scientific reports

Check for updates

OPEN

An intelligent deep representation learning with enhanced feature selection approach for cyberattack detection in internet of things enabled cloud environment

Hayam Alamro[1], Sami Saad Albouq[2], Jahangir Khan[3], Meshari H. Alanazi[4]✉, Nojood O. Aljehane[5], Jehad Saad Alqurni[6], Mohammed Mujib Alshahrani[7] & Ohud Alasmari[8]

Users of computer networks can take advantage of cloud computing (CC), a relatively new concept that provides features such as processing, in addition to storing and sharing data. Cloud computing (CC) is attracting global investment due to its services, while IoT faces rising advanced cyberattacks, making its cybersecurity crucial to protect privacy and digital assets. A significant challenge for intrusion detection systems (IDS) is detecting complex and hidden malware, as attackers use advanced evasion techniques to bypass conventional security measures. At the cutting edge of cybersecurity is artificial intelligence (AI), which is applied to develop composite models that protect systems and networks, including Internet of Things (IoT) systems. AI-based deep learning (DL) is highly effective in detecting cybersecurity threats. This paper presents an Intelligent Hybrid Deep Learning Method for Cyber Attack Detection Using an Enhanced Feature Selection Technique (IHDLM-CADEFST) approach in IoT-enabled cloud networks. The aim is to strengthen IoT cybersecurity by identifying key threats and developing effective detection and mitigation strategies. Initially, the data pre-processing phase uses the standard scaler method to convert input data into a suitable format. Furthermore, the feature selection (FS) strategy is implemented using the recursive feature elimination with information gain (RFE-IG) model to detect the most pertinent features and prevent overfitting. Finally, a hybrid Convolutional Neural Network and Long Short-Term Memory (CNN-LSTM) model is employed for attack classification, utilizing the RMSprop optimizer to enhance the performance and efficiency of the classification process. The experimentation of the IHDLM-CADEFST approach is examined under the ToN-IoT and Edge-IIoT datasets. The comparison analysis of the IHDLM-CADEFST approach yielded superior accuracy values of 99.45% and 99.19% compared to recent models on the dual dataset.

Keywords Cyber attack detection, Cybersecurity, Internet of things, Feature selection, Recursive feature elimination, Information gain, Cloud computing

A swift expansion of IoT has reshaped the field of information and communication technologies (ICT), resulting in an unmatched connection of systems and devices. It has promoted the advancement of emerging fields in several domains, including home appliances, healthcare, urbanization, and production[1]. However, the

[1]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, 11671 Riyadh, Saudi Arabia. [2]Department of Computer and Information Systems, Islamic University of Madinah, 42351 Medina, Saudi Arabia. [3]Department of Computer Science, Applied College at Mahayil, King Khalid University, Abha, Saudi Arabia. [4]Department of Computer Science, College of Sciences, Northern Border University, Arar, Saudi Arabia. [5]Department of Computer Science, Faculty of Computers and Information Technology, University of Tabuk, Tabuk, Saudi Arabia. [6]Department of Educational Technologies, College of Education, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, 31441 Dammam, Saudi Arabia. [7]Department of Information Systems and Cybersecurity, College of Computing and Information Technology, University of Bisha, P.O. Box 551, Bisha, Saudi Arabia. [8]Department of Computer Science, College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia. ✉email: Meshari.alanazi@nbu.edu.sa; ashraf.benmilad@nbu.edu.sa

employment of IoT systems has also led to a high number of novel and significant cybersecurity threats, where vulnerability and illegal access to information and vital infrastructure might be major concerns. The concept of IoT has offered a greater level of integrity, availability, accessibility, confidentiality, interoperability, and scalability regarding device connectivity[2]. Nevertheless, IoTs are exposed to cyber threats due to the combination of their numerous attack surfaces and their novelty, resulting in a shortage of security requirements and regulations. There is a wide range of cyberattacks that malicious actors use against IoTs, depending on the type of system they target and the objectives they aim to achieve through the attack[3]. As a result, a significant amount of research has been conducted into cybersecurity in IoT. To fully understand the potential of IoT, these devices often rely on CC platforms for scalable storage, real-time analytics, and advanced processing capabilities. The convergence of IoT with CC—IoT cloud systems—has enabled organizations to process larger amounts of data successfully, thereby fostering innovation and operational agility. To detect and mitigate those network attacks, scholars, practitioners, and academicians created IDS. A development that reinforces network security and defends organizational data[4]. This IDS informs the system administrator of any malicious behaviour happening within the network and hence acts as a data protection device that avoids such malicious threats. Intrusion occurs when someone obtains unauthorized access to or maliciously utilizes data resources. IDSs are a part of the subsequent protection line of the system[5]. IDS is a monitoring system that identifies malicious actions and generates warnings when they are detected, as well as when they are executed, along with security concerns and measures, including security systems, authentication, and encryption techniques, to reinforce security against cyberattacks[6]. The IDS can differentiate between malicious and non-malicious activity. IDS has further enhanced its effectiveness through the combination of AI, leveraging higher computational methods. One of the advancements in cybersecurity is AI, which is applied to creating advanced algorithms to safeguard systems and networks, such as IoT systems[7]. Attackers have learned to exploit AI and have even begun to utilize adversarial AI to conduct cybersecurity attacks. However, in the context of IoT, cyber attackers constantly hold the advantage, as they only need to identify a single weakness, whereas cybersecurity specialists must defend numerous targets[8]. This results in the enlarged utilization of AI by cyber enemies as well, to prevent sophisticated methods that identify abnormal activity and avoid detection[9]. AI has gained significant interest with the development of IoT technology. With this development, AI techniques are leveraged in IoT cybersecurity applications to identify attacks and potential threats[10].

This paper presents an Intelligent Hybrid Deep Learning Method for Cyber Attack Detection Using an Enhanced Feature Selection Technique (IHDLM-CADEFST) approach in IoT-enabled cloud networks. The aim is to strengthen IoT cybersecurity by identifying key threats and developing effective detection and mitigation strategies. Initially, the data pre-processing phase uses the standard scaler method to convert input data into a suitable format. Furthermore, the feature selection (FS) strategy is implemented using the recursive feature elimination with information gain (RFE-IG) model to detect the most pertinent features and prevent overfitting. Finally, a hybrid Convolutional Neural Network and Long Short-Term Memory (CNN-LSTM) model is employed for attack classification, utilizing the RMSprop optimizer to enhance the performance and efficiency of the classification process. The experimentation of the IHDLM-CADEFST approach is examined under the ToN-IoT and Edge-IIoT datasets. The significant contribution of the IHDLM-CADEFST approach is listed below.

- The IHDLM-CADEFST model utilizes a standard scaler to transform raw input data into a normalized format, ensuring consistent feature scaling, which enhances model convergence and learning stability. This improves the model's capability to process diverse IoT-cloud data efficiently. It plays a crucial role in preparing high-quality input for the classification stage.
- The IHDLM-CADEFST technique integrates the RFE model with an information gain effect, effectively mitigating data dimensionality by removing redundant and less informative features, thereby improving learning efficiency. This approach chooses the most relevant attributes to enhance detection accuracy. It significantly improves the model's performance by focusing on impactful input features.
- The IHDLM-CADEFST methodology incorporates a hybrid CNN-LSTM model, utilizing CNN for extracting spatial features and LSTM for learning temporal patterns, thereby enabling the effective detection of complex and evolving attack behaviours. This integration enhances the model's ability to capture both static and dynamic characteristics in IoT-cloud traffic. It enhances classification accuracy by utilizing the complementary strengths of both architectures.
- The IHDLM-CADEFST approach utilizes the RMSprop optimizer to adaptively update network weights, thereby promoting faster convergence and maintaining stability during training. This optimization method efficiently handles non-stationary data, which is common in IoT-cloud environments. It enhances training efficiency and facilitates achieving optimal model performance.
- The novelty of the IHDLM-CADEFST model lies in the seamless integration of RFE-IG-based feature selection with a hybrid CNN-LSTM architecture, optimized using RMSprop, thereby creating a unified framework for accurate and efficient intrusion detection. This approach is uniquely designed for IoT-cloud environments where both spatial and temporal patterns are crucial. It addresses the gap in existing research by integrating all these elements into a single, robust solution.

Related works

Naveeda and Fathima[11] presented an IoT-based cyberattack detection model (IoT-E-CADS) for advanced metering infrastructure (AMI). The presented IoT-E-CADS can recognize diverse forms of attacks. The isolation forest (IF) approach is employed at an original stage for identifying cyberattacks and anomalies in the systems. Then, the decision tree (DT) ML paradigm is applied to detecting cyberattacks and cases of false data injection (FDI). Thayalan et al.[12] proposed a novel architecture that integrates collaborative federated learning (FL) with an edge-cloud framework for defensive measures. This architecture features the two-stage attention integrated graph-

based multi-source spatio-temporal data fusion (2 S-AGMSTDF) model, which processes multiple data sources, including user behaviour patterns, cyber activity, and sensor inputs. The main modules contain Attention-Based LSTM for temporal feature extraction, a GCN-ResNet-based transformer (GRCMT) for spatial data analysis, and AKGCN for cyber feature embedding. Vellela et al.[13] presented a new cyberattack recognition technique utilizing a Bidirectional LSTM (BiLSTM) approach combined with a self-attention mechanism and GloVe word embeddings. The model's parameters are adjusted by the Greylag Goose Optimiser Algorithm (GLGOA) and the Single Candidate Optimiser Algorithm (SCOA), refining computational and recognition efficacy. Algarni et al.[14] presented an edge computing-based, attack behaviour-aware smart prioritization approach with dual as well as multi-dimensional detection and classification of cybersecurity intrusions by adapted ML approaches. This approach can enhance smart grid cybersecurity by providing a complete defence against intrusions. It also improves smart grid cybersecurity through a multi-criteria methodology. Sahu et al.[15] proposed an innovative method employing LSTM and FL models. FL enables model training within decentralized data resources without compromising data confidentiality. In contrast, LSTMs are very efficient in recognizing temporal relationships in sequential data, making them appropriate for examining cybersecurity time-series data.

Dey et al.[16] suggested a meta-heuristic-based intelligent and different architecture for cyber attack recognition, utilizing ensemble FS and classification techniques for overcoming the challenges. Primarily, a metaheuristic-enabled ensemble FS technique was built by an optimization algorithm for attaining an enhanced feature set to bypass the dimensionality for effective learning. Following that, DT and ensemble learning-enabled classification models are leveraged distinctly for detecting and classifying cyberattacks. Radjaa et al.[17] addressed the problem using IDS-empowered anomaly detection to prevent cyberattacks in IoT infrastructures. Specifically, recommended a federated DL (FDL) in a fog-based IDS framework, which uses the Bot-IoT dataset and LSTM architecture. Srinivasulu and Venkateswaran[18] addressed the grave necessity for enhanced threat detection by offering a cutting-edge DL approach leveraging CNN. Through the potential of AI, this method aims to predict cyber threats by conducting predictive analysis of complex cybersecurity information. However, current issues in the domain revolve around the limitations of traditional techniques in accurately detecting complex attacks and adapting to emerging attack methods. Ali et al.[19] proposed an industrial control system–IDS (ICS-IDS) methodology by employing Fisher Discriminant Analysis, k-Nearest Neighbours, and an instance-based learning approach to improve detection accuracy and robustness against advanced cyberattacks. Kaliyaperumal et al.[20] proposed a hybrid IDS integrating a deep autoencoder (dAE) technique for binary classification and hierarchical density-based spatial clustering of applications with noise (HDBSCAN) model for multiclass clustering to detect Distributed Denial of Service (DDoS) attacks effectively. Dhanvijay et al.[21] presented an advanced method named ensemble of DL with prediction scoring-based optimized feature sets (EDLM-PSOFS) for IoT networks. It integrates the global attention LSTM (GA-LSTM) technique for temporal learning, correlation-adaptive LASSO regression (CALR) model for feature selection, and the exploit prediction scoring system (EPSS) method for interpretability.

Li et al.[22] proposed a genetic algorithm-tuned ensemble of deep transfer learning for netflow-based IDS for IoT (NFIoT-GATE-DTL IDS) methodology using pre-trained convolutional neural networks (CNNs) like Xception, Inception, MobileNet, MobileNetV2, DenseNet121, and EfficientNetB0, optimized via GA, to achieve high-accuracy multiclass intrusion detection in IoT networks. Ullah et al.[23] presented a systematic evaluation framework using the Entropy method and evaluation based on the Distance from Average Solution (EDAS) to identify, weigh, and rank key security features in IoT devices, thereby aiding in the effective selection of security solutions. Butt et al.[24] developed and evaluated a fog-enabled smart surveillance system within Intelligent Transportation Systems (ITS) that utilizes IoT and radio-frequency identification (RFID) technologies to reduce response times and improve resource efficiency compared to cloud-only solutions. Khan et al.[25] evaluated key authentication features for IoT devices using the COmplex PRoportional ASsessment (COPRAS) technique for enhancing security and address compatibility challenges in diverse IoT environments. Karthikeyan et al.[26] developed an adaptive metaheuristic-based feature selection with ensemble learning model for privacy-preserving cyberattack detection (AMFS-ELPPCD) technique that utilizes adaptive Harris hawk optimization (AHHO) model and ensemble classifiers including bidirectional gated recurrent unit (Bi-GRU), Wasserstein autoencoder (WAE), and deep belief network (DBN) to improve intrusion detection accuracy in IoT environments. Duraibi and Alashjaee[27] developed an improved mayfly optimization algorithm with a hybrid DL-based intrusion detection (IMFOHDL-ID) approach that uses feature selection and a long short-term memory-based deep stacked sequence-to-sequence autoencoder (LSTM-DSSAE) model, optimized by the dipper-throated optimization algorithm (DTOA) technique to improve cyberattack detection. Wu et al.[28] developed three novel stacked DL models, namely StackMean, StackMax, and StackRF, integrated with the synthetic minority oversampling technique (SMOTE) to improve cyberattack detection accuracy and robustness in Industrial IoT (IIoT) systems.

Existing studies lack a comprehensive evaluation across diverse datasets and real-time deployment scenarios, thereby restricting their practical applicability. Various techniques do not adequately address class imbalance or adversarial robustness, which are critical in IoT and IIoT environments. The utilized studies do not sufficiently explore FL with edge-cloud frameworks and often concentrate either on binary or multiclass detection without fully handling the complexity of evolving attack patterns. The research gap is in developing more generalized, adaptive, and scalable IDS solutions that strike a balance between detection accuracy, computational efficiency, and robustness in dynamic IoT ecosystems.

Materials and methods

This paper presents an IHDLM-CADEFST model for IoT-enabled cloud networks. The primary objective of this paper is to identify and enhance cybersecurity measures for IoT networks by pinpointing key threats and proposing effective strategies for detecting and mitigating these threats. To achieve that, the IHDLM-CADEFST

technique contains data pre-processing, feature selection, and classification. Figure 1 portrays the complete working flow of the IHDLM-CADEFST model.

Data pre-processing

Initially, the data pre-processing phase utilizes the standard scaler method to transform the input data into a suitable pattern. Standard Scaler is an effective normalization technique, which converts features[29]. This model ensures that all features have a mean of 0 and a standard deviation of 1, which helps normalize input data and perform feature scaling. All features x are converted as shown mathematically in Eq. (1):

$$x_{scaled} = \frac{x - \mu}{\sigma} \tag{1}$$

whereas μ and σ represent the mean and the standard deviation, respectively. The Standard Scaler is vital for normalizing features with varying kinds, thus ensuring that all features contribute consistency to the learning dynamics of the models.

Feature selection procedure

Besides, the IHDLM-CADEFST model utilizes RFE-IG for the feature selection process[30]. This model is chosen for its effectual capability in combining the merits of RFE and IG models, ensuring both relevance and ranking of features. Unlike conventional methods that depend solely on statistical correlation or mutual data, RFE-IG systematically removes less crucial features while retaining those with the highest predictive value. The model effectually prevents overfitting by reducing noise and improving model interpretability. The technique also mitigates computational overhead by removing redundant and irrelevant data. RFE-IG maintains the semantic meaning of features, which is essential for cybersecurity applications, compared to models such as principal component analysis (PCA) or simple filter methods. Overall, it contributes significantly to improved model accuracy and efficiency.

RFE serves as a beneficial device in ML, desired for its ability to enhance the model's performance and increase interpretability by highlighting the most essential characteristics. In a step-wise method, RFE prunes the less relevant features from the dataset until both the pre-defined feature counts are achieved or the model's performance reaches its best state. This streamlined method not only aids in avoiding overfitting but also enhances the model's interpretability, allowing for a clear understanding of the fundamental data forms and driving more informed analysis. The removal of low-informative features enables the IDS to focus on the most relevant data features. Thus, the IDS is becoming more efficient in identifying new intrusion patterns, improving its capability to detect novel and hidden data.

It involves a step-by-step procedure for eliminating less significant features and retraining the method. By adopting this systematic approach, this model ensures that the most pertinent features are retained, resulting

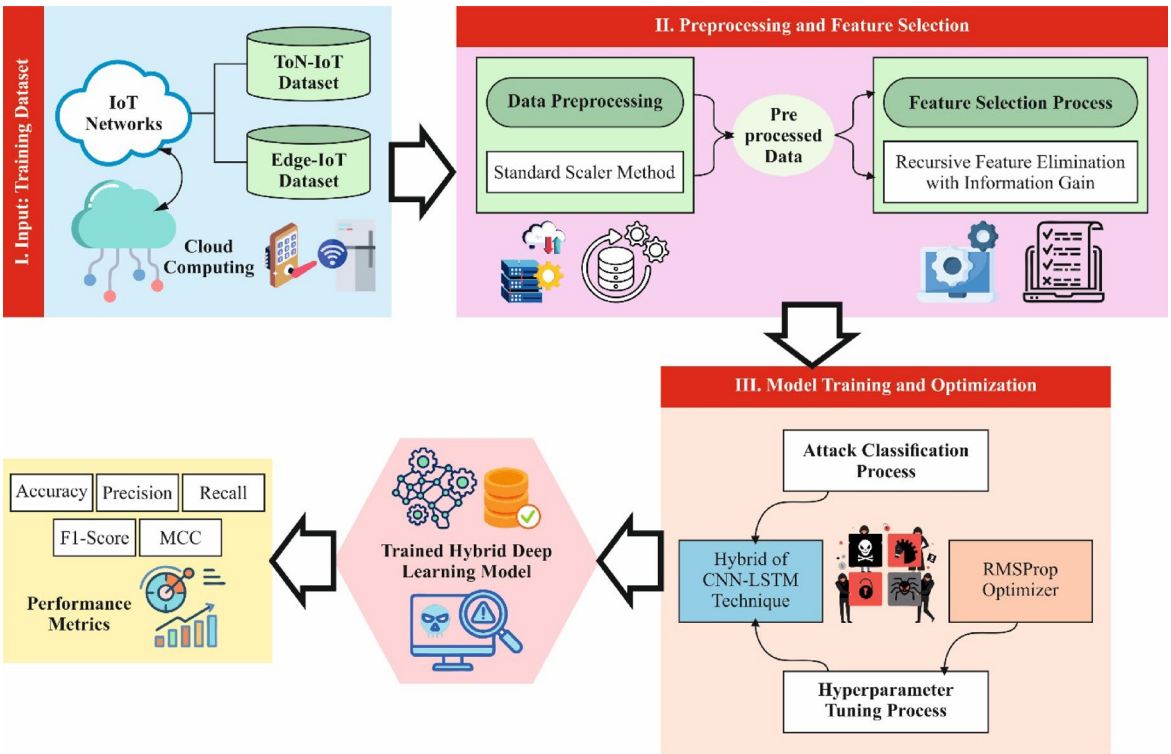

Fig. 1. Overall working flow process of the IHDLM-CADEFST approach.

in improved performance of the model utilizing random forest (RF). The iterative removal and retraining procedure continues until both the selected feature counts are achieved and the model achieves an adequate performance level.

RF starts by separating the new dataset into numerous subsets, utilizing a model named bootstrapped sampling. During the method, data points are selected at random with substitution to create every subset. These subsets act as the training data for single DTs. All trees are constructed by selecting the optimal feature from the arbitrarily chosen feature subset at every node. At each node, an arbitrary subset of k features is selected from the n features in the dataset. The significance of feature fi is calculated as shown:

$$IS\,(fi) = \sum_{r=1}^{T} \frac{Impuritydecrease_t\,(fi)}{T} \tag{2}$$

whereas fi means the ith feature, tree counts in RF is T, and the impurity generated by feature fi is signified as impurity reduction (fi).

The FS takes place in 2 steps. The RFE model designates the primary feature level, and the last feature level is made by utilizing the IG model. IG helps in the recognition of features, which provide the maximum insight into the classes, and render them robust competitors to divide the dataset. Features representing better IG are ordered as they lead to more significant drops in entropy, finally contributing to the making of efficient methods for classification targets. IG evaluates how successfully a particular feature, after being used to divide the dataset, reduces its entropy. It is described utilizing Eq. (3):

$$Entropy\,(F) = -\sum fi \times \log_2 p\,(fi) \tag{3}$$

whereas, $p\,(fi)$ denotes the occurrence probability of fi. A greater IG specifies that the feature holds better value in categorizing the data. IG is calculated utilizing Eq. (4):

$$IG\ (Fi) = Entropy\,(F) - \sum \nu \in values\,(F) \left(\frac{|F'|}{|F|}\right) \times entropy\left(F'\right) \tag{4}$$

whereas, values (F) are the promising values of the feature F and F' is a subset of F. The presented model utilizes IG to define features with high correlation to the chosen features, employing RFE. This also removes features with a lower score on IG.

Hybrid classification model

Also, the hybridization of the CNN-LSTM is employed for attack classification[31]. This model is chosen for its efficiency in extracting local spatial features from input data, whereas LSTM excels in capturing long-term temporal dependencies. This integration is beneficial in intrusion detection, where both spatial patterns and time-sequenced behaviours are critical. The technique also utilizes temporal correlations, or LSTM, which may overlook spatial hierarchies; however, the hybrid model captures both dimensions comprehensively. The method also outperforms conventional classifiers such as RF or support vector machine (SVM). This approach results in higher detection accuracy and robustness against complex and evolving attack vectors in IoT-cloud environments. Figure 2 represents the CNN-LSTM architecture.

CNN is a special DL approach intended to handle data using a grid-like structure. The main modules of the CNN are:

Convolutional layers: These layers utilize convolutional processes, employing learnable filters, to remove temporal or spatial features. It is formulated as:

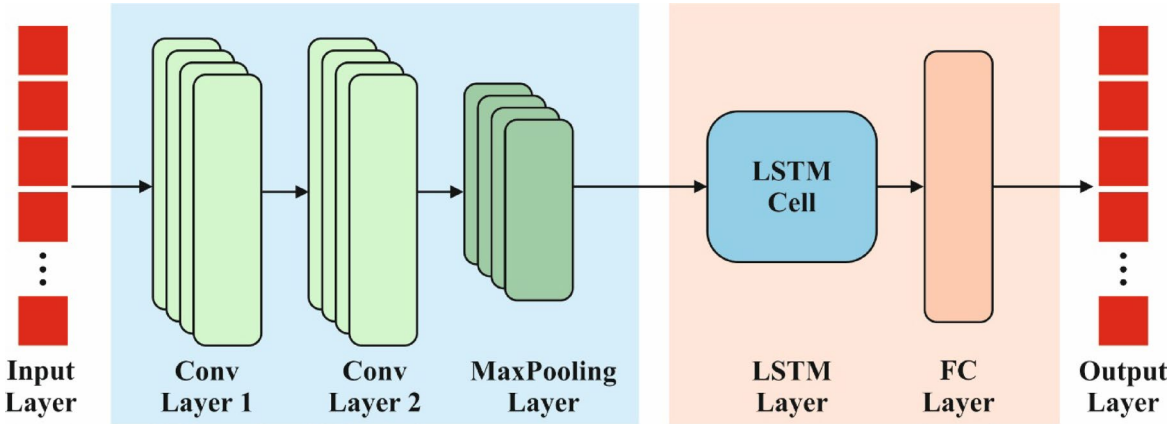

Fig. 2. Architecture of CNN-LSTM.

$$z_{i,j,k} = \sum_{m=1}^{M} \sum_{n=1}^{N} x_{i+m-1,j+n-1} \cdot w_{m,n,k} + b_k \tag{5}$$

whereas $z_{i,j,k}$ mean output feature mapping, x refers to input data, $w_{m,n,k}$ signify the kth filter of dimensions Mx N, and b_k refers to the biased term.

Pooling layers: These layers downsample the feature mapping and typically use average or max pooling to reduce calculation and dimensionality.

Fully connected (FC) layers: These layers map the removed features to the output class or value.

LSTM is a type of RNN capable of learning longer-term dependencies. The major equations of the LSTM cell are shown below:

$$f_t = \sigma\ (W_f \cdot\ [h_{t-1},\ x_t] + b_f) \tag{6}$$

$$i_t = \sigma\ (W_i \cdot\ [h_{t-1},\ x_t] + b_i) \tag{7}$$

$$\widetilde{C}_t = \tanh\left(W_C \cdot\ [h_{t-1},\ x_t] + b_C\right) \tag{8}$$

$$C_t = f_t \odot\ C_{t-1} + i_t \odot\ \widetilde{C}_t \tag{9}$$

$$o_t = \sigma\ (W_0 \cdot\ [h_{t-1},\ x_t] + b_0) \tag{10}$$

$$h_t = o_t \odot\ \tanh\left(C_t\right) \tag{11}$$

whereas $_{ft}$, o_t, represent forget, input, and output gates, consistently, $\widetilde{C}_t$ and C_t denote candidate and upgraded cell states, respectively. h_t denotes HL at time-step t, $tanh$ and σ represent hyperbolic tangent and sigmoid activation functions, respectively. This model is a new structure that utilizes the power of LSTM and CNN networks for modelling sequences. This incorporation is mainly efficient for data that uses either spatial or temporal features, as it allows the removal of localized designs while taking into account longer-term dependencies. It comprises four major elements: the Input Layer, Transition Layer, Sequential Layer (LSTM), and Feature Extraction (CNN).

Input layer

It accepts time-series data. These features are usually multi-dimensional, comprising either temporal or spatial data. The input data is organized to connect with the following layers for processing.

Feature extraction (CNN)

The CNN element is responsible for removing temporal or spatial characteristics from the input data. This model begins with a convolutional layer that utilizes numerous filters to identify patterns such as textures, edges, or specific features within the input data. Following the convolutional processes, the ReLU introduces nonlinearity to enhance the method's ability to capture seizure composite relations. Pooling layers, specifically max-pooling, reduce the spatial size of feature maps while preserving essential data.

Transition layer

If the feature mapping is created, the following stage is to reduce their sizes for additional sequential handling. It is achieved by both fattening the feature mapping into a 1D vector and using global pooling processes. These processes convert the feature mapping into compact representations that retain essential information, making them suitable for sequential handling. The lessened feature mapping is redesigned and considered as a sequential dataset.

Sequential layer (LSTM)

It processes the removed characteristics in sequence, permitting it to account for temporal dependencies of the model and consider designs over time. The gating mechanisms and memory cells of the LSTM ensure the maintenance of relevant information, while the removal of low-priority data makes it highly efficient for tasks. The CNN layer's output, after being pooled or flattened, serves as the input to the LSTM layers. This incorporation enables the method to leverage the sequence modelling capabilities of LSTMs and the spatial extraction abilities of CNNs.

Output layer

The last layer is a dense layer that gives the forecast output. The hybrid CNN-LSTM structure illustrates the data flow from an input layer through the CNN and LSTM layers, ultimately reaching an output layer. This structure is tailored to successfully process the time-series data complexity by merging CNN and LSTM.

RMSprop is an adaptable learning process that tries to improve AdaGrad[32]. It computes an exponential moving average before calculating the total quantity of squared gradients, as AdaGrad does.

$$w_{c+1} = w_c - \frac{\alpha_{\tau}}{(v_c + \epsilon)^{\frac{1}{2}}} \times \left[\frac{\delta L}{\delta w_c}\right] \tag{12}$$

Therefore,

$$v_\tau = \beta\, v_{\tau-1} + (1-\beta) \times \left[\frac{\delta L}{\delta w_\tau}\right]^2 \tag{13}$$

whereas, W_t signifies the weight at t time, ∂L specifies the derivative of the function of loss, W_{t+1} displays the weight at time $t+1$, α_f epitomizes the rate of learning at time t, ∂W_t symbolizes the weight at time t, β indicates the move average parameter, y_f designates the amount of the square of previous gradients, ϵ suggests the smallest positive constant. The final model of the Adam optimizer is gained by capturing the equation utilized in the above-mentioned dual techniques:

$$m_c = \beta_1 m_{c-1} + (1-\beta_1)\left[\frac{\delta L}{\delta w_\tau}\right] v_c = \beta_2 v_{c-1} + (1-\beta_2)\left[\frac{\delta L}{\delta w_\tau}\right]^2 \tag{14}$$

In Eq. (13), β_1 and β_2 represent the average decay rates of the gradient in the above dual techniques. α displays the rate of learning.

Experimental analysis

The IHDLM-CADEFST methodology is evaluated using a dual dataset: ToN-IoT[33] and Edge-IIoT[34]. The ToN-IoT dataset comprises a total of 119,957 samples under nine attack types. The dataset contains 63 attributes, but only 28 of these are selected for analysis. Whereas, the Edge-IIoT dataset comprises 36,000 samples across 12 types of attacks. It holds 42 features in total, but only 24 were chosen. The complete details of this dataset are presented in Table 1 below.

Figure 3 shows the classifier results of the IHDLM-CADEFST approach. Figure 3a,b present the confusion matrix, showing the accurate detection and classification of each class label at a 70:30 split of the ToN-IoT dataset. While the Fig. 3c,d displays the confusion matrix, showing the precise classification of each class on a 70:30 split of the Edge-IIoT dataset.

Table 2; Fig. 4 illustrate the cybersecurity detection capabilities of the IHDLM-CADEFST model on the ToN-IoT dataset. With 70% TRPHE, the IHDLM-CADEFST model attains an average $accu_y$ of 99.43%, $prec_n$ of 92.52%, $reca_l$ of 88.29%, $F1_{Score}$ of 89.45%, MCC of 89.47%, and Kappa of 89.53%. Finally, under 30% TSPHE, the IHDLM-CADEFST model attains an average $accu_y$ of 99.45%, $prec_n$ of 91.01%, $reca_l$ of 87.61%, $F1_{Score}$ of 88.51%, MCC of 88.47%, and Kappa of 88.53%.

Table 3; Fig. 5 establish the cybersecurity detection of the IHDLM-CADEFST method on the Edge-IIoT dataset. Based on 70% TRPHE, the IHDLM-CADEFST model obtains an average $accu_y$ of 99.19%, $prec_n$ of 95.12%, $reca_l$ of 95.12%, $F1_{Score}$ of 95.12%, MCC of 94.68%, and Kappa of 94.74%. At last, on 30% TSPHE, the IHDLM-CADEFST model obtains an average $accu_y$ of 99.14%, $prec_n$ of 94.86%, $reca_l$ of 94.87%, $F1_{Score}$ of 94.85%, MCC of 94.39%, and Kappa of 94.46%.

Dataset	Attack type	Cardinality
ToN-IoT dataset Total features: 63 Selected features: 28	"Normal"	78,369
	"MiTM"	336
	"DoS"	5440
	"DDoS"	5987
	"Password"	6016
	"Injection"	5867
	"XSS"	5951
	"Ransomware"	5976
	"Backdoor"	6015
	Total	119,957
Edge-IIoT dataset Total features: 42 Selected features: 24	"Normal"	3000
	"DDoS-UDP"	3000
	"DDoS-ICMP"	3000
	"SQL injection"	3000
	"DDoS-TCP"	3000
	"Password"	3000
	"DDoS-HTTP"	3000
	"Uploading"	3000
	"Backdoor"	3000
	"XSS"	3000
	"Ransomware"	3000
	"Fingerprinting"	3000
	Total	36,000

Table 1. Details of ToN-IoT and Edge-IIoT dataset.

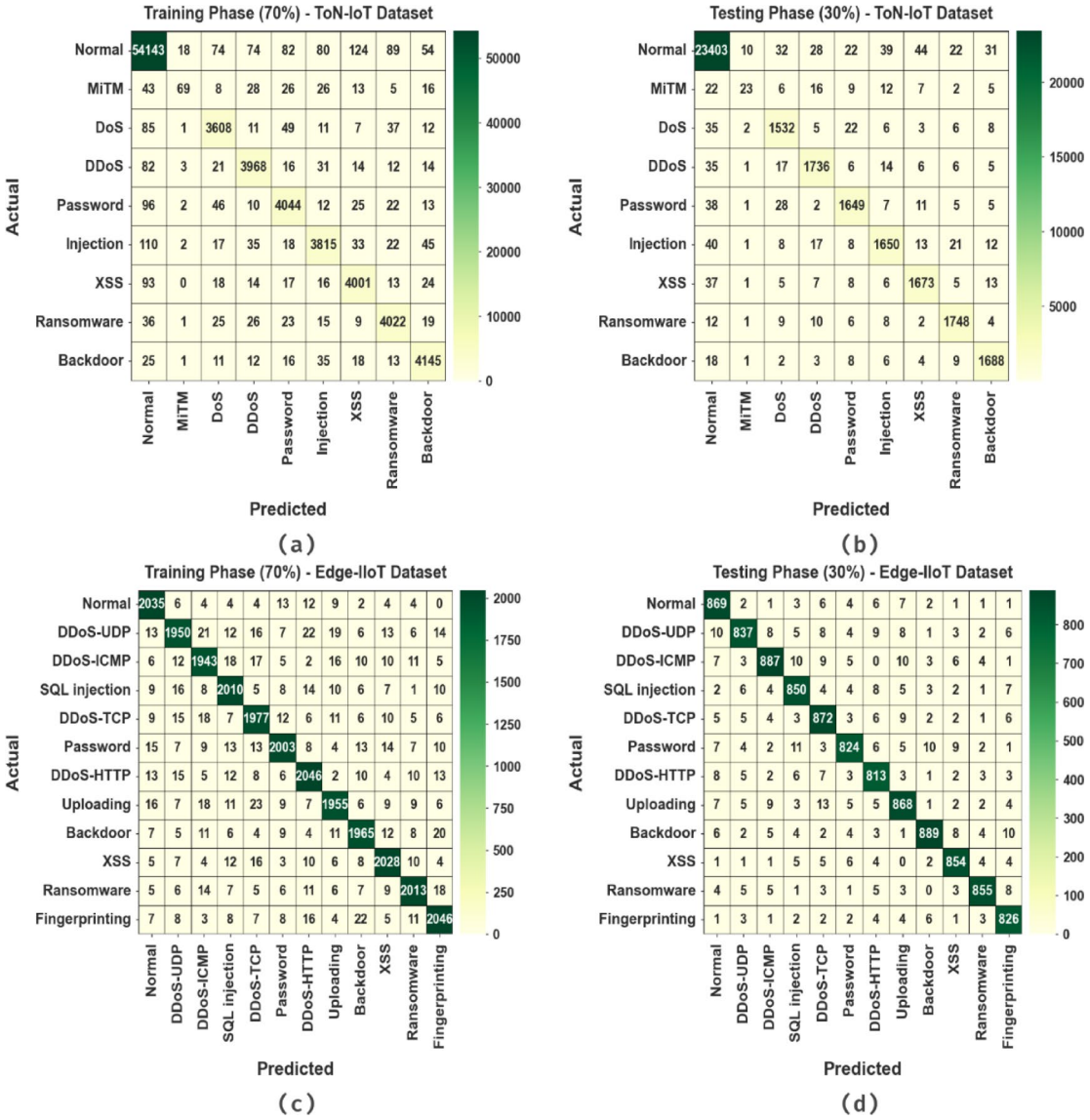

Fig. 3. Confusion matrices of 70:30 (**a**,**b**) ToN-IoT dataset and (**c**,**d**) Edge-IIoT dataset.

Figure 6 demonstrates the classifier solutions of the IHDLM-CADEFST methodology on the ToN-IoT and Edge-IIoT datasets. Figure 6a,c exhibits the accuracy analysis of the IHDLM-CADEFST technique. The figure suggests that the IHDLM-CADEFST model achieves its maximum values during rising epochs. Likewise, the increasing validation over training elucidates that the IHDLM-CADEFST model effectively learns from the test dataset. Eventually, Fig. 6b,d showcases the loss investigation of the IHDLM-CADEFST model. It is observed that the IHDLM-CADEFST model learns effectively from the testing dataset.

Figure 7 represents the classifier performance of the IHDLM-CADEFST approach on ToN-IoT and Edge-IIoT datasets. Figure 7a and c exemplifies the PR examination of the IHDLM-CADEFST method. The outcomes specified that the IHDLM-CADEFST resulted in an elevated PR value. Furthermore, the IHDLM-CADEFST method reaches a superior value of PR in each class. However, Fig. 7b and d exemplifies the ROC inspection of the IHDLM-CADEFST method. Moreover, the IHDLM-CADEFST method can reach elevated ROC values for each class.

Table 4; Figs. 8 and 9 present the comparative outcome of the IHDLM-CADEFST model on the ToN-IoT and Edge-IIoT datasets, along with current methods, at various metrics[20–22,35–38]. In the ToN-IoT dataset, the table values indicated that the present models, such as dAE, HDBSCAN, CALR, DNN, CART, XGBoost, CNN-RNN, RepuTE, Neural Network, and SVM, have shown the worst performance. Whereas, the IHDLM-CADEFST technique achieved higher $accu_y$, $prec_n$, $reca_l$, and $F1_{Score}$ of 99.45%, 91.01%, 87.61%, and 88.51%, respectively. In the Edge-IIoT dataset, the table values emphasized that the existing techniques, namely EDLM-PSOFS, GA-LSTM, EfficientNetB0, RF, KNN, SVM, XGBoost, LightGBM, TabPFN, and Voting Classifier, illustrated worse performance. In the meantime, the IHDLM-CADEFST model has obtained the highest $accu_y$, $prec_n$, $reca_l$, and $F1_{Score}$ of 99.19%, 95.12%, 95.12%, and 95.12%, correspondingly.

	Class labels	$Accu_y$	$Prec_n$	$Recal_l$	$F1_{Score}$	MCC	Kappa
ToN-IoT Dataset	TRPHE (70%)						
	Normal	98.61	98.96	98.91	98.94	96.94	97.00
	MiTM	99.77	71.13	29.49	41.69	45.71	45.78
	DoS	99.48	94.25	94.43	94.34	94.07	94.13
	DDoS	99.52	94.97	95.36	95.17	94.91	94.98
	Password	99.44	94.24	94.71	94.47	94.18	94.25
	Injection	99.40	94.41	93.12	93.76	93.44	93.50
	XSS	99.48	94.27	95.35	94.81	94.54	94.59
	Ransomware	99.56	94.97	96.31	95.64	95.41	95.48
	Backdoor	99.61	95.46	96.94	96.19	95.99	96.05
	Average	99.43	92.52	88.29	89.45	89.47	89.53
	TSPHE (30%)						
	Normal	98.71	99.00	99.04	99.02	97.13	97.19
	MiTM	99.73	56.10	22.55	32.17	35.46	35.52
	DoS	99.46	93.47	94.63	94.05	93.77	93.84
	DDoS	99.51	95.18	95.07	95.12	94.86	94.94
	Password	99.48	94.88	94.44	94.66	94.39	94.45
	Injection	99.39	94.39	93.22	93.80	93.49	93.56
	XSS	99.52	94.90	95.33	95.11	94.86	94.93
	Ransomware	99.64	95.83	97.11	96.47	96.28	96.34
	Backdoor	99.63	95.31	97.07	96.18	95.99	96.05
	Average	99.45	91.01	87.61	88.51	88.47	88.53

Table 2. Cybersecurity detection of the IHDLM-CADEFST model on the ToN-IoT dataset.

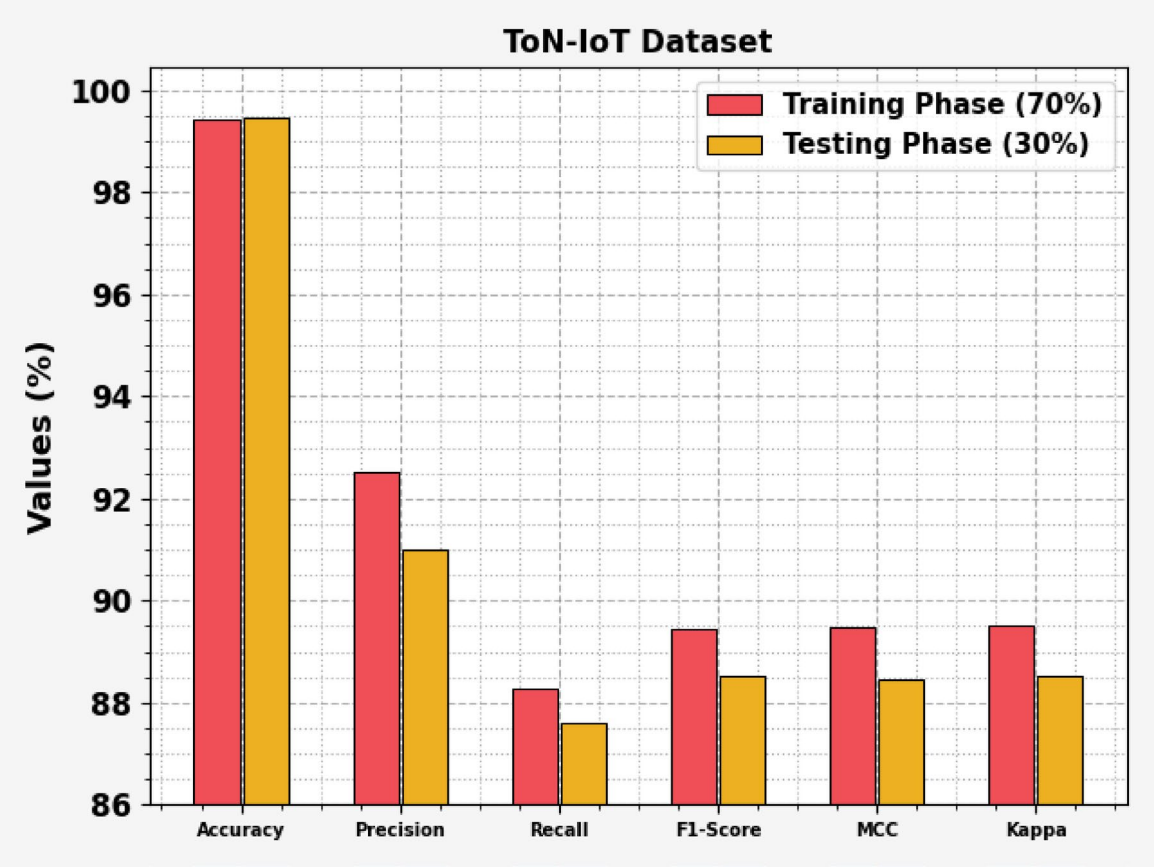

Fig. 4. Average values of the IHDLM-CADEFST model on the ToN-IoT dataset.

	Class labels	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{Score}$	MCC	Kappa
Edge-IIoT dataset	TRPHE (70%)						
	Normal	99.34	95.09	97.04	96.06	95.70	95.77
	DDoS-UDP	99.00	94.94	92.90	93.91	93.37	93.42
	DDoS-ICMP	99.10	94.41	94.55	94.48	93.99	94.06
	SQL injection	99.19	94.81	95.53	95.17	94.73	94.79
	DDoS-TCP	99.12	94.37	94.96	94.66	94.18	94.24
	Password	99.21	95.88	94.66	95.27	94.84	94.92
	DDoS-HTTP	99.17	94.81	95.43	95.12	94.66	94.73
	Uploading	99.13	95.23	94.17	94.70	94.22	94.28
	Backdoor	99.23	95.34	95.30	95.32	94.90	94.96
	XSS	99.28	95.44	95.98	95.71	95.31	95.38
	Ransomware	99.30	96.09	95.54	95.81	95.43	95.50
	Fingerprinting	99.19	95.07	95.38	95.23	94.78	94.85
	Average	99.19	95.12	95.12	95.12	94.68	94.74
	TSPHE (30%)						
	Normal	99.15	93.74	96.23	94.97	94.52	94.60
	DDoS-UDP	99.03	95.33	92.90	94.10	93.58	93.65
	DDoS-ICMP	99.07	95.48	93.86	94.66	94.16	94.23
	SQL injection	99.08	94.13	94.87	94.50	94.00	94.06
	DDoS-TCP	99.00	93.36	94.99	94.17	93.63	93.69
	Password	99.06	95.26	93.21	94.23	93.72	93.80
	DDoS-HTTP	99.08	93.56	94.98	94.26	93.77	93.85
	Uploading	98.97	94.04	93.94	93.99	93.43	93.50
	Backdoor	99.26	96.63	94.78	95.69	95.29	95.35
	XSS	99.33	95.63	96.28	95.96	95.59	95.65
	Ransomware	99.40	96.94	95.74	96.34	96.01	96.06
	Fingerprinting	99.26	94.18	96.61	95.38	94.99	95.05
	Average	99.14	94.86	94.87	94.85	94.39	94.46

Table 3. Cybersecurity detection of IHDLM-CADEFST model on Edge-IIoT dataset.

Table 5; Figs. 10 and 11 illustrate the computational time (CT) analysis of the IHDLM-CADEFST technique in comparison to existing models under the ToN-IoT and Edge-IIoT datasets. For the ToN-IoT dataset, the IHDLM-CADEFST technique achieved a CT of just 3.29 s, outperforming existing approaches such as DNN at 6.74 s, CNN-RNN at 10.54 s, and SVM at 11.91 s. Similarly, for the Edge-IIoT dataset, the IHDLM-CADEFST model attained a CT of 6.82 s, which is notably faster than methods like GA-LSTM at 11.91 s, RF at 21.23 s, and EfficientNetB0 at 26.79 s. This highlights the efficiency and scalability of the IHDLM-CADEFST model for real-time detection tasks.

Table 6; Figs. 12 and 13 demonstrate the ablation study of the IHDLM-CADEFST methodology. For the ToN-IoT dataset, the IHDLM-CADEFST methodology achieved an $accu_y$ of 99.45%, $prec_n$ of 91.01%, $reca_l$ of 87.61%, and $F1_{Score}$ of 88.51%, outperforming RFE-IG with 97.53%, 89.17%, 85.72%, and 86.25%, RMSProp with 98.06%, 89.72%, 86.35%, and 87.03%, and CNN-LSTM with 98.67%, 90.23%, 87.02%, and 87.77%, for all metrics respectively. Similarly, for the Edge-IIoT dataset, the IHDLM-CADEFST model attained top performance with an $accu_y$ of 99.45%, $prec_n$ of 91.01%, $reca_l$ of 87.61%, and $F1_{Score}$ of 88.51%, surpassing RFE-IG at 97.42%, 88.89%, 85.90%, and 86.51%, RMSProp at 98.07%, 89.68%, 86.55%, and 87.11%, and CNN-LSTM at 98.65%, 90.42%, 87.11%, and 87.78%, for all metrics respectively. These results highlight the superior generalization capability and robustness of the IHDLM-CADEFST model across diverse IoT datasets.

Conclusion

This paper presents an IHDLM-CADEFST model for IoT-enabled cloud networks. This paper aims to explore and enhance cybersecurity measures for IoT networks by identifying key threats and proposing effective strategies for detecting and mitigating these threats. At the primary stage, the data pre-processing phase utilizes the standard scaler method to transform the input data into a suitable pattern. Furthermore, the FS strategy is implemented using the RFE-IG model to identify the most relevant features and prevent overfitting. Finally, a hybrid CNN-LSTM classifier is employed for the attack classification method, with the RMSprop optimizer used to enhance classification performance. The experimentation of the IHDLM-CADEFST approach is examined under the ToN-IoT and Edge-IIoT datasets. The comparison analysis of the IHDLM-CADEFST approach illustrated superior accuracy values of 99.45% and 99.19%, respectively, compared to recent models on the dual dataset. The limitations of the IHDLM-CADEFST approach comprise the dependence on simulated datasets. The model is not effectually examined under highly dynamic network conditions and varying attack intensities,

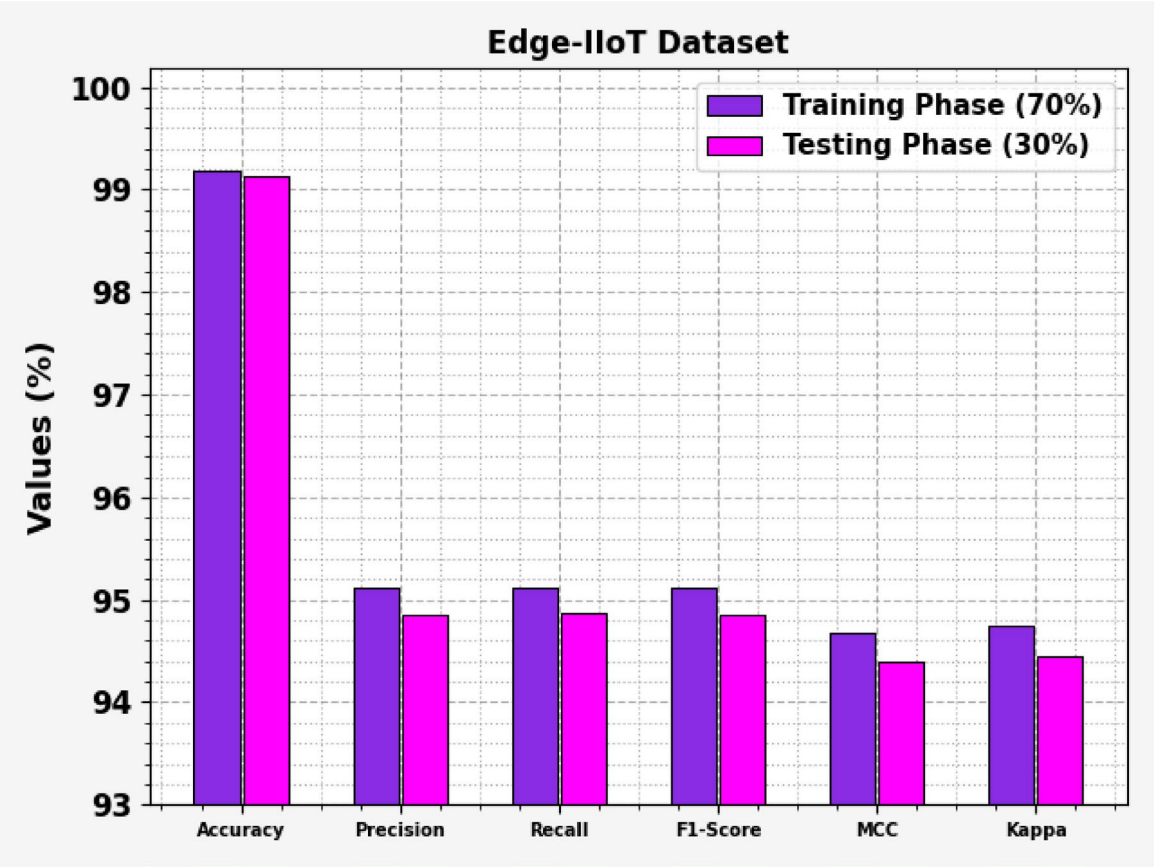

Fig. 5. Average values of the IHDLM-CADEFST model on the Edge-IIoT dataset.

and also does not fully capture real-world IoT network complexities and traffic patterns. The computational overhead associated with continuous monitoring and analysis could pose challenges for resource-constrained IoT devices. Potential privacy concerns related to data sharing in distributed environments are also not appropriately addressed. Future studies should focus on validating the model with real-world data, optimizing algorithms for low-power devices, and improving privacy-preserving mechanisms for ensuring secure and efficient deployment in diverse IoT settings.

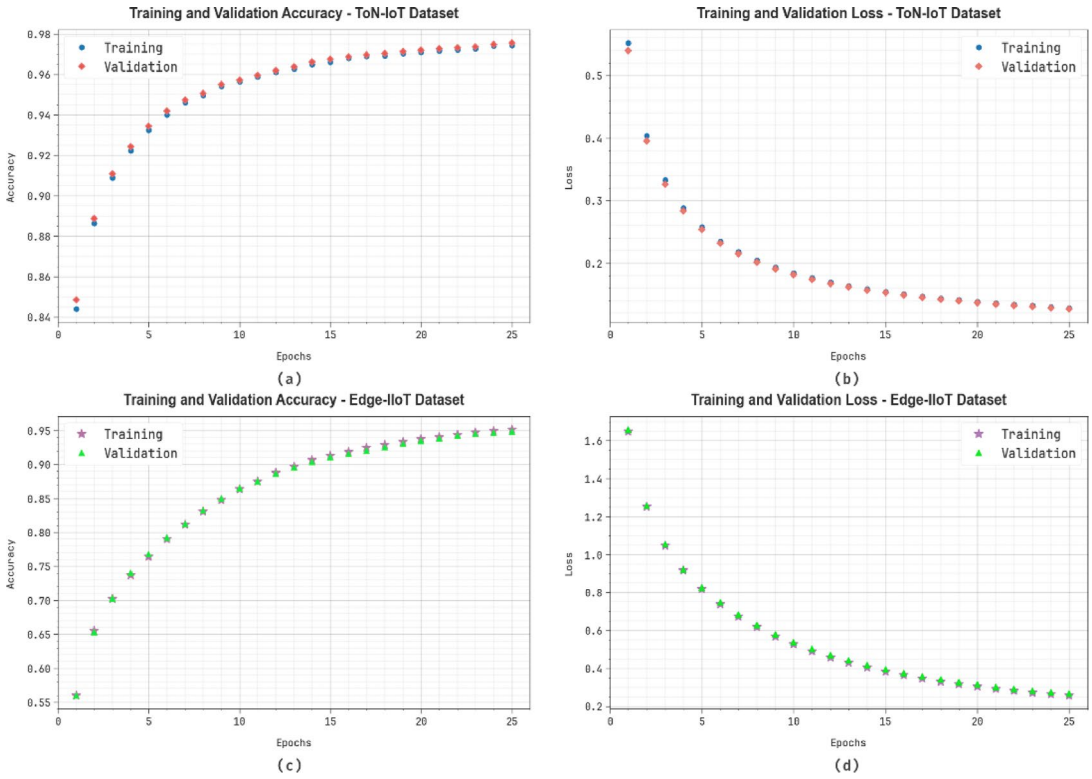

Fig. 6. (**a**–**c**) $Accu_y$ and (**b**–**d**) Loss curves of the IHDLM-CADEFST model on the ToN-IoT and Edge-IIoT datasets.

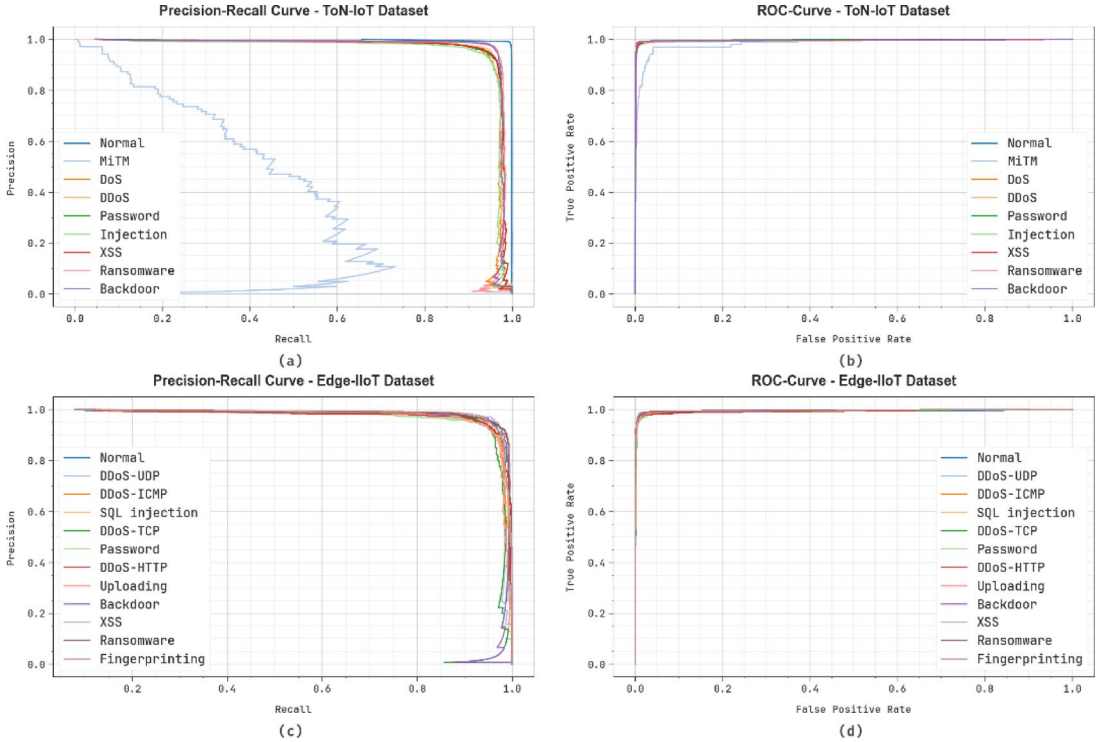

Fig. 7. (**a**–**c**) PR and (**b**–**d**) ROC curves of IHDLM-CADEFST model on ToN-IoT and Edge-IIoT dataset.

Dataset	Approach	$Accu_y$	$Prec_n$	$Recal$	$F1_{Score}$
ToN-IoT dataset	dAE	87.78	90.70	87.03	85.05
	HDBSCAN	97.13	88.87	85.50	82.00
	CALR	92.74	90.41	83.65	86.42
	DNN	94.17	88.66	81.92	81.45
	CART	77.00	90.08	86.33	84.46
	XGBoost	96.50	88.32	84.94	81.23
	CNN-RNN	91.97	89.88	83.00	85.82
	RepuTE algorithm	99.18	87.34	81.10	82.77
	Neural network	97.12	87.02	81.95	83.85
	SVM	90.97	89.56	81.94	86.88
	IHDLM-CADEFST	99.45	91.01	87.61	88.51
Edge-IIoT dataset	EDLM-PSOFS	94.06	92.76	92.13	93.96
	GA-LSTM	95.39	95.61	93.48	89.79
	EfficientNetB0	91.02	90.61	91.11	93.38
	RF	93.42	92.17	91.45	93.36
	KNN	94.60	94.88	92.77	89.27
	SVM	90.28	90.01	90.54	92.66
	XGBoost	93.37	91.39	89.54	91.86
	LightGBM	93.02	89.73	90.69	92.32
	TabPFN	96.86	92.35	89.95	90.63
	Voting classifier	89.95	94.67	92.50	92.95
	IHDLM-CADEFST	99.19	95.12	95.12	95.12

Table 4. Comparative study of IHDLM-CADEFST model on ToN-IoT and Edge-IIoT dataset[20–22,35–38].

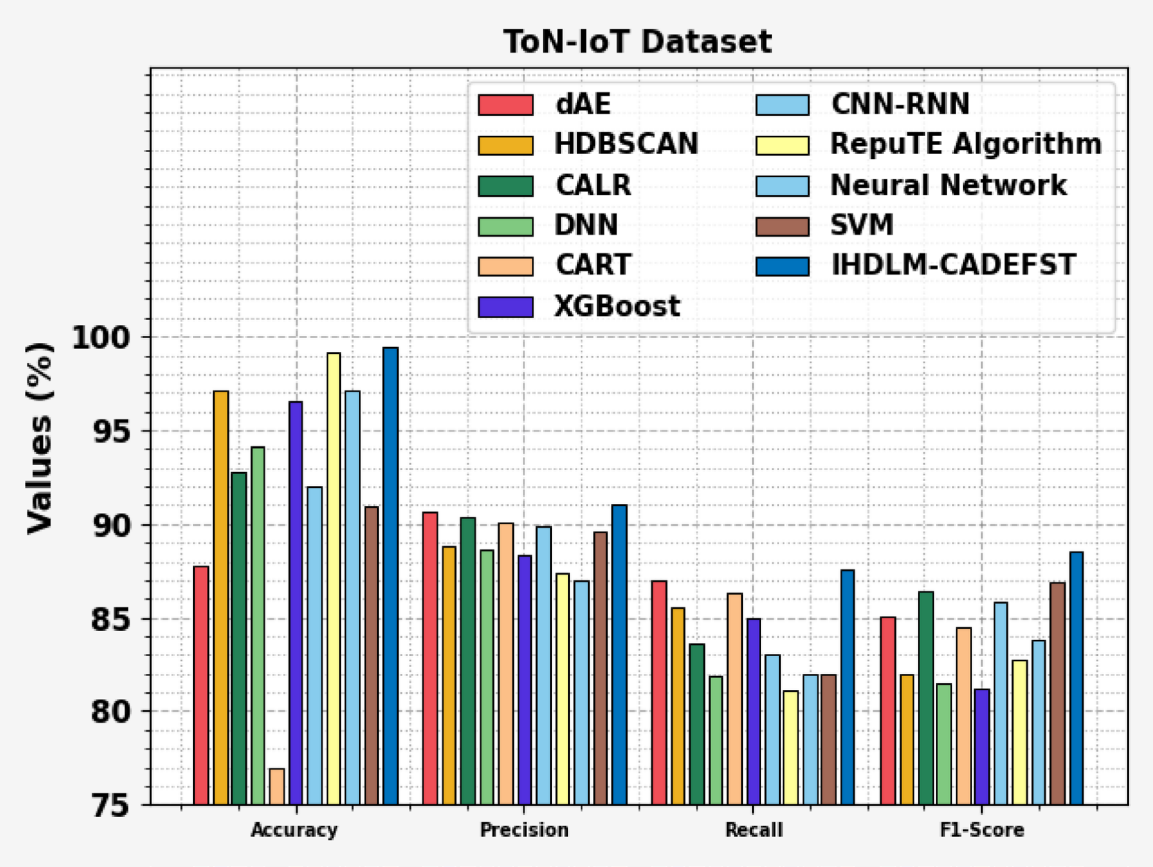

Fig. 8. Comparative study of IHDLM-CADEFST model under the ToN-IoT dataset.

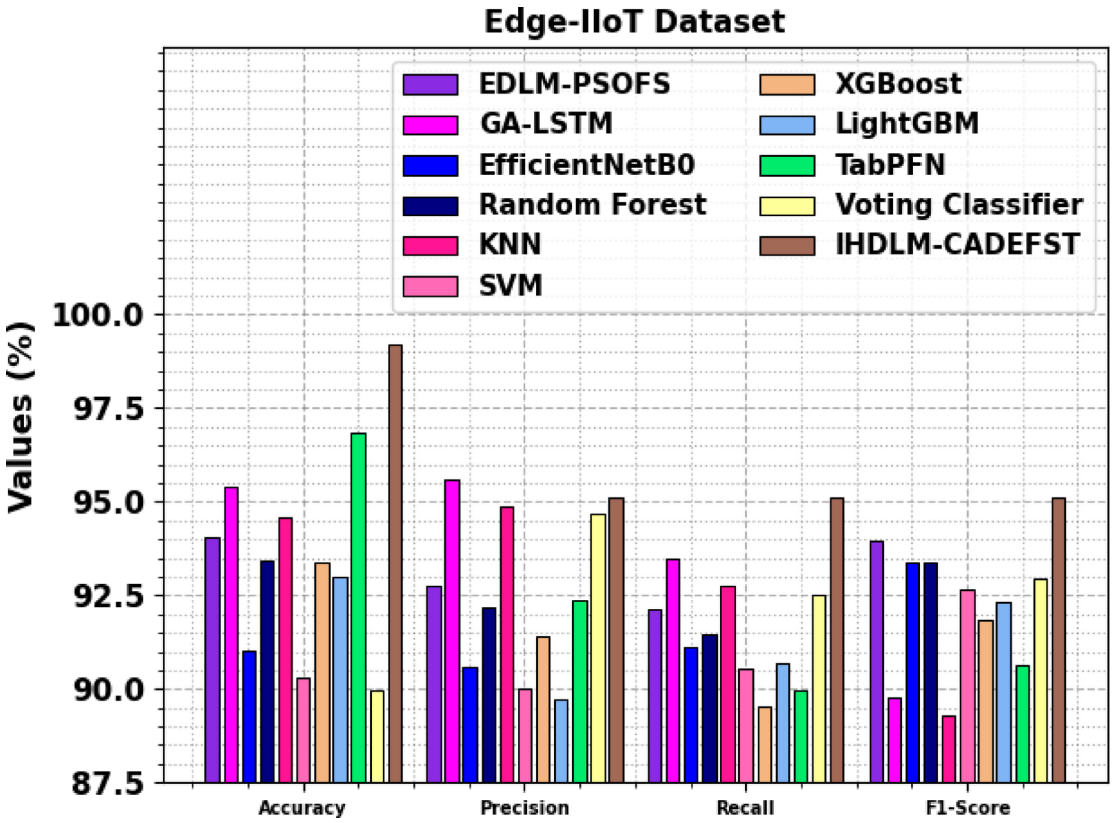

Fig. 9. Comparative study of IHDLM-CADEFST model under the Edge-IIoT dataset.

Dataset	Approach	CT (s)
ToN-IoT dataset	dAE	13.70
	HDBSCAN	8.39
	CALR	10.94
	DNN	6.74
	CART	12.26
	XGBoost	8.87
	CNN-RNN	10.54
	RepuTE algorithm	12.58
	Neural network	14.23
	SVM	11.91
	IHDLM-CADEFST	3.29
Edge-IIoT dataset	EDLM-PSOFS	12.56
	GA-LSTM	11.91
	EfficientNetB0	26.79
	Random forest	21.23
	KNN	19.36
	SVM	11.90
	XGBoost	24.79
	LightGBM	12.95
	TabPFN	26.84
	Voting classifier	10.26
	IHDLM-CADEFST	6.82

Table 5. CT analysis of IHDLM-CADEFST technique with existing models under ToN-IoT and Edge-IIoT datasets.

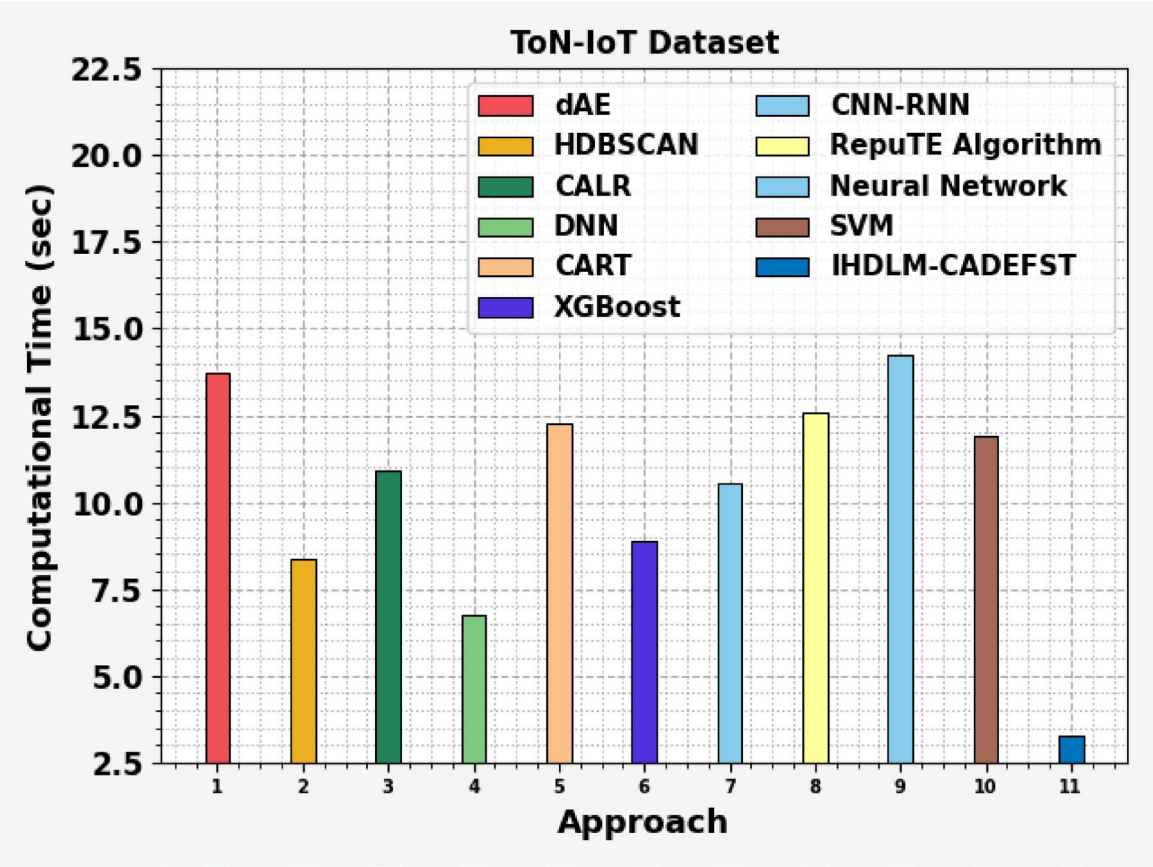

Fig. 10. CT analysis of IHDLM-CADEFST technique with existing models under the ToN-IoT dataset.

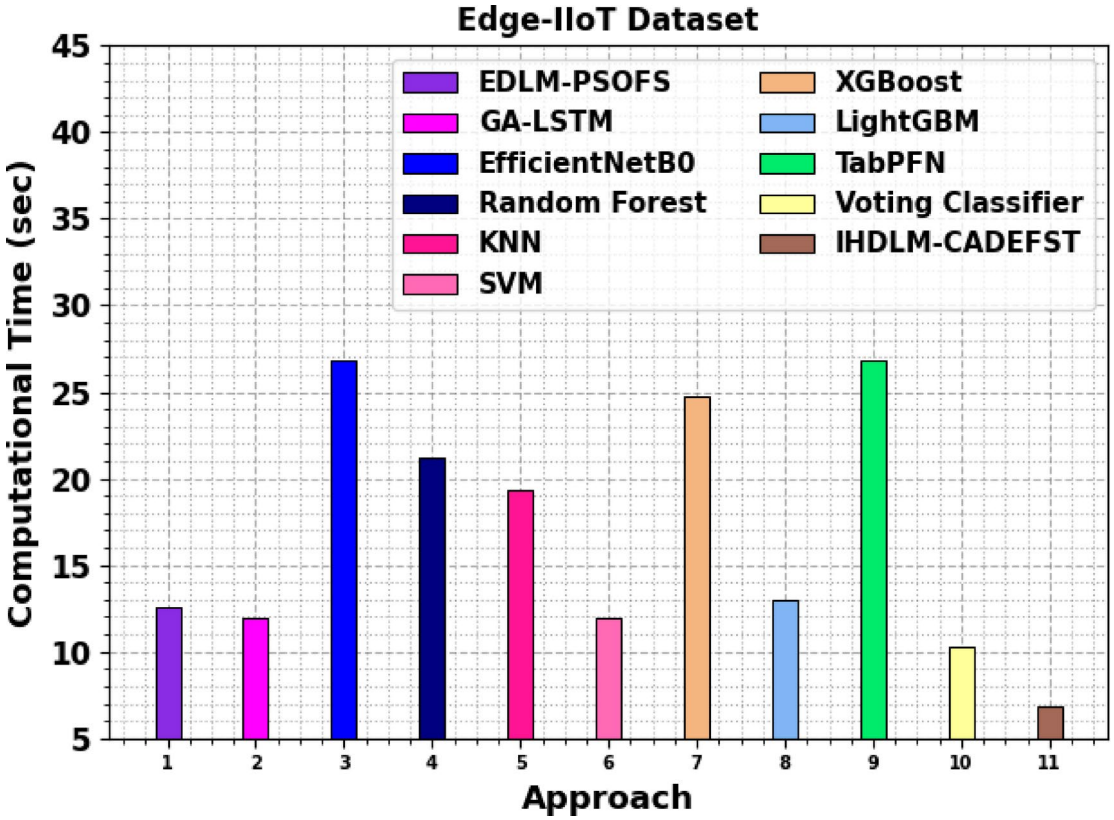

Fig. 11. CT analysis of IHDLM-CADEFST technique with existing models under the Edge-IIoT dataset.

Dataset	Approach	$Accu_y$	$Prec_n$	$Recal$	$F1_{Score}$
ToN-IoT dataset	RFE-IG	97.53	89.17	85.72	86.25
	RMSProp	98.06	89.72	86.35	87.03
	CNN-LSTM	98.67	90.23	87.02	87.77
	IHDLM-CADEFST	99.45	91.01	87.61	88.51
Edge-IIoT dataset	RFE-IG	97.42	88.89	85.90	86.51
	RMSProp	98.07	89.68	86.55	87.11
	CNN-LSTM	98.65	90.42	87.11	87.78
	IHDLM-CADEFST	99.45	91.01	87.61	88.51

Table 6. Result analysis of the ablation study of the IHDLM-CADEFST methodology.

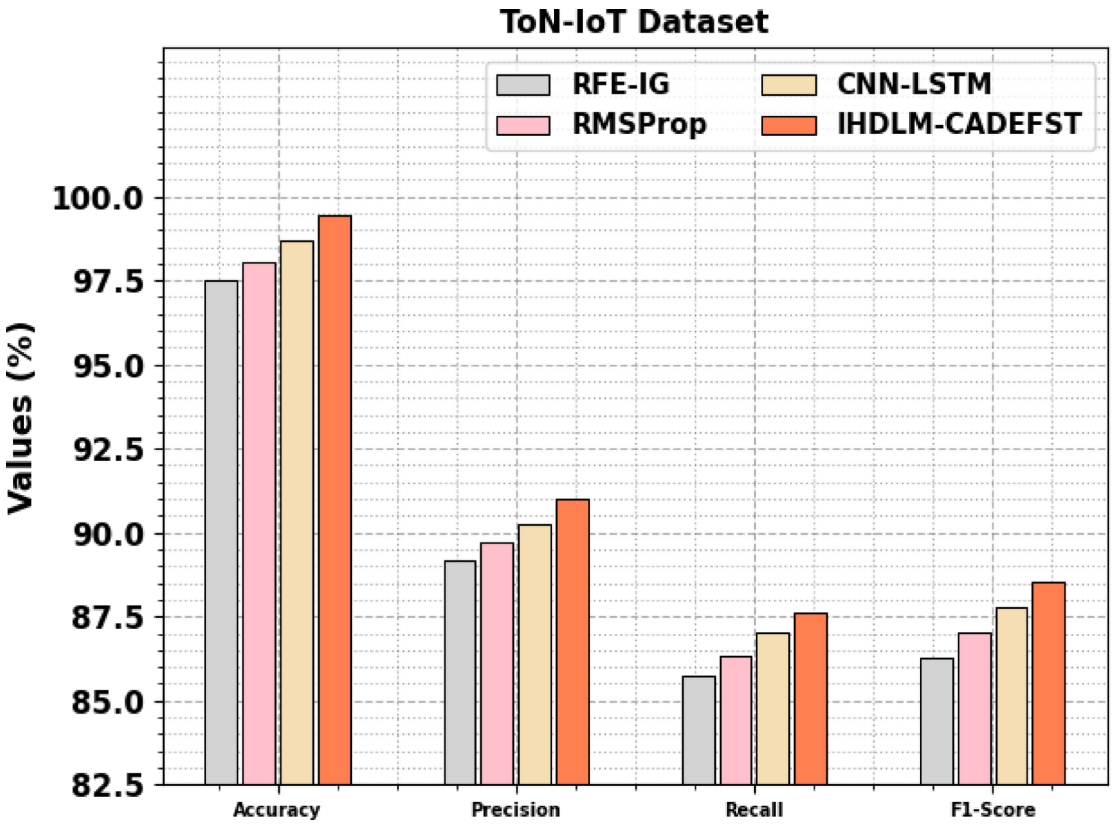

Fig. 12. Result analysis of the ablation study of the IHDLM-CADEFST methodology under the ToN-IoT dataset.

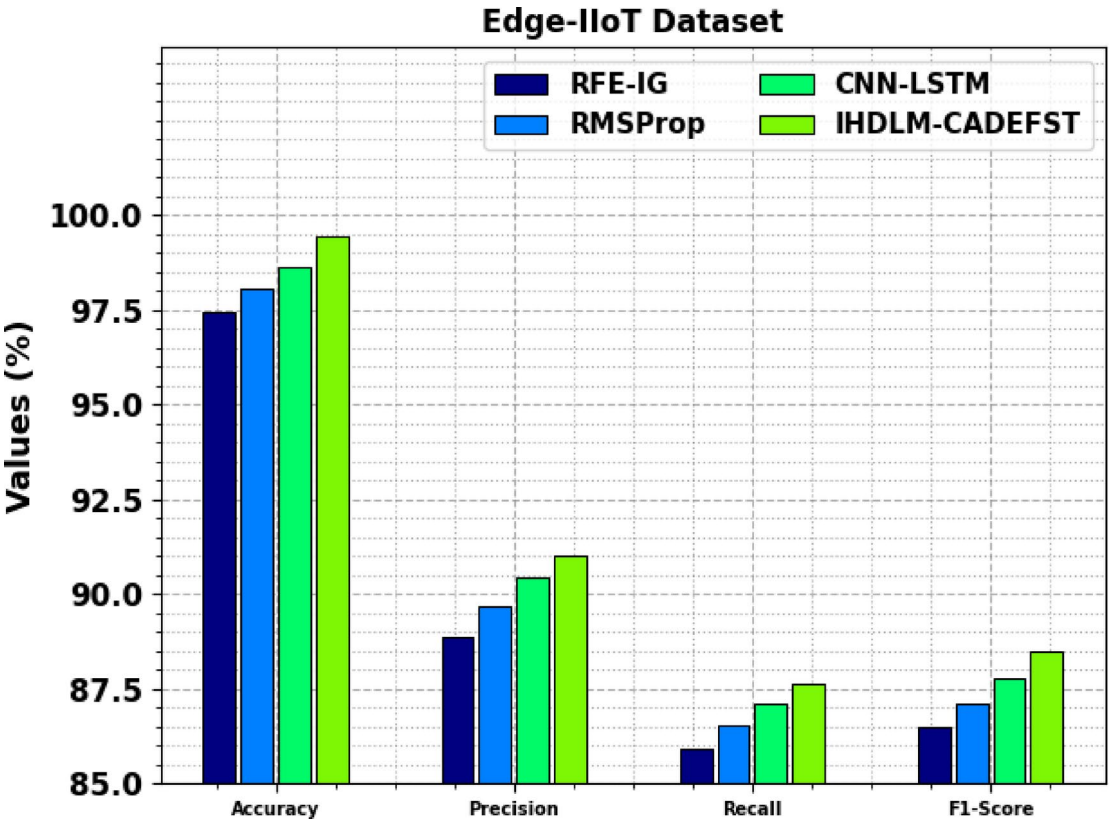

Fig. 13. Result analysis of the ablation study of the IHDLM-CADEFST methodology under the Edge-IIoT dataset.

Data availability

The data that support the findings of this study are openly available in the Kaggle repository at https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot, https://www.kaggle.com/datasets/dhoogla/cictoniot, reference number[33,34].

Received: 15 June 2025; Accepted: 24 July 2025
Published online: 30 September 2025

References

1. Lee, I. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet*. **12**(9), 157 (2020).
2. Kuzlu, M., Fair, C. & Guler, O. Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover. Internet Things*. **1**(1), 7 (2021).
3. Andrade, R. O., Yoo, S. G., Tello-Oquendo, L. & Ortiz-Garcés, I. A comprehensive study of the IoT cybersecurity in smart cities. *IEEE Access*. **8**, 228922–228941 (2020).
4. Al-Hagery, M. A. & Abdalla Musa, A. I. Enhancing network security using possibility neutrosophic hypersoft set for cyberattack detection. *Int. J. Neutrosophic Sci. (IJNS)*. **25**(1). (2025).
5. Altulaihan, E., Almaiah, M. A. & Aljughaiman, A. Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. *Electronics*. **11**(20), 3330 (2022).
6. Ganji, K. & Afshan, N. A bibliometric review of the internet of things (IoT) on cybersecurity issues. *J. Sci. Technol. Policy Manag.* (2024).
7. Tareq, I., Elbagoury, B. M., El-Regaily, S. & El-Horbaty, E. S. M. Analysis of ton-iot, unw-nb15, and edge-iiot datasets using dl in cybersecurity for iot. *Appl. Sci.* **12**(19), 9572 (2022).
8. Sadaram, G. et al. Internet of things (IoT) cybersecurity enhancement through artificial intelligence: A study on intrusion detection systems. *Univers. Libr. Eng. Technol.* (2022).
9. Moustafa, N. October. New generations of internet of things datasets for cybersecurity applications based machine learning: TON_IoT datasets. In *Proceedings of the eResearch Australasia Conference, Brisbane, Australia*, 21–25 (2019).
10. Thilakarathne, N. N. & Mahendran, R. K. Cyber attacks evaluation targeting internet facing iot: an experimental evaluation. *J. Cybersecur. Inf. Manag.* **9** (1), 18–26 (2021).
11. Naveeda, K. & Fathima, S. S. S. Real-time implementation of IoT-enabled cyberattack detection system in advanced metering infrastructure using machine learning technique. *Electr. Eng.* **107** (1), 909–928 (2025).
12. Thayalan, S. et al. *Real-Time Threat Detection and AI-Driven Predictive Security for Consumer Applications* (IEEE Transactions on Consumer Electronics, 2025).
13. Vellela, S. S. et al. Cyber threat detection in industry 4.0: Leveraging GloVe and self-attention mechanisms in BiLSTM for enhanced intrusion detection. *Comput. Electr. Eng.* **124**, 110368 (2025).

14. Algarni, A., Ahmad, Z. & Ala'anzy, M. A. An edge computing-based and threat behavior-aware smart prioritization framework for cybersecurity intrusion detection and prevention of ieds in smart grids with integration of modified lgbm and one class-SVM models. *IEEE Access*. (2024).
15. Sahu, A. et al. Federated LSTM model for enhanced anomaly detection in cyber security: A novel approach for distributed threat. *Int. J. Adv. Comput. Sci. Appl.* **15**(6). (2024).
16. Dey, A. K., Gupta, G. P. & Sahu, S. P. A metaheuristic-based ensemble feature selection framework for cyber threat detection in IoT-enabled networks. *Decis. Anal. J.* **7**, 100206 (2023).
17. Radjaa, B., Nabila, L. & Salameh, H. B. October. Federated deep learning-based intrusion detection approach for enhancing privacy in fog-iot networks. In *2023 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 156–160 (IEEE, 2023).
18. Srinivasulu, A. & Venkateswaran, R. Enhancing cybersecurity through advanced threat detection: a deep learning approach with Cnn for predictive analysis of ai-driven cybersecurity data. *J. Res. Eng. Comput. Sci.* **1** (5), 65–77 (2023).
19. Ali, B. S. et al. ICS-IDS: application of big data analysis in AI-based intrusion detection systems to identify cyberattacks in ICS networks. *J. Supercomput*. **80** (6), 7876–7905 (2024).
20. Kaliyaperumal, P. et al. Enhancing cybersecurity in Agriculture 4.0: A high-performance hybrid deep learning-based framework for DDoS attack detection. *Comput. Electr. Eng.* **126**, 110431 (2025).
21. Dhanvijay, D. M., Dhanvijay, M. M. & Kamble, V. H. Cyber intrusion detection using ensemble of deep learning with prediction scoring based optimized feature sets for IOT networks. *Cyber Secur. Appl.* **3**, 100088 (2025).
22. Li, J. et al. NFIoT-GATE-DTL IDS: Genetic algorithm-tuned ensemble of deep transfer learning for NetFlow-based intrusion detection system for internet of things. *Eng. Appl. Artif. Intell.* **143**, 110046 (2025).
23. Ullah, I. et al. Protecting IoT devices from security attacks using effective decision-making strategy of appropriate features. *J. Supercomput*. **80** (5), 5870–5899 (2024).
24. Butt, A. U. R. et al. Proactive and data-centric internet of things-based fog computing architecture for effective policing in smart cities. *Comput. Electr. Eng.* **123**, 110030 (2025).
25. Khan, H. U. et al. Prioritizing the multi-criterial features based on comparative approaches for enhancing security of IoT devices. *Phys. Commun.* **59**, 102084 (2023).
26. Karthikeyan, M. et al. Integration of metaheuristic based feature selection with ensemble representation learning models for privacy aware cyberattack detection in IoT environments. *Sci. Rep.* **15**(1), 22887 (2025).
27. Duraibi, S. & Alashjaee, A. M. Enhancing cyberattack detection using dimensionality reduction with hybrid deep learning on internet of things environment. *IEEE Access.* **12**, 84752–84762 (2024).
28. Wu, W., Fouzi, H., Benamar, B., Sidi-Mohammed, S. & Ying, S. Deep learning-based stacked models for cyber-attack detection in industrial internet of things. *Neural Comput. Appl.* 1–35 (2025).
29. Ghazwani, M. & Hani, U. Data-driven analysis of tablet design via machine learning for evaluation of the impact of formulation properties on the disintegration time. *Ain Shams Eng. J.* **16**(9), 103512. (2025).
30. Sundaram, K., Natarajan, Y., Perumalsamy, A. & Yusuf Ali, A. A. A Novel hybrid feature selection with cascaded LSTM: Enhancing security in IoT networks. *Wirel. Commun. Mob. Comput.* **2024**(1), 5522431 (2024).
31. Sulaiman, M. H. & Mustaffa, Z. Chiller power consumption forecasting for commercial building based on hybrid convolution neural networks-long short-term memory model with barnacles mating optimizer. *Next Energy*. **8**, 100321 (2025).
32. Ragab, M. et al. Enhancing cybersecurity in higher education institutions using optimal deep learning-based biometric verification. *Alex. Eng. J.* **117**, 340–351 (2025).
33. https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot.
34. https://www.kaggle.com/datasets/dhoogla/cictoniot.
35. Meziane, H. & Ouerdi, N. A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems. *Sci. Rep.* **13**(1), 21255 (2023).
36. Alqahtany, S. S., Shaikh, A. & Alqazzaz, A. Enhanced Grey Wolf Optimization (EGWO) and random forest based mechanism for intrusion detection in IoT networks. *Sci. Rep.* **15**(1), 1916 (2025).
37. Assmi, H. et al. A robust security detection strategy for next generation IoT networks. *Comput. Mater. Continua*. **82**(1). (2025).
38. Ruiz-Villafranca, S., Roldán-Gómez, J., Gómez, J. M. C., Carrillo-Mondéjar, J. & Martinez, J. L. A TabPFN-based intrusion detection system for the industrial internet of things. *J. Supercomput*. **80** (14), 20080–20117 (2024).

Acknowledgments

The authors extend their appreciation to the Deanship of Research and Graduate Studies at King Khalid University for funding this work through Large Research Project under grant number RGP2/ 271/46. Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R361), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the project number "NBU-FFR-2025-1180-05. The authors are thankful to the Deanship of Graduate Studies and Scientific Research at University of Bisha for supporting this work through the Fast-Track Research Support Program.

Author contributions

H.A.: Conceptualization, methodology, validation, investigation, writing—original draft preparation, S.S.A.: Conceptualization, methodology, writing—original draft preparation, writing—review and editing. J.K.: methodology, validation, writing—original draft preparation. M.H.A.: software, visualization, validation, data curation, writing—review and editing. N.O.A.: validation, original draft preparation, writing—review and editing. J.S.A.: methodology, validation, conceptualization, writing—review and editing. M.M.A.: methodology, validation, original draft preparation. O.A.: validation, original draft preparation, writing—review and editing.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to M.H.A.