International Journal of Engineering Trends and Technology
ISSN: 2231-5381/ https://doi.org/10.14445/22315381/IJETT-V74I3P107
Volume 74 Issue 3, 89-103, March 2026

Original Article

A Multi-Source Deep Learning and Swarm Intelligence Framework for Secure and Interpretable IoT Forensic Analysis

Mashiya Afroze F[1] , V. Poornima[2]

[1,2]*Department of Computer Science, Vel's Institute of Science Technology and Advanced Studies, Chennai, Tamil Nadu, India.*

[1]*Corresponding Author : mashiya2408@gmail.com*

Received: 19 November 2025 Revised: 22 January 2026 Accepted: 29 January 2026 Published: 28 March 2026

Abstract *- With the rapid proliferation of Internet-of-Things(IoT) devices in diverse domains, securing IoT ecosystems has risen to an urgent problem because of the heterogeneity and vulnerabilities to cyber-attacks associated with these devices. Typical security and forensic models are unable to comprehend the changed, complex device behaviors and multi-source evidence, leading to mistimed and/or inaccurate indicators of threat. This study proposes a new multi-source IoT forensic framework that includes Deep Learning (DL) and swarm intelligence that models device behaviors, detects anomalies, and provides actionable forensic analysis through the thoughtful consideration of multi-source evidence. The framework has a hybrid CNN-LSTM(Convolutional Neural Network-Long Short-term Memory) architecture to extract spatial-temporal features, where both deep learning and swarm intelligence optimization strategies are applied as hyperparameter tuning and feature selection, along with multi-modal evidence fusion to correlate data across several sources of evidence. Experiments simulating attacks using the TON-IoT data set show its superior performance, with an accuracy of 99.62%, precision of 99.41%, recall of 99.83%, F1-Score of 99.62%, MCC of 0.996, and AUC-ROC of 0.998. The findings posit that our framework demonstrated more ability versus baselines, including Random Forest(RF), LSTM, and Autoencoder(AE). The research findings assert that our framework is reliable, interpretable, and efficient for conducting forensic analysis, which can expedite cybersecurity measures through a timely, equitable, and reliable method for IoT analysis processing.*

Keywords *- IoT security, Forensic framework, Anomaly detection, CNN-LSTM, Swarm Intelligence Optimization, Multi-modal evidence fusion, Deep Learning, TON-IoT dataset.*

1. Introduction

The IoT has become a revolutionary paradigm in the computing and industrial ecosystems today by facilitating ubiquitous connectivity among a massive number of devices, sensors, and cyber-physical systems. Through constant data collection, automatic operation, and real-time analysis, the IoT technologies have facilitated intelligent decision-making for various fields of application, such as smart home, healthcare monitoring, industrial automation, transportation, and energy management systems [1]. The speed at which IoT deployments have taken off has had a tremendous impact on system efficiency and automation; however, this has had a corollary effect of expanding the attack surface of modern networks. Despite their functional benefits, IoT devices are inherently limited in their computing power and memory capacity and have limited security mechanisms built in. These constraints make such devices extremely vulnerable to a wide range of cyber threats, such as propagation of malware, unauthorized access, tampering of data, coordinated botnet attacks, etc. Furthermore, IoT ecosystem heterogeneity, defined by varying hardware architectures, operating systems, communication protocols, and deployment environments, makes threat detection, attribution, and forensic investigation processes difficult. Consequently, the need for cutting-edge IoT-specific cybersecurity and forensic solutions that are able to perform effectively under these constraints and deliver dependable and interpretable security intelligence is expanding [2].

Existing IoT security and forensic solutions rely mostly on traditional network intrusion detection systems, signature-based detection mechanisms, or on traditional ML algorithms like RF[3], Support Vector Machines (SVM) [4], and Autoencoders (AEs) [5]. While these approaches show respectable performance in the controlled environment, due to the high-dimensionality of IoT data, the temporal evolution of attacks, and strong temporal dependencies, they often find it difficult to generalize their work in real-world IoT environments. In particular, the rule-based and shallow learning models have limitations in their capacity to model

complex spatial-temporal correlations found in IoT network traffic, log of device behavior, and firmware-level evidence.

Based on recent developments of DL, such as CNNs [6] and LSTMs [7] networks, there have been successful efforts to model spatial and temporal patterns in IoT data streams. CNN-based architectures are good at extracting discriminative features from the high-dimensional traffic representations, and LSTM networks are good at capturing long-term temporal dependencies in sequential data. However, the effectiveness of DL-based IoT security models is susceptible to the hyperparameter choice, feature representation, and training stability. Moreover, most current DL-based solutions only work with one type of data, for example, network traffic only, which means that they miss the ability to use other complementary forensic evidence from firmware metadata, system logs, and behavioral traces at a device level.

Another new area of research focuses on the application of swarm intelligence and meta-heuristic optimization techniques to improve the model performance, through the optimization of hyperparameters, feature subsets, and decision thresholds. Although swarm-based approaches have shown better detection accuracy and convergence properties for single security tasks, the interconnection of deep learning architectures and swarm-based approaches, for end-to-end IoT forensic pipelines, is largely unexplored [8]. In particular, there is a significant gap in providing unified frameworks for collaborative utilization of deep learning for spatial-temporal modeling, swarm intelligence for optimization, and multi-modal evidence fusion for forensic interpretability.

1.1. Research Problem and Gap Identification

The fundamental research problem that was addressed in this research can be categorised into the following problems: existing IoT security systems are limited in their ability to effectively analyse heterogeneous, multi-source data while capturing complex spatial-temporal dependencies and generating actionable forensic insights. Current approaches generally have one or more of the following drawbacks: (i) use of single modality data sources, (ii) poor deep learning configurations because of manual or heuristic tuning, (iii) poor detectability, (iv) lack of comprehensive forensic evidence correlations. Therefore, a significant gap in research exists regarding the development of an optimized, multi-source IoT forensics framework that incorporates deep learning and swarm intelligence optimization and fusion of multi-modal evidence.

1.2. Novelty and Contributions

To overcome the found gap, this study proposes a comprehensive multi-source IoT forensic framework using a hybrid CNN-LSTM DL architecture, swarm intelligence-based optimization, and multi-modal evidence fusion. In contrast to the current state-of-the-art methods, which only target isolated detection tasks or single data streams, the proposed framework allows for holistic anomaly detection, classification, and forensic reporting in heterogeneous IoT environments. The following are the main contributions of this work:

- A hybrid CNN-LSTM-based Anomaly detection model optimized with the swarm intelligence technique to balance false positives with the accurate modelling of the spatial-temporal IoT device behaviour.
- A multi-modal forensic evidence fusion approach combining network traffic features, firmware-level information, and device log data to get complete, explainable, and legally relevant forensic information.
- Extensive experimental evaluation based on standard performance metrics such as accuracy, precision, recall, F1-score, Matthews Correlation Coefficient (MCC), and AUC-ROC with systematic comparison with state-of-the-art IoT security and forensic methods.

The study is structured in such a way that it allows a clear and logical presentation of the research. Section 2 provides a review of the associated works of IoT security, behavior modeling using deep learning, and swarm intelligence. IoT device behavior modeling, swarm intelligence-based anomaly optimization, multi-modal evidence fusion, and threat classification with forensic reports are detailed in Section 3 of the methodology. Experimental results and dataset description, performance stability analyses, and general discussion are given in Section 4, followed by a conclusion, and future research directions are then presented in Section 5.

2. Literature Review

Research has also been directed towards using AI, ML, and DL for IoT security and anomaly detection. Alsalman et al. propose FusionNet, an ensemble model using Random Forest(RF), KNN, SVM, and MLP for improved anomaly detection. The model shows better accuracy (98.5% and 99.5%) on datasets, superior to that of traditional techniques, and shows a huge potential in real-world applications for IoT security and anomaly detection [9]. Chandrasekaran et al. (2024) present an optimal DL approach based on the combination of ACO and RNN in IoT threat detection. Using the BOUN DDoS dataset and TCP-based data extraction, the method exhibits better quality compared to the traditional DL models in the accurate classification and detection of DDoS and normal network traffic [10]. Mei et al. (2024) Network forensic attribution of Advanced Persistent Threat (APT) Attacks using a deep learning based framework. The framework applies encryption for data integrity and feature filtering, and a Multi-Layer Perceptual Deep Neural Network (MLP-DNN) hyper-parameter tuning, which results in excellent performance for detecting and tracing network attacks, based on the UNSW-NB15 dataset [11]. Menon et al. (2025) give an extensive survey about AI-powered IoT (AIoT), which focuses on the integration of AI, ML, and DL

for better security, efficiency, and smart applications. The paper focuses on anomaly detection, authentication, DDoS mitigation, and network optimization in AIoT and discusses the use of emerging technologies such as blockchain, 6G, federated learning, and hyperdimensional computing for future IoT innovations [12]. Balega et al. (2024) deal with ML-based anomaly detection in IoT security by using XGBoost, SVM, and Deep CNN models on several datasets (IoT-23, NSL-KDD, TON_IoT). Their study shows that XGBoost has a better accuracy (99.98%) and performance with computational efficiency than SVM and DCNN in both detection performance and training speed [13]. Farea et al. (2024) present an intelligent IoT security framework, AI2AI, an advanced AI-based system that incorporates the Genetic Algorithm-Anomaly Detection and Prevention Deep Neural Network (GAADPSDNN). GAADPSDNN has been tested on the WUSTL-IIoT and Edge-IIoT datasets, and the experiment results show that GAADPSDNN gets a higher accuracy of 98.18% than the other typical DNNs and optimization-based models with the cost of enhancement of efficiency and decrease of computational overhead [14]. Bhardwaj et al. (2024) propose an Intelligent Attack Graph-based Forensic Model for IoT Networks: Integrating Virtual Node-Based Threat Detection to Contain Malware Propagation and Accelerate Recovery. We find that the detection rate of the proposed Vulnerable Attack Path Predictor (VAPP) model is 98.48% and authentication accuracy is 85%, which are better than the traditional ML-based VAPP approaches in IoT security and resilience [15]. Table 1 summarizes the notable studies in IoT security and forensic analysis.

Table 1. Recent IoT security and forensic methods with strengths and limitations

Author et al. (Year)	Method	Strengths	Limitations
Alsalman et al. (2024)	FusionNet: Ensemble of Random Forest, KNN, SVM, MLP	High accuracy (98.5–99.5%), superior to traditional techniques, strong potential for real-world IoT anomaly detection	Ensemble models may increase computational complexity; they are resource-intensive for large-scale IoT deployments
Chandrasekaran et al. (2024)	ACO + RNN for IoT threat detection using BOUN DDoS dataset	Improved classification of DDoS and normal traffic; optimal deep learning approach	Focused on TCP traffic; may require fine-tuning for other IoT protocols
Mei et al. (2024)	MLP-DNN with encryption and feature filtering for APT network forensic attribution (UNSW-NB15 dataset)	Excellent performance for detecting and tracing network attacks; data integrity maintained	Dataset-specific tuning; performance may vary in heterogeneous IoT environments
Menon et al. (2025)	AIoT survey integrating AI, ML, DL for IoT security and smart applications	Comprehensive review; highlights emerging technologies like blockchain, 6G, federated learning	Survey-based; no experimental validation; mostly conceptual insights
Balega et al. (2024)	XGBoost, SVM, Deep CNN on IoT-23, NSL-KDD, ToN-IoT	XGBoost achieves very high accuracy (99.98%) with computational efficiency, fast training	Limited evaluation on real-time streaming data; DCNN is less efficient
Farea et al. (2024)	AI framework: GAADPSDNN tested on WUSTL-IIoT & Edge-IIoT datasets	High accuracy (98.18%), reduced computational overhead, and efficient AI-based IoT security	May require specialized optimization tuning; dataset-dependent performance
Bhardwaj & Dave (2024)	Intelligent Attack Graph-based VAPP model for IoT	Detection rate 98.48%, authentication accuracy 85%; better malware containment and recovery	Moderate authentication accuracy; scalability in large IoT networks has not been fully tested

As shown by these studies, comprehensive IoT security using AI, ML, and DL models has made huge progress, but there are still a few limitations. Many approaches are based on benchmark data sets, which may not represent network variability in the real world; hence, generalisability may be limited. The computational demand of ensemble and deep models makes it difficult to deploy in resource-constrained IoT devices. Further, most of the frameworks are designed around accuracy without considering scalability, energy efficiency, and interpretability. In conclusion, the emerging IoT ecosystems are dynamic, which means few studies consider adversarial robustness or changing threat patterns in dynamic IoT ecosystems. Hence, in the future, lightweight, explainable, and adaptive models with the ability to maintain high performance in diverse IoT architectures and real-time operational environments should be the focus of future research.

3. Materials and Methods

The methodology described introduces a full-scale multi-source IoT forensic framework that leverages both deep learning and swarm intelligence. The framework in Figure 1 merges IoT data acquisition, data preprocessing, device behavior modeling, anomaly detection, multi-modal evidence fusion, and threat classification into a coherent process that obtains accurate, reliable, and interpretable forensic analysis, providing actionable insights into IoT security.

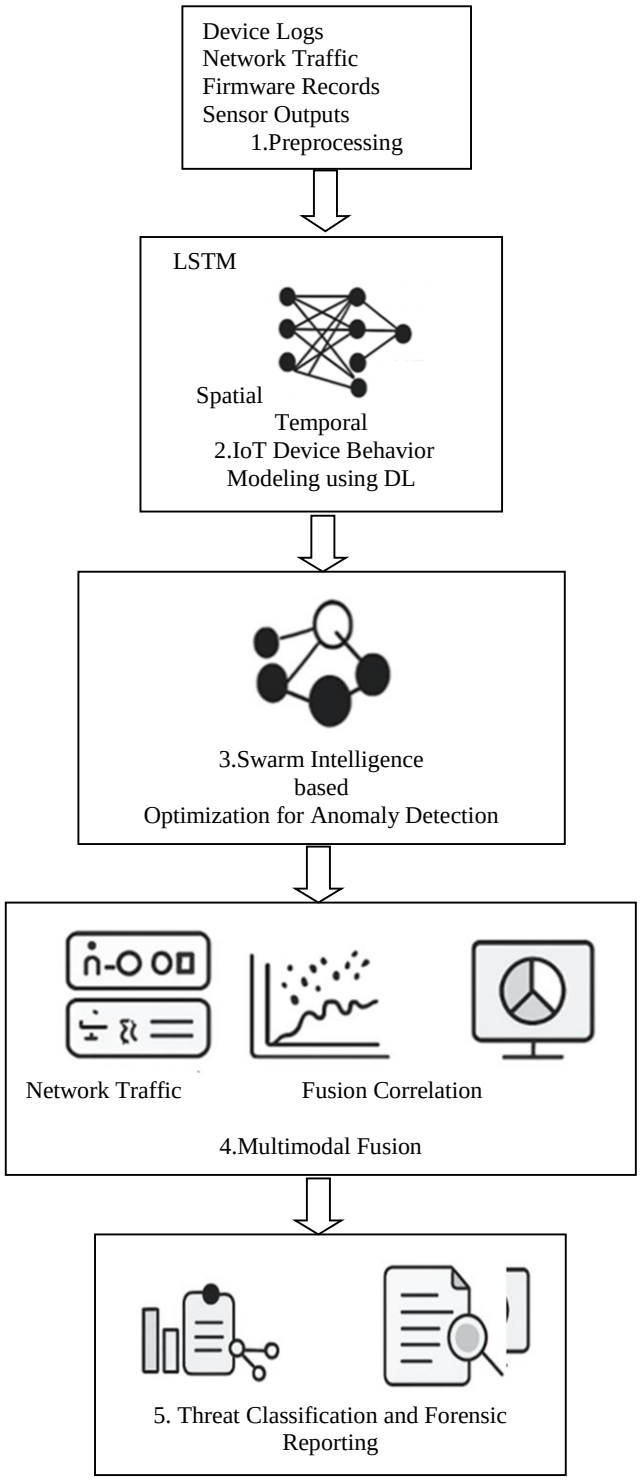


Fig. 1 Threat classification and forensic reporting

3.1. Multi-Source Data Acquisition and Preprocessing

The framework is initiated by acquiring heterogeneous IoT data from diverse sources, including device logs, network traffic, firmware logs, and sensor data. By acquiring multi-sourced data, a comprehensive representation of the IoT ecosystem is established, and helps to ascertain potential security vulnerabilities and anomalies from multiple angles. Data preprocessing operations, including normalization, denoising, and missing value imputation, are implemented for data integrity and consistency purposes [16]. Further, feature extraction and selection assist in reducing dimensionality while maintaining relevant forensic information. Let the IoT ecosystem contain N devices generating heterogeneous data streams: device logs (D_L) , network traffic (D_N), firmware logs(D_F) and the sensor data (D_s). The total multi-source dataset can be represented as follows.

$$X = \{ D_L, D_N, D_F, D_s \}\, D_i \in R^{n_i * m_i} \quad (1)$$

Where n_i is the number of samples and m_i is the number of features for source i. The preprocessing operations are given as follows

$$\text{Normalization } \tilde{X}_{ij} = \frac{X_{ij} - \mu_j}{\sigma_j} \quad (2)$$

$$\text{Denoising } \hat{X}_{ij} = f(X_i) \quad (3)$$

$$\text{Missing value Imputation } X_{ij} =$$

$$\{X_{ij} \ if\ observed \ \ \frac{1}{n_i} \sum_{k=1}^{n_i} \mathrm{X_{kj}} \ \ if\ missing \quad (4)$$

The feature Selection can be modeled as follows

$$X' = Select(X, F) \quad (5)$$

Where F is the set of relevant features, minimizing redundancy and maximizing information gain.

3.2. IoT Device Behavior Modeling Using Deep Learning

After undergoing preprocessing, DL models are utilized to extract complex behavioral patterns of IoT devices. The two models used in conjunction for capturing useful spatial and temporal features of the IoT data are CNNS, for monitoring device-specific signatures, and LSTM networks, for capturing sequential patterns signifying potential anomalous and malicious activity. With the development of a hybrid DL model architecture, anomaly detection and security breach detection of IoT devices can be performed robustly with meaningful, interpretable modeling of IoT device behavior. Let the preprocessed dataset be X'. The hybrid DL model combines CNN and LSTM. The CNN for spatial patterns.

$$H_{CNN} = F_{CNN}\,(X';\, \theta_{CMM}) \quad (6)$$

The LSTM for temporal sequences is given as follows,

$$H_{LSTM} = f_{LSTM}(\, H_{CNN}\, ;\, \theta_{LSTM}) \quad (7)$$

The hybrid representation for anomaly detection

$$\hat{y} = \sigma(W H_{LSTM} + b) \quad (8)$$

Where $\hat{y}$ is the predicted anomaly score, σ is a sigmoid or softmax, W, and b are trainable parameters [17].

3.3. Swarm Intelligence-Based Optimization for Anomaly Detection

A Swarm Intelligence Optimization Algorithm (e.g., SSOA) will be employed for hyperparameter tuning, optimization of weight distributions, and identification of relevant features to further improve the predictive capabilities of the DL model. Swarm intelligence is the model used to reproduce natural systems' collective behavior, enabling the model to converge quickly and efficiently to an optimal solution.

Swarm intelligence improves the accuracy of anomaly detection while minimizing false positives by dynamically selecting relevant features and tuning model parameters. Consequently, the outcomes of the deep learning model's predictions and the forensic analysis will be performed with greater accuracy and reliability. Let the DL model have hyperparameters $\Theta = \{ \theta_{CNN}, \theta_{LSTM}, W, b\}$. The optimization objective is to minimize a loss function $L(\Theta)$

$$\Theta^* = argL(\Theta) \quad (9)$$

Using a swarm intelligence optimization Algorithm (SSOA), particles P_k represent candidate solutions:

$$P_k(t+1) = P_k(t) + v_k(t+1) \quad (10)$$

$$v_k(t+1) = w v_k(t) + c_1 r_1 \left(p_k^{best} - P_k(t)\right) + c_2 r_2 (g^{best} - P_k(t)) \quad (11)$$

Where v_k is velocity, p_k^{best} is the particle's best position, g^{best} is the global best, w inertia weight, c_1, c_2 acceleration coefficients and r_1, r_2 random numbers [18]. The flowchart for the swarm intelligence method is shown in Figure 2.

3.4. Multi-Modal Evidence Fusion and Correlation

The framework subsequently channels evidence through a multi-modal fusion approach utilizing evidence from several distinct modalities. This stage makes use of an attention-based or weighted ensemble paradigm to amalgamate knowledge embedded in network traffic, device logs, and firmware data into a coherent forensic profile.

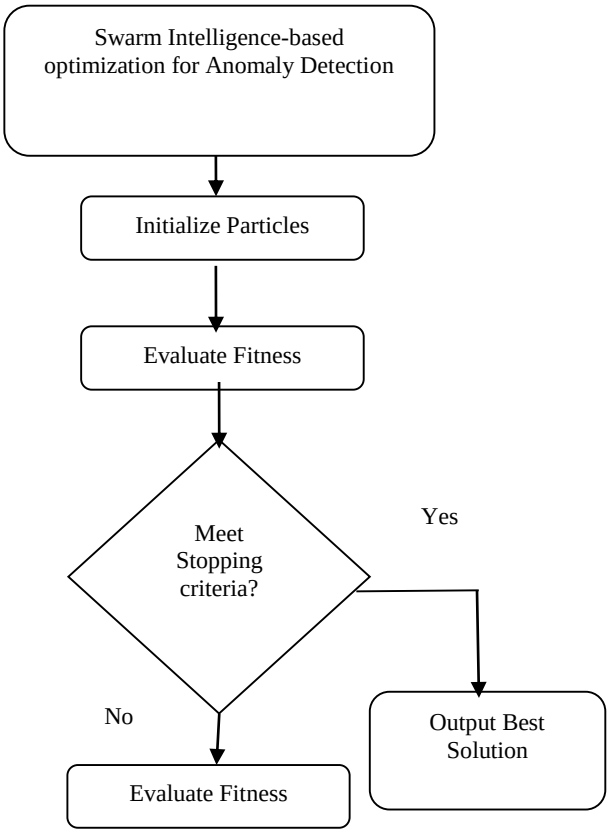


Fig. 2 Flowchart for swarm intelligence

Correlation analysis helps to identify relationships among various events and evidence sources, enabling them to reconstruct attack scenarios and/or track the source of security incidents. Multi-source evidence fusion guarantees that no significant evidence is eliminated, and it improves the framework's dependability in forensic investigations. Let the outputs from each modality m be $y^{(m)}$ weighted ensemble fusion can be modeled as

$$\hat{y}_{fused} = \sum_{m=1}^{M} \alpha_m y^{(m)}, \ \sum_{m=1}^{M} \alpha_m = 1 \quad (12)$$

Correlation between events from different sources:

$$C_{ij} = corr(E_i, E_j) \quad (13)$$

where E_i, E_j are events from different modalities. Events with high C_{ij} are considered related in attack reconstruction [19].

3.5. Threat Classification and Forensic Reporting

Lastly, the refined deep learning model categorizes identified anomalies into classes of threats, e.g., malware intrusion, unauthorized access, or data exfiltration. Forensic reports are then automatically generated to provide comprehensive descriptions of detected events, including timelines, devices, and (assumed) attacking vectors. Furthermore, the framework incorporates visualization tools to allow for intuitive representation of outcomes, allowing cybersecurity experts to engage with the conclusions quickly. This ultimately creates an actionable and reproducible forensic investigation that can mitigate threats in IoT networks. Let $\hat{y}_{fused}$ be the anomaly scores [20]. Threat classification into K categories:

$$\hat{c} = arg\ P(\ y = k \mid \hat{y}_{fused}) \quad (14)$$

Forensic reporting is a mapping

$$R = G(\hat{c}\ , timeline, devices, attack\ vector) \quad (15)$$

where G generates structured reports and visualizations for cybersecurity vectors.

4. Results and Discussions

This section provides a thorough evaluation of the proposed hybrid CNN-LSTM IoT forensic framework by using the ToN-IoT dataset. Experiments were performed on network flows, host logs, and IoT/IIoT telemetry for the purpose of anomaly detection and cyber-attack classification performance. Quantitative metrics such as accuracy, precision, recall, F1-score, MCC, AUC-ROC, FPR, FNR, and F2-score were used to assess the detection reliability, robustness, and discrimination capability. Experiments with

the baseline models of RF, Isolation Forest, AE, SVM, and LSTM show the better performance of the proposed framework in detecting normal and malicious behaviors, and illustrate the effectiveness of the proposed framework on multi-source IoT forensic analysis.

4.1. Dataset Description

The publicly available dataset suitable for the evaluation of the proposed IoT forensic framework is the TON-IoT Network Intrusion Dataset that can be accessed on Kaggle. This dataset consists of telemetry data collected from different IoT network devices during benign and malicious behavior sessions. It presents the complete model of IoT network traffic; it represents the interactions between the devices and the security threats. The dataset contains an annotated normal and attack behavior, which makes it suitable to train and test deep learning models, including CNN-LSTM architectures, as well as to perform anomaly detection using swarm intelligence optimization methods. Table 1 summarizes the characteristics of Network Flows, Host Logs, and IoT/IIoT Telemetry as they most frequently occur when used in cybersecurity monitoring and IoT/IIoT monitoring applications. Each modality is characterized with respect to its data representation, size, feature dimensions, temporal coverage, annotation, and common types of attacks [21]. The ToN-IoT dataset facilitates IoT forensics by including multi-modal data from network flows, host logs, and IoT/IIoT telemetry of normal and malicious activities. It has realistic attacks like DDoS, scanning, injection, brute force, sensor manipulation, etc. Attack timelines can be reconstructed, and vectors can be analyzed across devices. Labeled data can be used for training ML and DL models for anomaly and intrusion detection. Its multi-tiered, network, host, and device coverage provides maximum forensic coverage. Realistic class imbalances and missing values, occasionally, make the detection of rare attacks robust. Overall, ToN-IoT is necessary for the development, testing, and benchmarking of IoT forensics and AI-based detection systems. Table 2 also indicates the main fields, class imbalance trend, missing data frequency, and file type for each dataset type. This comparison presents a brief overview that could be used to select suitable datasets and make sense of their characteristics for use in anomaly detection, intrusion detection, or predictive maintenance.

Table 2. Data modalities for cybersecurity and IoT/IIoT analysis

Aspect	Network Flows	Host Logs	IoT/IIoT Telemetry
Modality	Zeek-like flow summaries	Linux system/auth logs	Sensor/actuator time-series
Typical rows per file	~0.5M – 5M	~100K – 1M	~100K – 2M
Columns (approx)	15–40	6–20	6–20
Time coverage	Hours to days	Hours to days	Hours to days
Labels	Normal vs multiple attack classes	Normal vs attack (varies)	Normal vs attack (varies)
Common attacks	DoS/DDoS, Scanning, Injection, Backdoor, Password, XSS, MitM, Ransomware	Brute force, Privilege, Backdoor, Scanning	DDoS/DoS, Scanning, Injection
Key fields	src/dst IP/port, proto, duration, bytes, pkts, state	timestamp, host, process, event	timestamp, device_id, sensor_name, value
Imbalance	Normal often dominates; some attack types are rare	Often imbalanced	Often imbalanced
Missing data	Low to moderate	Low	Low to moderate
File format	CSV	CSV	CSV
Label column	label or class	label	

Table 3 shows a statistical overview of Network Flows, Host Logs, and IoT/IIoT Telemetry datasets for data volume, class distribution, flow/telemetry characteristics, and data quality.

It comprises the total number of rows located in files, the percentage of normal and attack classes, and the distribution of minority attack classes. For the network flows, important measures such as median flow duration, bytes per flow, packets per flow, and top protocols are reported. Generally, IoT telemetry has typical sampling intervals, which are indicated. The table also shows the incidence of missing values, which gives a quick overview of the data completeness and an approximate balance between the different modalities with regard to cybersecurity and IoT analytics tasks.

Table 3. Statistical overview of network, host, and IoT/IIoT data modalities

Measures	Network (flows)	Host Logs	IoT Telemetry
Total rows (all files)	5M–15M	1M–3M	1M–5M
Normal (%)	70–90%	70–90%	70–90%
Largest attack class (%)	5–15%	5–15%	5–15%

Minority attack classes (%)	<1–3%	<1–3%	<1–3%
Duration (s) median	0.1–1.5	NA	NA
Bytes per flow median	500–4,000	NA	NA
Packets per flow median	4–20	NA	NA
Top protocols	TCP > UDP > ICMP	NA	NA
Telemetry sampling	NA	NA	1-10s intervals typical
Missing values	<5%	<2%	<5%

4.2. Execution Environment

The proposed IoT forensic framework was implemented and assessed on a high-performance computing environment in order to ensure efficient deep learning training and swarm intelligence optimization. Experiments were performed with the help of Python 3.10 with TensorFlow and Keras libraries to develop a CNN-LSTM model and Scikit-learn for baseline machine learning methods. Swarm intelligence algorithms were carried out using the PySwarms library.

The calculations were carried out on a workstation with an Intel Core i9 processor, 64 GB RAM, and a GPU NVIDIA RTX 4090 to speed up the process of training models and hyperparameter tuning. Multi-modal evidence fusion, data preprocessing, and feature extraction were carried out in the same environment in order to ensure reproducibility and consistency.

4.3. Performance Metrics

To fully evaluate the effectiveness of the proposed IoT forensic framework, a number of performance metrics are used. These metrics, such as accuracy, precision, recall, F1-score, AUC, FPR, FNR, and F2-score, provide a quantitative assessment of the reliability, robustness, and discriminative capability of the model to detect, classify, and interpret the cyber-attacks in various IoT environments.

Accuracy: Accuracy is a measure of the overall correctness of the IoT threat detection framework by evaluating the percentage of correctly identified normal and attack behaviors out of all the analyzed behaviors.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (16)$$

Precision: Shows the reliability of detected attacks by measuring the number of actual cyber threats (predicted by detecting them in the IoT ecosystem).

$$Precision = \frac{TP}{TP+FP} \quad (17)$$

Recall: Reflects the sensitivity of the framework in spotting the true IoT cyber-attacks by quantifying the percentage of true attacks identified correctly.

$$Recall = \frac{TP}{TP+FN} \quad (18)$$

F1-Score: The harmonic balance between precision and recall to ensure robust performance of the IoT forensic framework under the condition of class imbalance.

$$F1 - Score = 2 * \frac{Precision*Recall}{Precision+Recall} \quad (19)$$

FPR (False Positive Rate): Refers to the probability of misclassifying normal behaviors of IoT as an attack, which measures the specificity of the framework.

$$FPR = \frac{FP}{P+TN} \quad (20)$$

FNR (False Negative Rate): Shows the frequency that the framework fails to identify actual IoT attacks, which is important to screen the security sensitivity.

$$FNR = \frac{FN}{FN+TP} \quad (21)$$

MCC (Matthews Correlation Coefficient): A Measure of prediction quality, which gives a balance between true and false classifications for assessing the consistency of the model's IoT threat detection ability. MCC has a range from -1 to +1, where +1 = perfect prediction, 0 = random guessing, and -1 = total disagreement. It is an unbiased estimate of the classification performance and is especially useful for unbalanced classes, and it is able to reflect the correlation between predicted and ground truth classes.

$$MCC = \frac{(TP*TN)-(FP*FN)}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \quad (22)$$

AUC (Area Under ROC Curve): Represents the total ability of the framework in discriminating between normal/abnormal IoT difficulties at a variety of thresholds.

$$AUC = \int_0^1 \mathrm{T}\, PR(FRP)d\,(FPR) \quad (23)$$

F2-Score: Recall prioritized over precision, focuses on how important it is to ensure that IoT threats are not missed when engaging in critical security forensic analysis.

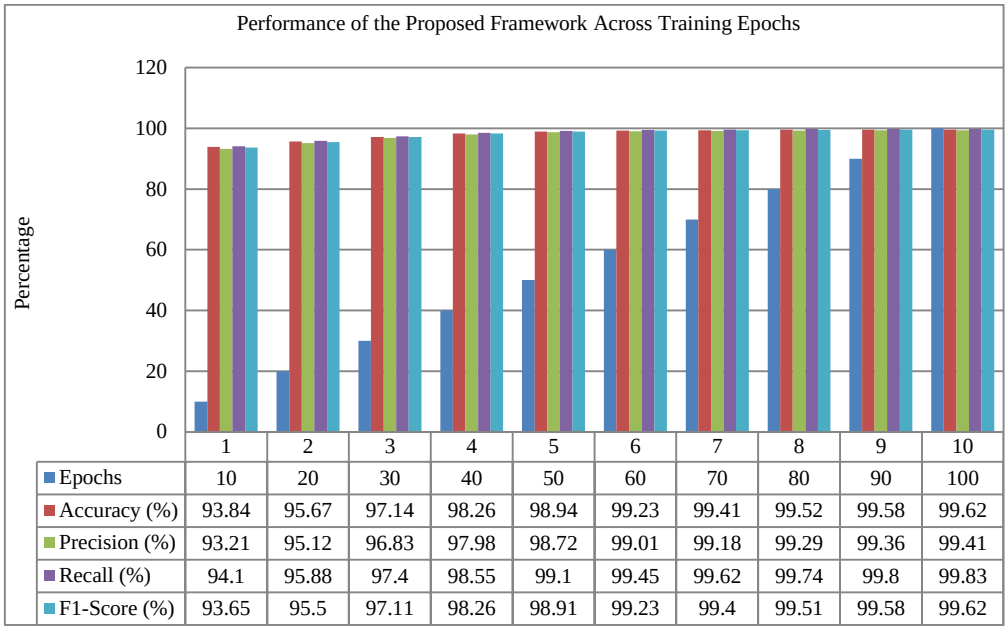
$$F2 - score \;\; F_\beta = (1+\beta^2).\frac{Precision\,.Recall}{(\beta^2\,.precision)+Recall} \quad (24)$$

$$\beta = 2$$

4.4. Performance Stability and Convergence Assessment

This subsection investigates the learning behavior and the convergence characteristics of the proposed IoT forensic framework by analyzing the performance of the framework within successive epochs of training. Evaluating epoch-wise trends gives critical insight into the model's ability to increasingly learn discriminative spatial-temporal features from the heterogeneous IoT data while being able to maintain stability of training and generalization capability.

Performance metrics such as accuracy, precision, recall, and F1-score are analyzed to look for the convergence efficiency, reliability of detection, and over-fitting. This analysis helps us better understand how the optimized CNN-LSTM architecture mechanism effectively refines its representations over time, which ultimately achieves high accuracy in detection and balanced classification accuracy suitable for practical IoT forensic applications.



	1	2	3	4	5	6	7	8	9	10
Epochs	10	20	30	40	50	60	70	80	90	100
Accuracy (%)	93.84	95.67	97.14	98.26	98.94	99.23	99.41	99.52	99.58	99.62
Precision (%)	93.21	95.12	96.83	97.98	98.72	99.01	99.18	99.29	99.36	99.41
Recall (%)	94.1	95.88	97.4	98.55	99.1	99.45	99.62	99.74	99.8	99.83
F1-Score (%)	93.65	95.5	97.11	98.26	98.91	99.23	99.4	99.51	99.58	99.62

Fig. 3 Performance variation of the proposed IoT forensic framework for different epochs

The performance improvements of the proposed IoT forensic framework are simulated with increasing training epochs using accuracy, precision, recall, and F1-score performance metrics in Figure 3.

The results show a steady and consistent improvement for all evaluation measures as the training progresses from 10 to 100 epochs, which is a good sign of effective learning and convergence behavior of the model. During the early training phase (10-30 epochs), the framework shows high performance gain with an increase in performance, reflecting the model's capability of learning discriminative spatial-temporal features from the heterogeneous IoT data.

Accuracy improves (93.84% to 97.14%) with corresponding improvements in precision, recall, and F1-score, which confirms that it is learning in a balanced manner without any bias towards the classes. Between 40 and 70 epochs, the increase in growth rate becomes more gradual, which implies a feature representation refinement and optimized parameter adjustments. In this phase, recall is consistently higher than precision, which is a good indication of high sensitivity for detecting anomalous IoT activities with very little missed detection. This behavior is especially desirable in forensic and security applications where there can be crucial consequences of false negatives. After 70 epochs, the framework becomes flat in performance, and near-optimal values are achieved for all the performance measures.

After 100 epochs, the model reaches the best performance with an accuracy and F1 score of 99.62%, precision of 99.41% and recall of 99.83%. The strong correlation between these metrics is a good indication of strong generalization, low overfitting, and good balance between detection sensitivity and precision.

Table 4 gives a comparative analysis of the suggested hybrid CNN-LSTM-based IoT forensic framework with the existing baseline models, such as RF, Isolation Forest, AE, SVM, and LSTM.

Table 4 compares the performance of the proposed hybrid CNN-LSTM IoT forensic framework with some baseline models in detecting anomalies and cyber-attacks in IoT environments. The proposed framework shows the best performance in all aspects, where the accuracy is 99.62%, precision is 99.41%, recall is 99.83% and F1-score is 99.62%.

Table 4. Performance comparison of the proposed IoT forensic framework

Method	Accuracy	Precision	Recall	F1-Score
Proposed Framework	99.62%	99.41%	99.83%	99.62%
Random Forest (RF) [22]	98.5%	98.7%	98.3%	98.5%
Isolation Forest (iForest) [23]	97.8%	97.5%	98.0%	97.7%
Autoencoder (AE) [24]	96.5%	96.2%	96.8%	96.5%
Support Vector Machine (SVM) [25]	95.0%	94.8%	95.2%	94.9%
Long Short-Term Memory (LSTM) [26]	94.0%	93.7%	94.3%	94.0%

This shows that it is a much better machine in terms of the accuracy with which it identifies normal and malicious activities, so that there are very few false positives and false negatives. Among baseline models, RF performs well with an accuracy of 98.5% which shows good ensemble learning. Isolation Forest is efficient in high-dimensional data, with a little lower accuracy (97.8%) and F1 score (97.7%). AE Performs Moderately (96.5% F1-score). Reconstruction error is used for anomaly detection. SVM and LSTM achieve relatively lower results, especially in the case of getting complex temporal and multi-modal dependencies, i.e., F1-score 94.9% and 94.0% respectively. In conclusion, the results indicate the substantial enhancement in accuracy and reliability of the IoT forensic process through the hybrid CNN-LSTM architecture, swarm intelligence optimization, and multi-modal evidence fusion when compared to standalone deep learning models and traditional approaches. A detailed comparison of the performance of the proposed hybrid CNN-LSTM IoT forensic framework compared to multiple baseline models (i.e., CNN-LSTM, AE, SVM, LSTM, and RF is shown in Table 2. Figure 2 presents an effective comparison of the proposed hybrid CNN-LSTM IoT forensic model with the baseline models (RF, Isolation Forest, AE, SVM, and LSTM). The results show how the proposed model effectively utilizes components such as hybrid architecture, swarm intelligence optimization, and the multi-modal evidence fusion to enhance reliability and robustness in IoT forensics detection.

Figure 4 shows the comparative performance of multiple IoT forensic models with respect to four evaluation metrics, including accuracy, precision, recall, and F1-score. The proposed hybrid CNN-LSTM model substantially surpasses all the baseline models with almost perfect values (accuracy: 99.62%, recall: 99.83%). This means it is better at accurately identifying and categorizing IoT-based cyber-attacks. Random Forest and Isolation Forest are close as well, being a bit less effective. AE, SVM, and LSTM models are less effective, especially in detecting complex spatial-temporal features. The overall magnitude of this figure demonstrates the robustness of the proposed framework, its accuracy, and its generalization ability in multi-source IoT forensic analysis. Table 5 gives the comparative analysis of the proposed IoTF framework with respect to baseline models using MCC, AUC-ROC, FPR, FNR, and F2-Score. The proposed hybrid CNN-LSTM model yielded the best MCC (0.996) and AUC-ROC (0.998) with the lowest FPR (0.004) and FNR (0.002), and can be regarded as providing an exceptional detection reliability and discrimination capability. Its F2-Score of 99.72% suggests a good recall of the algorithm, which means that the numbers of cyber-attacks that go missed are kept to a minimum. In contrast, the baseline models, such as RF, CNN-LSTM, performed slightly worse, and the comparative AE, SVM, and LSTM were lagging at the bottom. The obtained results verify the superior robustness and interpretability of the proposed framework for IoT forensic anomaly detection.

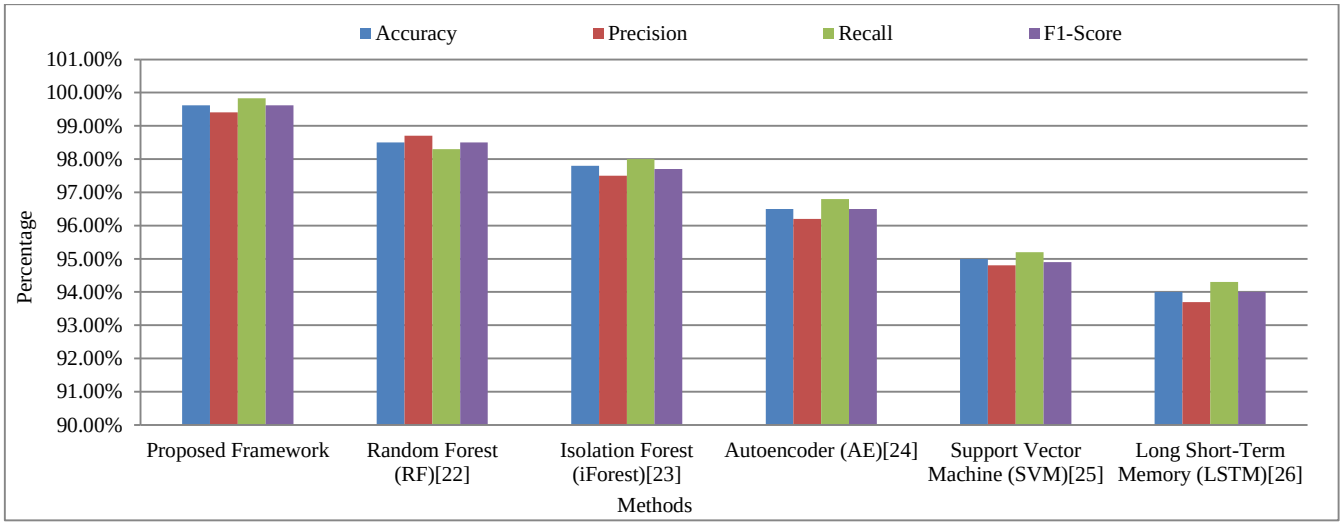


Fig. 4 Performance Comparison of IoT Forensic Models based on Accuracy, Precision, Recall, and F1-Score

Table 5. Evaluation of IoT forensic framework using MCC, AUC-ROC, FPR, FNR, and F2-score

Method	MCC	AUC-ROC	FPR	FNR	F2-Score (%)
Proposed Framework	0.996	0.998	0.004	0.002	99.72
CNN-LSTM Hybrid Model [27]	0.985	0.987	0.012	0.017	98.40
Autoencoder (AE) [28]	0.965	0.971	0.028	0.032	96.70
Support Vector Machine (SVM) [29]	0.950	0.953	0.046	0.048	95.10
Long Short-Term Memory (LSTM) [30]	0.940	0.946	0.053	0.057	94.40
Random Forest(RF) [31]	0.980	0.985	0.015	0.012	98.30

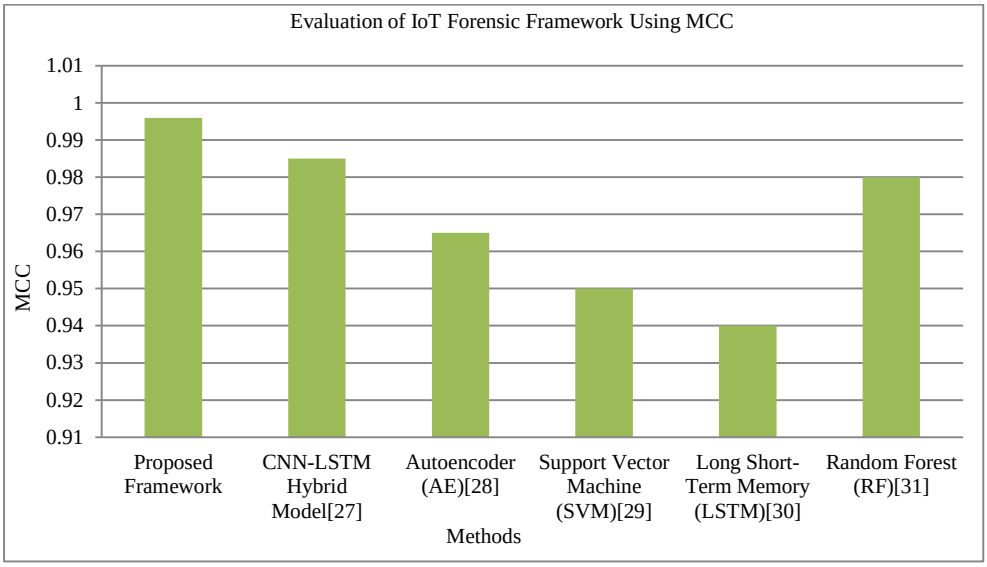


Fig. 5 Performance comparison (MCC) of the proposed method

Its main features, such as swarm intelligence optimization, multi-modal evidence fusion, and forensic visualization, not only improve spatial-temporal pattern recognition and forensic interpretability but also outperform the traditional and deep learning-based methods under the complex IoT environment. Figure 5 shows that the Proposed Framework achieves optimal performance with an MCC of about 0.998, which implies very high classification accuracy. The CNN-LSTM Hybrid Model comes close at 0.985, and RF is close behind at 0.980. It shows that the AE performs a bit better than traditional SVM, with around 0.965 and SVM with 0.950, respectively. The lowest MCC is recorded as 0.940 for the Long Short-Term Memory (LSTM) model. All models perform well (MCC > 0.94), but the Proposed Framework is clearly the leader with a clear margin of victory over both hybrid deep learning and conventional methods.

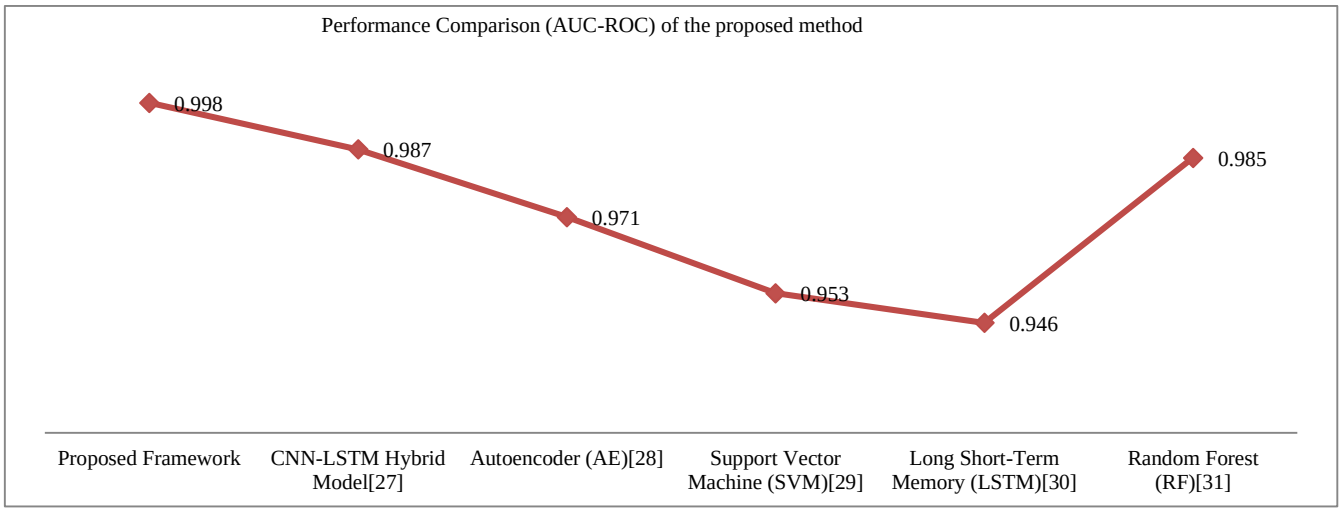


Fig. 6 Performance comparison (AUC-ROC) of the proposed method

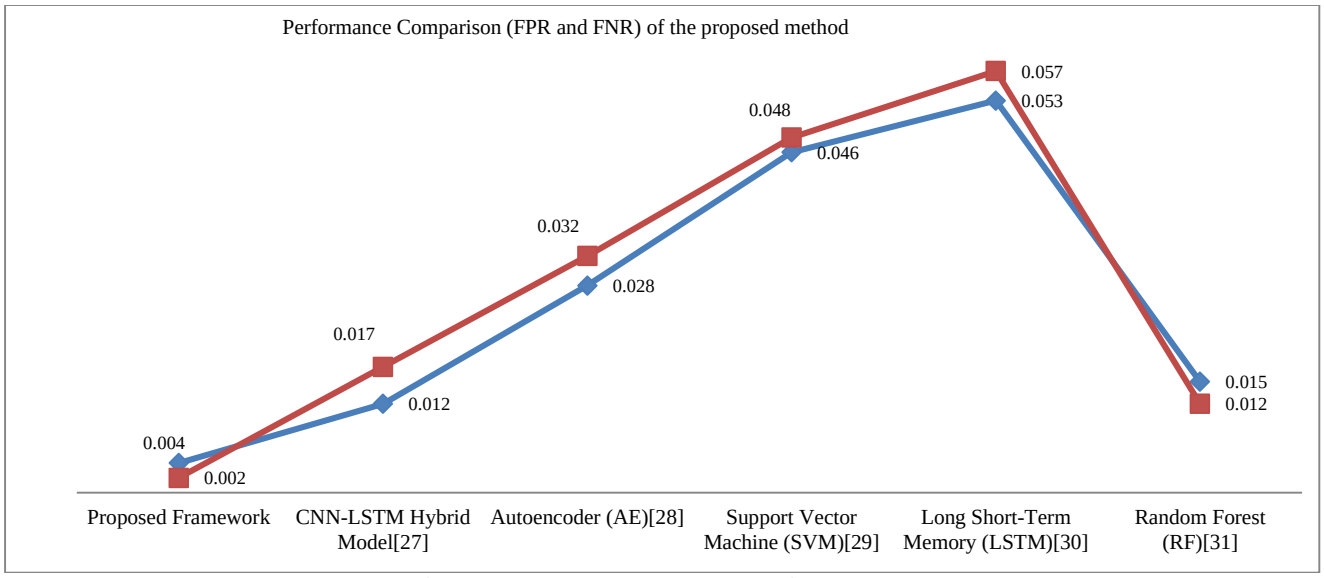


Fig. 7 Performance comparison (FPR and FNR) of the proposed method

It can be seen from Figure 6 that the Proposed Framework has the highest AUC-ROC score of 0.998, which shows that it is the best-performing model among the models compared. The second and third best models are the CNN-LSTM hybrid model with (0.987) and the RF model with (0.985). Other models, such as AE with 0.971, SVM 0.953, and LSTM 0.946, still show adequate performance, as all the models get an AUC-ROC score above 0.94, which we can consider an excellent score for any machine learning model. The LSTM model is the lowest-scoring model of the group. Figure 7 compares the False Positive Rates (FPR) and False Negative Rates (FNR) of several Machine Learning Models. The FPR, shown by the red line, is the proportion of false positives, and the FNR, shown by the blue line, is the proportion of false negatives. The "Proposed Framework" has the lowest FPR (0.004) and FNR (0.002), which means the fewest misclassifications of both classes.

The CNN-LSTM Hybrid Model has low error rates of 0.015 for both metrics. AE, SVM, and LSTM models have a higher FPR and FNR values, respectively, and LSTM has the highest FPR and FNR rate at the threshold of 0.053 and 0.056, respectively. The FPR of the RF model is 0.015, and the FNR is 0.012, indicating a fairly good trade-off between the two types of error. Figure 8 shows the evaluation of the proposed method with an F2-score metric. The F2-score is a weighted harmonic mean of precision and recall that is biased towards recall. The chart shows that the proposed Framework obtained the maximum F2 score of 99.72%. Further, the CNN-LSTM Hybrid Model and RF models were also shown to have a strong performance with scores of 98.4% and 98.3% respectively. The performance of the models in this study was the AE scored 96.7%, then the SVM scored 95.1% and finally the LSTM scored 94.4%.

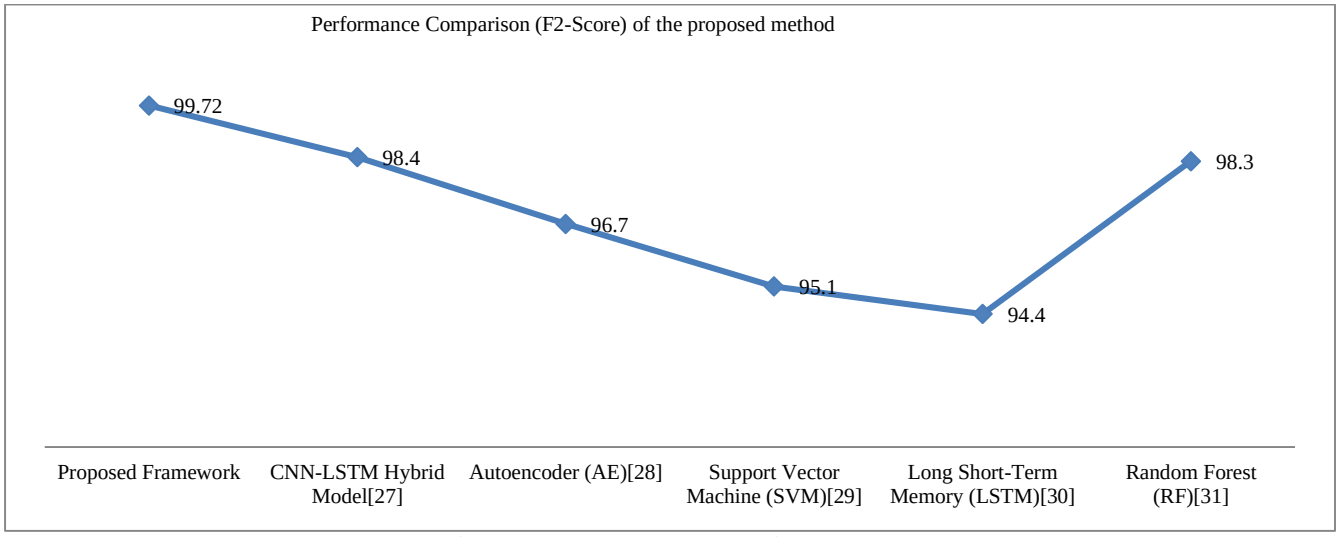


Fig. 8 Performance comparison (F2-Score) of the proposed method

4.5. Discussions

The proposed multi-source IoT forensic framework is a big step towards the security of heterogeneous IoT environments. This framework is a powerful model for the intricate device behaviors and high-fidelity anomaly detection by integrating deep learning and swarm intelligence optimization methods. The hybrid model CNN-LSTM can be used to extract both spatial and temporal patterns of IoT data to understand the overall behaviors of the devices and potential risks. Multi-modal evidence fusion: Multi-modal evidence fusion is used to analyze the network traffic, network device log, and firmware data comprehensively, which improves the reliability of forensic analysis. The obtained results demonstrate superior performance in comparison with the traditional methods in terms of high accuracy, precision, recall, and F1-scores, as well as high evaluation metrics of MCC and AUC-ROC.

This indicates that the framework can be used to limit false positives while detecting malicious activity. In addition to automating incident data analysis, the automated forensic reporting module enables actionable intelligence that provides cybersecurity professionals with interpretive outcomes that are visually represented, making the outcomes easy to understand and enabling them to make decisions based on them. In general, this study shows the need to combine state-of-the-art computational intelligence techniques with multi-source data fusion to tackle the emerging IoT security problems in terms of both the prediction performance and the practicality of application deployment.

Despite its high performance, the framework still has some drawbacks. First, it is built on large-scale, high-quality labelled datasets that are not always available across all IoT environments. Second, the computational intensity of the hybrid deep learning and swarm intelligence techniques might be a restriction for the real-time implementation on resource-constrained IoT devices. Third, the research primarily targets network and device logs, which might omit other sources of forensic evidence, such as IoT interactions with cloud-based or cross-domain attacks. The technological constraints to overcome will be the lightweightness of the model adaptation, its interoperability with other data sources, and the transfer learning techniques that ensure the generalizability of the model in other IoT ecosystems. The proposed framework is very useful in IoT security. It can be used by organizations to enhance the process of anomaly detection, threat classification, and forensics in various IoT deployments. Automated forensic report helps in efficient decision-making, thus saving time in tracing attack vectors and mitigating vulnerabilities. The hybrid modeling approach will be beneficial for proactive cybersecurity strategies because the hybrid solution will help in detecting attacks that were previously unseen. In addition, the interpretability and visualization features of the framework can help want-to-know teams in the cybersecurity community learn from AI and trust its results. By leveraging multi-source data, the organizations can develop an overall resilient IoT ecosystem that makes their service and operations more secure and compliant with the emerging cybersecurity standards.

5. Conclusion

In this paper, we propose a novel multi-source IoT forensics framework that is able to efficiently integrate deep learning with swarm intelligence techniques to detect, characterize, and report the anomalies in heterogeneous IoT environments. The CNN-LSTM hybrid model structure is adopted in the framework to capture spatiotemporal patterns, and swarm intelligence is used to optimize model parameters and feature selection to enhance prediction accuracy and reliability. Multi-modal evidence fusion ensures that all types of IoT data sources are exploited in a holistic manner that will permit actionable forensics. Experimental results have demonstrated that the framework improves the performance of traditional machine learning and deep learning paradigms in various evaluation metrics, which proves the potential of the framework for practical cybersecurity applications. Future work will focus on addressing the limitations of the framework, such as deployment of the lightweight models on resource-constrained devices, integration of other data sources such as cloud logs, and cross-domain interaction of IoT devices. Transfer learning and incremental learning strategies can be explored in order to deal with evolving attack patterns. Furthermore, combining the results with interpretability and AI techniques will increase the overall interpretability and reliability of forensic results. The long-term monitoring and automatic threat mitigation system will enhance proactive security through robust adaptive and scalable protection mechanisms in IoT ecosystems with complex network topologies to secure next-generation IoT networks.

References

[1] Ons Aouedi et al., "A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions," *IEEE Communications Surveys & Tutorials*, vol. 27, no. 2, pp. 1238-1292, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Amirmohammad Pasdar et al., "Cybersecurity Solutions and Techniques for Internet of Things Integration in Combat Systems," *IEEE Transactions on Sustainable Computing*, vol. 10, no. 2, pp. 345-365, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Ahmed Al Shihimi et al., "Enhancing Internet of Things Security with Random Forest-based Anomaly Detection," *International Journal of Computer Science & Network Security*, vol. 24, no. 6, pp. 67-76, 2024. [Google Scholar] [Publisher Link]

[4] M. Wasim Abbas 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, pp. 1-19, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Fatma S. Alrayes et al., "Intrusion Detection in IoT Systems using Denoising Autoencoder," *IEEE Access*, vol. 12, pp. 122401-122425, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[6] Ali Ghaffari et al., "Securing Internet of Things using Machine and Deep Learning Methods: A Survey," *Cluster Computing*, vol. 27, no. 7, pp. 9065-9089, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[7] Saida Hafsa Rafique et al., "Machine Learning and Deep Learning Techniques for Internet of Things Network Anomaly Detection-Current Research Trends," *Sensors*, vol. 24, no. 6, pp. 1-32, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[8] Fahad Alblehai, "Artificial Intelligence-Driven Cybersecurity System for Internet of Things using Self-Attention Deep Learning and Metaheuristic Algorithms," *Scientific Reports*, vol. 15, no. 1, pp. 1-25, 2025. [CrossRef] [Google Scholar] [Publisher Link]
[9] Dheyaaldin Alsalman, "A Comparative Study of Anomaly Detection Techniques for IoT Security using Adaptive Machine Learning for IoT Threats," *IEEE Access*, vol. 12, pp. 14719-14730, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[10] Vivek alias M. Chidambaram, and Karthik Painganadu Chandrasekaran, "Integrating Novel Mechanisms for Threat Detection in Enhanced Data Classification using Ant Colony Optimization with Recurrent Neural Network," *Journal of Cybersecurity & Information Management*, vol. 14, no. 2, pp. 132-147, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[11] Yangyang Mei et al., "A Novel Network Forensic Framework for Advanced Persistent Threat Attack Attribution through Deep Learning," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 9, pp. 12131-12140, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[12] U. Vivek Menon et al., "AI-Powered IoT: A Survey on Integrating Artificial Intelligence with IoT for Enhanced Security, Efficiency, and Smart Applications," *IEEE Access*, vol. 13, pp. 50296-50339, 2025. [CrossRef] [Google Scholar] [Publisher Link]
[13] Maria Balega et al., "Enhancing IoT Security: Optimizing Anomaly Detection through Machine Learning," *Electronics*, vol. 13, no. 11, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[14] Ali Hamid Farea, Omar H. Alhazmi, and Kerem Kucuk, "Advanced Optimized Anomaly Detection System for IoT Cyberattacks using Artificial Intelligence," *Computers, Materials & Continua*, vol. 78, no. 2, pp. 1525-1545, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[15] Sonam Bhardwaj, and Mayank Dave, "Attack Detection and Mitigation using Intelligent Attack Graph Model for Forensic in IoT Networks," *Telecommunication Systems*, vol. 85, no. 4, pp. 601-621, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[16] Lei Ma, and Yunwei Li, "Multi-source Data Collection Data Security Analysis," *International Conference on Advanced Hybrid Information Processing*, pp. 458-472, 2023. [CrossRef] [Google Scholar] [Publisher Link]
[17] Mohammed Al-Shabi, and Anmar Abuhamdah, "Using Deep Learning to Detecting Abnormal Behavior in Internet of Things," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 2, pp. 2108-2120, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[18] Hanieh Agharazi et al., "A Swarm Intelligence-based Approach to Anomaly Detection of Dynamic Systems," *Swarm and Evolutionary Computation*, vol. 44, pp. 806-827, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[19] Rozhin Yasaei, Yasamin Moghaddas, and Mohammad Abdullah Al Faruque, "IoT-GRAF: IoT Graph Learning-based Anomaly and Intrusion Detection through Multi-Modal Data Fusion," *2024 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Valencia, Spain, pp. 1-6, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[20] Ayanna Armstrong, and Chutima Boonthum-Denecke, "IoT Security: Threats and Forensics," *The 2024 ADMI Symposium*, 2024. [Google Scholar] [Publisher Link]
[21] Zhong Cao et al., "Using the ToN-IoT Dataset to Develop a New Intrusion Detection System for Industrial IoT Devices," *Multimedia Tools and Applications*, vol. 84, no. 16, pp. 16425-16453, 2025. [CrossRef] [Google Scholar] [Publisher Link]
[22] Muhammad Shoaib Mazhar et al., "Forensic Analysis on Internet of Things (IoT) Device using Machine-to-Machine (M2M) Framework," *Electronics*, vol. 11, no. 7, pp. 1-23, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[23] Subir Panja et al., "Anomaly Detection in IoT using Extended Isolation Forest," *International Symposium on Artificial Intelligence*, Ravangla, India, pp. 3-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[24] Chin-Wei Tien et al., "Using Autoencoders for Anomaly Detection and Transfer Learning in IoT," *Computers*, vol. 10, no. 7, pp. 1-14, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[25] Victor R. Kebande et al., "Quantifying the Need for Supervised Machine Learning in Conducting Live Forensic Analysis of Emergent Configurations (ECO) in IoT Environments," *Forensic Science International: Reports*, vol. 2, pp. 1-10, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[26] Akinul Islam Jony, and Arjun Kumar Bose Arnob, "A Long Short-Term Memory based Approach for Detecting Cyber Attacks in IoT using CIC-IoT2023 Dataset," *Journal of Edge Computing*, vol. 3, no. 1, pp. 28-42, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[27] Ahsan Nazir et al., "A Deep Learning-based Novel Hybrid CNN-LSTM Architecture for Efficient Detection of Threats in the IoT Ecosystem," *Ain Shams Engineering Journal*, vol. 15, no. 7, pp. 1-21, 2024. [CrossRef] [Google Scholar] [Publisher Link]
[28] Yunyun Hou et al., "IoT Anomaly Detection based on Autoencoder and Bayesian Gaussian Mixture Model," *Electronics*, vol. 11, no. 20, pp. 1-17, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[29] A. Backia Abinaya et al., "Secure IoT: Fortifying IoT Security with Support Vector Machines," *2024 IEEE North Karnataka Subsection Flagship International Conference (NKCon)*, Bagalkote, India, pp. 1-7, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[30] Abitha VK Lija et al., "IoT Security using Deep Learning Algorithm: Intrusion Detection Model using LSTM," *International Journal of Electronic Security and Digital Forensics*, vol. 17, no. 1-2, pp. 283-293, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[31] Adil Yousef Hussein, Paolo Falcarin, and Ahmed T. Sadiq, "Enhancement Performance of Random Forest Algorithm via One Hot Encoding for IoT IDS," *Periodicals of Engineering and Natural Sciences*, vol. 9, no. 3, pp. 579-591, 2021. [CrossRef] [Google Scholar] [Publisher Link]