




Intelligent LSTM (iLSTM)-Security Model for HetIoT

Shalaka S. Mahadik¹ · Pranav M. Pawar¹  · Raja Muthalagu¹ · Neeli Rashmi Prasad² · Dnyaneshwar Mantri³

Accepted: 1 December 2023 / Published online: 22 December 2023

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract

Distributed denial-of-service (DDoS) is the most recent lethal threat, and several industrial and academic researchers are concentrating on defending the heterogeneous IoT (HetIoT) infrastructure from it. The research presents a novel intelligent security system using deep learning (DL)-based long short-term memory (LSTM) techniques, i.e., the iLSTM-Security model, for the HetIoT network. The research addressed the steps needed to prepare the data after complete data analysis and feature extraction using the principal component analysis (PCA) method. The research also highlighted the asymptotic time complexity analysis for the proposed iLSTM-Security model. The proposed iLSTM-Security model efficiently identifies and nullifies the different DDoS threats. The research analyzes binary (2 class) and multiclass classification (7 class and 13 class) for optimal DDoS threat detection. The proposed iLSTM-Security model's efficacy is assessed against two state-of-the-art DL approaches, and the findings show that the proposed iLSTM-Security model surpasses them. The proposed iLSTM-Security model effectively recognizes different DDoS threats with an accuracy rate of 99.98% for 2 classes, 98.8% for 7 classes, and 99.97% for 13 class classifications. Additionally, the research assesses the individual accuracy of 7 classes and 13 classes with state-of-the-artwork. Further, the research reveals that the proposed iLSTM-Security model is lighter, simpler, and considerably less complicated than the existing state-of-the-art models.

Keywords Heterogeneous · CICDDoS2019 · Cyber security · Distributed denial-of-service · Long short-term memory · Intelligent

1 Introduction

The Internet of Things (IoT) is a rapidly advancing technology that has revolutionized various aspects of daily life, including wearables, health monitoring, fleet administration, and traffic control. While this technology is becoming more widespread, it also faces challenges like standardization, network model, communication protocol, power consumption, etc. Apart from this, the most significant obstacles are heterogeneity and security [1, 2]. The heterogeneity of the IoT's network structure and protocols is implicit. It includes a wide range of network communication techniques and protocols, such as Bluetooth low energy (BLE), 5 G/6 G technology, mobile communication, ZigBee, long-range (LoRa),

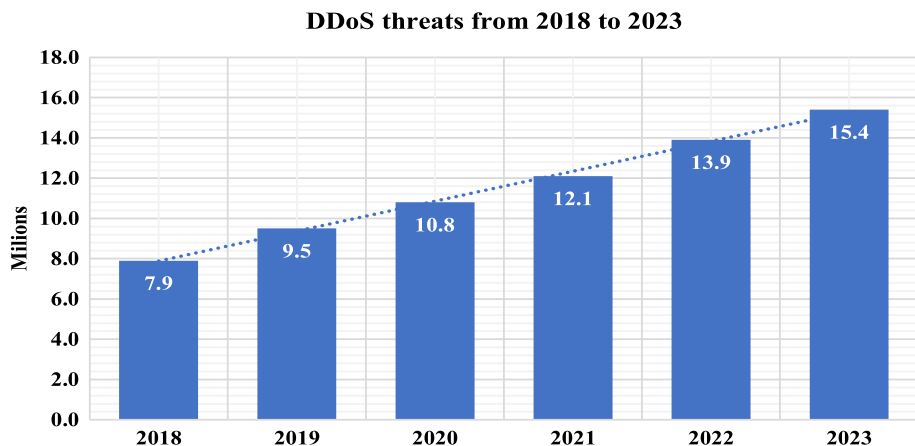


Fig. 1 Cisco's annual DDoS forecast [11, 12]

and lightweight M2M, among others [3–5]. According to a recent statistical study [6], the limited memory and low cost of resources in HetIoT networks render them more susceptible to different kinds of threats. Conventional security measures, such as cryptographic techniques and access control mechanisms, are impracticable in the current environment [2, 7]. Consequently, the protection of HetIoT infrastructures requires novel lightweight security mechanisms.

DDoS attacks caused significant damage and made the HetIoT environment worthless. The 2016 Dyn attack, the February 2018 GitHub DDoS attack, and the February 2020 AWS DDoS attack were among the real-time DDoS threat incidents documented by Cloudflare [8]. According to AWS, the assailants utilized the CLDAP protocol (connection-less lightweight directory access protocol) during the February 2020 DDoS attack. According to the DDoS statistical report by NexuSGuard [9], the total volume of attacks escalated by 75.60%. A shred of additional evidence presented in [10] is that IoT-DDoS is expected to become a more significant concern in the future. As the IT and economic sectors become more reliant on online services and real-time data processing, they become more vulnerable to DDoS attack paths such as HTTP and UDP request flooding. These organizations incur immense revenue losses and gain a negative reputation due to DDoS attacks. The events listed above indicate the escalating prevalence of DDoS threats. According to the annual projection from Cisco, illustrated in Fig. 1, DDoS attacks are anticipated to rise from seven million in 2018 to approximately fifteen million in 2023.

DL approaches provide promising results for defending against DDoS threats, according to a review of the relevant literature [3, 13–17]. Furthermore, the utilization of DL approaches in developing intelligent security models has grown in prominence over the past five years, as demonstrated in Fig. 2. Given this rationale, the research centers on intelligent LSTM, a DL methodology that leverages the recurrent neural networks (RNN) technique. One issue with RNN is the vanishing gradient problem, which means that back-propagation ceases to contribute to the learning process when the gradient value becomes extremely small. Consequently, the gradient layers containing negligible values will remain unchanged; thus, learning failure creates a persistent dependency issue. The LSTM serves as a viable substitute for the vanishing gradient problem and aids in resolving long-term dependency issues encountered in RNN. Furthermore, it acts as a highly efficient method

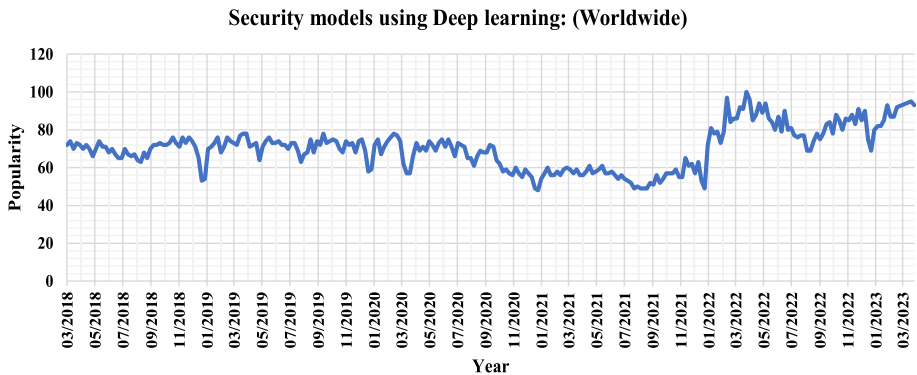


Fig. 2 Rise in DL-based intelligent security models (Google trends)

for delineating the correlation between present and past occurrences and for enhancing the forecasting of network traffic [18]. Therefore, it is frequently spotted within academia [14, 19–22].

1.1 Motivation and Objective

The antecedent discourse inspires the research to focus on creating a security model that uses DL techniques to defend the HetIoT network against DDoS threats. The main objective of the research is to develop an intelligent security model that safeguards the HetIoT network architecture by identifying and classifying DDoS threats using the LSTM approach. Furthermore, the research seeks to devise a simple and less complicated intelligent security model.

The rest of the research is structured as follows: Sect. 2 details the literature study with a comparison analysis. Section 3 represents the contribution of the research, the description of the dataset used, details of the PCA technique employed, the proposed iLSTM-Security model methodology, including its architecture, and an asymptotic time complexity analysis. Section 4 details the experimental settings, metrics, and assessment outcomes with a discussion and summary. The research is summarized with conclusions in Sect. 5.

2 Literature Work

The segment investigates several DL-based approaches that solely employed the CICDDoS2019 dataset from 2020 to 2022. The University of New Brunswick (UNB) and the Canadian Institute for Cybersecurity (CIC) jointly present the CICDDoS2019 DDoS assessment dataset [23, 24]. To protect 5 G mobile networks from DDoS threats, author [25] proposed a trustworthy modified DDoSNet based on the DL technique using RNN with autoencoder (AE) in the software-defined network (SDN) context. The performance parameters under consideration include precision, recall, f1-score, and accuracy for binary classification [26]. A smart edge-IoT mechanism to protect against various DDoS threats has been proposed by the author [17]. The CICDDoS2019 dataset and the dataset generated by SlowHTTPTest and BoNeSi simulators are utilized for creating the model using LSTM and convolutional neural network (CNN) techniques.

The author [13] proposed a cuda-based LSTM model using the CICDDoS2019 dataset for DDoS threat detection. The proposed model utilized four classes, benign, DNS, LDAP, and MSSQL, to train-test its performance. The effectiveness of the model is determined using the receiver operating characteristic (ROC) curve, precision, recall, f1-score, and accuracy. Next, author [27] considers CNN, LSTM, bidirectional LSTM (Bi-LSTM), stacked-LSTM, and gated recurrent network (GRU) models to detect DDoS threats using the CICDDoS2019 dataset. The models' performance is assessed against two classes: benign and portmap. The stacked LSTM provides the best results among the other DL models mentioned above. The author [14] proposed a framework to safeguard against 5 G and beyond-5 G networks using the DL technique. The proposed framework combines two dense neural network (DNN) models to detect various DDoS threats and protect the network mentioned above. Each DNN1 and DNN2 model consists of seven dense layers, two dropout layers, and one input layer. The author compares the model's results and performance to other state-of-the-art models.

Moving forward, the author [15] proposed an SDN-based architecture that used a hybrid DL method to detect multiple DDoS threats. The proposed architecture combines cuda-based DNN-LSTM and GRU methods to train and verify the model's performance. The author mentioned various DDoS threats, including benign, MSSQL, SSDP, DNS, WebD-DoS, Portmap, Syn, UDP, and UDP-Lag. The author [16] presented an intrusion detection system (IDS) for DDoS threat identification from the perspective of an agriculture 4.0 application. The proposed IDS considers DNN, LSTM, and CNN techniques for binary and multiclass classifications. The performance of all three IDSs is evaluated using the two datasets, CICDDoS2019 and TON-IoT. The author [28] proposed two DL techniques, DNN and CNN, for multiclass classification using the CICDDoS20219 dataset. The proposed DNN model contains five dense layers with neurons 8192, 4096, 2048, 1024, and 512, excluding the input and output layers. The highest accuracy reported by the author is 87

Based on the preceding literature study outcomes, the DL-based model is immensely effective at assessing network information and identifying DDoS threats to defend the HetIoT infrastructure. Table 1 outlines the different state-of-the-art DL-based models regarding model names, DL techniques employed, types of attack classification, i.e., binary or multiclass, each model's fundamental details, and constraints regarding layers and neurons used.

The literature review indicates that except model [16], all other contemporary DL-based algorithms solely account for binary or multiclass classification and not both. The security models highlighted in the literature perform well; however, they fail to account for all current DDoS threats in the CICDDoS2019 dataset. Furthermore, these models comprise complicated structures with more layers and neurons; as a result, they demand high computational power and more training time.

The research aims to address the abovementioned gap and reach the research objective by creating an intelligent security model based on LSTM, i.e., the iLSTM-Security model. The iLSTM-Security model facilitates research in detecting and classifying all recent DDoS threats in the CICDDoS2019 dataset using binary (2 class) and multiclass (7 class and 13 class) classification. Further, the iLSTM-Security model is less complicated and more efficient than the existing literature survey models (refer to Table 1). The iLSTM-Security model considers two LSTM layers, each with 32 and 64 neurons, and one fully connected layer.

Table 1 Comparative summary of current DL-based models (2020-2022)

Year	Model name	DL technique	Accuracy (%)	Classification type	Fundamental details	Constraint
2020	Flowguard	LSTM	98.9	Binary	Edge protection method for identifying, classifying, and mitigating IoT-DDoS threats, [17]	More processing power and more training time are required due to the 1280 neurons
2020	Cuda base LSTM	LSTM	99.6	Multiclass (4 class)	With the help of Cuda libraries, achieved good results in identifying four classes of DDoS threats, [13]	Few threats are targeted, Intricate calculation with 3-LSTM layers, 4-dense layers, and 1-dropout layer
2021	Stacked-LSTM	LSTM	99.55	Binary	Attain high accuracy for 2-class classification using the 'portmap.csv' file, [27]	Various DDoS threats are not focused, Complex structure with 1-input layer, 2-LSTM layer(64 neurons each), 1-dense layer(128 neurons), and 1-output layer
2021	Composite framework for B5G	DNN	99.66	Multiclass (10 class)	Two separate DNN models with seven layers each are concatenate to identify DDoS threats, [14]	Complex structure with 2-DNN models, each model with 1-input layer, 7-hidden layers, and 2-dropout layers
2021	Hybrid approach	CuDNNLSTM and CuDNNGRU	99.74	Multiclass (8 class)	Attain better results using Cuda libraries to identify DDoS threats, [15]	Complex structure with 2-CuDNN-LSTM layers (500,300 neurons), 1-CuDNNGRU layer(200 neurons), 4-dense layers, and 1-dropout layer)
2021	DL based IDS	LSTM	99.94	Binary	Three different models are proposed to secure agriculture 4.0 framework against DDoS threats, [16]	Complex structure with 5-LSTM layers with 67, 300, 600, 300, 67 neurons, 4-dropout layers, and 1-dense layer
2022	DL model	DNN, CNN	94.99 94.88 87, 91.9	Multiclass (7 class) Multiclass (13 class) Multiclass (13 class)	Two DL models are proposed to detect various DDoS attacks, [28]	Heavy model with more numbers of neurons for DNN (i.e. 5 dense layer with 8192, 4096, 2048, 1024, 512 neurons) and for CNN (i.e. 4 convolutional layer, 2 max-pooling layer, 2 upsampling layer)

Table 1 (continued)

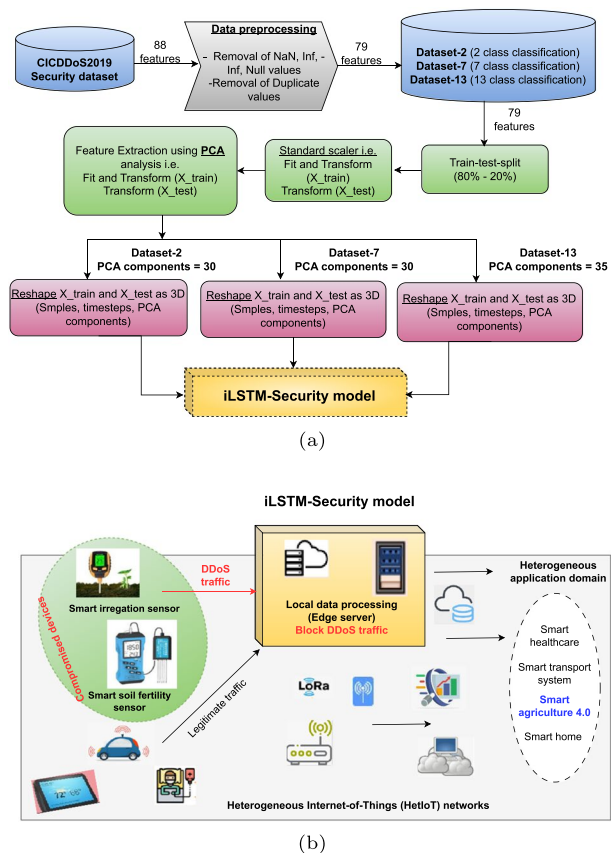
Year	Model name	DL technique	Accuracy (%)	Classification type	Fundamental details	Constraint
2022	Modified DDoSNet	RNN with AE	99.83	Binary class	Proposed DDoS attack detection to secure 5 G mobile network architecture, [25]	No multiclass classification, 1 input layer, 3 hidden layers, and 1 output layer

3 Intelligent LSTM (iLSTM)-Security Model

The iLSTM-Security model block diagram depicted in Fig. 3 outlines the steps to follow before training the model. The descriptions of the dataset (Sect. 3.2) and PCA technique (Sect. 3.3.1) are outlined in the preceding section and summed up in Fig. 3a. Data is converted from two to three dimensions since the iLSTM model requires three dimensions as input. Moreover, as shown in Fig. 3, the iLSTM-Security model can be positioned at the network layer by taking advantage of the *Edge Computing* technique [17, 29]. This technique helps to enhance the network's security by minimizing latency and data transfer costs. *Edge server* efficiently detects and blocks the DDoS traffic using the iLSTM-Security model. Additionally, implementing the iLSTM-Security model is lighter, simpler, and considerably less complicated; it requires less processing power to train and test the model. It allows the network administrator to immediately inspect all the incoming traffic, including data breaches as DDoS threats close to the edge devices at a network layer.

Moreover, Fig. 3b illustrates the real-world use case of the iLSTM-Security model. As depicted in Fig. 3b, the smart agriculture 4.0 subcomponents comprise the smart soil fertility and irrigation systems. Water conservation is enhanced by the smart irrigation system, which distributes water to plants or fields following their requirements. The system employs a soil moisture sensor to quantify soil moisture and, on the readings, applies water

Fig. 3 Block diagram of iLSTM-Security model for HetIoT [12]



to the plants or fields. Smart soil fertility systems employ NPK sensors to ascertain the nutrient ratio in the soil, thereby facilitating the detection of nutritional deficiencies or surpluses in growth-promoting soils.

Consider that in the event of a breach in a smart irrigation system; the transmitted data will be inaccurate, leading to water loss and subsequent harm to plants or fields. Likewise, a hacked smart fertility system will result in poor plant production quality. Such threats will result in financial losses and influence the farmers' decision to relinquish their interest in advanced technologies.

The network administrator promptly halts the ingress of traffic originating from the compromised devices while concurrently ensuring uninterrupted service usage for authorized users with benign traffic with the assistance of the iLSTM-Security model. Thus, the iLSTM-Security model eventually isolates and categorizes the DDoS threat to safeguard the mentioned HetIoT application domains.

3.1 Contributions

The key contributions of the research are as follows:

- The research outlines data preprocessing steps following comprehensive data analysis [30]. Feature extraction using the PCA technique with the analysis of explained variance graphs and cumulative explained variance graphs is also highlighted in the research.
- The research proposes an intelligent security system using the deep learning-based LSTM technique, i.e., the Intelligent LSTM (iLSTM)-Security model, to identify various DDoS threats on HetIoT networks.
- The research highlights the performance evaluation with binary (2 class) and multi-class (7 class and 13 class) classification utilizing CICDDoS2019 [24], a well-known benchmark dataset. Precision, recall, f1-score, and accuracy are used to evaluate the outcomes.
- The proposed iLSTM-Security model detects DDoS threats for binary (2 class) and multiclass (7 class and 13 class) classification with reasonable accuracy, i.e., 99.98% for 2 class, 98% for 7 class, and 99.97% for 13 class classifications.
- The proposed iLSTM-Security model is lighter, simpler, and less complicated regarding the LSTM layers and neurons utilized.
- The research also investigated the most recent security model and compared it with the iLSTM-Security model using asymptotic time complexity analysis. The result shows that the iLSTM-Security model is more efficient regarding processing time.

3.2 Dataset

CICDDoS2019 is a publicly accessible real-time benchmark dataset actively used by several academics [24, 31]. While numerous other security datasets exist, the CICDDoS2019 dataset stands out because it focuses solely on DDoS threats and includes the most DDoS classes. Therefore, it enjoys widespread acclaim among experts. Consequently, the research utilized it in the development of the iLSTM-Security model.

The classification of the various HetIoT-based DDoS threats is presented in Fig. 4, which includes Naive-based attacks, Protocol exploitation-based attacks, and reflection & amplification-based flooding attacks. In naive-based attacks, many repetitive

communication requests are used to fill up the victim's cache memory, rendering him unable to accept any new requests, making it hard for legitimate users to fulfill their requests. The protocol-based flooding attacks involve a three-way handshake protocol. In such DDoS attacks, the attacker will send many 'syn' messages to the sender. As a result, the sender's limited cache memory is complete, and he cannot handle any additional requests. In reflection and amplification-based flooding attacks, the attacker will send a forged request packet to the server with an altered origin address, and the server will be unable to identify it; hence, large reply packets are then delivered to the victim designated by the altered origin address. The characteristics of the various DDoS attacks utilized in the research are summarized as follows:

- (a) UDP (user datagram protocol)-lag attack: This kind of DDoS threat is most commonly utilized in online games when players want to slow down or hinder the progress of their competitors.
- (b) NTP (network time protocol) attack: In this DDoS threat, the attacker uses publicly accessible NTP servers to overload the victim with UDP packets. [32].
- (c) TFTP attack: This reflection-based DDoS threat targets internet-connected TFTP servers. It generates a default file request, and the victim TFTP server returns data to the requesting host machine despite a file name mismatch. [33].
- (d) MSSQL (Microsoft SQL) attack: This type of DDoS attack launches a reflection-based DDoS threat by interrupting the operation of the Microsoft SQL server resolution protocol. When an MSSQL server responds to a client query or request, the hacker attempts to exploit this protocol, which is listening on UDP port 1434 [34].
- (e) SSDP (simple service discovery protocol) attack: This kind of DDoS threat utilizes universal plug-and-play (UPnP) networking protocols to send high traffic to a specific victim, exceeding their infrastructure and knocking their web resource offline [35].
- (f) LDAP (lightweight directory access protocol) attack: In this kind of DDoS threat, an intruder uses an application layer protocol known as LDAP, which usually serves to obtain a human-readable URL (such as msn.com). The intruder uses this protocol for sending requests to a susceptible public LDAP server that generates significant responses [31].
- (g) SNMP (simple network management protocol) attack: The SNMP protocol is utilized to set up and collect data from network devices such as servers, gateways, access points, modems, and printers. The intruder utilizes this protocol to produce attack sizes of hundreds of megabytes per second to flood the victim's network connections [16, 36].

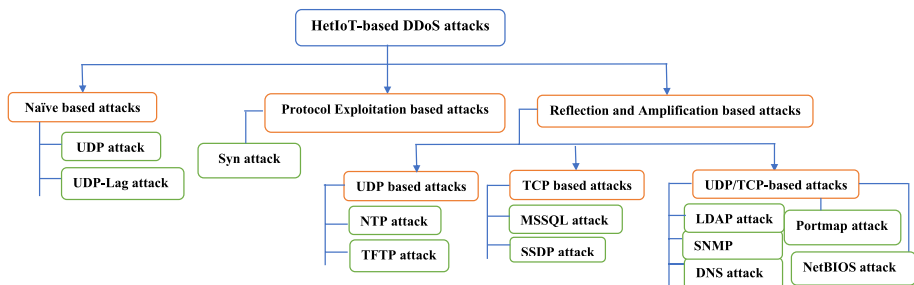


Fig. 4 Classification of DDoS threats [4, 23, 24]

- (h) DNS (domain name system) attack: This is an amplification-based DDoS threat in which DNS requests are incorrectly handled, leading users to be forcibly sent to fraudulent websites [16, 37].
- (i) NetBIOS (network basic input–output system) attack: This DDoS attack uses a flaw in “Windows OS.” NetBIOS is designed to be used on local area networks to allow machines on the network to share information. The weakness of NetBIOS is that it may be used across the Web, allowing an attacker to access your device remotely.
- (j) Portmap attack: Portmap is a remote procedure call (RPC) service that always listens on TCP and UDP ports and maps other RPC services to their respective server port numbers. The portmap is used to locate the RPC server when a remote host calls it. Querying portmapper is a simple request that generates a massive response, making it an ideal target for DDoS threats. [27].

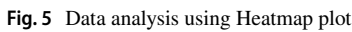
The dataset includes seven individual CSV files for testing and thirteen for training. Each CSV file contains a distinct type of DDoS threat, comprising over 50 million instances and 87 distinct features. The research investigates all features except flow-id, sourceIp, destinationIp, smillarHTTP, time stamp, sport, dport, and unnamed, which are uninformative or constructed within the simulation environment [26], during the data pre-processing step. The instances with nan, null, infinity, and repeating values are discarded to prevent the model from overfitting. The standard scaler is the normalization method most frequently employed in scientific investigations. It aids in the enhancement of the DL technique’s overall efficacy. The research consequently incorporated it [12, 38]. Finally, seventy-nine features, along with a label column, are utilized to build three distinct datasets (refer to Fig. 3a), namely, Dataset-2, Dataset-7, and Dataset-13. The specifics of each dataset’s training and testing instances are provided in Tables 6, 7, and 8. The implementation of the iLSTM-Security model is explored in depth in the next segment.

3.3 Proposed Methodology

3.3.1 PCA Technique

HetIoT applications produce an enormous volume of data that is challenging to handle. The PCA method has the potential to handle such massive amounts of data by lowering the dimensionality [19, 39]. The research examines all three datasets by performing extensive data analysis with a heatmap plot and the Pearson correlation technique and finds that each dataset contains many redundant features, as illustrated in Fig. 5. As depicted in Fig. 5, features with a yellow color represent positive correlations, while those with a violet color represent negative correlations. E.g., a feature like ‘Flow IAT Mean, Flow IAT Std, Flow IAT Max’ is positively correlated with ‘Flow duration’ Hence, the research adopted the PCA technique to remove such features and collect important information with high variance. This technique enables the iLSTM-Security model to reduce complexity and attain superior outcomes by extracting more convenient features.

Algorithm 1 highlights the pseudocode for the PCA technique employed in the research. To find the number of principal components, the first step is to standardize the dataset (Dataset-2, Dataset-7, and Dataset-13) by calculating each feature’s mean and standard deviation. The covariance matrix is computed for all three datasets separately to identify the correlations between the features. Further, eigenvalues and eigenvectors are calculated through the linear transformation of the covariance matrix. The principal

 Springer

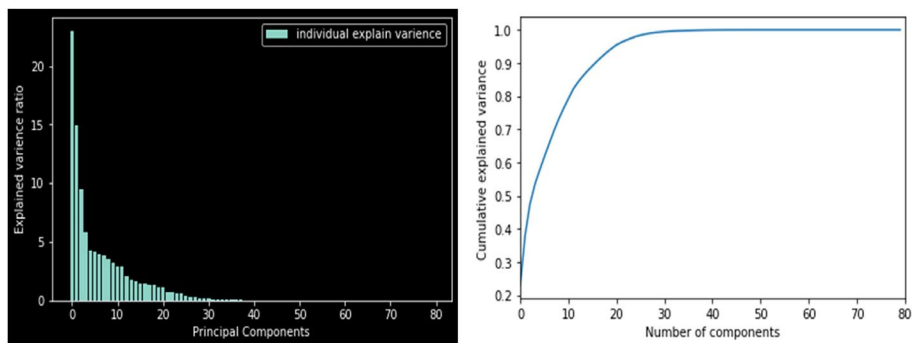


Fig. 6 Variance graph for Dataset-2 [12]

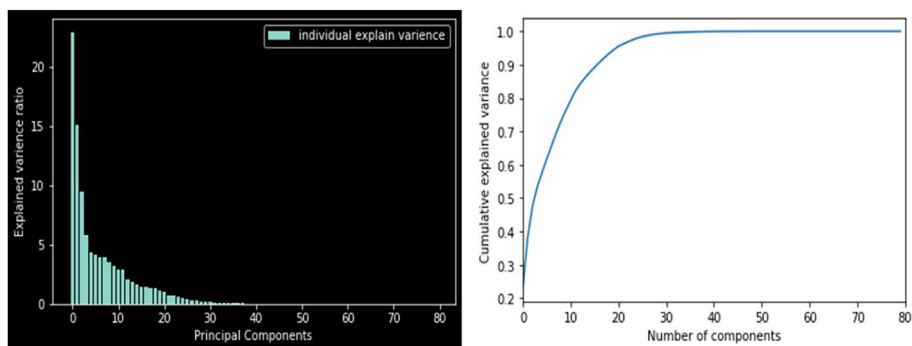


Fig. 7 Variance graph for Dataset-7 [12]

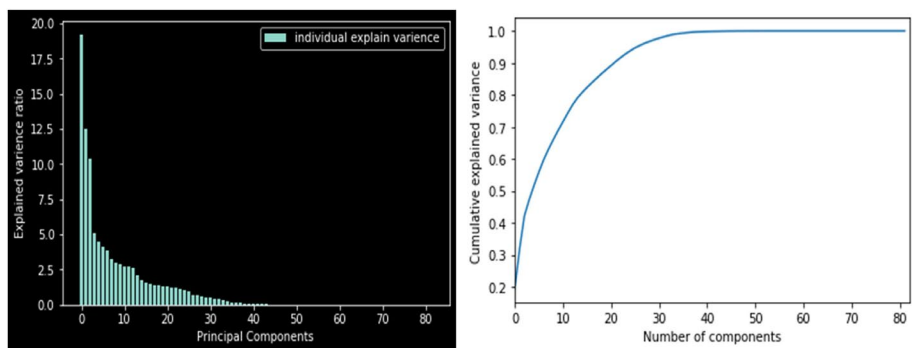


Fig. 8 Variance graph for Dataset-13 [12]

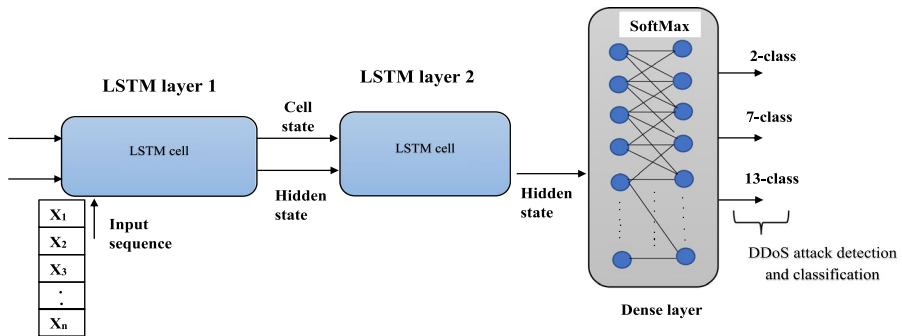


Fig. 9 Architecture of iLSTM-Security model

Algorithm 1 Pseudocode for PCA technique

Input: number of features=79

Output: Number of PCA components

- 1: Compute mean and standard deviation for each feature-column (let be f_1, f_2, \dots, f_n)
- 2: Compute covariance matrix ($COV(x, y)$) with standardized data and the size of the matrix is $f_n \times f_n$ using an equation, $COV(x, y) = \sum_{i=1}^n \frac{(x_i - \bar{x})(y_i - \bar{y})}{n-1}$
- 3: Calculate eigenvalues (λ) on the covariance matrix (i.e., f_1, f_2, \dots, f_n) using equation, $COV(x, y) - \lambda I = 0$, where I = Identity matrix
- 4: Calculate eigenvectors ($EigV$) for each eigenvalues(λ) using equation, $COV(x, y)EigV = \lambda EigV$
- 5: Sort all eigenvalues in decreasing order and select the number of PCA components
- 6: Plot Explained variance graph and visualized PCA components that capture maximum variance
- 7: Plot Cumulative explained variance graph and visualized variance captured by each PCA components
- 8: Select the number of PCA components using Explained variance and Cumulative explained variance graph
- 9: Fit and transform training set (i.e., X_{train})
- 10: Transform testing set (i.e., X_{test})

3.3.2 Architecture

The single-cell construction of the iLSTM-Security model is depicted in Fig. 10 below. It contains three main gates: the input gate (i), the forget gate (f), and the output gate (o) along with the cell state (c) and hidden state (h). The cell state stores and loads the information (i.e., long-term memory), whereas the hidden state helps to carry information from the previous state and overwrite it. The three gates assist the iLSTM-Security model in learning which information should be retained or ignored. The forget gate f^t takes the input as x^t and h^{t-1} along with its weights (w_{fx}^t, w_{fh}^{t-1}). The sigmoid function σ is used to decide which information needs to be retained and which needs to be ignored. The mathematical equation for f^t is given as,

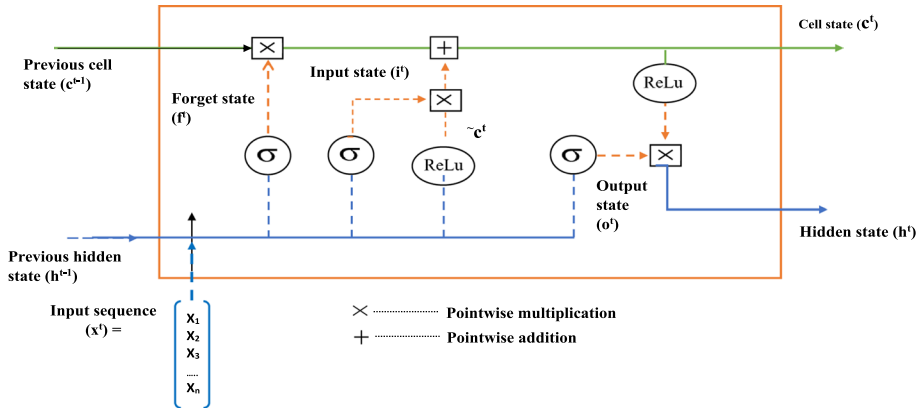


Fig. 10 Single LSTM cell structure for iLSTM-Security model

$$f^t = \sigma(W_{fh}^{t-1} \cdot h^{t-1} + W_{fx}^t \cdot x^t + b_f) \quad (1)$$

where t is the current state, $t - 1$ is the previous state, and b is the bias.

The output of the forget gate f^t is multiplied by the previous cell state c^{t-1} as shown in Fig. 10, and the value of the c^{t-1} will get updated.

The next step is input gate i^t that takes the input as x^t and h^{t-1} and analyses the data for what new information it can add to the current state using the following mathematical equation:

$$i^t = \sigma(W_{ih}^{t-1} \cdot h^{t-1} + W_{ix}^t \cdot x^t + b_i) \quad (2)$$

$$c^t = \text{ReLU}(W_{ch}^{t-1} \cdot h^{t-1} + W_{cx}^t \cdot x^t + b_c) \quad (3)$$

The previous cell state c^{t-1} will get updated into the new cell state c^t with additional information. It is represented using the following mathematical equation:

$$c^t = f^t \times c^{t-1} + i^t \times c^t \quad (4)$$

Moving toward the final step, the output gate o^t helps to decide what information the new hidden state h^t will hold. The output of the o^t and cell state c^t using the activation function 'ReLU' will get multiplied to get the new hidden state information using the following equation:

$$o^t = \sigma(W_{oh}^{t-1} \cdot h^{t-1} + W_{ox}^t \cdot x^t + b_o) \quad (5)$$

$$h^t = o^t \times \text{ReLU}(c^t) \quad (6)$$

Further, the above process will be repeated iteratively, and the information will be updated. Lastly, the iLSTM-Security model cell output is forwarded to the dense layer, that is, the resultant layer, to identify and categorize the different DDoS threats.

Algorithm 2 highlights the pseudocode for the iLSTM-Security model utilized in the research. The iLSTM-Security model implements two LSTM layers and one

fully connected layer, which is the output layer, to attain optimal performance. The ‘GridSearch’ hyperparameter settings [40] are utilized to determine the number of the neuron as 32 and 64 with activation function as ‘ReLU (Rectified Linear Unit)’. The ‘ReLU’ is currently the most efficient and advanced activation function compared to the ‘sigmoid’ and ‘tanh’. It aids in the elimination of the vanishing gradient problem that exists in RNN [41, 42]. Since the ‘ReLU’ is a significantly faster activation function than other activation functions, the research adopted it to reduce the training time and attain higher accuracy. The proposed model applied ‘sparse_categorical_crossentropy’ as a loss function since target classes are integers, not one_hot encoded [43]. The ‘RMSprop (Root Mean Square Propagation)’ algorithm utilizes an adaptable learning rate with mini-batch learning [44]. As mentioned in [21], this optimizer with a default learning rate produces superior results; hence, it is included in the research. The hyper-parameter configuration employed in the research is highlighted in Table 5.

Algorithm 2 Pseudocode for iLSTM-Security model

Input: Batch size=128, Epoch = 25, Number of features = PCA components,
Output: Accuracy, Precision, Recall, and F1-Score (for 2 classes or, 7 classes, or 13 classes) state Define sequential model

- 1: **for** Epochs = 1 to 25 **do**
- 2: Add 1st LSTM layer with neurons = 32, return_sequence = ‘true’, activation = ‘relu’
- 3: Add 2nd LSTM layer with neurons = 64, return_sequence = ‘false’, activation = ‘relu’
- 4: Add Dense layer with neurons = 2 or 7 or 13, activation = ‘softmax’
- 5: Build the model with optimizer = ‘RMSprop’, loss function = ‘sparse_categorical_crossentropy’
- 6: Fit the model on X_train and y_train, validation_set = 0.20
- 7: Recur with steps 3 to 7 for each Epochs
- 8: **end for**
- 9: Display model summary
- 10: Evaluate model for X_test and y_test
- 11: Display testing_set loss and accuracy
- 12: Display confusion_matrix and classification_report
- 13: Plot cumulative training and testing loss
- 14: Plot cumulative training and testing accuracy

3.3.3 Computational Analysis

The segment analyzes the asymptotic time complexity of the iLSTM-Security model. As mentioned by [45, 46], the asymptotic time complexity for the input gate, output gate, forget gate, and cell state is the same and explained below.

Consider Equ. 1,

$$f^t = \sigma(W_{fh}^{t-1} \cdot h^{t-1} + W_{fx}^t \cdot x^t + b_f)$$

Where,

- $x^t \in \mathbb{R}^d$: input vector to the LSTM cell,
- $f^t \in \mathbb{R}^h$: forget gate activation vector,
- $i^t \in \mathbb{R}^h$: input gate activation vector,
- $o^t \in \mathbb{R}^h$: output gate activation vector,
- $h^t \in \mathbb{R}^h$: hidden state vector (i.e., output vector of the LSTM cell),

- $c^t \in \mathbb{R}^h$: cell input activation vector,
- $c^t \in \mathbb{R}^h$: cell state vector,
- $W_x \in \mathbb{R}^{h \times d}$, $W_h \in \mathbb{R}^{h \times h}$, $b \in \mathbb{R}^h$: weight matrices and bias vectors, which need to be learned during the training periods,
- d : number of input features,
- h : number of hidden units.

Now, the estimation of the time complexity for each operation (refer Equ. 1) is as follows,

- Time complexity for $W_{fh}^{t-1} \cdot h^{t-1}$ is $\mathcal{O}(h^2)$ (matrix–vector multiplication of size $h \times h$),
- Time complexity for $W_{fx}^t \cdot x^t$ is $\mathcal{O}(hd)$ (matrix–vector multiplication of size $h \times d$),
- Time complexity for b_f is $\mathcal{O}(h)$ (sum of two vectors with size $h \times h$).

Therefore, the asymptotic time complexity for the forget gate f is,

$$\mathcal{O}(h^2) + \mathcal{O}(hd) + \mathcal{O}(h) = \mathcal{O}[h(h + d + 1)] \quad (7)$$

Similarly, for Equ. 2, 3, 5 the asymptotic time complexity for the input gate i , cell state c , and output gate o is the same, which is expressed as, $\mathcal{O}[4h(h + d + 1)]$.

The activation function σ & $ReLU$ has constant time complexity for all four gates, which will not affect the overall asymptotic time complexity of the model; hence, it is ignored in all the above four gates.

Further, Equ. 4, cell state (c^t) perform element-wise multiplication; so the operation has time complexity as, $\mathcal{O}(2h)$; as well as Equ. 6, hidden state (h^t) has time complexity as, $\mathcal{O}(2h)$.

So overall, the forward pass of a single LSTM layer has the asymptotic time complexity as,

$$\mathcal{O}[4h(h + d + 1)] + \mathcal{O}(2h) + \mathcal{O}(2h) = \mathcal{O}[4h(h + d + 2)] \quad (8)$$

The iLSTM-Security model employs one dense layer as a resultant layer. This layer takes the input from the LSTM layers hidden state, h_{fc}^t and connects to each SoftMax activation neuron, I_s . So, the time complexity with a dense layer is, $\mathcal{O}(h_{fc}^t I_s)$ [4]. The overall asymptotic time complexity for the iLSTM-Security model with two LSTM layers and a dense layer is $2 * \mathcal{O}[4h(h + d + 2)] + \mathcal{O}(h_{fc}^t I_s)$.

The research also analyses the asymptotic time complexity for the state-of-the-art model [16] that comprises five LSTM layers, four dropout layers, and one dense layer. Therefore, the overall asymptotic time complexity for the state-of-the-art model [16] is, $5 * \mathcal{O}[4h(h + d + 2)] + \mathcal{O}(h_{fc}^t I_s)$.

The comparative asymptotic time complexity for the iLSTM-Security model and the state-of-the-art model in [16] is shown below in Table 2. The iLSTM-Security model used fewer layers than the state-of-the-art model [16]; hence, the computational cost is comparable and less. As a result, the iLSTM-Security model is lighter, simpler, significantly less complicated, and more efficient in processing time.

Table 2 Comparative asymptotic time complexity

	Asymptotic time complexity
[16]	$\{ 5 * \mathcal{O}[4h(h + d + 2)] + \mathcal{O}(h_{fc}^t I_s) \}$
iLSTM-Security model	$\{ 2 * \mathcal{O}[4h(h + d + 2)] + \mathcal{O}(h_{fc}^t I_s) \}$

Table 3 Experimental analysis of training, testing and total time

Time in second	[16]			iLSTM-Security model		
	2 class	7 class	13 class	2 class	7 class	13 class
Training time	9253.76	12104.86	3013.07	1385.04	1320.31	486.3
Testing time	96.08	100.26	34.55	27.12	26.2	11.34
Total time	9349.84	12205.12	3047.62	1412.16	1346.51	497.64

The training and testing time is crucial during model development because it indicates the efficacy of the proposed model. Essentially, the model exhibits enhanced performance if it takes less time to build the network behavior model and identifies various threats successfully[47]. Therefore, the iLSTM-Security model and the state-of-the-art model in [16] have experimented on the CICDDoS2019 dataset to ascertain the time required for training and testing. The comparative analysis of training and testing time required for both models concerning 2 class, 7 class, and 13 class is depicted in Table 3. Table 3 shows that the iLSTM-Security model outperforms the state-of-the-art model in [16].

4 Results and Discussion

The section examines the performance of the iLSTM-Security model to appropriately detect and classify various DDoS threats by considering 2 class, 7 class, and 13 class classifications. The simulation settings, evaluation indicators, and evaluation analysis are mentioned below.

- (i) Simulation settings: The configuration of the software and hardware setting is provided in Table 4.
- (ii) Evaluation indicators: The standard evaluation indicators such as accuracy, precision, recall, and f1-score are used to assess the iLSTM-Security model performance [4, 22]. A confusion matrix is another effective way of evaluating a classification model. It provides detailed information about how accurately the model categorizes the classes based on the data given or how the classes are misclassified. As a result, the confusion matrix for three datasets is highlighted in the research to exhibit the effectiveness of the iLSTM-Security model.

Table 4 Simulation settings

Software setting:	
Software tool-	Spyder 5.0 IDE
Programming language-	Python 3.9, Scikit library, Matplotlib 3.5
API tool-	Keras API, TensorFlow 2.8.0
Hardware setting:	
Processor i7-10750 H CPU @ 2.59GHz, 16GB ram,	
Windows 10 64-bit OS, dedicated 4GB NVIDIA GEFORCE GTX 1650Ti	

Table 5 Hyper-parameter configurations

Hyper-parameter configurations	Value
Learning rate	0.001
Optimizer	RMSprop
Activation function	Relu
Classification function	SoftMax
Batch Size	128
Epoch	25
Loss function	Sparse_categorical_crossentropy

- (iii) Evaluation analysis: Fig. 3 portrays all of the processes associated with data preprocessing, forming three separate datasets and the computing PCA components for each dataset. The training set includes a 20% validation_set to verify that all outcomes are unbiased. Table 5 shows the hyper-parameter configurations that enable the iLSTM-Security model throughout the learning process not to overfit or underfit but simultaneously minimize the loss and improve the accuracy at each epoch.

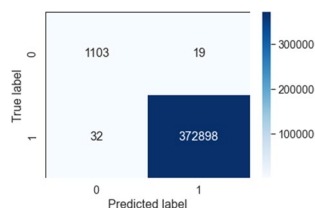
4.1 Binary Classification (2 Class)

Dataset-2 is utilized to perform binary classification, which includes two classes: benign and DDoS attacks. Details about the training and testing instances after data preprocessing are provided in Table 6. The confusion matrix presented in Fig. 11 shows that the iLSTM-Security model correctly predicts benign class and DDoS threat, whereas few instances are misclassified.

The assessment of the iLSTM-Security model is investigated using the state-of-the-art model [16] as depicted in Fig. 12. The iLSTM-Security model yields a 99.98% overall accuracy rate; on the other hand, the state-of-the-art model [16] attains 99.94% accuracy

Table 6 Details of Dataset-2

Label	Class name	Total instance	Training instance	Testing instance
0	Benign	5,565	4,443	1,122
1	DDoS attack	1,864,694	1,491,764	372,930
		1,870,259	1,496,207	374,052

Fig. 11 Confusion matrix for 2 class

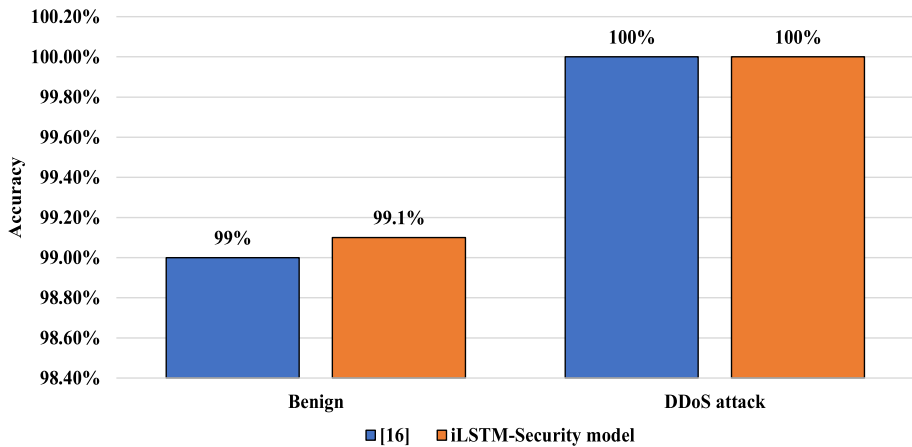


Fig. 12 Accuracy outcomes for 2 class

results. The iLSTM-Security model and the state-of-the-art model [16] successfully identify the DDoS threat with 100% accuracy. The individual class evaluation depicted in Fig. 12 reveals that the iLSTM-Security model identifies the DDoS threat and benign traffic with a modest improvement over the state-of-the-art model [16].

4.2 Multiclass Classification (7 Class)

A seven-class classification is carried out using Dataset-7, which includes benign, LDAP, MSSQL, NetBIOS, Syn, UDP, and UDPLag classes. The training and testing instances about the diverse DDoS threats are detailed in Table 7. The accuracy of the iLSTM-Security model in predicting benign classes and diverse DDoS threats is demonstrated by the confusion matrix in Fig. 13; only a small number of instances are incorrectly classified.

The assessment of the iLSTM-Security model is investigated using the state-of-the-art model [16] as depicted in Fig. 14. The iLSTM-Security model identifies UDP attacks with 100% accuracy, MSSQL attacks with 98% accuracy, and UDPLag attacks with 18% accuracy. The number of instances available for UDPLag attacks is less, i.e., 171. Yet, preliminary data analysis and features acquired using the PCA approach assist the iLSTM-Security

Table 7 Details of Dataset-7

Label	Class name	Total instance	Training instance	Testing instance
0	Benign	5,599	4,475	1,124
1	LDAP	187,226	149,850	37,376
2	MSSQL	558,347	446,829	111,518
3	NetBIOS	351,500	281,112	70,388
4	Syn	455,990	364,395	91,595
5	UDP	378,814	303,330	75,484
6	UDPLag	171	143	28
		1,937,647	1,550,134	387,513

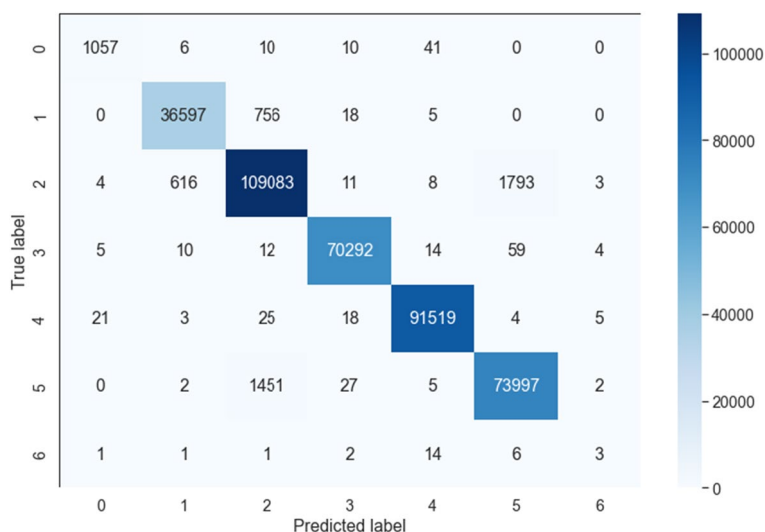


Fig. 13 Confusion matrix for 7 class

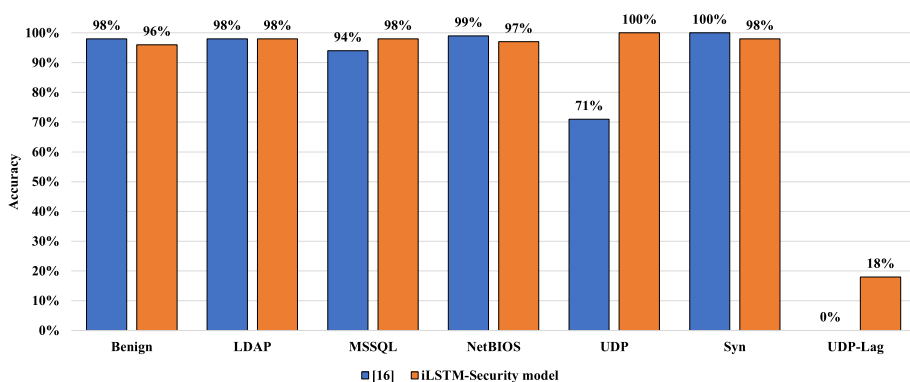
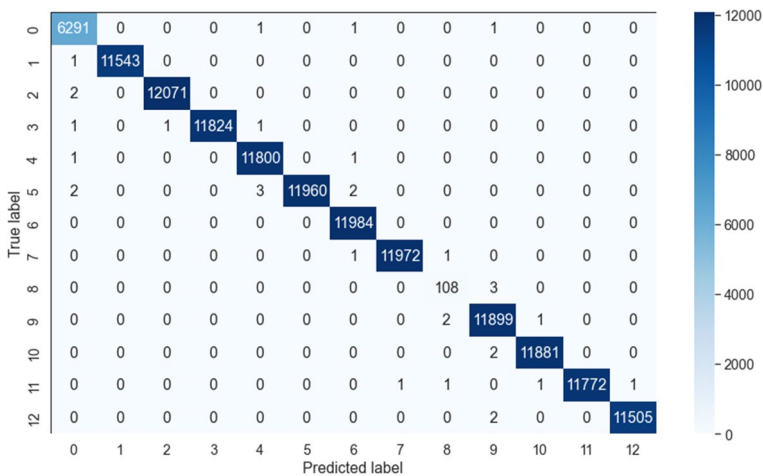


Fig. 14 Accuracy outcomes for 7 class

model in adequately training and identifying the threat with a precision of 50% and an accuracy rate of 18%. Nevertheless, the cutting-edge model [16] cannot identify UDPlag attacks; UDP and MSSQL attacks are identified with an accuracy rate of 71% and 94%, respectively. Further, the iLSTM-Security model and the state-of-the-art model [16] identify the LDAP attack with 98% accuracy. Compared to the iLSTM-Security model, the state-of-the-art model [16] identifies Syn attack with 100% accuracy and NetBIOS with 99% accuracy. In contrast, the iLSTM-Security model attains 98% accuracy for Syn attack and 97% accuracy for NetBIOS. The overall comparative accuracy in identifying six distinct DDoS threats and benign traffic enhanced using the iLSTM-Security model over the cutting-edge model [16].

Table 8 Details of Dataset-13

Label	Class name	Total instance	Training instance	Testing instance
0	Benign	31,880	25,586	6,294
1	LDAP	60,000	48,456	11,544
2	MSSQL	60,000	47,927	12,073
3	NetBIOS	60,000	48,173	11,827
4	Syn	60,000	48,198	11,802
5	UDP	60,000	48,033	11,967
6	UDPLag	60,000	48,016	11,984
7	TFTP	60,000	48,026	11,974
8	WebDDoS	439	328	111
9	NTP	60,000	48,098	11,902
10	SSDP	60,000	48,117	11,883
11	SNMP	60,000	48,224	11,776
12	DNS	60,000	48,493	11,507
		692,319	555,675	136,664

**Fig. 15** Confusion matrix for 13 class

4.3 Multiclass Classification (13 Class)

A thirteen-class classification is carried out using Dataset-13, which includes benign, LDAP, MSSQL, NetBIOS, Syn, UDP, UDPLag, TFTP, WebDDoS, NTP, SSDP, SNMP, and DNS classes. Details about the training and testing instances of the various DDoS threats after data preprocessing are provided in Table 8. The accuracy of the iLSTM-Security model in predicting benign classes and diverse DDoS threats is demonstrated by the confusion matrix in Fig. 15; only a small number of instances are incorrectly classified.

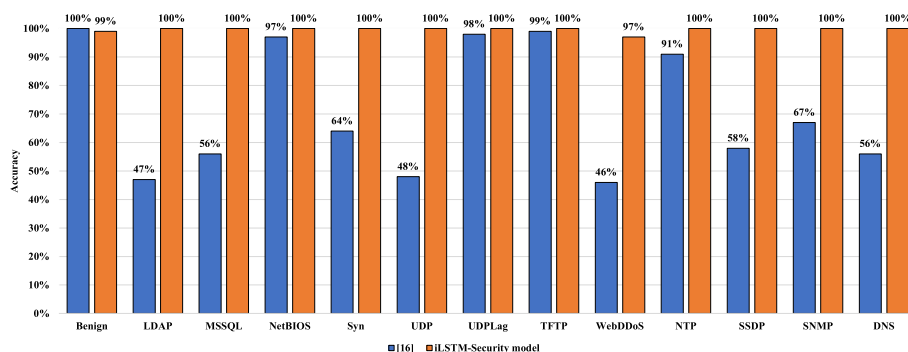


Fig. 16 Accuracy outcomes for 13 class

The assessment of the iLSTM-Security model is analyzed using the state-of-the-art model [16] as depicted in Fig. 16. The iLSTM-Security model effectively identifies LDAP, MSSQL, NetBIOS, Syn, UDP, UDP-lag, TFTP, NTP, SSDP, SNMP, and DNS threats with a 100 percent accuracy rate, whereas WebDDoS attacks attain 97% accuracy. The state-of-the-art model [16] attains the accuracy rate for LDAP as 47%, MSSQL as 56%, NetBIOS as 97%, Syn as 64%, UDP as 48% WebDDoS as 46%, SSDP as 58%, and DNS as 56%. However, it successfully identifies UDPLag, TFTP, and NTP with better accuracy. The overall comparative accuracy in identifying twelve separate DDoS threats and benign traffic surpasses using the iLSTM-Security model compared to the state-of-the-art model [16]. As discussed earlier, the data cleaning steps, the number of PCA components utilized, and the hyper-parameter configuration employed to train-test the iLSTM-Security model contribute to the superior outcomes over the cutting-edge model [16].

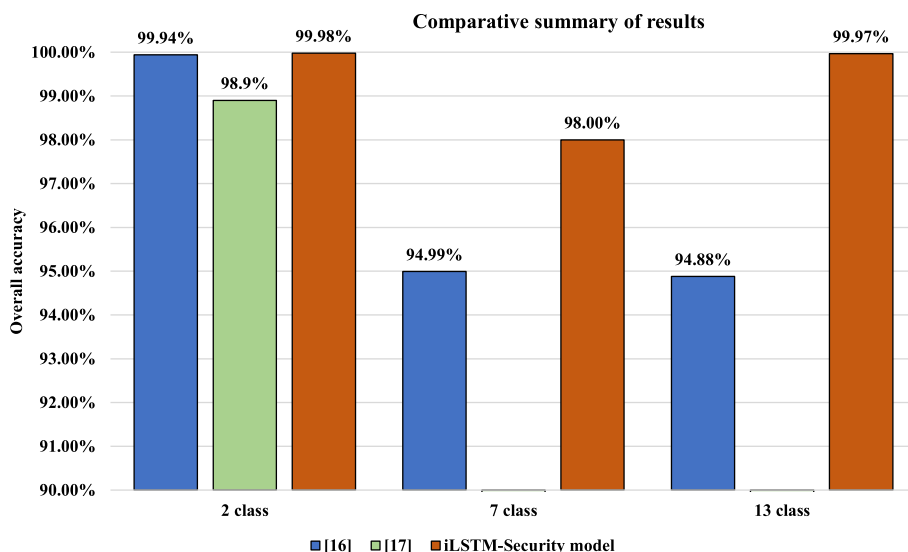


Fig. 17 Overall accuracy outcomes with state-of-the art model

4.4 Summary of Results

The comparison of the overall accuracy of the iLSTM-Security model and the state-of-the-art models [16] and [17] is depicted in Fig. 17. Figure 17 reveals that the iLSTM-Security model excels with the state-of-the-art models. The iLSTM-Security model achieves 99.98% accuracy for 2 classes, 98.8% accuracy for 7 classes, and a 99.97% accuracy rate for 13 class classifications, which is superior to the state-of-the-art model provided in [16] and [17]. Data pre-processing steps, the information extracted after PCA analysis, and hyper-parameter settings, including the number of *neurons*, *RMSprop* optimizer, and *ReLU* activation function, contribute to a more effective and efficient iLSTM-Security model training and testing process. In a nutshell, the iLSTM-Security model excels in specific DDoS threat detection accuracy and overall accuracy rate. The iLSTM-Security model, consisting of two LSTM layers and one fully connected layer, is compact, straightforward, and less complicated. The state-of-the-art model [17] includes one input layer, one LSTM layer with neuron 1280, and an output layer. Another state-of-the-art model [16] involves five LSTM layers, four dropout layers, and one output layer. Additionally, section 3.3.3 outlines that a comparable state-of-the-art model [16] takes more training time than the proposed iLSTM-Security model.

Protecting HetIoT infrastructures from diverse DDoS attacks, the iLSTM-Security model exhibits superior performance compared to existing state-of-the-art work. The iLSTM-Security model has yet to be evaluated against HTTP flooding attacks, one of the most dangerous DDoS threats expanding with the IoTs. The reason behind this is the CICDDoS2019 dataset doesn't contain this flooding threat. Also, portmap is another DDoS threat in the CICDDoS2019 dataset, and the iLSTM-Security model is not performing well. It demands further hyper-parameter settings and several LSTM layers.

5 Conclusions

The research presented an intelligent LSTM-based security model for HetIoT infrastructure to protect against DDoS threats. Compared to state-of-the-art models, the extensive data analysis and PCA techniques utilized in the research aid the iLSTM-Security model to work efficiently and attain better outcomes. The asymptotic time complexity analysis further demonstrated that the present iLSTM-Security model is time-efficient and less complex than state-of-the-art models. The research also discussed and compared the assessment of the individual and overall accuracy of the proposed iLSTM-Security model with the state-of-the-art intelligent security models. Furthermore, compared to the existing state-of-the-art models, the overall evaluation of the iLSTM-Security model is good. The proposed iLSTM-Security model shows 99.98% accuracy for 2 classes, 98% accuracy for 7 classes, and 99.97% accuracy for 13 class classifications. Further research will be dedicated to exploring the potential of federated learning in safeguarding the privacy of HetIoT applications while combating and avoiding DDoS cyberthreats.

Author Contributions Not Applicable

Funding Not Applicable

Availability of data and materials Not Applicable

Declarations

Conflict of interest/Conflict of interest Not Applicable

Ethics approval Not Applicable

Consent to participate Not Applicable

Consent for publication Not Applicable

Code availability Not Applicable

References

1. Mahadik Shalaka S., Pranav M. Pawar, & Muthalagu, Raja. (2023). Edge-HetIoT Defense against DDoS attack using Learning Techniques, Computers & Security, Elsevier, pp.103347
2. Mahadik, S. S., Pawar, P. M., & Muthalagu, R. (2023). *Heterogeneous IoT (HetIoT) security: techniques, challenges, and open issues* (pp. 1–42). Springer: Multimedia Tools and Applications.
3. Qiu, T., Chen, N., Li, K., Atiquzzaman, M., & Zhao, W. (2018). How Can Heterogeneous Internet of Things build our Future A survey. *IEEE Communications Surveys & Tutorials*, 20(3), 2011–2027.
4. Mahadik, S., Pawar, P. M., & Muthalagu, R. (2023). Efficient Intelligent Intrusion Detection System for Heterogeneous Internet of Things (HetIoT). *J Netw Syst Manage, Springer*, 31, 2. <https://doi.org/10.1007/s10922-022-09697-x>
5. Harbi, Y., Aliouat, Z., Harous, S., Bentaleb, A., & Refoufi, A. (2019). A review of security in internet of things. *Wireless Personal Communications, Springer*, 108, 325–344.
6. SCOTT IKEDA, IoT-Based DDoS Attacks Are Growing and Making Use of Common Vulnerabilities [Online]. Available: <https://www.cpomagazine.com/cyber-security/iot-based-ddos-attacks-are-growing-and-making-use-of-common-vulnerabilities/>. [Accessed: 25-Mar-2020].
7. Gasmi, R., Hammoudi, S., Lamri, M., & Harous, S. (2023). Recent Reinforcement Learning and Blockchain Based Security Solutions for Internet of Things: Survey. *Wireless Personal Communications*, 132(2), 1307–1345.
8. Cloudflare-Famous DDoS attack [Online]. Available: <https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/>.
9. DDoS Statistical Report [Online]. Available: <https://blog.nexusguard.com/threat-report/ddos-statistical-report-for-1hy-2022>. [Accessed: 05-Dec-2022].
10. DDoS 2.0 [Online]. Available: <https://thehackernews.com/2023/09/ddos-20-iot-sparks-new-ddos-alert.html>. [Accessed: 15-Sep-2023].
11. Cisco DDoS Annual Report (white paper) [Online]. Available: <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html>. [Accessed: 9-MAR-2020].
12. Mahadik, S. S., Pawar, P. M., Muthalagu, R., Prasad, N. R., & Mantri, D. (2022). Smart LSTM-based IDS for Heterogeneous IoT (HetIoT), In 2022 25th International Symposium on Wireless Personal Multimedia Communications (WPMC), Herning, Denmark, pp. 23–28. <https://doi.org/10.1109/WPMC55625.2022.10014866>.
13. Badamasi, U. M., Khaliq, S., Babalola, O., et al. (2020). A Deep Learning based approach for DDoS attack Detection in IoT-enabled Smart environments'', International Journal of Computer Networks and Commu. *Security*, 8(10), 93–99.
14. Amaizu, G. C., Nwakanma, C. I., Bhardwaj, S., et al. (2021). Composite and Efficient DDoS attack Detection framework for B5G networks''. *Computer Networks, Elsevier*, 188(107), 871.
15. Javed, D., Gao, T., & Khan, M. T. (2021). SDN-enabled Hybrid DL-driven framework for the Detection of Emerging Cyber Threats in IoT''. *Electronics, MDPI*, 10(8), 918.
16. Ferrag M.A., Shu L., Djallel H., & Choo K.-K.R. (2021). Deep Learning-Based Intrusion Detection for Distributed Denial of Service Attack in Agriculture 4.0'', *Electronics, MDPI*, vol. 10, pp.1257–1283. <https://doi.org/10.3390/electronics10111257>.
17. Jia, Y., Zhong, F., Alrawais, A., et al. (2020). Flowguard: An intelligent Edge Defense Mechanism against IoT DDoS attacks''. *IEEE Internet of Things Journal, IEEE*, 7(10), 9552–9562.

18. Novaes, M. P., Carvalho, L. F., Lloret, J., & Proença, M. L. (2020). Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment. *IEEE Access*, 8, 83765–83781. <https://doi.org/10.1109/ACCESS.2020.2992044>
19. Laghrissi, F., Douzi, S., Douzi, K., et al. (2021). Intrusion Detection Systems using Long Short-Term Memory (LSTM)”. *Journal of Big Data, Springer*, 8, 65. <https://doi.org/10.1186/s40537-021-00448-4>
20. Rohith Gandhi, A Look at Gradient Descent and RMSprop Optimizers [Online]. Available: <https://towardsdatascience.com/a-look-at-gradient-descent-and-rmsprop-optimizers-f77d483ef08b>. [Accessed: 05-Nov-2019].
21. Hossain, M. D., Ochiai, H., Fall, D., & Kadobayashi, Y. (2020). LSTM-based Network Attack Detection: Performance Comparison by Hyper-parameter Values Tuning”, In 2020 7th IEEE International Conf. on Cyber Security and Cloud Computing (CSCloud), pp.62–69 <https://doi.org/10.1109/CSCloud-EdgeCom49738.2020.00020>.
22. Gaur, V., & Kumar, R. (2021). *Analysis of Machine Learning Classifiers for Early Detection of DDoS Attacks on IoT Devices*” (pp. 1–22). Springer: Arabian Journal for Science and Engineering.
23. Sharafaldin I, Lashkari AH, Hakak S, et al, Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy”, In: 2019 International Carnahan Conf. on Security Technology (ICST), IEEE, pp.1–8, (2019).
24. CICDDoS2019 Dataset [Online]. Available: <https://www.unb.ca/cic/datasets/ddos-2019.html>. [Accessed: 2019].
25. Gojic, J., & Radakovic, D. (2022). Proposal of security architecture in 5G mobile network with DDoS attack detection, In 2022 7th International Conference on Smart and Sustainable Technologies (SpliTech), Split / Bol, Croatia, pp. 1-5. <https://doi.org/10.23919/SpliTech55088.2022.9854338>.
26. Elsayed, M. S., Le Khac, N. A., Dev, S. & Jurcut, A. D. (2020). DDoSnet A Deep Learning Model for Detecting Network Attacks”, In: 21st International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), IEEE, pp.391–396.
27. Meenakshi, K. Kumar & Behal, S. (2021). Distributed Denial of Service Attack Detection using Deep Learning Approaches ”, In 2021 8th International Conf. on Computing for Sustainable Global Development (INDIACom), IEEE, pp. 491–495
28. Boonchai, J., Kitchat, K., & Nonsiri, S. (2022). The classification of DDoS attacks using deep learning techniques, In 2022 7th International Conference on Business and Industrial Research, IEEE, pp. 544–550.
29. Saranya, N., Geetha, K., & Rajan, C. (2020). Data Replication in Mobile Edge Computing Systems to Reduce Latency in the Internet of Things. *Wireless Pers Commun*, 112, 2643–2662. <https://doi.org/10.1007/s11277-020-07168-7>
30. Prasad Patil, Exploratory Data Analysis (EDA) [Online]. Available: <https://towardsdatascience.com/exploratory-data-analysis-8fc1cb20fd15/>. [Accessed: 23-MAR-2018].
31. Wei, Y., Jang-Jaccard, J., Sabrina, F., Singh, A., Xu, W., & Camtepe, S. (2021). AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification. *IEEE Access*, 9, 146810–146821. <https://doi.org/10.1109/ACCESS.2021.3123791>
32. NTP amplification Attack [Online]. Available: <https://www.imperva.com/learn/ddos/ntp-amplification/>. [Accessed: 02-Jan-2023].
33. TFTP Attack [Online]. Available: <https://securityintelligence.com/news/trivial-file-transfer-protocol-used-in-new-ddos-attack/>. [Accessed: 07-Jan-2016].
34. MSSQL Reflection Attack [Online]. Available: <https://ddos-guard.net/en/terminology/attack-type/mssql-reflection-attack/>. [Accessed: 02-Jan-2023].
35. SSDP DDoS Attack [Online]. Available: <https://www.cloudflare.com/learning/ddos/ssdp-ddos-attack/>. [Accessed: 02-Jan-2023].
36. SNMP Reflection Attack [Online]. Available: <https://www.imperva.com/learn/ddos/snmp-reflection/>. [Accessed: 02-Jan-2023].
37. DNS Attack [Online]. Available: <https://www.imperva.com/learn/application-security/dns-hijacking-redirection/>. [Accessed: 02-Jan-2023].
38. Jeff Hale, Normalize with Scikit-Learn [Online]. Available: <https://towardsdatascience.com/scale-standardize-or-normalize-with-scikit-learn-6ccc7d176a02>, [Accessed: 4-Mar-2019].
39. Aditya Sharma, Principal Component Analysis (PCA) [Online]. Available: <https://www.datacamp.com/tutorial/principal-component-analysis-in-python>, [Accessed: 1-Jan-2020].
40. Jason Brownlee, Hyperparameter Optimization With Random Search and Grid Search [Online]. Available: <https://machinelearningmastery.com/hyperparameter-optimization-with-random-search-and-grid-search/>, [Accessed: 19-Sep-2020].
41. Divyang Goswami, Comparison of Sigmoid, Tanh and ReLU Activation Functions [Online]. Available: <https://www.aitude.com/comparison-of-sigmoid-tanh-and-relu-activation-functions/>, [Accessed: 19-Aug-2020].

42. Devrim Akgun, Selman Hizal, Unal Cavusoglu, A new DDoS attacks Intrusion Detection Model based on Deep Learning for Cybersecurity", *Computers & Security*, Elsevier, Vol.118, pp.102748, (2022), ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2022.102748>.
43. Christian Versloot, How-to-use-sparse-categorical-crossentropy-in-keras [Online]. Available: <https://github.com/christianversloot/machine-learning-papers/blob/main/how-to-use-sparse-categorical-crossentropy-in-keras.md>, [Accessed: 01-Feb-2020].
44. Vitaly Bushaev, Understanding RMSProp [Online]. Available: <https://towardsdatascience.com/understanding-rmsprop-faster-neural-network-learning-62e116fcf29a>, [Accessed: 02-Sept-2018].
45. Time complexity for LSTM [Online]. Available: <https://ai.stackexchange.com/questions/33927/what-is-the-time-complexity-for-testing-a-stacked-lstm-model>, [Accessed: 02-Dec-2022].
46. Murat Karakaya, LSTM-Understanding the Number of Parameters [Online]. Available: <https://www.kaggle.com/code/kmkarakaya/lstm-understanding-the-number-of-parameters>, [Accessed: 12-Dec-2022].
47. Aydın, H., Orman, Z., & Aydın, M. A. (2022). A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment. *Computers & Security*, 118, 102725.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.



Shalaka Shankar Mahadik is a Ph.D. Scholars in the Department of Computer Science at Birla Institute of Technology and Science (BITS) Pilani, Dubai campus, UAE. Her research interest includes Computer Networks, Information Security, Internet of Things (IoT), and Mobile communication. She has done her B.E and M. E. (Computer Engineering) from the Department of Computer Engineering at Mumbai University, Maharashtra, India in 2005 and 2011 respectively. She worked as a lecturer from 2005-to 2011 and as an Asst. Professor during the year 2011-to 2014. She has participated in and organized various Workshops and National Conferences. Currently, her research work is based on Security and Privacy in heterogeneous IoT (HetIoT). She published her research work in well-known, reputed conferences and journals from IEEE, Springer, and Elsevier. She also received honors for Best Paper Presentation in 2022 at the BITS Pilani Dubai Campus and Best Research Proposal in 2023 at the University of Sharjah in the UAE.



Pranav M. Pawar graduated in Computer Engineering from Dr. Baba-saheb Ambedkar Technological University, Maharashtra, India, in 2005, received a Master in Computer Engineering from Pune University, in 2007, and received Ph.D. in Wireless Communication from Aalborg University, Denmark in 2016, his Ph.D. thesis received a nomination for Best Thesis Award from Aalborg University, Denmark. Currently, he is working as an Assistant Professor in the Dept of Computer Science, Birla Institute of Technology and Science, Dubai, before BITS he was a postdoctoral fellow at Bar-Ilan University, Israel from March 2019 to October 2020 in the area of Wireless Communication and Deep Learning. He is the recipient of an outstanding post-doctoral fellowship from the Israel Planning and Budgeting Committee. He worked as an Associate Professor at MIT ADT University, Pune from 2018-to 2019 and also as an Associate Professor in the Department of Information Technology, STES's Smt. Kashibai Navale College of Engineering, Pune from 2008-2018. From 2006 to 2007, was working as System Executive in POS-IPC, Pune, India. He

received Recognition from Infosys Technologies Ltd. for his contribution to the Campus Connect Program and also received different funding for research and attending conferences at the international level. He published more than 40 papers at the national and international levels. He is IBM DB2 and IBM RAD certified professional and completed NPTEL certification in different subjects. His research interests are Energy efficient MAC for WSN, QoS in WSN, wireless security, green technology, computer architecture, database management system, and bioinformatics.



Raja Muthalagu is currently an Associate Professor with Birla Institute of Technology and Science, Pilani, Dubai Campus, Dubai, UAE. He was a Postdoctoral Research Fellow with Air Traffic Management Research Institute, Nanyang Technological University, Singapore, from 2014 to 2015. Dr. Muthalagu was the recipient of the Canadian Commonwealth Scholarship Award 2010 for the Graduate Student Exchange Program in the Department of Electrical and Computer Engineering, University of Saskatchewan, Saskatoon, SK, Canada. His research interest includes wireless communication, signal processing, aeronautical communication, and cyber security.



Neeli R. Prasad CTO of SmartAvatar B.V. Netherlands and VehicleAvatar Inc. USA, IEEE VTS Board of Governor Elected Member & VP Membership. She is also full Professor at Department of Business Development and Technology (BTech), Aarhus University. Neeli is a cybersecurity, networking and IoT strategist. She has throughout her career been driving business and technology innovation, from incubation to prototyping to validation and is currently an entrepreneur and consultant in Silicon Valley. She has made her way up the “waves of secure communication technology by contributing to the most ground breaking and commercial inventions. She has general management, leadership and technology skills, having worked for service providers and technology companies in various key leadership roles. She is the advisory board member for the European Commission H2020 projects. She is also a vice chair and patronage chair of IEEE Communication Society Globecom/ICC Management & Strategy Committee (COM-SOC GIMS) and Chair of the Marketing, Strategy and IEEE Staff Liaison Group. Dr. Neeli Prasad has led global teams of researchers across

multiple technical areas and projects in Japan, India, throughout Europe and USA. She has been involved in numerous research and development projects. She also led multiple EU projects such as CRUISE, LIFE 2.0, ASPIRE, etc. as project coordinator and PI. She has played key roles from concept to implementation to standardization. Her strong commitment to operational excellence, innovative approach to business and technological problems and aptitude for partnering cross-functionally across the industry have reshaped and elevated her role as project coordinator making her a preferred partner in multinational and European Commission project consortiums. She has 4 books on IoT and WiFi, many book chapters, peer-reviewed international journal papers and over 200 international conference papers. Dr. Prasad received her Master's degree in electrical and electronics engineering from Netherland's renowned Delft University of Technology, with a focus on personal mobile and radar communications. She was awarded her Ph.D. degree from Università di Roma “Tor Vergata”, Italy, on Adaptive Security for Wireless Heterogeneous Networks.



Dnyaneshwar S. Mantri is graduated in Electronics Engineering from Walchand Institute of Technology, Solapur (MS) India in 1992 and received Masters from Shivaji University in 2006. He has awarded PhD. in Wireless Communication at Center for TeleInFrastruktur (CTIF), Aalborg University, Denmark. He has teaching experience of 25 years. From 1993 to 2006 he was working as a lecturer in different institutes [MCE Nilanga, MGM Nanded, and STB College of Engg. Tuljapur (MS) India]. From 2006 he is associated with Sinhgad Institute of Technology, Lonavala, Pune and presently he is working as Professor in Department of Electronics and Telecommunication Engineering. He is IEEE member, Life Member of ISTE and IETE. He has published three books, 09 Journal papers in indexed and reputed Journals (Springer, Elsevier, IEEE etc.) and 19 papers in IEEE conference s. He is reviewer of international journals (Wireless Personal Communication, Springer, Elsevier, IEEE, Communication society, MDPI etc.) and conferences organized by IEEE. He worked as TPC member for various IEEE conferences and also organized IEEE conference

GCWCN2014. He worked on various committees at University and College. His research interests are in Adhoc Networks, Wireless Sensor Networks, Wireless Communications specific focus on energy and bandwidth.

Authors and Affiliations

Shalaka S. Mahadik¹ · Pranav M. Pawar¹  · Raja Muthalagu¹ · Neeli Rashmi Prasad² · Dnyaneshwar Mantri³

✉ Pranav M. Pawar
pranav@dubai.bits-pilani.ac.in

Shalaka S. Mahadik
p20200002@dubai.bits-pilani.ac.in

Raja Muthalagu
raja.m@dubai.bits-pilani.ac.in

Neeli Rashmi Prasad
neeli.prasad@ieee.org

Dnyaneshwar Mantri
dsmantri.sit@sinhgad.edu

¹ Department of Computer Science, Birla Institute of Technology and Science Pilani, Dubai Campus, Dubai, UAE

² TrustedMobi “VehicleAvatar Inc.”, Mountain View, CA, USA

³ Sinhgad Institute of Technology, Lonavala, India