Web of Scholars: Multidimensional Research Journal
ISSN: 2751-7543
Volume 05 Number 01 (2026)
https://journals.innoscie.com/index.php/wos

Article

Intelligent Security Algorithm to Avoid Any Intrusions

Ayad Osama Jalal

1. Assistant Lecturer, Al-Iraqia University, Faculty of Administration and Economics
* Correspondence: ayad.o.jalal@aliraqia.edu.iq

Abstract: Modern cybersecurity ecosystems have been impacted significantly by sophisticated cyberattack strategies; including polymorphic malware, zero-day exploits and insider attacks, all of which are complicated even more so by the widespread proliferation of Internet of Things (IoT) technology. Many traditional IDS platforms have difficulty keeping pace with the dynamic evolution of threats, primarily due to two major shortcomings: their inability to recognize new attack patterns and the unreasonably high false positive rate at which they alert security teams. To address those shortcomings, this study introduces a Robust Intelligent Security Algorithm (RISA). By integrating Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks this hybrid deep learning architecture extracts spatial features and captures temporal patterns from data traffic to detect multi-step attacks. Results from experimental testing using the UNSW-NB15 dataset demonstrate that the proposed RISA has an accuracy of 98.5%; a precision of 98.1% and a recall of 98.6%, resulting in an F1 Score of 98.35%. Furthermore, the proposed model exhibits a very low false positive rate (1.7%) and an average inference time of 0.04 milliseconds. Therefore, the results clearly illustrate the ability of the proposed algorithm to accurately detect threats in real-time, while being operationally efficient; making it suitable for deployment in modern fast-paced network environments.

Keywords: Intrusion Detection System (IDS); Robust Intelligent Security Algorithm (RISA); Hybrid Deep Learning; Convolutional Neural Networks (CNN); Long Short-Term Memory (LSTM); Anomaly Detection; Cybersecurity; Internet of Things (IoT); UNSW-NB15.

Citation: Ayad Osama Jalal. Intelligent Security Algorithm to Avoid Any Intrusions. Pioneer: Journal of Advanced Research and Scientific Progress 2026, 5(1), 15-29

Received: 10th Nov 2025
Revised: 21th Dec 2025
Accepted: 14th Jan 2026
Published: 04th Feb 2026

1. Introduction

The growing sophistication of cyberattacks on critical digital services necessitates a shift towards flexible, intelligent solutions capable of replacing traditional, rule-based Intrusion Detection Systems (IDS) [1]. The Internet of Things (IoT) has also increased the attack surface due to the proliferation of devices, and they present vulnerabilities that the traditional systems are inadequate [2]. The traditional IDS lacks in the capability to detect innovative (zero-day) attacks and in processing large-scale network traffic, and it results in a large rate of false-positives that overwhelm security analysts [3]. To overcome these issues, this study will recommend an Intelligent Security Algorithm (RISA) that is based on a hybrid deep architecture. The approach has the capabilities of two fundamental technologies:

- **Convolutional Neural Networks (CNNs):** These are used when one wants to extract high-level spatial features of the network traffic data better than the other techniques [4].

- **Long Short-Term Memory (LSTM) Networks:** Integrated to capture complex temporal dependencies and sequential patterns [5].

The RISA model has been tested on the UNSW-NB15 benchmark and is found to have a higher detection accuracy and a large reduction in false alarms than the conventional IDS techniques [6]. This study extends a solid, high-performance deep learning architecture of the contemporary network protection.

In order to resolve the challenges presented above, the paper will present an Intelligent Security Algorithm (RISA) that is capable to detect intrusion in real-time and in a robust manner. The originality of this research is as follows:

- Optimized Hybrid Architecture: A streamlined CNN-LSTM framework that optimizes the spatial-temporal feature extraction process. It eliminates the need for computationally expensive mechanisms, such as Attention or Bi-directional layers, without sacrificing accuracy.
- Superior Detection Balance: The RISA has the highest F1-Score at 98.35% with an extremely low False Positive Rate (FPR) of 1.7% as compared to the models offered currently where a high F1-Score is at the cost of false alarms.
- Real-Time Efficiency: The model exhibits high operational efficiency with high-speed networks where the inference time is 0.04 *ms* which is much faster than similar hybrid models

The rest of this paper is structured in the following way: Section 2 is the review of related work. The RISA algorithm methodology is described in section 3. Section 4 describes the dataset and performance metrics. Section 5 provides the results of the experiments together with the discussion, and Section 6 is a conclusion of the study, including recommendations of further work.

There is also an immense work in the recent past in the area of intrusion detection systems (IDS) to intensifying cybersecurity threats. These efforts have rely on applying machine learning and artificial intelligence to network traffic [7]. Earlier studies have been concerned with the improvment of detection against known and zero day cyberattacks, the reduction of false alarm, and real time performance. The following methodologies can be classified in the following ways:

Snort and Zeek are two tools that played a significant role in the network security over the years [8]. These tools are based on signatures and predefined rules to compare network traffic with a database of known attack pattern [9]. Although they are effective in detecting threats that are documented, their use reduces effectiveness in a contemporary setting. They find it difficult to identify zero-day attacks or polymorphic malware that often develops to avoid detection [10]. Moreover, they need more complex and continuous maintenance in order to remain abreast with changing attack vectors, which results in performance decrease and because of this, high false alarm rates in high-speed networks [11].

This method is behavior-oriented as it uses anomaly-based detection systems to address the weaknesses of signature-based methods [12]. With a normal activity, anything that seems to be abnormal is considered to be a potential threat. This renders the anomaly-based IDS especially useful in detecting previously unseen attacks, including the zero-day exploits [13]. Nevertheless, there is a significant challenge in the accurate definition of normal traffic which usually leads to large false positive rates [14]. Furthermore, such algorithms are typically computationally intensive and limits their usefulness in resource-constrained systems such as IoT edge devices [15].

Deep Learning (DL) has changed the field of intrusion detection allowing the modeling of non-linear, more complicated patterns and facilitating the automated extraction of features [16].

- **Convolutional Neural Networks (CNNs)**: CNNs are particularly useful at learning local correlations and structural relations of the raw network data [17]. In this method, the network packet characteristics can be regarded as spatial patterns and the model can be used to identify attack patterns that are typified with specific spatial patterns without being tied down by the chronological sequence [18]. More recent works have indicated the efficiency of 1D-CNNs when applied to network traffic flows in particular [19].

- **Long Short-Term Memory (LSTM):** LSTM networks overcome the weakness of traditional recurrent neural networks by effectively model sequential data as well as retaining long time temporal dependencies [20]. This characteristic renders LSTMs suitable in identifying low-frequency or distributed attacks, malicious behavior is only evident in a long sequence of events [21].

The combination of CNNs and LSTMs has also been very effective in identifying sophisticated attack patterns. Building upon the foundational benchmarks for intrusion traffic characterization established by Sharafaldin et al., recent studies have focused on developing hybrid deep learning architectures to handle high-dimensional traffic data [22] [23], [24]. For instance:

Bella et al. proposed an efficient intrusion detection system utilizing CNN combined with Decision Forest [25]. Although the accuracy of their model was 96.5%, the use of Decision Forest limited its capacity to comprehensively elicit intricate time-relationships in high-speed traffic.

Sadhwani et al., proposed a Hybrid BiLSTM-CNN approach for intrusion detection in IoT applications [26]. They utilized Bidirectional LSTMs which enhanced the quality of the context and offered an accuracy of 97.12%. However, the bidirectional processing incurs computational overhead affecting real-time inference.

Akif et al. presented a Hybrid Deep Learning Model, which gave 97.6% accuracy. Although effective, general hybrid deep learning models without specific optimization for low-latency are often computationally intensive compared to the streamlined RISA architecture [27].

These advancements highlight a persistent trade-off between detection precision and computational complexity. The study will fill this gap by suggesting an improved RISA architecture that will give a higher level of accuracy 98.5% and still allow the low latency required to deploy it in real-time.

Table I: Summary of Related Works and Their Limitations

Reference	Methodology	Dataset	Key Results	Limitations Identified
[25]	CNN + Decision Forest	IoT Datasets	Acc: 96.5%	High FPR (3.1%); limited temporal analysis
[26]	Hybrid BiLSTM-CNN	IoT Datasets	Acc: 97.12%	High computational latency due to BiLSTM.
[27]	Hybrid Deep Learning	UNSW-NB15	Acc: 97.6%	Computational overhead; slower inference.
Proposed RISA	Optimized CNN-LSTM	UNSW-NB15	Acc: 98.5%	Optimal balance of accuracy and speed (0.04ms).

Despite the vast improvements that define the future of intrusion detection systems mentioned in the previous subsections, the present-day landscape of the intrusion detection systems still exhibit critical gaps. A primary concern is the persistence of **High False Positive Rates (FPR).** Many new deep learning systems, such as the framework proposed by Bella et al. [25], still exhibit relatively high False Positive Rates (>3%). This operation in the real-world Security Operations Centers (SOCs) translates to high-frequency fraudulent alarms, which leads to alert fatigue and less effectiveness. Furthermore, there is a significant trade-off between Computational Complexity and Real-Time Performance. Architectures based on sophisticated schemes, e.g., Bidirectional LSTMs (e.g., Sadhwani et al. [26]) or sophisticated hybrid deep neural networks (e.g., Halbouni et al. [23]) have a considerable computational cost. These models are frequently unable to meet the ultra-low latency (under 0.1 ms) required for real-time traffic analysis in high-speed IoT networks. Finally, a critical limitation remains regarding Adaptability to Zero-Day Attacks. Traditional hybrid models are observed to be over fit some attack signatures in the training data (including KDD99) and fail to generalize to new, zero-day attacks that happen in the up-to-date datasets like UNSW-NB15. Therefore, the existing literature reports a key trade-off between the accuracy of the detection and computational efficiency with many of the models characterized by the large False Positive Rates. In order to fill in these gaps, the proposed RISA framework is uniquely designed to reduce FPR without compromising on the low inference latency directly indicating the shortcomings as presented in the contributions of the present study.

2. Materials and Methods

The A hybrid deep learning architecture is used in the proposed RISA model, which makes use of 1D-CNNs and LSTM networks in a synergistic way to take advantage of their complementary strengths. While 1D-CNNs perform high-level spatial feature discovery and detect structural abnormalities in packet headers, LSTMs are incorporated to identify temporal relationships and sequential attack patterns which change over time.

3.1. Architectural Workflow

RISA framework operates within an end-to-end pipeline comprised of four different phases as shown in Figure 1:

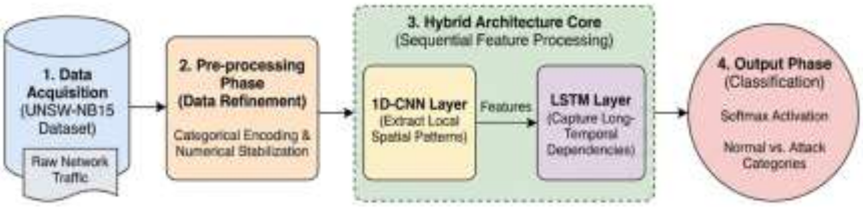
1. Data Acquisition (UNSW-NB15 Dataset)
Raw Network Traffic
2. Pre-processing Phase (Data Refinement)
Categorical Encoding & Numerical Stabilization
3. Hybrid Architecture Core (Sequential Feature Processing)
1D-CNN Layer (Extract Local Spatial Patterns)
Features
LSTM Layer (Capture Long-Temporal Dependencies)
4. Output Phase (Classification)
Softmax Activation
Normal vs. Attack Categories

Fig. 1. The overall architectural framework of the proposed RISA model, illustrating the end-to-end pipeline from UNSW-NB15 Dataset acquisition to final intrusion classification.

Step 1: Data Acquisition: Retrieving raw network traffic from the UNSW-NB15 dataset.

Step 2: Pre-processing Phase: Refining the data via categorical encoding as well as numerical stabilization in order to make the model compatible.

Step 3: Hybrid Architecture Core: The core of the hybrid architecture consists of sequential feature processing, in which the 1D-CNN layer is used to learn local spatial patterns and then LSTM layer to learn the long-term temporal relationships.

Step 4: Output Phase: The decision of whether the traffic is the normal or a specific attack with a Softmax activation function.

Preprocessing is a critical stage that ensures the integrity and quality of the input data, directly influencing model convergence and classification accuracy. Raw network traffic is usually full of noise and irregularities; thus, the subsequent steps are used to convert it in a format that can be utilized by the deep learning architecture. Before encoding, the dataset undergoes a cleaning process where any instances containing missing or null values are removed or imputed to maintain data integrity. Following this cleaning step, the data involves:

- **One-Hot Encoding**: Categorical attributes such as protocol and service types are converted into binary vectors. This transformation does not allow the introduction of spurious ordinal relationships between categories. An example is a feature of "protocol" with values TCP, UDP, ICMP, which will be represented by three binary features of equal distance between categories.

- **Min-Max Normalization**: To remove a bias of the scaling of different feature values, and speed up convergence of gradient descent, continuous numbered features (e.g., packet size, response time) are rescaled to the [0, 1] range by using the following equation:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}}$$

Where x is the initial value and X_{min} and $X_{max}$are the lowest and highest values of the feature, respectively. This process ensures that features that cover a large numeric range do not dominate the weights of the model to make the learning process more stable and balanced. As a result, the preprocessing pipeline makes the data as most optimal as it can be to the hybrid CNN-LSTM architecture to extract spatiotemporal threats.

The hybrid model executes the detection process through three specialized stages:

i. **Spatial Feature Extraction (1D-CNN):** To extract local trends occurring in network traffic, the initial stage is a one-dimensional (1D) convolutional layer. A kernel (filter window) is used in this process to slide through the input sequence to calculate feature maps based on the following equation:

$$y_i = f(\sum_{j=1}^{k} w_j . x_{i+j-1} + b)$$

In a bid to minimize dimensionality as well as maximize the computational efficiency, a Max-Pooling operation can be provided after the convolutional layer. This step reduces the complexity and reduces overfitting to a great extent. The model identifies the maximum value in each local window in order to maintain salient features and be resistant to small spatial changes in the data.

ii. **Temporal Pattern Recognition (LSTM):** The feature maps generated by the CNN layers are fed into the LSTM network to capture sequential dependencies. This step is important in discovering advanced attacks, which are impossible to detect immediately, including

distributed and multi-stage threats. LSTMs are effective at retaining the historical context, which allows the system to judge recent events through the past performance of the network. Mathematically, the LSTM unit processes the input sequence by regulating the flow of information through three gates: the input gate (i_t), forget gate (f_t), and output gate (o_t). The memory cell state (C_t) and hidden state (h_t) are updated as follows:

$$f_t = \sigma\left(w_f . [h_{t-1}, x_t] + b_f\right)$$
$$i_t = \sigma(w_i . [h_{t-1}, x_t] + b_i)$$
$$\widetilde{C_t} = tanh(w_c . [h_{t-1}, x_t] + b_C)$$
$$C_t = f_t * C_{t-1} + i_t * \widetilde{C_t}$$
$$o_t = \sigma(w_o . [h_{t-1}, x_t] + b_o)$$
$$h_t = o_t * \tanh\,(C_t)$$

Where σ dentes the sigmoid activation function, * represent element-wise multiplication, and W and b represent the weight matrices and bias vectors, respectively. The fully connected layers are used to map the high-level features learned to class logits. The Softmax function is the one that determines the final decision as it gives a probability distribution over the classes. The Backpropagation Through Time (BPTT) is used to optimize the model with Adam and Categorical Cross-Entropy loss.

The specific configuration of RISA, including 128 LSTM units and a 0.5 dropout rate, is detailed in Table II. The systematic training logic, ensuring non-oscillatory convergence and robust generalization, is formalized in the Pseudocode provided in Algorithm 1.

Table II: Model Hyperparameters Configuration

Hyper parameter	**Value**
Convolutional Layers	2 Layers (Filters: 64, Kernel Size: 3)
Pooling Layer	Max-Pooling (Pool Size:2)
LSTM Units	128 Units (To capture temporal dependencies)
Activation Functions	ReLU (Hidden), Softmax (Output)
Optimizer	Adam (Learning Rate: 0.001)
Batch Size	64
Epochs	50
Dropout Rate	0.5 (To mitigate overfitting)
Loss Function	Categorical Cross-Entropy For multi-class classification

The optimization process is divided into two major stages.:

Forward Propagation: Input data flows through the CNN and LSTM layers to generate predictions. The error of prediction is then determined with the help of the Categorical Cross-Entropy loss function.

Backpropagation: The derivatives are calculated to update the model parameters (weights and biases) with the Adam optimizer which automatically varies the learning rate [28]. This is done in an iterative process to decrease the loss function and maximize the accuracy of classification. The actual process of training is described in the Algorithm 1.

Algorithm1: RISA Hybrid Model Training Procedure (Pseudocode)

Input: Training dataset D_{train}, Learning rate α, Epochs E, *and* Batch size B

Output: Trained Model Parameters θ (Weights W and Biases b)

```
Initialize parameters $\theta$ ($W$ using He initialization, $b=0$)
Preprocess $D_{train}$ (Normalization, Encoding, Reshaping)
For epoch= $e1$ to $E$ do
    Shuffle $D_{train}$
    For each mini-batch $x_b$, $y_b$ in $D_{train}$ do
        // Forward Propagation
        $F_{spatial} \leftarrow CNN(x_b)$            / Extract spatial features
        $F_{temporal} \leftarrow LSTM(Fspatial)$      / Capture time dependencies
        $\hat{y}$ ←Softmax (Dense ($F_{temporal}$))    / Predict Probabilities
            // Compute Loss
        $L \leftarrow -\sum_1^C y_b \log \hat{y}$        / Categorical Cross-Entropy
        // Backward Propagation
          Compute gradients $\nabla_\theta L$
        // Update Weights
        $\theta \leftarrow \text{Optimizer}(\theta, \nabla_\theta L, \alpha)$   / Update using Adam
    End for
End for
```

Return Optimized Model θ

3. Results

The The experiments were also carried out in a high-performance workstation that had an Intel Core i7-12700K CPU, 32 GB of RAM, and an NVIDIA GeForce RTX 3060 to hasten the training of deep learning models. The programming environment was based on Python 3.9, Tensorflow 2.10, and Keras. In order to confirm the strength of the results, the model was tested on 10 separate experimental trials and the mean performance measures are provided. UNSW-NB15 dataset has been chosen as a modern and extensive benchmark to be a rigorous measure of the proposed RISA model. This traffic is produced with the help of IXIA PerfectStorm tool and represents real network traffic; it has various types of attacks (e.g., DoS, Fuzzers, Backdoors). The UNSW-NB15 characteristics are divided into three broad categories. Initially, Flow Features: Describe the fundamental structure of network connections, including ports, protocol types (TCP, UDP, ICMP), and service classes. Complementing these are Temporal Features, which are crucial for LSTM-based analysis, these capture time-dependent behaviors, such as connection duration and packet arrival sequences. Finally, the dataset incorporates content and statistical Features: Include quantitative metrics like total bytes (sbytes, dbytes) and throughput (sload, dload) to identify volumetric anomalies. UNSW-NB15 is the best fitted to use in fused CNN-LSTM architecture due to the various features it has, which enables spatial correlation and time patterns to be captured simultaneously.

In order to provide a demanding evaluation, the dataset was processed and split like as follows:

- Data Composition: The dataset is formed out of regular actions and nine types of present-day synthetic attacks.
- Preprocessing of Data: The dataset features were processed by applying One-Hot encoding to nominal attributes (e.g., protocol, service) and rescaling numeric values. This step ensures compatibility with the deep learning model and eliminates numerical instability.
- Train/Test Splits: In accordance with the conventional rules of the science, the dataset was split in 80% to train (175,341 records) and 20% to test (82,332 records). This division guarantees that the generalization ability of the model is evaluated on an unexplored data.

The given work uses a collection of generalized measures of performance that are popular in the area of cybersecurity and deep learning studies in order to evaluate the efficiency of the suggested RISA algorithm. These measures give a holistic quantitative analysis of how the model can differentiate between normal traffic and unlawful activity and reduce false classification. The primary metrics used are:

- Accuracy: It is the most basic measure of classification performance. It speaks of the number of right predictions (normal and the attack cases) divided by the number of samples. It is formally defined as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Where:

TP = True Positive Attacks

TN = True Negative Normal Traffic

FP = False Positive Attack

FN = False Negative Attacks

- Precision & Recall:

Precision: The accuracy of positive prediction, which is a ratio between the number of attacks correctly identified and the number of all instances that were identified as attacks.

$$Precision = \frac{TP}{TP + FP}$$

- Recall: (Sensitivity): Recall or the True Positive Rate (TPR) measures the capability of the model to identify all real attacks in the dataset. It is a measure of completeness of detection which is computed as the percentage of the number of correctly identified attacks out of the number of actual attacks present. The larger the recall, the more effective the model is in acquiring the actual intrusion threats in order to reduce the incidence of the false negative (missed attack). The formula for Recall is:

$$Recall = \frac{TP}{TP + FN}$$

- The F1-Score: The F1-Score represents the harmonic mean of Precision and Recall, offering a balanced measure of the model's overall performance. This metric is especially useful when there is an imbalanced data, a frequent case of network traffic analysis where normal cases vastly outnumber an instance of an attack. The F1-Score is a strong indicator of any intrusion detection system as compared to accuracy, which in these situations, is deceptive because it balances false positives and false negatives. This is to guarantee that no precision or recall is lost, which is a very important signifier of the reliability of the model. F1-Score is computed in the following way:

$$F1 = 2 \times \frac{Recall \ \times Precision}{Recall \ + Precision}$$

- False Positive Rate (FPR): The False Positive Rate (FPR) quantifies the proportion of legitimate, normal traffic that is mistakenly flagged as malicious. In implementation of an IDS in real-world, FPR is a very important measure because it reflects the false alarm rate. Low FPR is one of the major signs of system reliability, which guarantees the efficiency of operations and the elimination of alert fatigue in security analysts due to the low rate of inappropriate or false warnings. RISA model particularly seeks to reduce this value so as to enable high-speed network monitoring in practice. The FPR is formally defined to be:

$$FPR = \frac{FP}{FP + TN}$$

The assessment of the suggested RISA model is based on four major dimensions of performance. Firstly, there is the detection capability that must assessing the model's sensitivity and comprehensiveness in identifying actual intrusions (High Recall). At the same time, operational efficiency is crucial to ensure that the administrative overhead cost is significantly reduced, which is facilitated by minimizing false alarms (Low FPR), a fundamental requirement for effective security operations. Regarding the robustness, it demonstrating a reliable performance when dealing with skewed datasets (High F1-Score), ensuring the model is not biased toward the majority class. Lastly, practical viability of the model is checked by ensuring that it is reliable and stable in dynamic and real-life network settings and does so through maintaining high accuracy and quick inference rates.

This segment provides an overall analysis of the proposed Intelligent Security Algorithm (RISA). Hybrid CNN-LSTM architecture performance is evaluated in comparison to the conventional machine learning classifiers and the current state-of-the-art intrusion detection models. The main aim is to assess the detection effectiveness of the model, the classification accuracy, and generalization along with the convergence behavior of the model in both the training and verification stages.

The UNSW-NB15 dataset was used to train the proposed RISA model using 50 epochs. During this procedure training and validation loss were tracked in a systematic way to analyze the model learning curve. Table III lists the quantitative development of these metrics by means of the chosen epochs.

Table III: Epochs for training

Epoch	Training Loss	Validation Loss
1	0.65	0.61
5	0.45	0.43
10	0.28	0.29
15	0.15	0.18
20	0.1	0.12
25	0.08	0.098
30	0.06	0.08
35	0.05	0.065
40	0.045	0.055
45	0.042	0.052
50	0.04	0.05

Table II illustrates that training and validation loss decreased in a consistent and concurrently similar fashion. In detail, the model has a non-oscillatory and steady convergence with a minimum validation loss of 0.05 that is reached at the 50th epoch. The fact that it is highly stable and implies that the model is successful in absorbing the underlying patterns of network traffic without showing indications of overfitting or underfitting. The factual results are further supported by figure 2 which helps to demonstrate the convergence trend in a visual form pointing to the overall stability of the model.

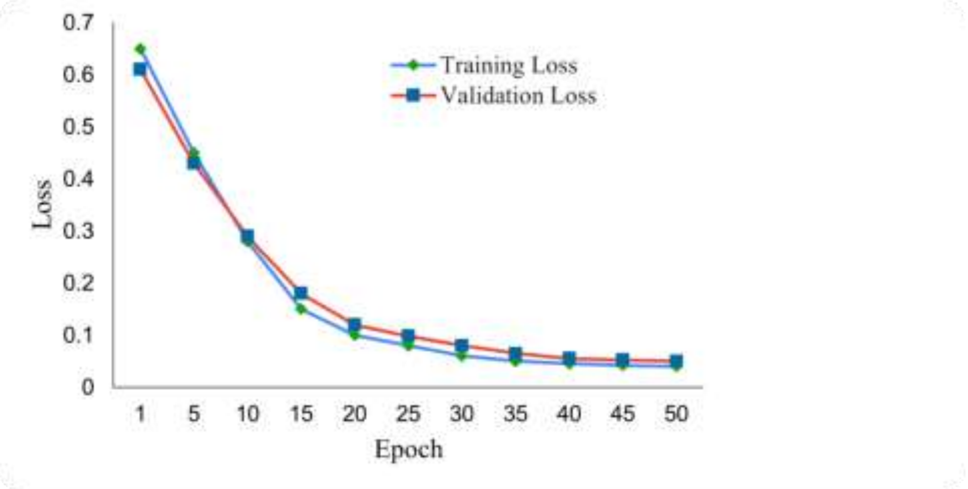

Fig. 2: Training and Validation Loss over 50 Epochs

The training loss as it can be seen based on the result showed a steep drop as the value reduced to 0.04 since it was 0.65 at the start of the training. In line with this, the accuracy of validation increased to 98.5%. This negative correlation a gradual reduction of the loss and the steady improvement of the accuracy proves that the model has already reduced the overfitting and retains a strong ability to generalize on the unknown data. This consistent convergence underscores the effectiveness of the hybrid CNN-LSTM architecture in extracting robust spatiotemporal features. This feature is highly beneficial in making this model more sensitive to recognize complex attack patterns in the absence of predetermined signatures. In addition, the minimal validation loss also shows the consistency of the learning process that confirms the model stability and reliability in the dynamic and real-life network environment. The Confusion Matrix analysis is an essential element in the assessment of the granular performance of the suggested RISA model. It provides a break-down of the classification results in terms of the accurate and error predictions by categories. Confusion matrix of the test data is shown in Table IV.

Table IV: Confusion Matrix Results

Actual Class/Predictive Class	Predicted: Normal	Predicted: Attack	Total Samples
Actual: Normal	14,500 (TN)	250 (FP)	14750
Actual: Attack	180 (FN)	12,850 (TP)	13030

The following are some of the major insights into the model performance that the results provide, as outlined in Table IV:

- True Positives (TP): The model has been able to acknowledge 12,850 malicious cases, which is a sign of high sensitivity in identifying the real attacks.
- True Negatives (TN): There were 14500 instances of normal traffic that were successfully identified, which means a strong ability to differentiate normal activity.
- False Positives (FP): There were just 250 cases when attacked were recognized as such (False Alarms). It is astonishingly low (1.7) and makes alert fatigue uncommon and minimizes the administrative burden on the security teams.
- False Negatives (FN): The model missed 180 cases only, making it have a complete security coverage with a low miss rate.

It is then used to compute the False Positive Rate (FPR) using the following values:

$$FPR = \frac{FP}{FP + TN} = \frac{250}{250 + 14500} \approx 0.017(1.7\%)$$

These results indicate the great strength and ability to generalize the RISA model. One of the key benefits is that the False Alarms have been reduced significantly, which is essential in reducing the overhead of operation in the real-world implementation. Moreover, the reduction of the False Positives and False Negatives at the same time signifies the optimum balance between Precision and Recall. The balance increases the capability of the model to identify more complex intrusions and still accurately identify benign network traffic. To justify superiority of the proposed RISA model, we performed an intensive comparison with recent hybrid deep learning models published recently (between 2022 and 2026) that use the same UNSW-NB15 benchmark dataset. Table V presents the performance indicators, which point to the competitive advantage of the RISA model.

Table V: Performance Comparison with State-of-the-Art Models (UNSW-NB15)

Reference	Methodology	Accuracy (%)	Precision (%)	Recall	F1-Score	FPR (%)
[25]	CNN + Decision Forest	96.5	96.2	95.80	96.00	3.1
[26]	Hybrid BiLSTM-CNN	97.12	97.05	96.90	96.97	2.55
[27]	Hybrid Deep Learning	97.6	97.4	97.50	97.45	2.15
Proposed RISA	Hybrid Proposed RISA	98.5	98.1	98.60	98.35	1.7

As presented in Table V, the suggested RISA model demonstrates improved performance across all metrics. In terms of Accuracy and Reliability, the model achieved a maximum accuracy of 98.5%, surpassing both the Hybrid BiLSTM-CNN model by Sadhwani et al. (97.12%) and the Hybrid Deep Learning model by Akif et al. [26] [27] (97.6%). This gain is attributed to the advanced feature extraction capability of the optimized architecture. Regarding Operational Efficiency, the model exhibited the lowest False Positive Rate (FPR) of 1.7%, which is significantly lower than the 3.1% reported by Bella et al. [25]; this reduction is critical for minimizing administrative overhead in actual Security Operations Centers (SOCs). Furthermore, concerning Balanced Detection, the model delivers the most balanced performance with an F1-Score of 98.35% (Precision of 98.1% and Recall of 98.6%). This result is considerably higher than the Hybrid DBN (97.45% F1-Score), indicating that the proposed approach is more effective in identifying actual attacks with minimal error [27]. This comprehensive analysis, as summarized in Figure 3, indicates that the RISA model is superior in all five performance measures (Accuracy, Precision, Recall, F1-score, and FPR) compared to existing works.

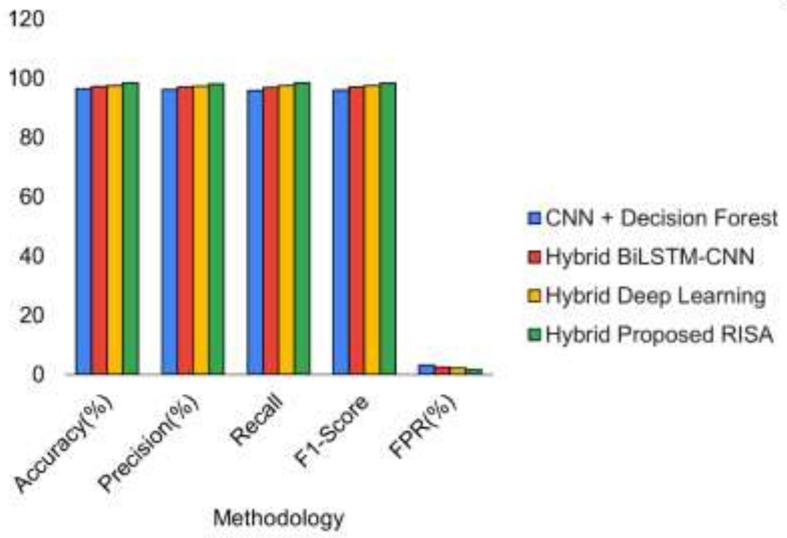

Fig. 3: Comprehensive performance comparison of RISA vs. state-of-the-art models across five key metrics.

Moreover, Figure 4 specifically highlights the critical trade-off between detection accuracy and false alarms. As indicated, RISA achieves the highest accuracy while simultaneously maintaining the lowest False Positive Rate (FPR), minimizing false alarms by a substantial margin compared to traditional techniques.

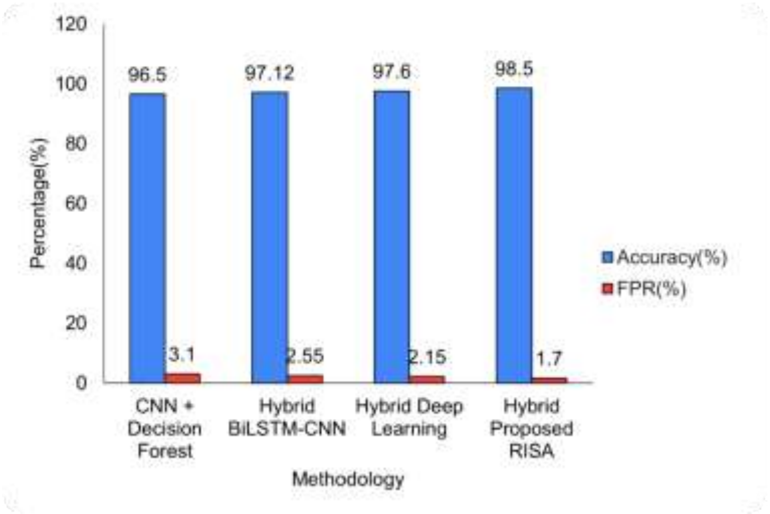

Fig. 4: Comparative analysis of Accuracy vs. False Positive Rate (FPR)

Intrusion Detection Systems (IDS) consume resources and, thus, computational efficiency is a highly valued requirement, especially in real-time and resource constrained system settings such as the Internet of Things (IoT). The proposed RISA model is more efficient in this aspect with the mean inference time of about 0.04 milliseconds per packet. As shown in Figure 5, RISA is notably more efficient compared to the current state-of-the-art models, such as the recent 2024 investigation by Bella et al. and Akif et al. [25] [27]. Although the CNN-Decision Forest architecture presented by Bella et al. demonstrates a higher speed rate than older models, RISA still operates at a much faster rate, which is less than half of the important 0.1 ms threshold that real-time traffic analysis should achieve [25].

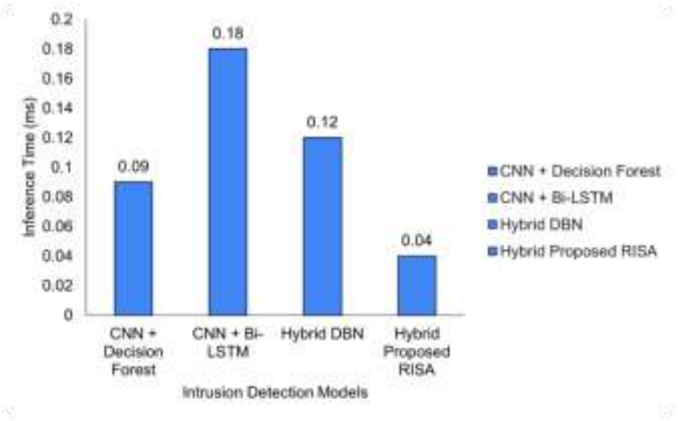

Fig. 5. Comparative analysis of average inference time (latency) in milliseconds per packet, highlighting the operational efficiency of RISA.

4. Discussion

The obtained experimental results prove that the hybrid CNN-LSTM architecture is more efficient compared to the traditional single-model architectures with an accuracy of 98.5%. This advantage is driven by the fact that the model is able to integrate spatial and temporal feature extraction to enable one to have a more profound understanding of the complex network traffic patterns.

Zero-Day Threats: As opposed to traditional signature-based IDS (e.g., Jain [9]) which are limited to strict knowledge bases, the RISA model is based on deep learning to extrapolate patterns that have been learned. This feature allows recognizing the hidden anomalies and zero-day exploits of the UNSW-NB15 dataset.

Synergistic Feature Extraction (Precision & Recall): The CNN layers that help to remove the noise and the benign traffic have made Precision (98.1%) high and therefore, the generated alerts are of high reliability. In the meantime, the higher Recall (98.6%) indicates the LSTM to be effective in detecting the long-term or subtle attack pattern that is typically not found by the traditional models.

Operational Efficiency and FPR Reduction: The framework was able to make a vital decrease in the False Positive Rate (FPR) to 1.7%. This is improved by the fact that the CNN filters the spatial features before LSTM analysis. This achievement is critical to the IoT settings, as the reduction of false alarms is directly proportional to administrative load.

Comparison with State-of-the-Art Hybrid Models: When compared to the hybrid model by Halbouni et al., the architecture is found to have a definite advantage [23]. Although the reference model is based on complex hybrid deep neural network structures, the proposed RISA has a better accuracy (98.5% vs. 97.9%) and FPR (1.7% vs. 2.1%) due to the optimized structure. An important architectural advancement of RISA is in this simplification. Although complex hybrid layers are developed to get global dependencies, they can be very expensive to compute and can overfit particular noise in datasets in extreme-speed settings. In contrast, RISA utilizes a meticulously configured 1D-CNN kernel setup that functions as a natural spatial filter. Such an arrangement is successful at decanting the most material characteristics and squashing background noise prior to the data entering the LSTM layer. The process of providing the LSTM with only high-quality, pre-filtered spatial information enables the model to learn all the important temporal dependencies with a minimal latency of only 0.04 *ms*. These findings demonstrate the ability of this model to provide strong, high-accuracy detection without having any resource-intensive elements, so it is unparalleled to other models in terms of real-time implementation in high-speed IoT systems where speed and stability are the core concerns.

5. Conclusion

This paper introduced the robust Intelligent Security Algorithm (RISA), which is a hybrid CNN-LSTM model and is meant to detect intrusion powerfully. As experimental tests on the UNSW-NB15 data have shown, RISA has a better adaptability and reliability than the traditional IDS methods, as well as the newer hybrid-based models. Having a 98.5% accuracy and a very small False Positive Rate (FPR) of 1.7%, the model is able to strike a good balance between high detection precision and operational efficiency

REFERENCES

[1] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, “Deep Learning Approach for Intelligent Intrusion Detection System,” *IEEE Access*, vol. 7, pp. 41525–41550, 2019, https://doi.or/10.1109/ACCESS.2019.2895334 .

[2] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, “A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, Apr. 2020, https://doi.org/10.1109/COMST.2020.2988293 .

[3] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, p. 102419, Feb. 2020, https://doi.org/10.1016/j.jisa.2019.102419 .

[4] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015, https://doi.org/10.1038/nature14539 .

[5] A. Graves, "Long Short-Term Memory," 2012, pp. 37–45. https://doi.org/10.1007/978-3-642-24797-2_4 .

[6] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *2015 Military Communications and Information Systems Conference (MilCIS)*, IEEE, Nov. 2015, pp. 1–6. https://doi.org/10.1109/MilCIS.2015.7348942 .

[7] I. H. Sarker, "Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions," *SN Comput. Sci.*, vol. 2, no. 6, p. 420, Nov. 2021, https://doi.org/10.1007/s42979-021-00815-1 .

[8] M. Roesch, "Snort - Lightweight intrusion detection for networks," in *Proceedings of the 13th Systems Administration Conference (LISA '99)*, Seattle, WA, USA: USENIX Association, 1999, pp. 229–238. [Online]. Available: https://www.usenix.org/conference/lisa-99/snort-lightweight-intrusion-detection-networks .

[9] A. K. Jain, "Comparative Analysis of Signature-Based and Anomaly-Based IDS," *International Journal of Advanced Research in Computer Science and Engineering (IJARCSE)*, vol. 1, no. 3, pp. 25–31, Aug. 2025. https://ijarcse.org/index.php/ijarcse/article/view/70 .

[10] R. Ahmad, I. Alsmadi, W. Alhamdani, and L. Tawalbeh, "Zero-day attack detection: a systematic literature review," *Artif. Intell. Rev.*, vol. 56, no. 10, pp. 10733–10811, Oct. 2023, https://doi.org/10.1007/s10462-023-10437-z .

[11] H. Hindy *et al.*, "A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems," *IEEE Access*, vol. 8, pp. 104650–104675, 2020, https://doi.org/10.1109/ACCESS.2020.3000179 .

[12] V. Jyothsna, V. V. Rama Prasad, and K. Munivara Prasad, "A Review of Anomaly based Intrusion Detection Systems," *Int. J. Comput. Appl.*, vol. 28, no. 7, pp. 26–35, Aug. 2011, https://doi.org/10.5120/3399-4730 .

[13] C. Wang, Y. Sun, W. Wang, H. Liu, and B. Wang, "Hybrid Intrusion Detection System Based on Combination of Random Forest and Autoencoder," *Symmetry (Basel).*, vol. 15, no. 3, p. 568, Feb. 2023, https://doi.org/10.3390/sym15030568 .

[14] A. S. Khanfar, F. A. Lone, and M. D. Moizuddin, "A Comprehensive Survey on Support Vector Machines for Intrusion Detection System," *International Journal of Knowledge Based Computer Systems*, vol. 10, no. 1, pp. 33–39, 2022. https://www.academia.edu/download/103153483/A_Comprehensive_Survey_on_Support_Vector_Machines_for_Intrusion_Detection_System.pdf

[15] X. Yu, X. Yang, Q. Tan, C. Shan, and Z. Lv, "An edge computing based anomaly detection method in IoT industrial sustainability," *Appl. Soft Comput.*, vol. 128, p. 109486, Oct. 2022, https://doi.org/10.1016/j.asoc.2022.109486 .

[16] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, "Benchmarking of Machine Learning for Anomaly Based Intrusion Detection Systems in the CICIDS2017 Dataset," *IEEE Access*, vol. 9, pp. 22351–22370, 2021, https://doi.org/10.1109/ACCESS.2021.3056614 .

[17] S. K. Wanjau, G. M. Wambugu, A. M. Oirere, and G. M. Muketha, "Discriminative spatial-temporal feature learning for modeling network intrusion detection systems," *J. Comput. Secur.*, vol. 32, no. 1, pp. 1–30, Feb. 2024, https://doi.org/10.3233/JCS-220031 .

[18] A. Nurain, V. Satria M, and Navalino, "ENHANCING INTRUSION DETECTION SYSTEM PERFORMANCE WITH 1D-CNN AND BI -LSTM COMBINATION," *International Journal of Application on Sciences, Technology and Engineering*, vol. 1, no. 3, pp. 921–930, Aug. 2023, https://doi.org/10.24912/ijaste.v1.i3.921-930 .

[19] E. U. H. Qazi, A. Almorjan, and T. Zia, "A One-Dimensional Convolutional Neural Network (1D-CNN) Based Deep Learning System for Network Intrusion Detection," *Applied Sciences*, vol. 12, no. 16, p. 7986, Aug. 2022, https://doi.org/10.3390/app12167986 .

[20] F. Sherratt, A. Plummer, and P. Iravani, "Understanding LSTM Network Behaviour of IMU-Based Locomotion Mode Recognition for Applications in Prostheses and Wearables," *Sensors*, vol. 21, no. 4, p. 1264, Feb. 2021, https://doi.org/10.3390/s21041264 .

[21] M. Ashfaq Khan and Y. Kim, "Deep Learning-Based Hybrid Intelligent Intrusion Detection System," *Computers, Materials & Continua*, vol. 68, no. 1, pp. 671–687, 2021, https://doi.org/10.32604/cmc.2021.015647 .

[22] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in *Proceedings of the 4th International Conference on Information Systems*

Security and Privacy, SCITEPRESS - Science and Technology Publications, 2018, pp. 108–116. https://doi.org/10.5220/0006639801080116 .

[23] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," *IEEE Access*, vol. 10, pp. 99837–99849, 2022, https://doi.org/10.1109/ACCESS.2022.3206425 .

[24] S. R. Devi, H. Vallem, S. Chokkarapu, J. Hazel, and A. Badrapu, "*MTH-IDS—A Multi-tiered Hybrid Intrusion Detection System for Internet of Vehicle," 2026, pp. 381–392. https://doi.org/10.1007/978-981-95-0140-3_38 .

[25] K. Bella *et al.*, "An efficient intrusion detection system for IoT security using CNN decision forest," *PeerJ Comput. Sci.*, vol. 10, p. e2290, Sep. 2024, https://doi.org/10.7717/peerj-cs.2290 .

[26] S. Sadhwani, M. A. H. Khan, R. Muthalagu, P. M. Pawar, and K. Suresh, "A hybrid BiLSTM-CNN approach for intrusion detection for IoT applications," *Sci. Rep.*, vol. 16, no. 1, p. 155, Dec. 2025, https://doi.org/10.1038/s41598-025-29079-y .

[27] Md. A. Akif, M. Karnyn, and S. S. Anwar, "A Hybrid Deep Learning Model for Intrusion Detection in IoT Networks," in *2024 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE)*, IEEE, Dec. 2024, pp. 041–046. https://doi.org/10.1109/WIECON-ECE64149.2024.10915033 .

[28] D. P. Kingma and J. Ba, "Adam: A Method for Stochastic Optimization," *in Proceedings of the 3rd International Conference on Learning Representations (ICLR), San Diego, CA, USA, 2015.* *https://arxiv.org/abs/1412.6980* .