Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 1, February 2026, pp. 669~679
ISSN: 2302-9285, DOI: 10.11591/eei.v15i1.11048

Hybrid AI-driven anomaly detection and sequential attack classification for securing IoT networks

Gauri Sameer Rapate[1], Ambuja Krishnappa[2], Sarala Duggonahalli Veeresh[2], Karanam Sunil Kumar[3], Bellary Kursheed[4]

[1]Department of Computer Science and Engineering, PES University, Bangalore, India
[2]Department of Computer Science and Engineering, BMS College of Engineering, Bangalore, India
[3]Department of Computer Science and Engineering, R.V. College of Engineering, Bengaluru, India
[4]Department of Computer Science and Engineering (Artificial Intelligence and Machine Learning), Don Bosco Institute of Technology, Bengaluru, India

Article Info

Article history:

Received Jul 16, 2024
Revised Oct 1, 2024
Accepted Dec 6, 2025

Keywords:

Anomaly detection
Artificial intelligence
Internet of things
Intrusion detection
Long short-term memory
Random forest

ABSTRACT

Internet of things (IoT) systems are often inherently heterogeneous and the constantly evolving cyber threat presents a variety of attack vectors that can expose sensitive data across multiple mission-critical applications. The existing intrusion detection methods are often prone to zero-day attacks and specific to limited known intrusions. This paper designs a hybrid and multi-level cyber-threat detection framework based on the robust data preprocessing scheme, correlation-based optimal feature selection and integrated anomaly and intrusion detection using a supervised learning approach. In the first stage, a random forest (RF)-based binary anomaly detector is designed as a fast primary threat filter against zero-day threats by detecting traffic anomalies without any prior attack signal. In the second stage, an adaptive, time-aware long short-term memory (LSTM) model performs multi-class intrusion classification using time-lag analysis in traffic flows to accurately identify and classify known attack types with high precision. The proposed framework is evaluated on the network flow–telemetry of network–internet of things–version 2 (NF-ToN-IoT-V2) dataset and achieved 99% accuracy in both binary and multiclass settings, with a lower response time of 7.8 ms.

Corresponding Author:

Gauri Sameer Rapate
Department of Computer Science and Engineering, PES University
Hosur Road, 1 km before Electronic City, Bengaluru, Karnataka - 560100, India
Email: gauri.rapate@pes.edu

1. INTRODUCTION

The internet of things (IoT) links billions of physical devices, sensors, actuators, and smart things that communicate data over the Internet. IoT is being utilized across the globe in real-world applications and has a dramatic rate of adoption in industrial systems and agricultural systems, enabling real-time monitoring, automated decisions, and overall improvements in efficiency [1]. However, the IoT is vulnerable to security concerns because it is highly distributed, has lower computation power, has various communication protocols, and has little-to-no authentication [2]. Cyber-attacks that include denial-of-service (DoS), man-in-the-middle (MITM), botnets, ransomware, and data leaks have demonstrated how perimeter security fails [3]. In addition, there are two major concerns, i.e., zero-day attacks, which exploit unknown vulnerabilities, and multi-stage intrusions that escalate over time [4]. The conventional signature-based detection methods often fail to identify such threats, as they are highly dependent on the predefined patterns [5], but with the

advancement in machine learning (ML) and deep learning (DL), there is an increasing trend towards developing intelligent anomaly detection and intrusion classification [6]. However, designing an effective artificial intelligence (AI-based) security system for IoT is not a straightforward process, as it is associated with various challenges such as imbalanced datasets, limited edge-device resources, difficulty in generalizing to new attacks, and a lack of model interpretability. Furthermore, achieving the best balance between predictions with low false-positives and model complexity also presents challenges when adopted in real-world scenarios.

In the recent literature, various research works have been presented towards developing an intrusion-detection-system (IDS) for IoT applications using different ML and DL models as well as their hybridized versions. The usage of k-nearest neighbour (KNN) is seen in the work of Babbar *et al.* [7] for detecting Android malware in IoT environments, which is effective in identifying known threats but may face difficulty with evolving cyber-attacks. Agbedanu *et al.* [8] introduced an adaptive KNN model for detecting zero-day attacks in industrial IoT, but this model may be a bit difficult to handle high-dimensional data. Nuha *et al.* [9] introduced a modified distance metric in KNN using third-order distance to classify flooding attacks in optical burst switching networks. Kaushik *et al.* [10] used a multinomial Naive Bayes (NB) classifier to analyze intrusions from traffic generated from smart IoT devices. Similarly, Prakash *et al.* [11] developed an NB-based IDS framework for anomaly detection, but it is not very adaptive and may result in high false-positive rates when subjected to different network datasets. Majeed *et al.* [12] suggested an NB-powered cybersecurity model for drone networks, but it lacked robustness against dynamic attack scenarios. In the work of Deshmukh and Ravulakollu [13], researchers designed a convolutional network-based IoT-IDS due to its automated feature learning, but this approach is sensitive to overfitting due to the use of fixed filters. Alabsi *et al.* [14] introduced a dual convolutional network architecture to improve feature learning, but its computational cost increases. Hairab *et al.* [15] applied convolutional operations with regularization to detect zero-day attacks. Okey *et al.* [16] explored transfer learning with convolutional neural networks (CNNs) for IoT-based IDS, but it lacks scalability for real-time deployment scenarios where continuous training on new features is required.

The studies towards applying deep recurrent models such as the gated recurrent unit (GRU) for modelling sequential dependencies in network traffic are seen in the work of Sagu *et al.* [17], where GRU is combined with convolutional networks to improve prediction accuracy on known attacks. Alshdadi *et al.* [18] developed a GRU integrated ResNet split-attention mechanism to detect distributed denial of service (DDoS) attacks, which provided better detection rate but with extensive computational resources. Bi *et al.* [19] introduced a temporal-convolutional network with bi-directional GRUs for attack prediction to capture temporal behaviours in the network traffic. Similarly, ALMahadin *et al.* [20] used GRU for detecting anomalies in vehicular ad hoc network (VANET) traffic, which demonstrated robust performance but may be prone to adversarial attacks. The work carried out by Gueriani *et al.* [21] explored an advanced recurrent model, i.e., long short-term memory (LSTM) networks, which is combined with convolutional layers to build a hybrid-IDS for detecting complex intrusion patterns. In a similar direction, development of the hybrid IDS based on the joint approach of CNN–LSTM is also found in the work of Altunay and Albayrak [22] and Sinha *et al.* [23] towards enhanced feature learning and classification of complex network intrusions in Industrial IoT. However, these models are not validated against zero-day or un-seen attacks, which is important for real-world deployment. However, the literature is diverse, but most of them highlight individual strengths without addressing trade-offs such as accuracy versus scalability or temporal modelling versus interpretability.

The identified research problem after reviewing existing system are as follows: i) the existing ML classifiers are only effective for known malware patterns [7]–[12], but have been found to be ineffective against emerging threats and zero-day attacks; ii) the existing DL-based IDSs [13]–[20] provide better accuracy, but suffer from overfitting, high resource demand, and poor scalability for edge deployments; iii) LSTM-based systems [21]–[23] show robust temporal modeling for stealth attacks, but often lack interpretability and have high latency, making them unsuitable for real-time IoT use; iv) the current approaches struggle with stateless and evolving attacks such as single-packet flooding or timing-based intrusions, which require both timing and behavioral analysis for effective detection; and v) also, in many real-world IoT scenarios, traffic patterns are not uniformly sampled and there are variable delays between events. The existing approaches often ignore this temporal gap that can distort the sequence modelling, which may limit performance when applied to real, noisy network data.

The proposed study presents an effective and hybridized cyber-threat countermeasure framework that integrates multiple AI-driven components for robust IoT security. Specifically, the proposed model is a multi-level security architecture: i) it applies data analytics techniques for feature correlation and optimal selection; ii) introduces anomaly detection using ML where a random forest (RF)-classifier is used for preliminary anomaly detection; and iii) implements intrusion classification via DL LSTM classifier enhanced

with adaptive temporal (AT) network traffic pattern analysis. The unique contribution of the proposed work is the inclusion of elapsed time between traffic events in the sequential classification that enables the model to adaptively discount outdated information and prioritize recent observations. As a result, the proposed system achieves high accuracy in classifying both known and previously unseen (zero-day) attacks.

2. METHOD

The schematic outline of the proposed multi-layer security framework is illustrated in Figure 1, which integrates data analytics, supervised-learning-based anomaly detection and intrusion classification in IoT environments. The system modelling is carried out in four distinct stages, such as: i) data preprocessing, ii) feature selection, iii) binary anomaly detection, and iv) multi-class intrusion classification. Unlike conventional models that attempt to address all tasks within a single implementation strategy, the proposed approach separates anomaly detection and threat classification into distinct yet interconnected stages. The input module of the proposed system incorporates a lightweight correlation-guided feature selection mechanism for reducing the dimensionality of the data and selecting optimal features without compromising detection capability. At the first stage of cyber-threat detection, the system employs an RF-based anomaly detector, which is trained on optimized features that allow the system to quickly flag abnormal traffic patterns. At this stage, the proposed model contributes to the early threat interception by acting as a first-layer security filter.

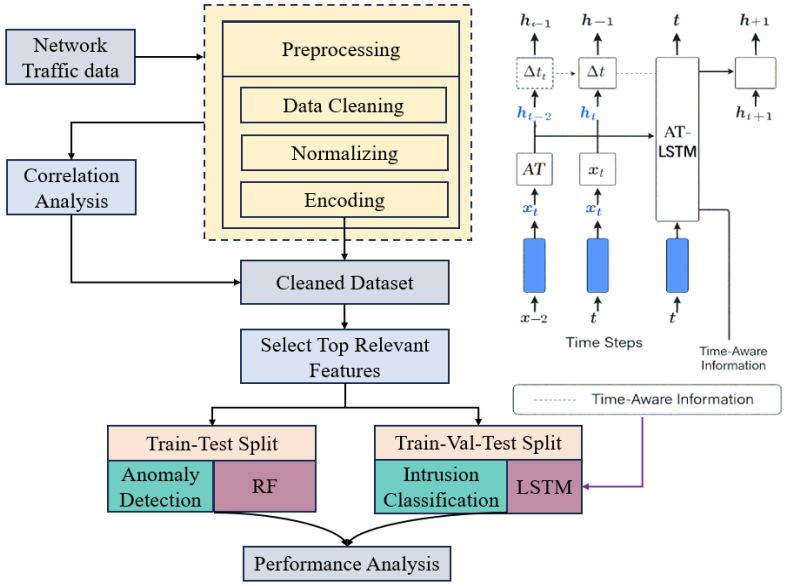


Figure 1. The schematic architecture of the proposed multi-level IoT security framework

Upon detection of anomalies, the framework activates a second-layer threat analysis via an AT-LSTM network, which is designed for sequence learning and is capable of modelling the temporal and contextual patterns of network traffic. It enables multi-class classification of threats of various IoT attack categories, i.e., from DoS and DDoS to cross-site scripting (XSS), injection, and ransomware, ensuring comprehensive threat labelling and future traceability. Finally, the framework is evaluated on a large-scale modern IoT dataset, towards justifying and validating its effectiveness against zero-day attacks and known cyber-threats. The development of the proposed IoT security solution is carried out in such a manner that it enhances both the speed of response and classification depth, thereby optimising performance for real-time and resource-constrained IoT environments.

2.1. Dataset description

This study utilises the network flow–telemetry of network–internet of things–version 2 (NF-ToN-IoT-V2) dataset [24], a recent benchmark from the ToN-IoT series, which is the Netflow version of the UNSW-ToN-IoT dataset. This dataset consists of the telemetry network traffic data obtained from the diverse IoT devices and industrial control systems, which consists of more than 13 million labelled data samples. This dataset comes with both normal traffic and nine different attack classes, where each samples are

associated with numerical and statistical features related to network sessions, packet count, flow duration, and header flags. For model development, the dataset is used in two tasks, viz; i) binary classification (anomaly detection), i.e., benign vs. attack, with an 80:20 train-test split and ii) multi-class classification (intrusion type classification) with an 80:10:10 train-validation-test split considering all ten classes. The detailed class-wise distribution is summarized in Table 1.

Table 1. Dataset distribution

Attack type	Train (80%)	Validation (10%)	Test (10%)	Total
Scanning	2,401,735	300,217	300,217	3,002,169
XSS	1,959,964	244,996	244,996	2,449,955
DDOS	1,397,272	174,659	174,659	1,746,590
Password	794,974	99,372	99,372	993,718
Injection	528,374	66,047	66,047	660,467
DOS	523,487	65,436	65,436	654,359
Backdoor	13,007	1,626	1,626	16,259
MITM	6,178	773	772	7,723
Ransomware	2,686	336	335	3,357
Benign	2,880,997	360,128	360,159	3,601,284
Total	10,508,674	1,313,590	1,313,619	13,135,881

2.2. Preprocessing and feature selection

The exploratory analysis of the adopted dataset reveals that the dataset has a total of 43 numerical and categorical attributes and 9,534,597 samples. Further investigation using descriptive statistics reveals that the dataset is not associated with any missing or zero values. However, it is found that the dataset is associated with class imbalance issues with different attack classes, which are handled using an upsampling approach on the training set using synthetic-minority-over-sampling-technique (SMOTE). The next process leads to data encoding, where categorical attributes are encoded to numerical representations, which are then standardised using the Z-score normalization approach by removing each feature's mean and scaling it to unit variance. Further steps are subjected to correlation analysis and feature selection to identify the most relevant and task-associated features for the target label. Figure 2 shows the top-15 selected features using the Pearson coefficient method.

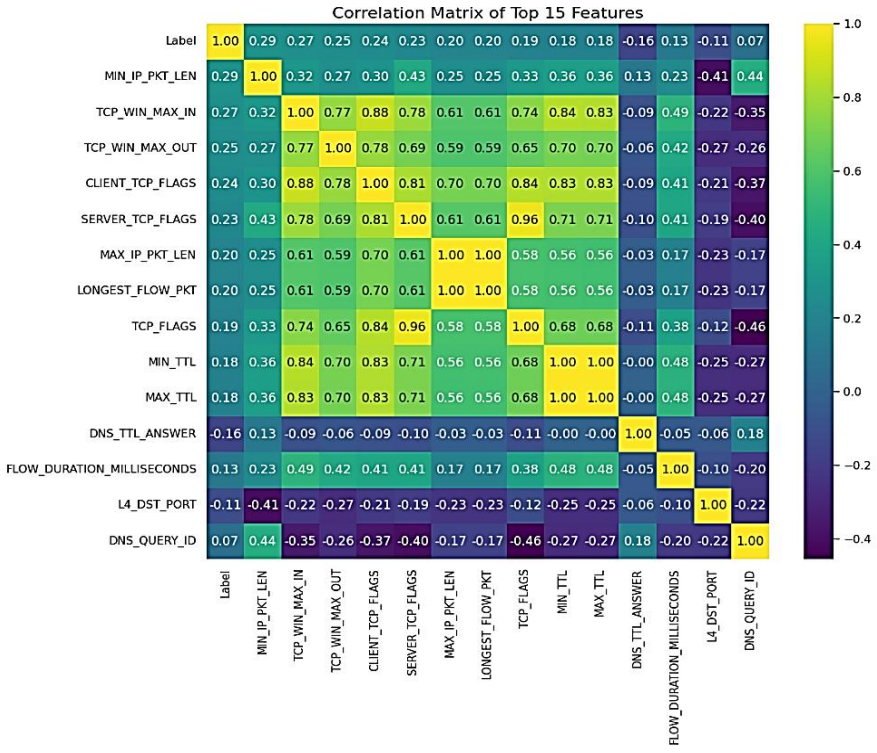


Figure 2. The top-15 features selected based on their relevance to the target class

The Figure 2 shows the correlation matrix of the top-15 features identified and most relevant to the target class. It can be seen that the features such as MIN_IP_PKT_LEN, TCP_WIN_MAX_IN, and CLIENT_TCP_FLAGS show a relatively higher positive correlation with the attack class, and this indicates their strong relevance or influence in distinguishing between benign and malicious traffic patterns. On the other hand, the other features like L4_DST_PORT and DNS_QUERY_ID show slight weak correlations, which suggests its limited direct impact on classification, but it has a significant contribution when considering with other features. Hence, these features are considered for the model training for both task anomaly detection and intrusion classification.

2.3. Anaomaly detection

This is the first phase of the proposed framework that focuses on anomaly detection, and is modelled as a binary classification problem. In this phase of the modelling, the RF algorithm is employed due to its robustness, high interpretability, and low susceptibility to overfitting. The reason behind selecting the RF classifier among other ML classifiers is its ability to handle high-dimensional data. It is an ensemble-based ML model that is designed based on the constructs of multiple decision trees and has less sensitivity to noise, and has fast inference speed, which is crucial for early-stage threat detection. In this work, RF is trained on the preprocessed feature set (as detailed in subsection 2.2) using 80% of the dataset, whereas the remaining 20% is used for evaluation. The output of this stage indicates whether the incoming traffic flow is anomalous, and if it flags network traffic as an attack, then the system quickly isolates malicious flows from the network and initiates the next phase for deep inspection using the proposed AT-LSTM model.

2.4. Intrusion classification

This is the second and final phase of the proposed framework towards accurately categorising the anomalies identified by the first module into their respective attack types. This phase of the system modelling is essential to understand the type and impact of the threats, even in dynamic real-world IoT environments with a possibility of known attacks as well as unseen attacks (zero-day). The intrusion classification task is modelled as a temporal sequence classification problem, where network traffic samples developed after the anomaly detection model has detected anomalies are sequentially processed by the AT-LSTM network in the same manner as their ordering, repeating processing the samples until the sequencing is concluded. Rather than treating all temporal transitions equally like conventional LSTM models, our AT-LSTM explicitly captures elapsed time (Δt) between input events as an additional input feature, through which the model can regulate its memory retention and forget mechanisms based on the temporal relevance of each input sample. Figure 3 outlines the workflow of the proposed AT-LSTM for intrusion classification. The main workflow and internel architecture are illustared in Figures 3(a) and (b) respectively.

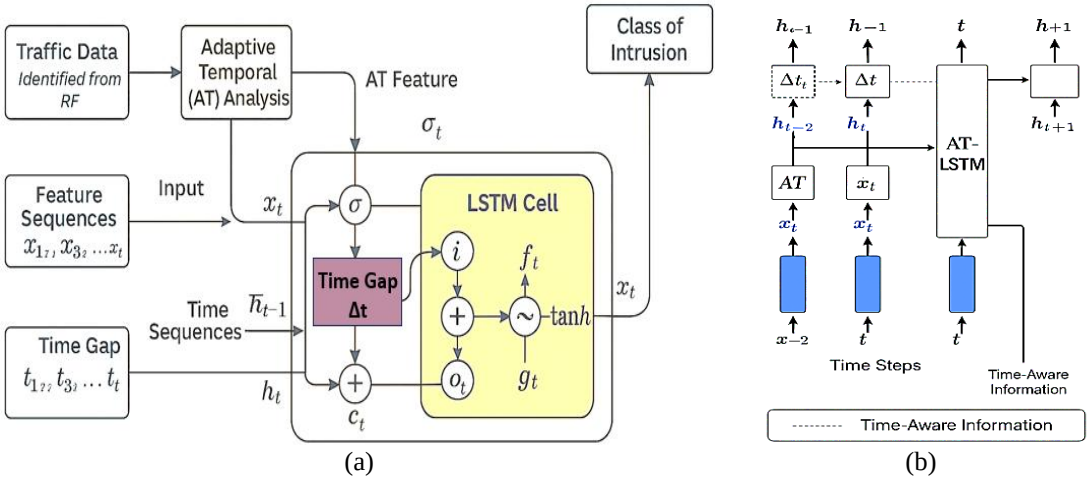


Figure 3. The workflow architecture of the AT-LSTM with; (a) main workflow and (b) internel architecture of the proposed AT-LSTM

As shown in the Figure 3, at each time step t, the AT-LSTM model considers two inputs: i) the traffic feature vector x_t and corresponding to the time gap Δt_t i.e., elapsed time between two consecutive network traffic events, which quantifies how much time has passed between two such events. The Δt is

computed using a numerical formula as in (1). Afterwards, the input original feature vector x_t is fused with Δt_t to compute a time-aware context vector, numerically expressed in (2).

$$\Delta t_t = t_t - t_{t-1} \quad (1)$$

$$\tilde{x}_t = f(x_t, \Delta t_t) \quad (2)$$

The obtained time-aware feature vector $\tilde{x}_t$ is then used to update the AT-LSTM states, where its internal gates are modified to incorporate the temporal decay, so that it can allow the network to discount outdated information when the time gap is large. This process of temporal sensitivity ensures that recent patterns are given higher importance, thereby enhancing the ability of the model to capture time-dependent behaviours in network traffic. The updated LSTM gate equations are defined as (3)-(8):

$$i_t = \sigma(W_i \times \tilde{x}_t + U_i \times h_{t-1} + b_i) \quad (3)$$

$$f_t = \sigma\left(W_f \times \tilde{x}_t + U_f \times h_{t-1} + b_f + \gamma \times \Delta t_t\right) \quad (4)$$

$$o_t = \sigma(W_o \times \tilde{x}_t + U_o \times h_{t-1} + b_o) \quad (5)$$

$$g_t = tanh(W_c \times \tilde{x}_t + U_c \times h_{t-1} + b_c) \quad (6)$$

$$c_t = f_t \odot c_{t-1} + i_t \odot g_t \quad (7)$$

$$h_t = o_t \odot \tanh(c_t) \quad (8)$$

Where, i_t, f_t, o_t are the input, forget, and output gates respectively, g_t is the candidate memory, c_t is the memory cell, and h_t is the hidden state. The associated learnable parameters (weights) are denoted as W and U, b denotes bias vectors, and γ is a learnable decay parameter controlling temporal relevance and σ is the sigmoid activation function for performing non-linear operation in learning sequential dependencies by the LSTM units. The model here dynamically attenuates the influence of outdated patterns by discounting hidden states associated with large Δt, and at the same time, it prioritizes the more recent events. This mechanism helps the model to detect asynchronous, multi-stage, or complex intrusion patterns that are often irregular at different time intervals. The final hidden state h_t is passed through a fully connected output layer with SoftMax activation to yield the predicted class of intrusion.

3. RESULT

The proposed multi-level intrusion detection framework is developed and executed using Python 3.9 with Tenforflow on a Windows system with an Intel Core i7 processor, 16 GB RAM, and an NVIDIA GPU (4 GB VRAM) to ensure efficient training and inference performance. The configuration details of the proposed multi-level security framework are highlighted in Table 2. The performance evaluation is done using standard classification metrics such as accuracy, precision, recall, and F1-score, along with confusion matrix analysis.

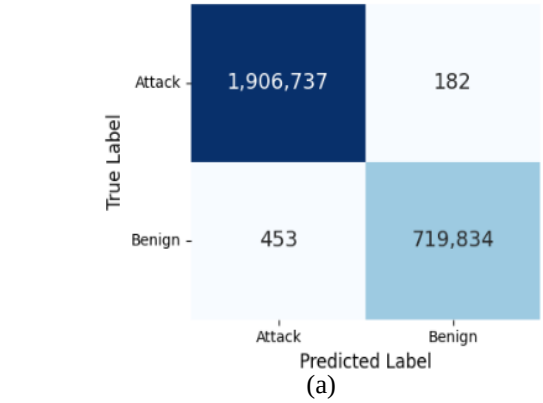
Table 2. Illustrates configuration details of the proposed multi-level security model

Module	Component	Parameter
Anomaly detection	Model type	RF
	Number of trees; splitting criterion; bootstrap sampling; and random state	100; Gini impurity; and enabled; 42
	Output type	Binary classification (benign vs. attack)
Intrusion classification	Model type	AT-LSTM
	Input features and input shape	15 selected; (batch size, time steps, and 16)
	LSTM units; activation; and recurrent activation	128; *tanh;* and *sigmoid*
	Dropout rate; dense units; and dense activation	0.3; 64; and *ReLU*
	Output units and output activation	10 (attack including normal) and *Softmax*
	Optimizer; learning rate; and loss function	Adam; 0.001; and categorical crossentropy
	Batch size; epochs; and validation split	512; 50; and 10%

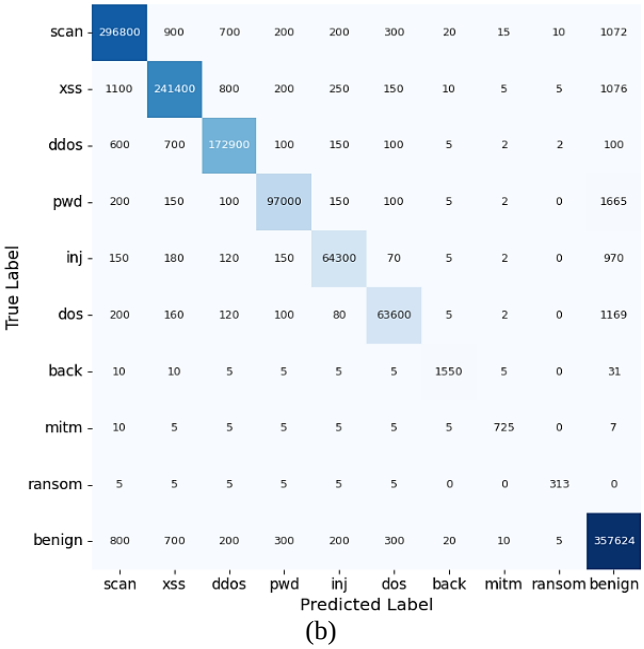
Figure 4 presents the confusion matrices of the proposed multi-level security framework based on AT-LSTM, where Figure 4(a) displays the performance of the binary anomaly detection task and Figure 4(b)

illustrates the results for the multiclass intrusion classification. It can also be seen in the case of the binary anomaly detection task (Figure 4(b)) that the model has achieved outstanding performance. The analysis of the confusion matrix reveals that the model has achieved high performance, where out of a total of 2,627,206 samples, the model correctly identifies 1,906,737 attack samples (true positives) and 719,834 benign samples (true negatives) and only 182 attack samples are misclassified as benign (false negatives), and 453 benign samples are misclassified as attacks (false positives).

The overall classification accuracy was found to be 99.974%, with a precision of 99.976%, a recall of 99.990% and the F1-score of 99.983%. The result shows that the RF model has extremely low false positive and false negative rates, which highlights the high sensitivity and specificity of the model for anomaly detection. On the other hand, in the multiclass intrusion classification task (Figure 4(b)), it can be observed that the proposed AT-LSTM model demonstrated a strong classification capability for all 10 categories, even for rare attacks such as ransomware and MITM. A detailed evaluation of class-wise precision, recall and F1-score metrics is presented in Table 3, where the effectiveness of the proposed system to handle imbalanced and complex intrusion types is extensively discussed.



(a)



(b)

Figure 4. Confusion matrix for; (a) binary anomaly detection and (b) multiclass intrusion classification task

Table 3 presents the performance metrics of the AT-LSTM model for multi-class intrusion classification across 10 traffic categories. The model consistently achieves high precision and recall (>97%) for major categories such as scanning, XSS, and DDoS, with an overall accuracy of 99.04%. Even for minority categories such as ransomware and MitM, the model maintains strong F1-scores above 0.95, indicating strong generalization. The highest precision (99.50%), recall (99.70%), and AUC (99.9%) are achieved for the benign class, thereby indicating the low false-positive rate of the model in real traffic.

Table 3. The quantified classification outcomes for multiclass intrusion classification

Attack type	Precision	Recall	F1-score	AUC	Support
Scanning	0.9915	0.9897	0.9906	0.998	300,217
XSS	0.9878	0.9853	0.9865	0.997	244,996
DDoS	0.9912	0.9899	0.9905	0.998	174,659
Password	0.9832	0.9760	0.9796	0.996	99,372
Injection	0.9850	0.9735	0.9792	0.995	66,047
DoS	0.9874	0.9720	0.9796	0.996	65,436
Backdoor	0.9812	0.9532	0.9670	0.994	1,626
MITM	0.9754	0.9398	0.9572	0.991	772
Ransomware	0.9843	0.9343	0.9587	0.990	335
Benign	0.9950	0.9970	0.9960	0.999	360,159
Overall accuracy:			0.9904		

3.1. Outcome discussion

Table 4 provides a comparative evaluation of the proposed multi-level intrusion detection system against recent methods on the NF-ToN-IoT-V2 dataset. Our model achieves 99% accuracy and F1-score in both binary and multiclass tasks using only 15 selected features. The method by Li *et al*. [25] obtained 98.8% accuracy using a pre-trained DL+generative adversarial network (GAN) model, but required all features, thereby increasing computational cost. On the other hand, our system achieves better accuracy with reduced feature space.

Table 4. Comparative analysis with recent existing works on the NF-ToN-IoT-V2 dataset

Reference	Method	Classification task	Accuracy	F1-score
[25]	Pre-trained DL+GAN	Multiclass	98.8%	98.8%
[26]	GNN	Binary	96.6	97.9
[27]	FSLLM	Multiclass	95.8	95.8
[28]	Stacked classifier and adaptive thresholding	Binary	93.715%	95.145%
[29]	AE-DTNN	Multiclass	98.30	98.30
[30]	MAS-LSTM	Binary	95.22	96.78
Proposed	Binary	Binary	99	99
Proposed	Multiclass	Multiclass	99	99

Similarly, Wang *et al*. [26] applied a GNN with 96.6% accuracy but also used all features, which limits their methodology's scalability. Ma *et al*. [27] used only 7 features but achieved lower accuracy (95.8%), which shows that minimal features alone aren't sufficient without robust modelling, and the work by Kamal *et al*. [29] and Qin *et al*. [30] also used all features, and achievd 98.3% and 95.2% accuracy respectively, but at higher model complexity. The proposed RF+AT-LSTM framework offers a better trade-off between performance and computational efficiency, which suggests that it can be suitable for real-time deployment under resource-constrained IoT deployments. In order to validate the proposed system design, Table 5 presents an Ablation study considering different ML classifiers and DL models along with hyperparameters such as batch size (bs), learning rate (lr) and Adam and RMSProp optimizers.

Table 5. Ablation study

Model	Task	Features	Accuracy	Response time (ms)	Remarks
NB	Binary	15	94.8%	9.5	Simple, fast, and lower accuracy
KNN	Binary	15	96.7%	17.9	Higher latency
SVM	Binary	15	97.8%	13.4	Better generalization
CNN	Multiclass	All	97.6%	25.3	Complex and high latency
GRU	Multiclass	20	98.0%	22.7	Effective for sequences
LSTM	Multiclass	20	98.2%	24.1	Long-range temporal capture
AT-GRU	Multiclass	15	98.6%	20.2	Time-aware GRU
AT-LSTM	Multiclass	20	98.8%	8.9	Slightly lower accuracy
AT-LSTM	Multiclass	All	98.6%	10.1	Higher compute and no gain
AT-LSTM (proposed)	Multiclass	15	99.0%	7.9	Best accuracy+speed
AT-LSTM (bs=32, lr=0.001, and Adam)	Multiclass	15	99.0	7.9	Optimal configuration
AT-LSTM (bs=16, lr=0.001, and Adam)	Multiclass	15	98.7	9.2	Smaller batch and slightly slower
AT-LSTM (bs=64, lr=0.001, and Adam)	Multiclass	15	98.6	6.5	Faster and slight drop in accuracy
AT-LSTM (bs=32, lr=0.005, and Adam)	Multiclass	15	98.4	7.9	Higher LR and less stable
AT-LSTM (bs=32, lr=0.001, and RMSProp)	Multiclass	15	98.8	8.3	Different optimizer

3.2. Scope and limitation

The proposed system offers multi-level protection with low response time by utilizing RF for early anomaly filtering, which reduces data load before deep analysis by AT-LSTM. Its efficiency and high accuracy make it suitable for real-time IoT/industrial internet of things (IIoT) deployment scenarios. However, the current design focuses on offline training; the future work will explore online learning, adaptive feature updates, and a data compression scheme in the communication layer or in the message queuing telemetry transport (MQTT) protocol to ensure a more efficient approach in integration with edge-computing platforms to enhance its adaptiveness under evolving threat patterns.

4. CONCLUSION

This paper has presented a hybrid and multi-level IDS with a RF classifier and adaptive time-aware LSTM to enhance the security of IoT applications against unknown, dynamic, and multi-vector cyber threats. The RF-based anomaly detector acts as an efficient primary filter to block adversarial traffic, and the AT-LSTM model performs secondary classification of known intrusions. The proposed multi-level approach ensures comprehensive protection by preventing complex threats at the initial stage and enables a detailed threat categorisation for informed response. The experimental evaluation on the NF-ToN-IoT-V2 dataset demonstrates high accuracy and low latency, thereby highlighting the suitability of the proposed security framework for real-time deployment with support of adaptability in diverse IoT/IIoT environments. The future work will explore lightweight DL models and online learning techniques to enhance real-time performance and resilience under high traffic and evolving attack scenarios.

FUNDING INFORMATION

The authors state no funding is involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Gauri Sameer Rapate	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Ambuja Krishnappa		✓				✓		✓	✓	✓	✓			
Sarala Duggonahalli Veeresh	✓		✓	✓			✓			✓	✓		✓	
Karanam Sunil Kumar	✓			✓	✓		✓	✓		✓	✓	✓	✓	
Bellary Kursheed		✓	✓	✓		✓	✓			✓	✓	✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] A. A. Laghari, H. Li, A. A. Khan, Y. Shoulin, S. Karim, and M. A. K. Khani, "Internet of Things (IoT) applications security trends and challenges," *Discover Internet of Things*, vol. 4, no. 1, pp. 1-22, 2024, doi: 10.1007/s43926-024-00090-5.

[2] A. Ghaffari, N. Jelodari, S. Pouralish, N. Derakhshanfard, and B. Arasteh, "Securing internet of things using machine and deep learning methods: a survey," *Cluster Computing*, vol. 27, no. 7, pp. 9065–9089, 2024, doi: 10.1007/s10586-024-04509-0.

[3] Y. B. Abushark, S. Hassan, and A. I. Khan, "Optimized AdaBoost support vector machine-based encryption for securing IoT-cloud healthcare data," *Sensors*, vol. 25, no. 3, p. 731, 2025, doi: 10.3390/s25030731.
[4] K. M. Abuali, L. Nissirat, and A. Al-Samawi, "Advancing network security with AI: SVM-based deep learning for intrusion detection," *Sensors*, vol. 23, no. 21, p. 8959, 2023, doi: 10.3390/s23218959.
[5] M. W. A. Ashraf *et al.*, "A hybrid approach using support vector machine rule-based system: detecting cyber threats in internet of things," *Scientific Reports*, vol. 14, no. 1, p. 27058, 2024, doi: 10.1038/s41598-024-78976-1.
[6] A. K. Pandey, R. Saxena, A. Awasthi, and M. P. Sunil, "Privacy preserved data sharing using blockchain and support vector machine for industrial IOT applications," *Measurement: Sensors*, vol. 29, pp. 1-7, 2023, doi: 10.1016/j.measen.2023.100891.
[7] H. Babbar, S. Rani, D. K. Sah, S. A. AlQahtani, and A. K. Bashir, "Detection of Android malware in the internet of things through the K-Nearest Neighbor algorithm," *Sensors*, vol. 23, no. 16, pp. 1-17, 2023, doi: 10.3390/s23167256.
[8] P. R. Agbedanu *et al.*, "A scalable approach to Internet of Things and Industrial Internet of Things security: Evaluating adaptive self-adjusting memory K-nearest neighbor for zero-day attack detection," *Sensors*, vol. 25, no. 1, p. 216, 2025, doi: 10.3390/s25010216.
[9] H. H. Nuha, S. A. Mugitama, A. A. Absa, and Sutiyo, "K-nearest neighbors with third-order distance for flooding attack classification in optical burst switching networks," *IoT*, vol. 6, no. 1, p. 1, 2024, doi: 10.3390/iot6010001.
[10] K. Kaushik *et al.*, "Multinomial naive Bayesian classifier framework for systematic analysis of smart IoT devices," *Sensors*, vol. 22, no. 19, p. 7318, 2022, doi: 10.3390/s22197318.
[11] V. Prakash *et al.*, "A secure framework for the Internet of Things anomalies using machine learning," *Discover Internet of Things*, vol. 4, no. 1, 2024, doi: 10.1007/s43926-024-00088-z.
[12] R. Majeed, N. A. Abdullah, and M. F. Mushtaq, "IoT-based Cyber-security of Drones using the Naïve Bayes Algorithm," *(IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 12, no. 7, pp. 1-6, 2021, doi: 10.14569/IJACSA.2021.0120748.
[13] A. Deshmukh and K. Ravulakollu, "An efficient CNN-based intrusion detection system for IoT: Use case towards cybersecurity," *Technologies*, vol. 12, no. 10, p. 203, 2024, doi: 10.3390/technologies12100203.
[14] B. A. Alabsi, M. Anbar, and S. D. A. Rihan, "CNN-CNN: Dual convolutional neural network approach for feature selection and attack detection on Internet of Things networks," *Sensors*, vol. 23, no. 14, pp. 1-17, 2023, doi: 10.3390/s23146507.
[15] B. I. Hairab, M. S. Elsayed, A. D. Jurcut, and M. A. Azer, "Anomaly Detection Based on CNN and Regularization Techniques Against Zero-Day Attacks in IoT Networks," *IEEE Access*, vol. 10, pp. 98427-98440, 2022, doi: 10.1109/ACCESS.2022.3206367.
[16] O. D. Okey *et al.*, "Transfer learning approach to IDS on cloud IoT devices using optimized CNN," *IEEE Access*, vol. 11, pp. 1023–1038, 2023, doi: 10.1109/ACCESS.2022.3233775.
[17] A. Sagu *et al.*, "Advances to IoT security using a GRU-CNN deep learning model trained on SUCMO algorithm," *Scientific Reports*, vol. 15, no. 1, p. 16485, 2025, doi: 10.1038/s41598-025-99574-9.
[18] A. A. Alshdadi *et al.*, "Enhanced IoT Security for DDOS Attack Detection: Split Attention-Based ResNeXt-GRU Ensembler Approach," *IEEE Access*, vol. 12, pp. 112368–112380, 2024, doi: 10.1109/ACCESS.2024.3443067.
[19] J. Bi, K. Xu, H. Yuan, J. Zhang, and M. Zhou, "Network Attack Prediction with Hybrid Temporal Convolutional Network and Bidirectional GRU," in *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 12619-12630, Apr. 2024, doi: 10.1109/JIOT.2023.3334912.
[20] G. ALMahadin *et al.*, "VANET Network Traffic Anomaly Detection Using GRU-Based Deep Learning Model," in *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 4548-4555, Feb. 2024, doi: 10.1109/TCE.2023.3326384.
[21] A. Gueriani, H. Kheddar, and A. C. Mazari, "Enhancing IoT Security with CNN and LSTM-Based Intrusion Detection Systems," in *2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, EL OUED, Algeria, 2024, pp. 1-7, doi: 10.1109/PAIS62114.2024.10541178.
[22] H. C. Altunay and Z. Albayrak, "A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks," *Engineering Science and Technology, an International Journal*, vol. 38, p. 101322, 2023, doi: 10.1016/j.jestch.2022.101322.
[23] P. Sinha *et al.*, "A high performance hybrid LSTM CNN secure architecture for IoT environments using deep learning," *Scientific Reports*, vol. 15, no. 1, p. 9684, 2025, doi: 10.1038/s41598-025-94500-5.
[24] UQ eSpace," Edu.au. [Online]. Available: https://espace.library.uq.edu.au/view/UQ:38a2d07. (Accessed: Sept. 10, 2025).
[25] F. Li, H. Shen, J. Mai, T. Wang, Y. Dai, and X. Miao, "Pre-trained language model-enhanced conditional generative adversarial networks for intrusion detection," *Peer-to-Peer Networking and Applications*, vol. 17, no. 1, pp. 227–245, 2024, doi: 10.1007/s12083-023-01595-6.
[26] Y. Wang *et al.*, "N-STGAT: Spatio-temporal graph neural network based network intrusion detection for near-Earth remote sensing," *Remote Sensing*, vol. 15, no. 14, p. 3611, 2023, doi: 10.3390/rs15143611.
[27] H. Ma, W. Zhang, D. Zhang, and B. Chen, "An IoT intrusion detection framework based on feature selection and large language models fine-tuning," *Scientific Reports*, vol. 15, no. 1, p. 21158, 2025, doi: 10.1038/s41598-025-08905-3.
[28] D. Krishnan and P. Shrinath, "Robust botnet detection approach for known and unknown attacks in IoT networks using stacked multi-classifier and adaptive thresholding," *Arabian Journal for Science and Engineering*, vol. 49, no. 9, pp. 12561–12577, 2024, doi: 10.1007/s13369-024-08742-y.
[29] H. Kamal and M. Mashaly, "AE-DTNN: Autoencoder–Dense–Transformer Neural Network model for efficient anomaly-based intrusion detection systems," *Machine Learning and Knowledge Extraction*, vol. 7, no. 3, p. 78, Aug. 2025, doi: 10.3390/make7030078.
[30] Z. Qin, Q. Luo, X. Nong, X. Chen, H. Zhang, and C. U. I. Wong, "MAS-LSTM: A Multi-Agent LSTM-Based Approach for Scalable Anomaly Detection in IIoT Networks," *Processes*, vol. 13, no. 3, p. 753, 2025, doi: 10.3390/pr13030753.

BIOGRAPHIES OF AUTHORS

Dr. Gauri Sameer Rapate is currently working as Associate Professor in Computer Science and Engineering department at PES University, Bangalore. She earned her Ph.D. in Computer Science and Engineering from Visvesvaraya Technological University, Belagavi, in 2024. She received her Masters of Engineering from Anna University, Coimbatore, in 2010, Bachelor of Engineering from Nagpur University, Nagpur, in 2005. She has 17 years of academic experience. She has published more than 10+ research articles in International Journal and Conferences proceedings. Her research interest includes IoT, networking, cyber security, and machine learning. She has actively contributed to research and academic development through publications and collaborative projects. She is passionate about integrating emerging technologies into practical applications and fostering innovation through interdisciplinary research. She can be contacted at email: gauri.rapate@pes.edu.

Ms. Ambuja Krishnappa is currently working as Assistant Professor in Computer Science and Engineering department at BMS College of Engineering (BMSCE), Bangalore. She received her Masters of Technology (M.Tech.) degree in Computer Science and Engineering from BNMIT, Visvesvaraya Technological University (VTU), Belagavi, in 2018, and Bachelor of Engineering (B.E.) degree in Computer Science and Engineering from CBIT, VTU, Belagavi, in 2016. She has 5 years of academic experience. Also, she is pursuing her Ph.D. degree from VTU Belagavi. Her research interest includes image processing, artificial intelligence, and machine learning. She can be contacted at email: ambuja.cse@bmsce.ac.in.

Dr. Sarala Duggonahalli Veeresh is currently serving as Assistant Professor in Department of Computer Science and Engineering, BMS College of Engineering, Bangalore. She earned her Ph.D. in Computer Science and Engineering from Visvesvaraya Technological University (VTU), Belagavi. She received her Masters of Technology (M.Tech.) degree in the field of Computer Science and Engineering from VTU, Belagavi in 2012 and Bachelor of Engineering (B.E.) degree in the field of Computer Science and Engineering from VTU, Belagavi in 2010. She has contributed to the academic community by publishing many international Journals/Conferences. Her area of interest includes computer vision, machine learning, and deep learning. She can be contacted at email: saraladv.cse@bmsce.ac.in.

Dr. Karanam Sunil Kumar is currently serving as an Assistant Professor at RV College of Engineering. He completed his Bachelor of Engineering (B.E.), Master of Technology (M.Tech.), and Ph.D. from Visvesvaraya Technological University (VTU), Belagavi. With a career spanning 16 years, he has a wealth of experience in his field. He has contributed to the academic community by publishing six journals, which have been indexed in top-tier categories ranging from Q1 to Q4. His research interests are computer vision, machine learning, big data, and deep learning. He can be contacted at email: ksunilkumar@rvce.edu.in.

Dr. Bellary Kursheed is currently serving as Associate Professor in Department of Computer Science and Engineering (Artificial Intelligence and Machine Learning), Don Bosco Institute of Technology, Bangalore. She earned her Ph.D. in Electronics and Communication Engineering from Visvesvaraya Technological University, Belagavi. She received her M.Tech. degree in the field of Computer Networks from Visveswaraya Technological University, Belagavi. Experienced as Academician from 21 years. She has contributed to the academic community by publishing many national and international Journals/Conferences. Had received 3 Lakhs funds from Government of Karnataka Vision Group on Science and Technology for the project “RFID based vehicle antitheft and automatic toll collection system” and received fund from KSTA and KSCST three times. Area of interest includes wireless communication, multimedia communication, cognitive radio, and micro controllers. She can be contacted at email: bkursheedofficial@gmail.com.