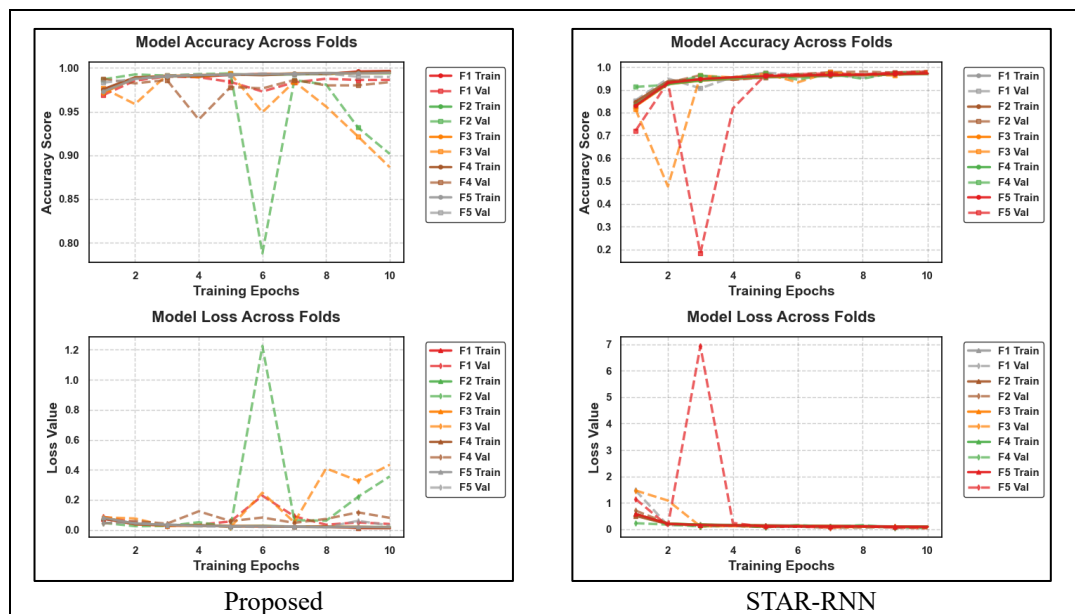


Figure 6: Training and validation accuracy and loss curves across 5-fold cross-validation for the baseline STAR-RNN and proposed model.

Source: Authors, (2026).

IV.5 MULTI-CLASS CONFUSION MATRIX ANALYSIS OF THE PROPOSED ASTRA-SAINT MODEL

The confusion matrices acquired for the proposed model throughout all five K-fold cross-validation folds are shown in the Figure 7. A high true positive rate for all attack categories is shown by the large number of samples along the main diagonal in each fold-level matrix. The model's capacity to learn discriminative spatiotemporal representations is demonstrated by the low off-diagonal values, which indicate little misclassification of attack classes even among structurally comparable observation and scanning attacks. Consistent performance over folds is further confirmed by the aggregated confusion matrix, whose dominating diagonal elements show robustness against class imbalance and steady generalization. Due to their small sample representation, minor confusions in low-frequency attack classes are expected, but they are still insignificant. Overall, this figure validates the appropriateness of the suggested Astra-SAINT model for actual IoT–cloud security deployments by showing that it performs accurate multi-class intrusion classification with high reliability and minimum cross-class interference.

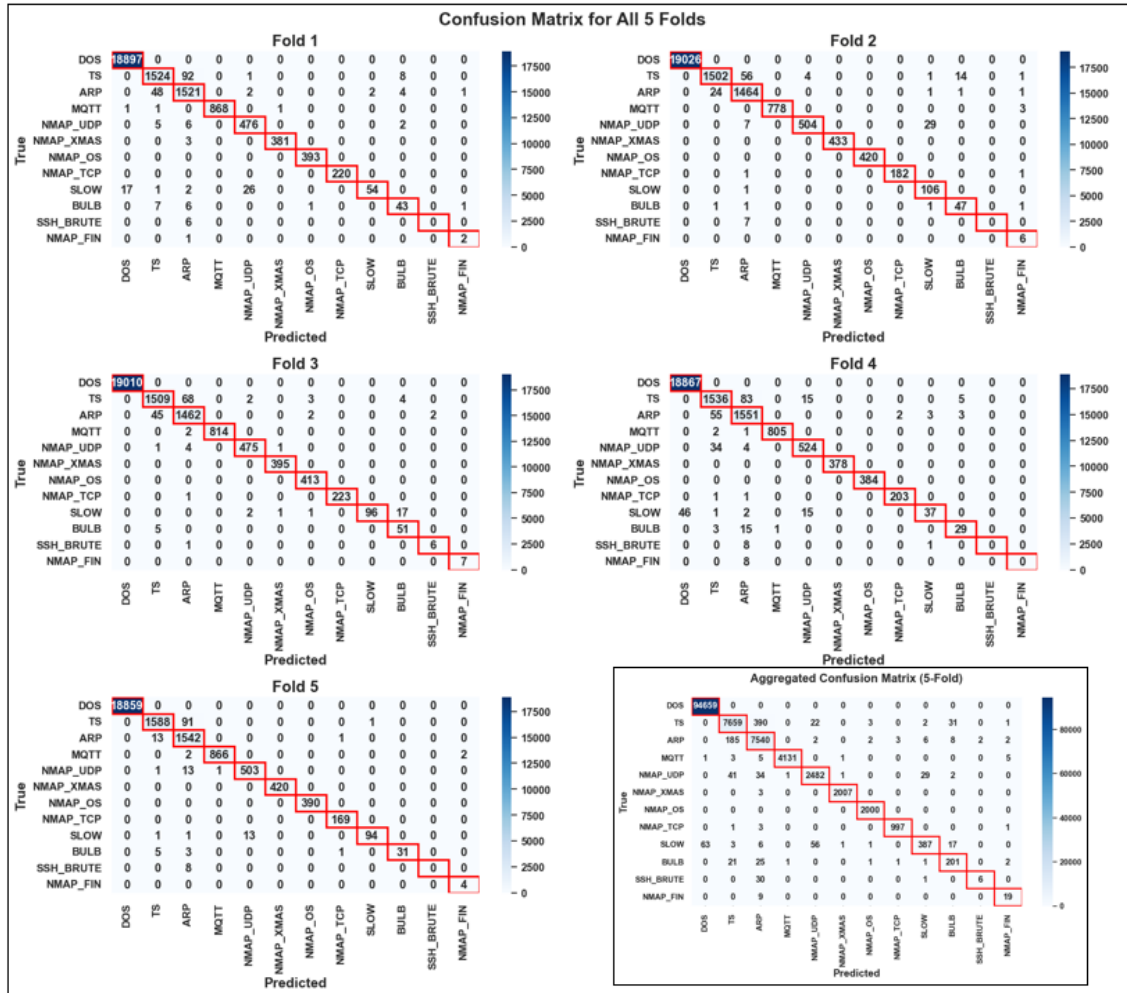


Figure 7: Confusion Matrix Analysis of the Proposed Astra-SAINT Model Across 5-Fold Cross-Validation. Source: Authors, (2026).

IV.6 CONFUSION MATRIX ANALYSIS OF THE BASELINE STAR-RNN MODEL

The confusion matrices for the baseline STAR-RNN (Spatio-Temporal Attention Recurrent Neural Network) model across all five K-fold cross-validation folds are shown in the Figure 8. Although the diagonal entries show that STAR-RNN can accurately identify popular attack classes like DoS, TS, ARP, and MQTT, there are obvious off-diagonal values show higher misclassification rates when compared to the suggested model. Class imbalance and limited training samples are the main causes of minority attack classes. These discrepancies are further highlighted by the aggregated confusion matrix, which shows greater cross-class interference and lower diagonal dominant characteristics. Overall, the figure shows that while STAR-RNN offers respectable baseline performance, the suggested Astra-SAINT model outperforms it in terms of classification reliability and generalization ability, which encourages the use of transformer-based attention mechanisms for reliable IoT intrusion detection.

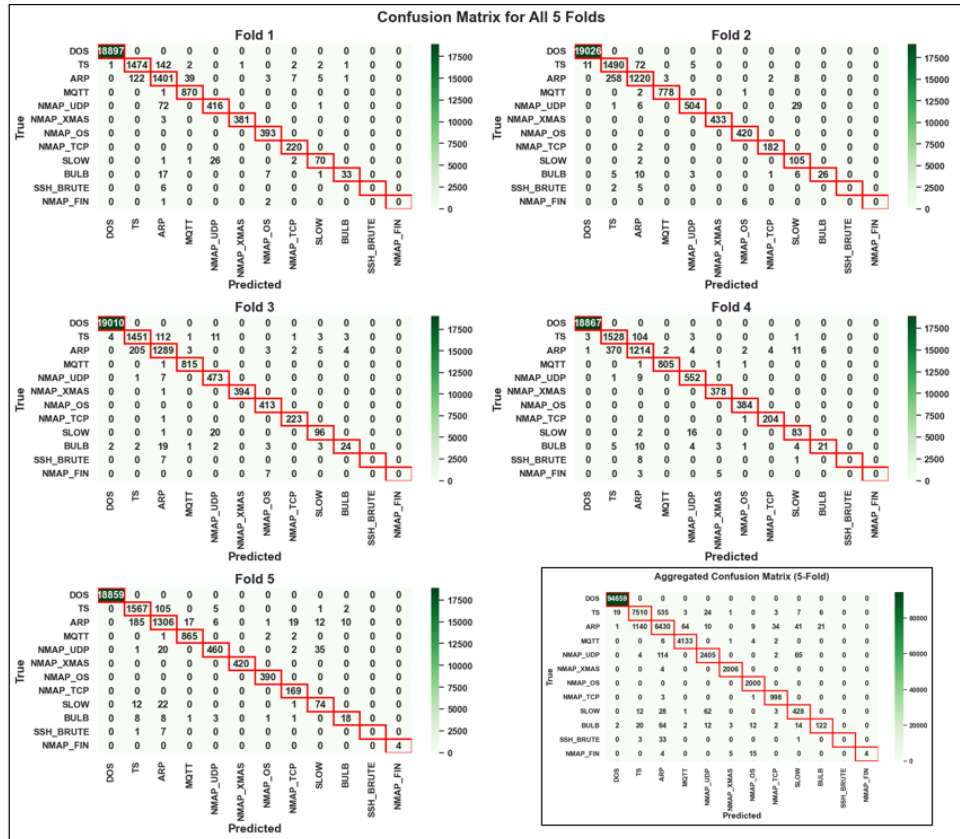


Figure 8: Confusion Matrix Analysis of the Baseline STAR-RNN Model Across 5-Fold Cross-Validation.
Source: Authors, (2026).

IV.7 ROC AND PRECISION-RECALL CURVE ANALYSIS FOR PROPOSED MODEL AND BASELINE STAR-RNN

The suggested model and STAR-RNN are contrasted in Figure 9 utilizing macro-averaged ROC and PR curves under 5-fold cross-validation. The suggested model performs better in terms of precision-recall and class discrimination especially for minority attack classes. On the other hand, STAR-RNN handles class imbalance less well, as seen by its minor decrease in ROC accuracy and lower PR performance ($AP = 0.8223$). Overall, the findings show that the suggested model outperforms the baseline in terms of resilience and detection reliability.

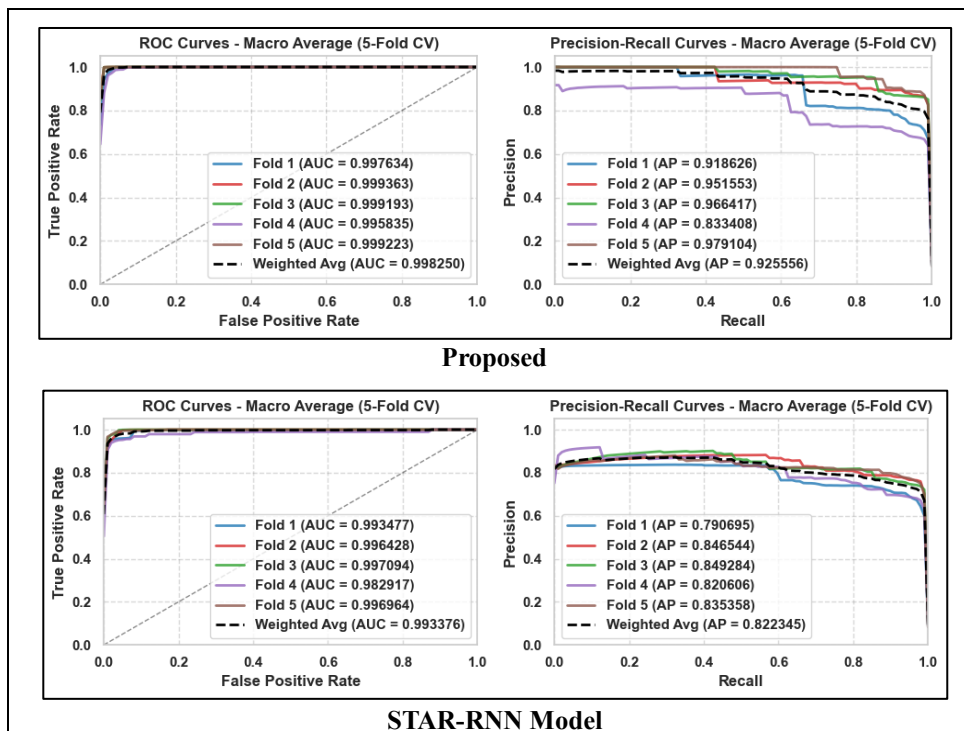


Figure 9: Comparison of ROC and Precision-Recall Curves for the Proposed Model and STAR-RNN (5-Fold Cross-Validation).
Source: Authors, (2026).

IV.8 ACCURACY STABILITY AND CONFIDENCE INTERVAL ANALYSIS FOR PROPOSED AND STAR-RNN MODELS

Figure 10 shows fold-wise accuracy trends on the right and the mean accuracy with 95% confidence intervals on the left. With a mean accuracy of 0.9916 and a narrow 95% CI of [0.9882, 0.9951], the suggested model performs incredibly consistently and dependably across folds. The STAR-RNN model exhibits relatively larger variability with a lower mean accuracy of 0.9803 and a broader 95% confidence range of [0.9772, 0.9834]. Its fold-wise trend exhibits more visible irregularities, especially a discernible decline in one-fold, indicating less resilience under different data splits. Overall, the figure makes it evident that the suggested model outperforms the baseline STAR-RNN in terms of accuracy, stability, and confidence throughout cross-validation folds. The overall performance measures of proposed and the existing method is shown in table 2.

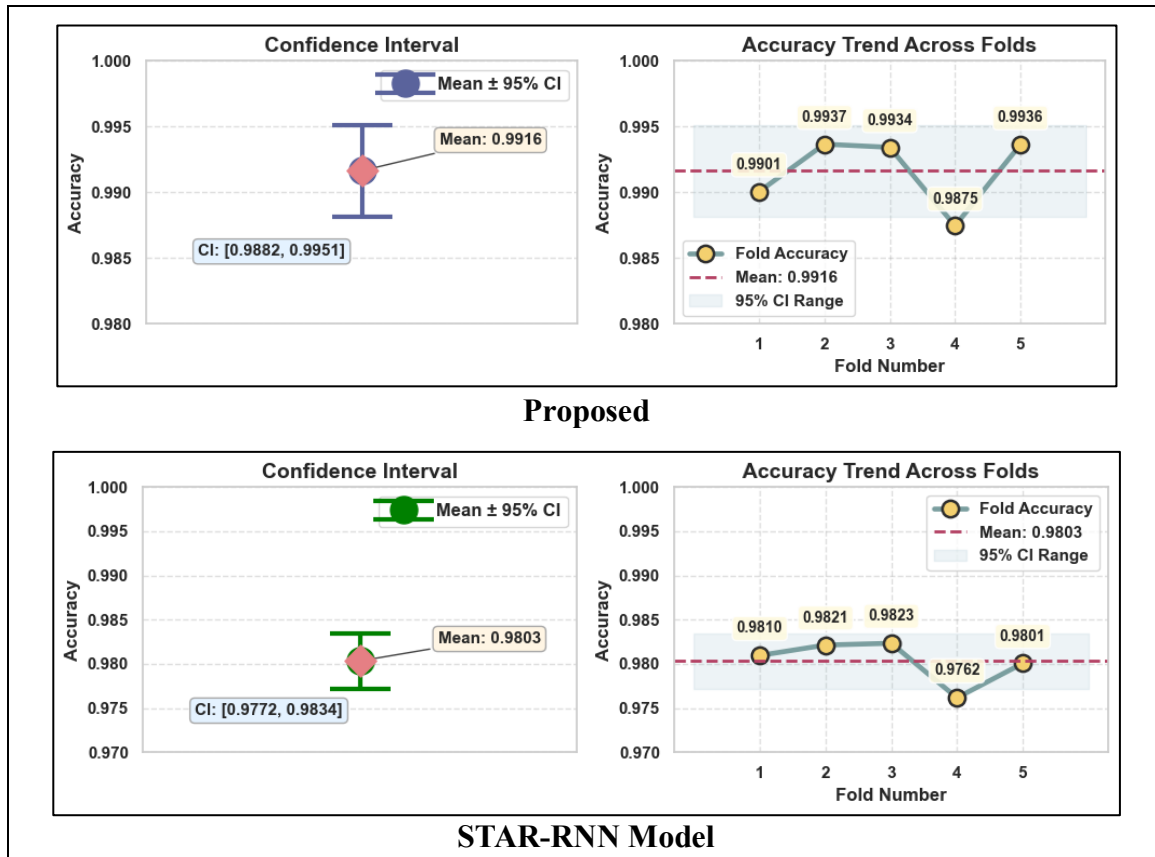


Figure 10: Accuracy Confidence Interval and Fold-Wise Performance Comparison Between Proposed and STAR-RNN Models.
Source: Authors, (2026).

Table 2: Overall performance measures.

Metrics	Proposed	Existing STAR-RNN
Accuracy	0.9916	0.9803
Precision (Macro)	0.9110	0.8512
Recall (Macro)	0.8521	0.7585
F1 Score (Macro)	0.8648	0.7742
Recall (Weighted)	0.9916	0.9803
F1 Score (Weighted)	0.9915	0.9799
Cohen's Kappa	0.9790	0.9506
Specificity (Macro)	0.9991	0.9982
Specificity (Weighted)	0.9978	0.9982
F2 Score (Macro)	0.8560	0.7630
F2 Score (Weighted)	0.9916	0.9801

Source: Authors, (2026).

IV.9 IMPLEMENTATION AND SYSTEM-LEVEL VALIDATION OF BDL-IDACS

The suggested BDL-IDACS framework's Java-based implementation and system-level validation are depicted in Figure 11. While dataset upload and management modules allow for regulated integration of RT-IoT2022 traffic data into the system, user identification and registration interfaces verify secure access activation. The preprocessing and feature-handling steps that get network traffic ready for Astra-SAINT-based intrusion analysis are represented by the file upload, dataset monitoring, and feature input displays. The monitoring interfaces enable ongoing observation of IoT behavior by reflecting real-time analysis of traffic characteristics and system parameters.

Smart contract-based dynamic access control is enforced by download and request management panels, which grant or restrict user capabilities based on trust assessment and validated intrusion predictions. Together, these interfaces verify that the suggested blockchain-assisted, privacy-preserving intrusion detection and access control framework is both operationally deployable and algorithmically effective, guaranteeing safe data handling, restricted access, and transparent auditing throughout the IoT-cloud infrastructure.

The screenshots illustrate the following pages and components of the ITEGAM-JETIA system:

- Registration Form:** Includes fields for User Id, Name, Password, Retype Password, Mobile, Email Id, and Date. Navigation links: HOME, ABOUT US, LOGIN, USER REGISTER, SERVICE, CONTACT US.
- Login Form:** Includes fields for User Name and Password. Navigation links: HOME, ABOUT US, LOGIN, USER REGISTER, SERVICE, CONTACT US.
- File Upload Details:** A page titled "FILE UPLOAD DETAILS" with navigation links: HOME, FILE UPLOAD, FILE UPLOAD, USER DETAILS, DATASET UPLOAD, DOWNLOADER DETAILS, VERIFY, LOGOUT.
- File Uploaded List:** A table showing uploaded files with columns: SELECT, FILE NAME, USER ID, FILE SIZE. Includes a "File Key" input and "Download" and "Submit" buttons. Navigation links: HOME, FILE UPLOAD, FILE UPLOAD, USER DETAILS, DATASET UPLOAD, DOWNLOADER DETAILS, VERIFY, LOGOUT.
- Customer Details:** A table showing user details with columns: USER ID, NAME, MOBILE, EMAIL ID. Navigation links: HOME, FILE UPLOAD, FILE UPLOAD, USER DETAILS, DATASET UPLOAD, DOWNLOADER DETAILS, VERIFY, LOGOUT.
- Dataset Upload:** A page titled "DATASET UPLOAD" with a "Choose File" button and "DATASET UPLOAD" and "DATASET DOWNLOAD" buttons. Navigation links: HOME, FILE UPLOAD, FILE UPLOAD, USER DETAILS, DATASET UPLOAD, DOWNLOADER DETAILS, VERIFY, LOGOUT.
- Downloaders Details:** A table showing download details with columns: USER ID, FILE ID, FILE NAME, DATE, DOWNLOAD STATUS. Navigation links: HOME, FILE UPLOAD, FILE UPLOAD, USER DETAILS, DATASET UPLOAD, DOWNLOADER DETAILS, VERIFY, LOGOUT.
- Acknowledge User Request:** A table showing user requests with columns: SELECT, FILE ID, FILE NAME, REQUESTER NAME, DATE. Includes "Accept" and "Deny" buttons. Navigation links: HOME, FILE UPLOAD, FILE UPLOAD, USER DETAILS, DATASET UPLOAD, DOWNLOADER DETAILS, VERIFY, LOGOUT.
- Login Form (repeated):** Same as the first login form screenshot.

HOME				FILE UPLOAD	FILE LIST	EDIT FILE	DATASET UPLOAD	DOWNLOADER DETAILS	VERIFY	LOGOUT	
User Id	sathish	Contact no			9791222222						
Name	sathish	Email Id			sathish@gmail.com						

FILE UPLOAD FORM				
File ID	1000003			
File Name	Choose File No file chosen			
File Key				
	Add	Cancel		

FILE LIST DETAILS			
SELECT OPTION	FILE NAME	USER ID	FILE SIZE
☐	Steaming.txt	sathish	31
☐	Steaming.txt	sathish	31
File Key			
		Download	Send Request

DATASET MONITORING	
ID NO	94659
id.orig_p	
id.resp_p	
Protocol	
Service	
flow_duration	
flow_pkts_tot	
bw_d_pkts_tot	
flow_data_pkts_tot	
bw_d_data_pkts_tot	
flow_pkts_per_sec	

FILE LIST REQUEST						
RID	FILE ID	FILE NAME	REQUESTER NAME	DATE	ACCESS CODE	
100001	1000001	Steaming.txt	sathish	2023-11-27 11:28:54	242023	
100002	1000002	Steaming.txt	sathish	2023-11-29 19:41:13	242023	

ACKNOWLEDGE USER REQUEST				
SELECT	FILE ID	FILE NAME	REQUESTER NAME	DATE
Accept Reject				

Figure 11: Java-based implementation of the proposed BDL-IDACS framework showing secure user authentication, dataset upload and monitoring, intrusion-aware access control, and system-level validation of blockchain-assisted IoT-cloud security.

Source: Authors, (2026).

IV.10 ABLATION STUDY AND STATISTICAL PERFORMANCE COMPARISON OF MODELS

A thorough ablation analysis and statistical performance comparison between the proposed approach and three baseline architectures STAR-RNN, Transformer, and BiLSTM-CNN are shown in tables 3 and 4. With an accuracy of 0.9916, superior macro-averaged precision (0.9110), recall (0.8521), and F1-score (0.8648), the suggested model consistently obtains the best performance across all measures, demonstrating strong equal effectiveness across all attack classes, even minority classes. The ability to adapt to class imbalance is further supported by the weighted metrics, which keep near-perfect values at 0.99. The baseline models have relatively lower macro-averaged scores, which indicate that they are less successful in managing class imbalance, especially when it comes to recall and F-scores. In comparison to other models, the suggested model's higher Cohen's Kappa value (0.9790) shows a stronger agreement beyond probability. Based on mean performance, standard deviation, and 95% confidence intervals derived from cross-validation, Table 4 provides a statistical comparison of model accuracy. Strong stability and the best mean accuracy (0.9916) are demonstrated by the suggested model, which has a low standard deviation (0.0025) and a small confidence interval [0.9882, 0.9951]. Although the Transformer and STAR-RNN models exhibit competitive accuracy, there is more performance variability indicated by their wider confidence ranges. Reduced consistency is highlighted by the BiLSTM-CNN model, which records the broadest confidence interval and the lowest accuracy. Overall, the findings support the suggested model's higher statistical reliability, robustness, and efficacy when compared to current DL baselines.

Table 3: Ablation study.

Metric	Proposed Model	STAR-RNN	Transformer	BiLSTM-CNN
Accuracy	0.9916	0.9803	0.9790	0.9748
Precision (Macro)	0.9110	0.8512	0.8433	0.8260
Precision (Weighted)	0.9916	0.9801	0.9790	0.9722
Recall (Macro)	0.8521	0.7585	0.7840	0.7391
Recall (Weighted)	0.9916	0.9803	0.9790	0.9748
F1 Score (Macro)	0.8648	0.7742	0.8065	0.7593
F1 Score (Weighted)	0.9915	0.9799	0.9788	0.9712
Cohen's Kappa	0.9790	0.9506	0.9478	0.9412
Specificity (Macro)	0.9991	0.9982	0.9980	0.9971
Specificity (Weighted)	0.9978	0.9982	0.9977	0.9969
F2 Score (Macro)	0.8560	0.7630	0.7944	0.7410
F2 Score (Weighted)	0.9916	0.9801	0.9782	0.9725

Source: Authors, (2026).

Table 4: Statistical Accuracy Comparison of the Proposed Model and Baseline Architectures.

Model	Mean Accuracy	Std. Dev.	95% Confidence Interval
Proposed Model	0.9916	0.0025	[0.9882, 0.9951]
STAR-RNN	0.9803	0.0022	[0.9772, 0.9834]
Transformer	0.9790	0.0031	[0.9729, 0.9851]
BiLSTM-CNN	0.9748	0.0034	[0.9681, 0.9815]

Source: Authors, (2026).

V. CONCLUSION

In order to evaluate the efficacy and dependability of the suggested iIDS, this study used five-fold cross-validation on the RT_IOT2022 dataset. It is evident from experimental results that the suggested model continuously outperforms baseline techniques in every important assessment criteria. With excellent accuracy, precision, recall, F1-score, F2-score, specificity, and Cohen's Kappa all of which together demonstrate great discriminative power and reliability and the method performs exceptionally well in multi-class IoT attack detection. Confusion matrix results show strong true positive rates across almost all attack categories, and additional validation using ROC and Precision-Recall analysis indicates improved class separability and robustness under imbalanced data situations. Furthermore, the model's stability and reliable generalization across cross-validation folds are highlighted by statistical evaluation that uses low standard deviation values and narrow confidence intervals. All things considered, these findings validate that the suggested method is appropriate for actual IoT security situations that call for precise and reliable intrusion detection.

V.1 FUTURE SCOPE

Even though the suggested model performs well, there are still a number of intriguing avenues for improvement. In order to evaluate its efficacy under dynamic network settings and continuous data streams, future research can examine its deployment in real-time IoT systems. Furthermore, investigating edge-level implementation and lightweight model optimization may aid in lowering energy consumption and computing complexity, making the strategy more appropriate for IoT devices with limited resources.

VI. AUTHOR'S CONTRIBUTION

Conceptualization: C. Ramya and A.Suphalakshmi.

Methodology: C. Ramya and A.Suphalakshmi.

Investigation: C. Ramya and A.Suphalakshmi.

Discussion of results: C. Ramya and A.Suphalakshmi.

Writing – Original Draft: C. Ramya.

Writing – Review and Editing: C. Ramya and A.Suphalakshmi.

Resources: A.Suphalakshmi.

Supervision: A.Suphalakshmi.

Approval of the final text: C. Ramya and A.Suphalakshmi.

VII. REFERENCES

- [1] D. Mishra, R. K. Mishra, and R. Agarwal, "Cyber-Physical Systems and Internet of Things (IoT): Convergence, Architectures, and Engineering Applications", *Advances in Engineering Science and Applications*, pp. 17-46, May 2025.
- [2] A. Mishra, A. V. Jha, B. Appasani, A. K. Ray, D. K. Gupta, and A. N. Ghazali, "Emerging technologies and design aspects of next generation cyber physical system with a smart city application perspective", *International Journal of System Assurance Engineering and Management*, vol. 14, no. Suppl 3, pp. 699-721, Jul. 2023.
- [3] C. Chen, Y. Li, Q. Wang, X. Yang, X. Wang, and L. T. Yang, "An intelligent edge-cloud collaborative framework for communication security in distributed cyber-physical systems", *IEEE Network*, vol. 38, no. 1, pp. 172-179, Oct. 2023.
- [4] F. Alserhani, "Intrusion detection and real-time adaptive security in medical IoT using a cyber-physical system design", *Sensors*, vol. 25, no. 15, pp. 4720, Jul. 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, no. 7, pp. 471, Sep. 2025.
- [6] N. Sharma, and P. G. Shambharkar, "Multi-layered security architecture for IoMT systems: integrating dynamic key management, decentralized storage, and dependable intrusion detection framework", *International Journal of Machine Learning and Cybernetics*, pp. 1-48, May 2025.
- [7] A. Awajan, "A novel deep learning-based intrusion detection system for IOT networks", *Computers*, vol. 12, no. 2, pp. 34, Feb. 2023.
- [8] V. Hnamte, and J. Hussain, "DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system", *Telematics and Informatics Reports*, vol. 10, pp. 100053, Jun. 2023.
- [9] Z. Wu, H. Zhang, P. Wang, and Z. Sun, "RTIDS: A robust transformer-based approach for intrusion detection system", *IEEE Access*, vol. 10, pp. 64375-64387, Jun. 2022.
- [10] M. Alazab, G. Manogaran, and C. E. Montenegro-Marin, "Trust management for internet of things using cloud computing and security in smart cities", *Cluster Computing*, vol. 25, no. 3, pp. 1765-1777, Jun. 2022.
- [11] Z. A. Hussien, H. A. Abdulmalik, M. A. Hussain, V. O. Nyangaresi, J. Ma, Z. A. Abduljabbar, and I. Q. Abduljaleel, "Lightweight integrity preserving scheme for secure data exchange in cloud-based IoT systems", *Applied Sciences*, vol. 13, no. 2, pp. 691, Jan. 2023.
- [12] A. Sharma, P. Bohara, M. Tiwari, M. M. Mijwil, M. Abotaleb, and K. K. Hiran, "Enhancing Cloud Computing Security with Blockchain: A Decentralized Approach to Data Integrity, Access Control, and Compliance", In *International Conference on Intelligence-Based Transformations of Technology and Business Trends*, pp. 629-646. Cham: Springer Nature Switzerland, May 2025.

- [13] S. Ahmed, "Enhancing Data Security and Transparency: The Role of Blockchain in Decentralized Systems", *International Journal of Advanced Engineering, Management and Science*, vol. 11, no. 1, pp. 593258, 2025.
- [14] V. Saravanan, M. Madijagan, S. M. Rafee, P. Sanju, T. B. Rehman, and B. Pattanaik, "IoT-based blockchain intrusion detection using optimized recurrent neural network", *Multimedia Tools and Applications*, vol. 83, no. 11, pp. 31505-31526, Mar. 2024.
- [15] A. Aljabri, F. Jemili, and O. Korbaa, "Convolutional neural network for intrusion detection using blockchain technology", *International Journal of Computers and Applications*, vol. 46, no. 2, pp. 67-77, Feb. 2024.
- [16] R. F. Mansour, "Artificial intelligence based optimization with deep learning model for blockchain enabled intrusion detection in CPS environment", *Scientific Reports*, vol. 12, no. 1, pp. 12937, Jul. 2022.
- [17] D. Saveetha, and G. Maragatham, "Design of Blockchain enabled intrusion detection model for detecting security attacks using deep learning", *Pattern Recognition Letters*, vol. 153, pp. 24-28, Jan. 2022.
- [18] E. B. Mbaya, E. Adetiba, J. A. Badejo, J. S. Wejin, O. Oshin, O. Isife, S. C. Thakur, S. Moyo, and E. F. Adebisi, "SecFedIDM-V1: A secure federated intrusion detection model with blockchain and deep bidirectional long short-term memory network", *IEEE Access*, vol. 11, pp. 116011-116025, Oct. 2023.
- [19] M. A. Alkhonaini, M. A. Alohal, M. Aljebreen, M. M. Eltahir, M. H. Alanazi, A. Yafaz, R. Alsini, and A. O. Khadidos, "Sandpiper optimization with hybrid deep learning model for blockchain-assisted intrusion detection in iot environment", *Alexandria Engineering Journal*, vol. 112, pp. 49-62, Jan. 2025.
- [20] B. H. Ali, M. A. Gunavathie, and P. Karthigaikumar, "Secure IoT Medical Data Storage and Intrusion Detection Using Blockchain Encryption and Optimized Two-Branch Attention Adversarial Transformer", *Biomedical Materials & Devices*, pp. 1-26, Dec. 2025.