Ain Shams Engineering Journal 14 (2023) 102211

Contents lists available at ScienceDirect

Ain Shams Engineering Journal

journal homepage: www.sciencedirect.com

Securing IoT and SDN systems using deep-learning based automatic intrusion detection

Rania A. Elsayed, Reem A. Hamada *, Mahmoud I. Abdalla, Shaimaa Ahmed Elsaid

Electronics and Communications Department, Faculty of Engineering, Zagazig University, Zagazig, Egypt

ARTICLE INFO

Article history:
Received 11 September 2021
Revised 16 January 2023
Accepted 18 February 2023
Available online 03 March 2023

Keywords:
Intrusion Detection System (IDS)
Internet of Things (IOT)
Deep Learning (DL)
Long Short-Term Memory (LSTM)
ToN-IoT dataset
InSDN dataset

ABSTRACT

Both Internet of Things (IoT) and Software Defined Networks (SDN) have a major role in increasing efficiency and productivity for smart cities. Despite that, they face potential security threats that need to be reduced. A new Intrusion Detection System (IDS) has become necessary to secure them. Many researchers have recently used recent techniques such as machine learning to analyze and identify the rapid growth of attacks and abnormal behavior. Most of these techniques have low accuracy and less scalability. To address this issue, this paper proposes a Secured Automatic Two-level Intrusion Detection System (SATIDS) based on an improved Long Short-Term Memory (LSTM) network. The proposed system differentiates between attack and benign traffic, identifies the attack category, and defines the type of sub-attack with high performance. To prove the efficiency of the proposed system, it was trained and evaluated using two of the most recent realistic datasets; ToN-IoT and InSDN datasets. Its performance was analyzed and compared to other IDSs. The experimental results show that the proposed system outperforms others in detecting many types of attacks. It achieves 96.35 % accuracy, 96 % detection rate, and 98.4 % precision for ToN-IoT dataset. For InSDN dataset, the results were 99.73 % accuracy, 98.6 % detection rate, and 98.9 % precision.

1. Introduction

To accommodate the rising population, metropolitan areas require infrastructure that facilities addressing environmental and transportation concerns. The fast development of low-cost devices such as sensors, actuators and radio-frequency identification, combined with wireless communication technologies as IoT-oriented infrastructure, has created an ideal environment for building numerous smart city applications [1–3], as in Fig. 1. IoT is a powerful platform for combining users worldwide without human interference, as in Fig. 2. It connects everything to the Internet via data sensing devices that enable intelligent identification, tracking, localization, administration, and supervision. It has several uses include intelligent health care, intelligent transport, and smart grids. Like other networks, this technology seeks to enhance our personal and professional lives [4,5].

Along with the fast growth of IoT systems and devices, the interconnectedness of various IoT sensors in smart networks offers a multitude of potential dangers to IoT devices in smart cities. Physical and cyber-attacks are both possible in a smart city. Physical attacks are initiated when attackers are physically closer to the equipment and thus have the opportunity to adapt the network's devices or sensors. Malicious code injection, radio frequency jamming, fake node injection, permanent denial of service, side channel attack, and sleep denial assault are all examples of these attacks. On the other hand, in cyber-attacks, the attacker attempts to inject malicious or malware software into network components in order to obtain unauthorized access to them. Man-in-the-Middle (MITM) attacks, Denial-of-Service (DoS) attacks, Distributed Denial-of-Service (DDoS) attacks, and Ransomware assaults are all examples of these types of attacks. Such attacks are becoming more prevalent at an alarming rate and can threaten the confidentiality, security, and availability of data [7,8].

Software-Defined Networking (SDN) is a recent technology which utilizes software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network. It helps drive the expansion of IoT-enabled devices, enhances the efficiency of network resource sharing and improves IoT service-level agreements.

Although combining IoT and SDN improves IoT operations and security by allowing full and remote control of network setup

* Corresponding author.
E-mail address: reemhamada@zu.edu.eg (R.A. Hamada).

https://doi.org/10.1016/j.asej.2023.102211

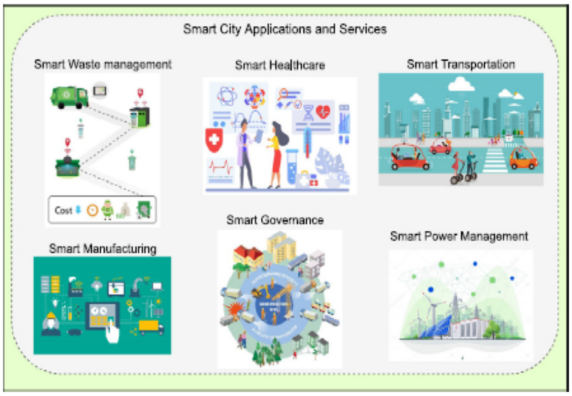


Fig. 1. Smart cities construction [1].

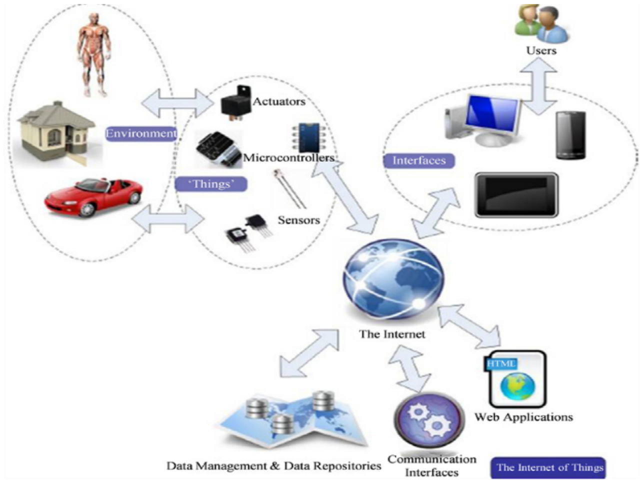


Fig. 2. IOT illustration [6].

without requiring direct contacts with IoT devices, an efficient IDS is required to protect the system from various types of attacks. An IDS system is a security mechanism that used to monitor the network traffic and protects authorized users against any malicious activities that compromises an information system's confidentiality, reliability, and availability. It alerts network administrator about that behaviors who acts to protect the network by preventing it [2,9–11]. To assess this massive amount of data and to give relevant knowledge for classification, decision-making, and cyber-attack detection, various IDS systems make use of artificial intelligence technologies such as machine learning (ML) or Deep Neural Network (DNN) approaches. The more extensive DNN networks are called Deep Learning (DL), which consider an ML border subfield. It is an artificial intelligence function that simulates the human brain's data processing and decision-making mechanisms. DL contains many hidden layers to solve many of the complicated problems in various applications. The input of each layer is the output of the previous layer, as in Fig. 3. Although DL gives high performance, its main limitation is a longer training time for more essential training data [9]. Convolution Neural Network (CNN) and Recurrent Neural Networks (RNN) are two popular types of DL models. CNN is used in computer image processing and language processing while RNN is used in the processing of natural language and text processing. LSTM network is considered an extension of the RNN network which is able to learn using line sequences pattern. So, it can be used to identify traffic type into attack or normal. The primary benefit of this form of deep learning is that the raw data is used directly [5].

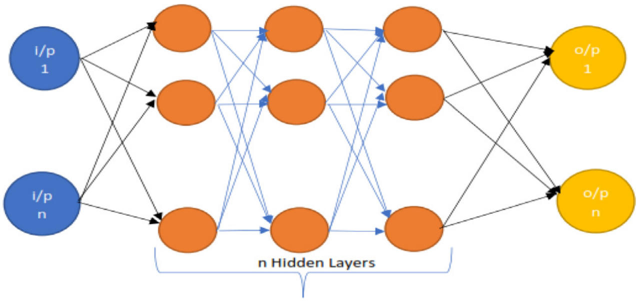


Fig. 3. Deep Learning model architecture.

1.1. Problem statement

Extensive study has been conducted on data security, privacy, reliability, detection, and mitigation of cyberattacks. However, there are a range of issues that must be solved in order to establish sustainable smart cities. Following are the issues to be addressed.

i. As the Internet of Things and other new technologies gain in popularity, the amount of data being generated will only increase. To examine such a large amount of data, new methods should be used.
ii. It is difficult to create a security mechanism that accurately distinguishes between normal and abnormal behavior in a dynamic and large-scale IoT environment.
iii. Many new methods and a wide diversity of data make it harder to learn features that can distinguish between normal and abnormal traffic.
iv. Using a real-world IoT-based dataset that reflects real-world IoT-based cyberattacks to evaluate the proposed IDS's performance is a challenging undertaking due to low-frequency attacks resulting from an unbalanced training set.

1.2. Our contribution

To address the issues raised in the preceding subsection, this paper presents a SATIDS system to protect IoT and SDN networks. It utilizes LSTM network that considered a qualified IDS to accurately identify suspicious activities and types of attack. The proposed system was trained and tested using two of the most recent datasets based on realistic data; ToN-IoT and InSDN datasets. The key contributions of this paper are:

- Building the proposed SATIDS system utilizing improved LSTM that classifies traffic into normal or attack. Then, it determines the attack category. Finally, it defines the attack sub-type.
- Testing the proposed system using the ToN-IoT and InSDN datasets, and comparing its performance was compared to other IDSs.

2. Literature review

Deep learning has several benefits in cyber defense, as it can help researchers and cyber analysts gain insights into threats and stay ahead of opponents. Attack detection and prevention continue to be a hot area of research that receives considerable attention due to the variety of attackers and possible damage. Recently, numerous researches have been carried out to detect network attacks using various DLs.

In [1], the authors presented a dependable privacy-preserving secure framework (TP2SF) for smart cities. This framework is comprised of three modules: a module for trustworthiness, a module with two levels of privacy, and an intrusion detection module. They used 19 features only from 43 features. The authors of [2] proposed a cyberattack detection system for IoMT networks based on ensemble learning and fog-cloud architecture. The ensemble design integrates the Decision Tree, Naive Bayes, and Random Forest models created by the individual learners.

A new method based on LSTM autoencoder and one-class support vector machine (OC-SVM) is shown in [9] to find anomaly-based attacks in an unbalanced dataset. The models are trained with only examples of normal classes. In [10], a model was made that takes the given features and pulls out the important ones. It then uses deep learning to classify incursions. Notably, the underlying data points can't be thought of as samples from a single distribution. Instead, they come from two different distributions, one that applies to all network intrusions and the other that is specific to one domain. Table 1 contains previous approaches in that field.

Table 1
Previous Ids Approaches.

Ref.	Technique	Dataset	Perfomance Analysis
[1]	Trustworthy Privacy-Preserving Secured Framework for smart cities is presented using three modules: a trustworthiness module, a two-level privacy module, and an intrusion detection module	ToN-IoT BoT-IoT	Accuracy of 98.84% Accuracy of 99.99%
[2]	Ensemble learning and fog-cloud architecture-driven cyberattack detection framework for IoMT networks	ToN-IoT	Accuracy of 96.35%
[9]	Hyper approach based on LSTM autoencoder and One-class Support Vector Machine to detect anomalies based attacks in an unbalanced dataset	InSDN	Accuracy of 90.5%
[10]	CNN technique with L2 regularization and the dropout methods to address the overfitting problem	InSDN	Accuracy of 93.01%
[11]	DL platform combination of binary bat algorithm, binary genetic algorithm, and binary gravitational search algorithm.	CICIDS2017	Accuracy of 99.002%
[12]	A clustering method based on unsupervised component selection and initialization of the cluster centre	KDD CICIDS2017 Wormhole	Accuracy of 93.07% Accuracy of 88% Accuracy of 94.06%
[13]	ML models (DNN and LSTM) for binary prediction of unknown DoS/DDoS attacks	CICIDS2017	99.8% True Positive Rate for DNN 99.9% True Positive Rate for LSTM
[14]	A novel technology for enhancing the high-efficiency identification rate of minority groups	UNSW-NB15 CICIDS2017	Detection Rate of 99.74% for binary classification and 96.54% for multiclass classification Detection rate of 99.85 %
[15]	A new method to reduce the feature subset for the web- attack classification.	CICIDS2017	Accuracy = 99.6191%

[16]	Scale-hybrid-IDS-AlertNet	KDDCup99
		NSL-KDD
		UNSW-NB15
		WSN-DS
		CICIDS2017
		Kyoto
			Accuracy = 93%
			Accuracy = 80.1%
			Accuracy = 84.5%
			Accuracy = 99.2%
			Accuracy = 96.3%
			Accuracy = 88.5%

[17]	Secured Privacy-Preserving Framework (SP2F) for smart agricultural UAV	ToN-IoT
		IoT Botnet
			Accuracy = 99.77%
			Accuracy = 99.98%

[18]	An enhanced-proof-of-work-technique-based blockchain	Power System
		UNSW-NB15
			Accuracy = 95.2%
			Accuracy = 98.1%

[19]	Fuzzy Gaussian Mixture-based Correntropy, based on the fuzzy rough set attribute reduction method	NGIDS-DS
		KDD-98
		ToN_IoT
			Accuracy = 95.48%
			Accuracy = 99.55%
			Accuracy = 97.54%

3. Subjects and methods

3.1. Database description

The IDSs performance is based on the quality of the training dataset. The lack of up-to-date real-world dataset is one of the key obstacles in deploying detection methods. The main reason why public data sets are not available for the intrusion detection area is privacy and legal considerations. The proposed algorithm is trained and evaluated using two of the most recent realistic datasets namely ToN-IoT and InSDN dataset.

3.1.1. ToN-IoT dataset

The ToN-IoT dataset is obtained from a practical and large-scale network developed by UNSW Canberra Cyber IoT Lab, School of Engineering and Information Technology (SEIT), UNSW Canberra at The Australian Defense Force Academy (ADFA) [19,20]. The dataset is compiled in parallel processing to collect a range of routine and cyber-attack events from IoT networks. A new testbed was built at the IoT lab to connect a range of virtual computers, physical tools, hacking systems, cloud and fog systems, and IoT sensors to simulate the functionality and scalability of the automotive IoT and Enterprise 4.0 networks. This dataset contains different recent smart city-based attacks such as DoS, DDoS, and ransomware. These attacks have been deployed against web applications, IoT gateways, and computer systems across the IoT network. This dataset contains 43 features with 4,61,043 total observations divided into 3,00000 normal and 1,61,043 attack observations. The dataset was divided into 70 % and 30 % of train and test set respectively. Table 2 shows the statistic of normal traffic and different attack vectors which was presented in the dataset [1,2].

3.1.2. InSDN dataset

The InSDN dataset covers many scenarios and attack classes, including Probe, DoS application, web attacks, Brute Force attack, password guessing, U2R, and DDos attacks. In addition, InSDN regular traffic also encompasses several common features. The dataset source of attacks originates from both an internal and an external network to imitate the actual attack scenarios. It covers about 80 statistical aspects in CSV format such as Protocol, Duration, Byte number, Packet number, etc. The overall number of dataset instances for normal and attack traffic is 343,939; a total of 68,424 for normal traffic and 275,515 for attack traffic as shown in Table 3.

The attack traffic emulates the same normal behavior since normal and malicious traffics are transmitted to the SDN controller for decision-making. Furthermore, the centralized perspective of the SDN network and the separation of the data plane from the control plane gives the attacker a new option compared to the traditional network of numerous attacks. These intrusions are not easy to be detected since the intruder is permitted to access to the victims' server.

As a result, such a data collection might be a good indicator for the model assessment that reflects the real-world scenario. Furthermore, the InSDN dataset contains no redundant records to

Table 2
Ton-Iot Database.

Attacks	No. of Instances	%
Normal	300,000	65.07
Backdoor	20,000	4.34
Scanning	20,000	4.34
Injection	20,000	4.34
Password	20,000	4.34
XSS	20,000	4.34
Ransomware	20,000	4.34
DDOS	20,000	4.34
DOS	20,000	4.34
MITM	1043	0.23

Table 3
InSDN Database.

Attacks	No. of Instances	%
Normal	68,424	52.32
DoS-Application	31,628	24.19
Probe	15,225	11.64
DDOS	9943	7.6
DoS-Network	3772	2.88
Brute force attack	1405	1.07
Web Application	192	0.147
Botnet	164	0.125
U2R	17	0.013

prevent the learner model from distracting itself from the most common records [9,10,21].

3.2. LSTM network

DNN is a type of neural network with a hierarchical structure and many hidden layers. The network becomes denser when the hidden layers increase. It becomes trendy among cybersecurity researchers in the last few years. LSTM network is RNN that uses the input information to predict the next sequence according to the detected pattern. The recurrence of the network delay, which represents the complex system output, is the RNN's most essential characteristic. Furthermore, RNNs maintain an activation vector that makes the RNN an intense neural network. However, due to explosion and gradient difficulties, it's also difficult to teach RNNs to rely on data from time series for a long time [17].

LSTM architecture makes it a good choice for solving the RNN extinction gradient problem. It uses a memory cell, which in sequential data may represent long-term dependencies. Fig. 4 shows the internal structure of the LSTM memory cell. The between memory units. The input gate decides whether the input signal will alter the memory cell's status or not. On the other hand, the output gate determines which memory cell status can be changed. The forgotten gate can decide to forget its status (or remember it). The activity of the LSTM hidden layer is calculated at each step, depending on the configuration of the LSTM, as shown in Fig. 4. The internal four memory gates are responsible for regulating the interlinkage. he interlinkage between memory units. The input gate decides whether the input signal will alter the memory cell's status or not. On the other hand, the output gate determines which memory status can be changed depending on the previous input. The forgotten gate can decide to forget its status (or remember it), under the following equations, at time t:

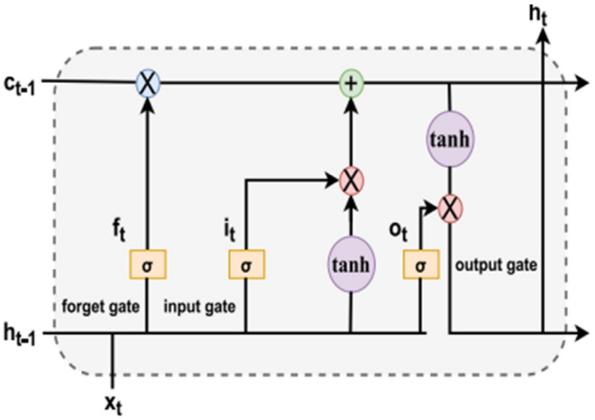


Fig. 4. LSTM internal architecture structure [18].

$$i_t = \sigma(W_{xi}x_t + W_{hi}h_{t-1} + W_{ci}c_{t-1} + b_i) \tag{1}$$

$$f_t = \sigma(W_{xf}x_t + W_{hf}h_{t-1} + W_{cf}c_{t-1} + b_f) \tag{2}$$

$$o_t = \sigma(W_{xo}x_t + W_{ho}h_{t-1} + W_{co}c_t + b_o) \tag{3}$$

$$c_t = f_t c_{t-1} + i_t \tanh(W_{xc}x_t + W_{hc}h_{t-1} + b_c) \tag{4}$$

$$h_t = o_t * \tanh(c_t) \tag{5}$$

Where i_t, f_t, o_t, and c_t are the input, forget, output and cell gate activations at any time t respectively.

σ: Logistic sigmoid function.
W_*: Weight matrices.
b_*: Variable biases.
h_{t-1}: Hidden state at time step t − 1.
c_{t-1}: Cell state step at time t − 1.

4. The proposed system

In multi-attack IDS system, the main target is to improve detection efficiency to be more accurate in defining attack type. That helps to face various forms of attack. To accurately detect the attack type, a SATIDS system based on LSTM network is proposed. This system achieves better performance than others IDSs. Fig. 5 presents the inner structure of the proposed SATIDS system. Rectified Linear Unit (Relu layer) activation function performs a threshold operation to an input element concerning zero as some input data contain negative values. Relu layer passes the positive input and gives zero value to the negative values. Then number of LSTM layers are used; each of them is followed by a 0.2 probability dropout layer. The dropout layer probability value was chosen 0.2 according to the try and error method to give the highest overall performance parameters as in Fig. 6. The dropout layer sets the input to avoid overfitting that decreases the network performance parameters. The initial learning rate was set to 0.0001, and LSTM batch size is 2000 to provide the highest performance parameters. A fully connected layer flattens the output of the previous layers and converts it to a single vector. Finally, the Softmax layer will

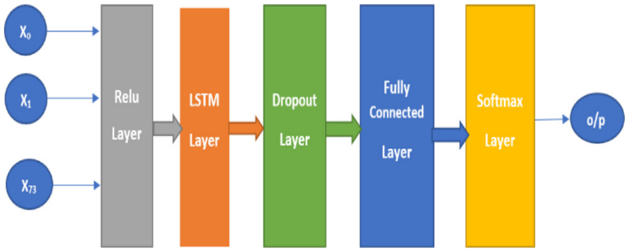


Fig. 5. Modified DL-based LSTM network.

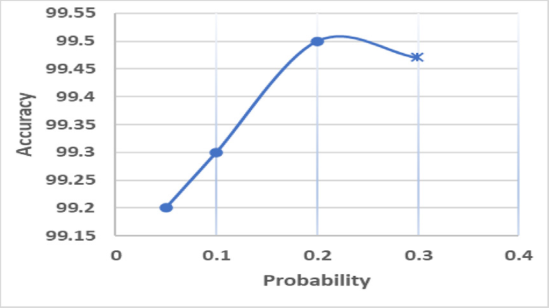


Fig. 6. Proposed algorithm parameters (Accuracy vs. Dropout layer probability).

eventually enter the classification layer classifying the data as benign or a form of attack.

```
Algorithm: SATIDS System
Input: Dataset (ToN-IoT or InSDN)
    Result: Traffic type
    Procedures:
    1 Remove IP address and time stack
    2 Divide the dataset into 70 % for training & 30 % for testing
    3 Insert training dataset to the proposed system
    4 For each record
    train network with each traffic record and consider the
    traffic label END FOR

    6 Input testing records to the trained system
    6 Identify traffic type (normal or malicious)
    7 If the traffic classified as anomaly, detect the type of
      attack
    8 Calculate network performance
```

The block diagram of the proposed SATIDS system is shown in Fig. 7. The algorithm below demonstrates the process of SATIDS system. ToN-Iot & InSDN datasets are used to train and test the proposed system. First, the IP address and time stake label were removed. Then, the dataset is divided into 70 % for training and 30 % for testing. Each line of data enters the network separately. After training the system using the training dataset, the system became ready to identify the category of data (normal or malicious traffic). For each testing record, the system first categorizes it as normal or attacks.

If an attack occurs, it deduces the type of attack, whether it is DDOS/DOS, Backdoor, Injection, Mitm, Password, Ransomware, Scanning, XSS, BFA, BotNet, Probe, U2R, or Web-Attack, according to the learning pattern. Finally, the network performance was tested by comparing the network output category with the actual testing record label.

5. Experimental results and discussion

Using MATLAB on an Intel Core-i7 processor with 8 GB RAM and Windows 10 platform, the proposed SATIDS system was implemented and its intrusion detection performance was tested. Using the confusion matrix and Receiver Operating Characteristic (ROC) curve, the system performance was measured. The performance of the proposed system was analyzed and compared with others.

Confusion matrix is a table structure commonly used for multiclass assessment. It includes information on current and forecast classifications. It consists of four main values determined for each class [17]:

- **True Positive (TP):** number of normal observations in dataset traffic which were classified by the technique correctly.
- **True Negative (TN):** number of intrusion observations which is properly classified by the algorithm as normal.
- **False Positive (FP):** number of normal traffic observations wrongly identified by the algorithm as abnormal.
- **False Negative (FN):** number of irregular observations wrongly identified by the algorithm as normal observations.

The key parameters to measure the network efficiency are Accuracy, Precision, Specificity, Detection rate, and F1 Score. The following equations were used to compute these parameters:

- **Accuracy:** The ratio of correctly calculated observations by the network to the total number of samples in the dataset.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{6}$$

- **Precision:** The number of corrected detected observations, divided by the total number of observations that the model identifies as an attack.

$$\text{Precision} = \frac{TP}{TP + FP} \tag{7}$$

- **Detection Rate** (DR)**:** The ratio of the corrected observations observed by the model to the total number of tests.

$$DR = \frac{TP}{TP + FN} \tag{8}$$

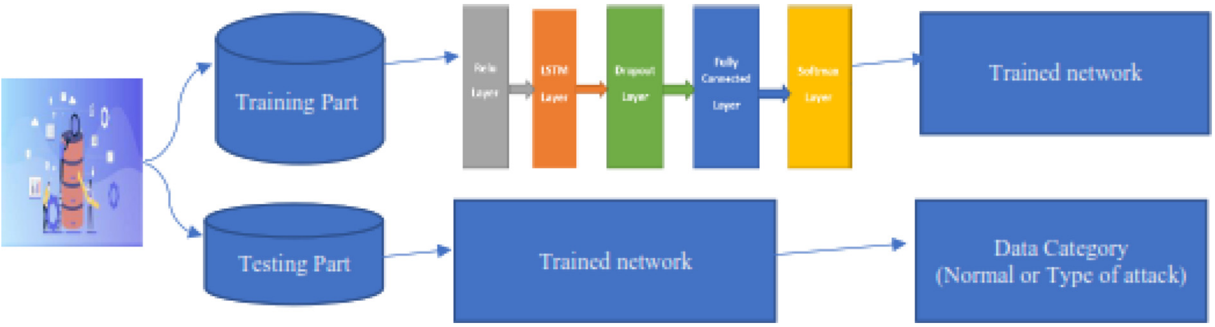


Fig. 7. Block diagram of the proposed SATIDS system.

- **Specificity (TNR):** The proportion of negatives that are detected correctly.

$$\text{Selectivity} = \frac{TN}{FP + TP} \tag{9}$$

- **F1-score:** Evaluating the test accuracy by calculating the average weight of the detection rate.

$$\text{F1} - \text{score} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \tag{10}$$

5.1. Performance Analysis

To get the highest performance of the proposed SATIDS model, the system performance was tested using different number of LSTM layers and various number of hidden layers.

5.1.1. TON-IOT dataset

– *Binary Classification (normal/anomaly)*

Table 4 and Fig. 8 represent the performance of the proposed SATIDS system at different numbers of hidden layers (H) and LSTM layers (L). It is obvious that the system records the highest accuracy in case of 500 hidden layers for 2 LSTM layers (accuracy = 96.35 %) and 3 LSTM layers (accuracy = 95.56 %). Also, the area under ROC curve has its highest value with 97.03 % for 2 LSTM layers and 96.51 % for 3 layers. FAR is the lowest in case of 2 LSTM layers and 500 hidden layers. Precision has its highest value in case of 2 LSTM layers and 500 hidden layers (Pr = 98.4 %).

Fig. 9 presents the performance of the proposed SATIDS system when facing Backdoor attack. As shown, the system has its highest performance when using 4 LSTM layers and 300 hidden layers: 95.7 % precision and 99.9 % detection rate. When facing DDOS attack, the performance of proposed SATIDS system is shown in Fig. 10. The network has its highest performance when using 3 LSTM layers and 500 hidden layers: 94.8 % precision and 92.7 % detection rate.

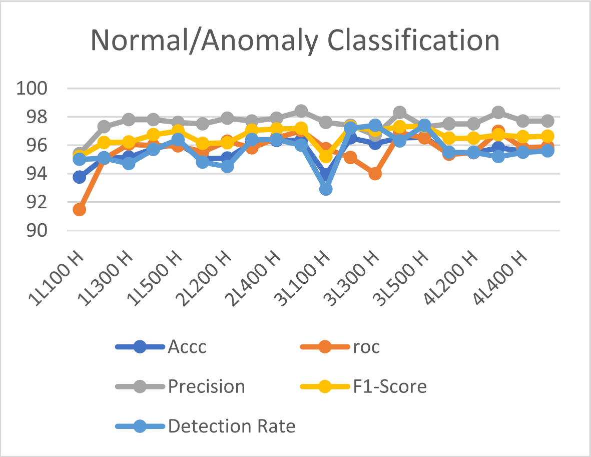


Fig. 8. Performance Analysis of the proposed system using TON-IOT Dataset.

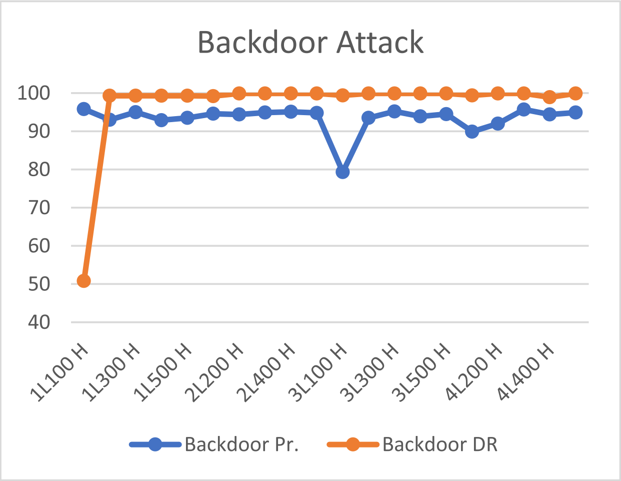


Fig. 9. Detecting Backdoor Attack.

Figs. 11–13 represent the performance of proposed SATIDS system when facing DOS attack, DDOS attack, and MITM attack, respectively. As shown, the network has its highest performance when using 3 LSTM layers and 500 hidden layers. When facing Password attack, Ransomware attack and scanning attack, the

Table 4
Performance Analysis of the proposed SATIDS system (using ToN-IoT Dataset).

# LSTM	# Hidden	ACC.	ROC	FAR	Precision	F1-Score	Detection Rate
1	100	93.75	91.46	8.5	95.4	95.2	95
1	200	95.11	95.06	4.9	97.3	96.19	95.1
1	300	95.15	96.07	3.9	97.8	96.225	94.7
1	400	95.77	95.97	4	97.8	96.739	95.7
1	500	96.12	95.95	4.3	97.6	97	96.4
2	100	95.06	95.54	4.5	97.5	96.13	94.8
2	200	95.09	96.28	3.7	97.9	96.17	94.5
2	300	96.17	95.81	4.2	97.7	97.05	96.4
2	400	96.34	96.51	3.8	97.9	97.144	96.4
2	500	96.35	97.03	3	98.4	97.19	96
3	100	93.91	95.75	4.3	97.6	95.19	92.9
3	200	96.51	95.13	4.9	97.4	97.3	97.2
3	300	96.13	93.99	6.2	96.7	97.05	97.4
3	400	96.52	96.86	3.1	98.3	97.3	96.3
3	500	96.56	96.51	5.1	97.3	97.35	97.4
4	100	95.44	95.36	4.6	97.5	96.49	95.5
4	200	95.47	95.49	4.5	97.5	96.49	95.5
4	300	95.82	96.97	3	98.3	96.73	95.2
4	400	95.59	95.79	4.2	97.7	96.59	95.5
4	500	95.68	95.9	4.1	97.7	96.63	95.6

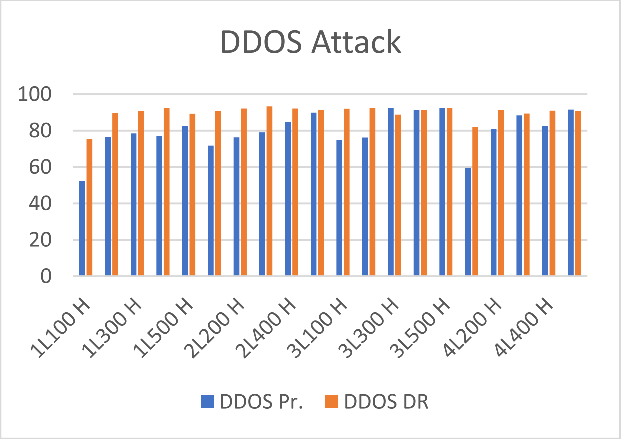


Fig. 10. Detecting DDOS Attack.

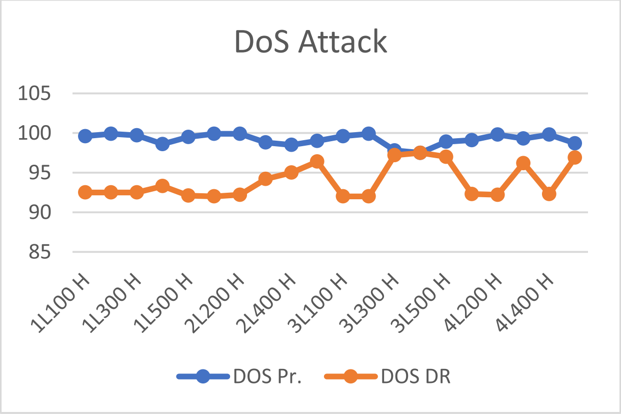


Fig. 11. Detecting DOS Attack.

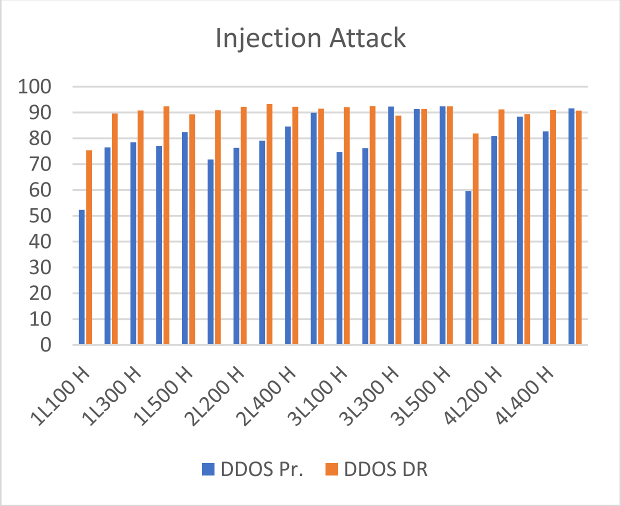


Fig. 12. Detecting Injection Attack.

performance of the proposed SATIDS system is shown in Figs. 14–16 respectively. As shown, the network also has its highest performance when using 3 LSTM layers and 500 hidden layers.

Detection Rate in case of using 3 LSTM layers and 500 hidden layers is the highest (DR = 97.4 %), unlike that of using 2 LSTM layers and 500 hidden layers (DR = 96 %). For all that, the system

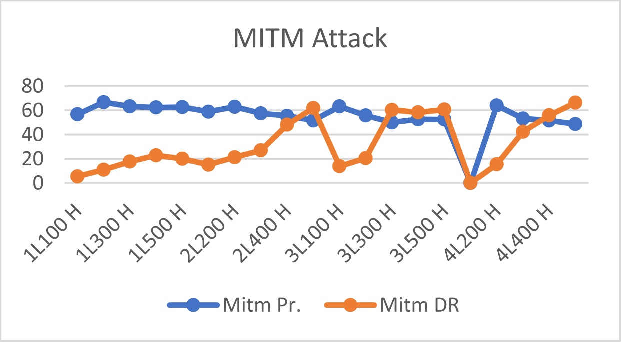


Fig. 13. Detecting MITM Attack.

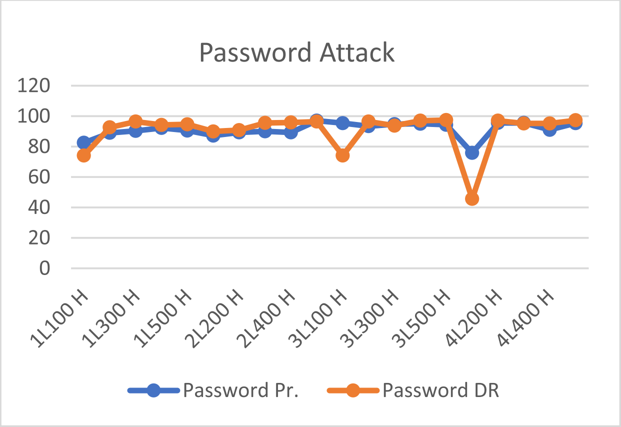


Fig. 14. Detecting Password Attack.

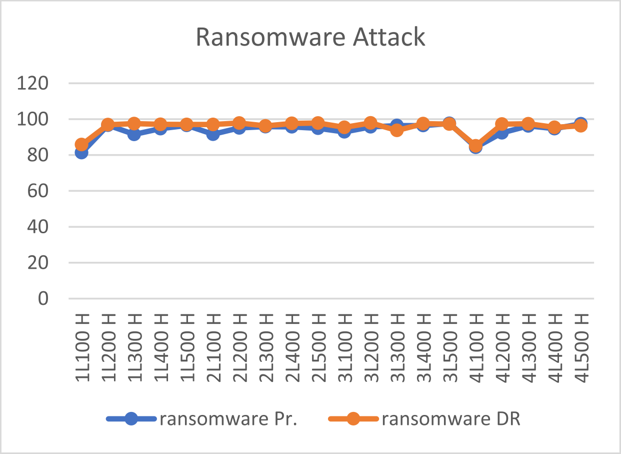


Fig. 15. Detecting Ransomware Attack.

setting was selected as 3 LSTM layers and 500 hidden layers in case of binary classification since it has the best performance.

– *Multi-attack classification*

Table 5 and Figs. 9–13 show the performance of the proposed SATIDS system in case of multiclassification using ToN-IoT dataset. For each attack, the accuracy and detection rate were recorded at different number of LSTM layers and hidden layers.

Fig. 17 represents the performance of the proposed SATIDS system when facing XSS attack. As shown, the network has its highest

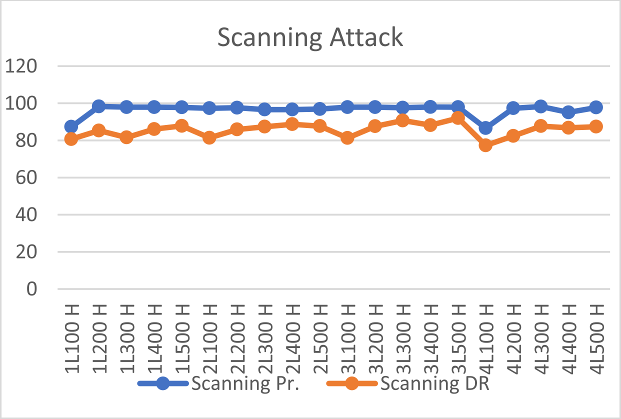


Fig. 16. Detecting Scanning Attack.

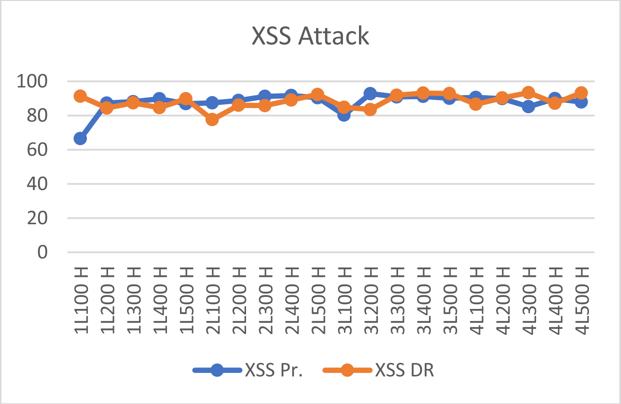


Fig. 17. Detecting XSS Attack.

performance when using 3 LSTM layers and 400 hidden layers: 91.2 % precision and 93.1 % detection rate. From Table 5 and Figs. 9–17, it is clear that using 3 LSTM layers and 500 hidden layers achieves the highest accuracy, precision and detection rate.

5.1.2. INSDN dataset

– *Binary Classification (normal/anomaly)*

Table 6 presents the system intrusion detection performance at different numbers of hidden layers (H) and LSTM layers. As shown in Fig. 18, in case of 500 hidden layers and 4 LSTM layers the network has its highest accuracy of 99.51 %, the highest RoC of 99.73 %, the lowest FAR of 0.3, and the highest precision and detection rate of 98.9 % and 98.6 % respectively. So, 4 layers LSTM and 500 hidden layers was selected in the proposed system as it has the best performance in case of binary classification.

– *Multi-attack classification*

Table 7 presents the output of our proposed SATIDS system when using InSDN database in case of identifying the type of attack. In this table, the number of LSTM layer and the number of hidden layers in LSTM layer are changed and the precision and detection rate for each attack at each time are recorded. Fig. 19 shows the performance of proposed SATIDS system when facing BFA attack. The network has its highest performance when using

Table 5
Performance Analysis of the proposed system using ToN-IoT Database.

# LSTM	# Hidden layer	Acc.	Backdoor		DDOS		DOS		Injection		Password		Ransomware		Scanning		XSS	
			Pr.	DR	Pr.	DR	Pr.	DR	Pr.	DR	Pr.	DR	Pr.	DR	Pr.	DR	Pr.	DR
1	100	78.66	95.8	50.8	52.3	75.4	99.6	92.5	92.1	82.4	82.5	74.1	81.3	85.8	87.3	80.7	66.5	91.3
1	200	90.42	93	99.3	76.5	89.6	99.9	92.5	86.9	86.9	89	92.6	96.6	96.9	98.3	85.3	87.3	84.4
1	300	91.24	95	99.3	78.5	90.8	99.7	92.5	92.9	88.3	90.3	96.4	91.5	97.5	97.9	81.6	88.1	87.4
1	400	91.48	92.9	99.3	77	92.4	98.6	93.3	93.1	88.5	92.2	94.2	94.7	97.1	97.9	86.1	89.8	84.6
1	500	91.91	93.5	99.3	82.4	89.3	99.5	92.1	90.7	89	90.5	94.6	96.5	97	97.8	87.8	86.9	89.8
2	100	88.8	94.6	99.2	71.8	90.9	99.9	92	87.1	86.2	87.2	89.9	91.6	97	97.3	81.4	87.4	77.6
2	200	90.68	94.4	99.9	76.3	92.2	99.9	92.2	88.7	84.3	89.3	90.8	95.1	97.8	97.6	85.9	88.8	86
2	300	92.04	94.9	99.9	79.1	93.3	98.8	94.2	93.8	87.4	90	95.5	95.8	96.2	96.6	87.4	91.2	85.8
2	400	92.78	95.1	99.9	84.6	92.2	98.5	95	93.7	86.5	89.3	95.8	95.7	97.6	96.6	88.7	91.7	89.1
2	500	94.24	94.8	99.9	89.9	91.5	99	96.4	94.2	93.5	97	96.4	94.9	97.8	96.9	87.7	90.4	92.3
3	100	87.84	79.3	99.4	74.7	92.1	99.6	92	93.1	87.5	95.4	74.1	92.9	95.4	97.9	81.3	80.3	84.8
3	200	91.70	93.5	99.9	76.2	92.5	99.9	92	89.2	87.5	93.4	96.4	95.7	97.9	97.9	87.6	92.8	83.5
3	300	93.92	95.2	99.9	92.3	88.8	97.8	97.2	89.5	93.5	94.7	93.7	96.4	93.7	97.6	90.7	90.9	91.9
3	400	94.42	93.9	99.9	91.4	91.4	97.5	97.5	94.8	92.7	95	97	96.4	97.5	98	88.2	91.2	93.1
3	500	94.75	94.5	99.9	92.4	92.4	98.9	97	95.2	91.1	94.3	97.4	97.6	97.2	97.9	92	90.1	92.9
4	100	80.63	89.9	99.4	59.6	81.9	99.1	92.3	68.6	81.2	75.8	45.6	84.3	85.1	86.6	77.3	90.6	86.6
4	200	92.25	92	99.9	80.9	91.2	99.8	92.2	93.4	91.7	95.5	97	92.4	97.2	97.3	82.4	89.9	90.3
4	300	93.52	95.7	99.9	88.4	89.4	99.3	96.2	92.7	91.8	95.5	95.2	96.2	97.4	98.2	87.7	85.2	93.4
4	400	92.14	94.4	98.9	82.7	91	99.8	92.3	93.5	92.3	91	95.2	94.7	95.4	95.1	86.8	89.9	87.2
4	500	94.16	94.9	99.9	91.6	90.7	98.7	96.9	93.7	93.2	95.4	97.3	97.4	96.3	97.7	87.4	87.9	93.2

Table 6
Performance analysis of the proposed system using InSDN Dataset.

# LSTM	# Hidden layer	ACC.	ROC	FAR	Precision	F1-Score	Detection Rate
1	100	97.97	99	1	95.9	94.84	93.8
1	200	98.32	99.2	0.8	96.7	95.74	94.8
1	300	98.59	99.24	0.8	96.9	96.45	96
1	400	98.41	99.05	1	96.2	96	95.8
1	500	98.46	99.12	0.9	96.4	96.1	95.8
2	100	98.8	99.40	0.6	97.5	96.89	96.3
2	200	99.06	99.33	0.7	97.3	97.65	98
2	300	99.25	99.55	0.4	98.2	98.15	98.1
2	400	99.26	99.49	0.5	97.9	98.15	98.4
2	500	99.20	99.42	0.6	97.7	98	98.3
3	100	98.65	99.14	0.9	96.5	96.6	96.7
3	200	99.23	99.62	0.4	98.4	98.05	97.7
3	300	99.26	99.48	0.5	97.9	98.15	98.4
3	400	99.34	99.69	0.3	98.7	98.35	98
3	500	99.39	99.64	0.4	98.5	98.45	98.4
4	100	98.81	99.45	0.6	97.7	96.94	96.2
4	200	99.31	99.00	0.5	98.2	98.3	98.4
4	300	99.31	99.42	0.6	97.7	98.3	98.9
4	400	99.39	99.56	0.4	98.2	98.45	98.7
4	500	99.51	99.73	0.3	98.9	98.75	98.6

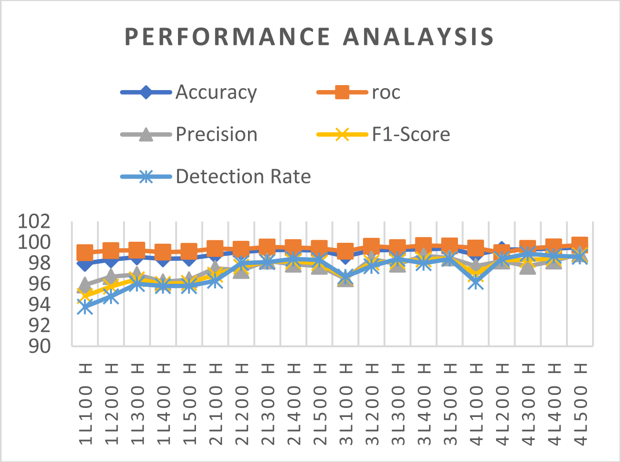


Fig. 18. Performance ANALYSIS OF the proposed system using InSDN DataSET.

4 LSTM layers and 300 hidden layers with 85.6 % precision and 59.1 % detection rate. Figs. 20 and 21 show the performance of proposed SATIDS system when facing BOTNET attack and DDOS attack respectively. As shown, the network has its highest performance when using 1 LSTM layer and 500 hidden layers for BOTNET attack and 3 LSTM layers and 500 hidden layers for DDOS attack.

For DOS attack, the performance of proposed SATIDS system is shown in Fig. 22, the network has its highest performance when using 4 LSTM layers and 400 hidden layers with 98.5 % precision and 99.1 % detection rate. Fig. 23 presents the performance of proposed SATIDS system when detecting Probe attack. As shown, the system has its highest performance when using 4 LSTM layers and 300 hidden layers with 98.8 % precision and 98.8 % detection rate. As for detecting Web-attack, the performance of proposed SATIDS system is shown in Fig. 24, the system has its highest performance when using 1 LSTM layers and 300 hidden layers with 77.8 % precision and 24.6 % detection rate.

From Table 7 and Figs. 19–24, it is obvious that using 4 LSTM layers (L) with 400 hidden layers (H) achieved the highest accuracy, precision and detection rate in multi classification experiment.

5.2. Performance comparison

- TON-IOT DATASET

Table 8 and Fig. 25 show a performance comparison among the proposed SATIDS system and other approaches when using ToN-IoT dataset. The proposed system outperforms others with precision of 97.3 %, and F1-score of 97.35 %. As for the Detection rate, techniques presented in [2] as E-ADS, SAE-IDS and Ensemble learning recorded higher DR than the proposed SATIDS.

Table 9 and Fig. 26 illustrate the comparison of performance while utilizing the feature selection technique. Minimum Redundancy Maximum Relevance (MRMR) approach was utilized with the proposed SATIDS to select 20 features out of the 43 features in ToN-IoT dataset. SP2F [17] extracted the 20 most essential features using a mutual information-based methodology. The TP2SF architecture proposed in [1] adopts the most fundamental statistical method based on the Pearson correlation coefficient (PCC). In terms of Accuracy, F1-score, precision, and detection rate, the proposed MRMR-SATIDS outperforms TP2SF [1]. In terms of f1-score and detection rate, the proposed system outperformed SP2F [17] as well. However, SP2F [17] is 0.76 % more accurate than MRMR-SATIDS.

- INSDN DATASET

Table 10 and Fig. 27 compare the performance of the proposed SATIDS system to other IDSs in case of using InSDN database. It is clear that the proposed system outperforms others with 98.4 % detection rate, 99.39 % accuracy, 99.64 % area under curve of

Table 7
Performance Analysis of the proposed system using InSDN Database.

# LSTM	# Hidden layer	Acc.	BFA		BOTNET		DDOS		DOS		Probe		U2R		Web-Attack	
			Pr.	DR	Pr.	DR	Pr.	DR	Pr.	DR	Pr.	DR	Pr.	DR	Pr.	DR
1	100	93.34	88.2	39	-	0	90	99.4	97.5	95.2	96.1	86	-	0	-	0
1	200	94	94.5	45.1	95.2	40	90	99.8	98	97.2	97.8	86	-	0	77.8	12.3
1	300	93.76	75.7	54.9	100	44	90	99.9	98.2	95.6	97.1	85.9	-	0	77.8	24.6
1	400	93.75	93.9	54.6	87.5	42	90	99.9	98	95.8	97	85.8	-	0	77.8	12.3
1	500	93.83	90.5	58.7	100	46	90	99.9	98.3	95.9	97.1	86	-	0	77.8	12.3
2	100	94.01	89.3	53.7	93.8	30	90	99.9	98.4	97	97.6	86	-	0	-	0
2	200	94.16	87.4	59.1	71.4	40	90	99.8	98.4	97.8	98.2	86	-	0	-	0
2	300	94.23	88.1	58	100	44	90	99.9	98.3	98	98.4	85.9	-	0	100	1.8
2	400	93.93	88.8	58.7	100	46	90	99.9	98.5	96.2	97.3	86.1	-	0	71.4	8.8
2	500	94.33	92.3	56.8	56.2	100	90	99.9	98.7	98.1	98.6	86.1	-	0	80	14
3	100	93.69	90.6	48	-	0	90	99.9	97.9	95.6	96.9	86	-	0	-	0
3	200	94.22	89.5	54.9	100	40	90	99.9	98.5	97.7	98.2	86.1	-	0	-	1.8
3	300	94.25	90.3	57.7	100	42	90	99.9	98.2	98.1	98.4	86	-	0	-	0
3	400	94.37	91.1	58.7	96	48	90	99.9	98.5	98.4	98.7	86.1	-	0	-	0
3	500	94.45	86.5	65.3	100	48	90.3	99.9	98.8	97.9	98.4	86.5	-	0	-	1.7
4	100	94.29	89.9	42.5	-	0	90.3	99.9	97.6	98.2	98.5	86.3	-	0	-	0
4	200	94.38	83.1	56.1	-	0	90.3	99.9	98.5	97.9	98.3	86.5	-	0	-	0
4	300	94.48	85.6	59.1	-	0	90.3	99.9	98.3	98.6	98.8	98.8	-	0	-	0
4	400	94.49	88.7	57.7	100	40	90	99.9	98.5	99.1	99.1	86.1	-	0	-	0
4	500	94.28	86.9	63.2	88.5	46	90	99.9	98.7	97.8	98.3	86.1	-	0	100	1.8

LSTM layer and 500 hidden layers for BOTNET attack and 3 LSTM layers and 500 hidden layers for DDOS attack.

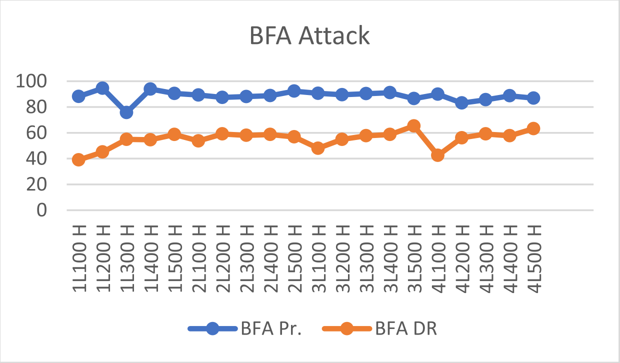


Fig. 19. Detecting BFA Attack.

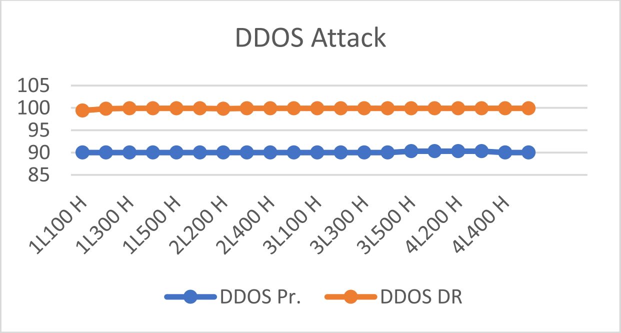


Fig. 21. Detecting DDOS Attack.

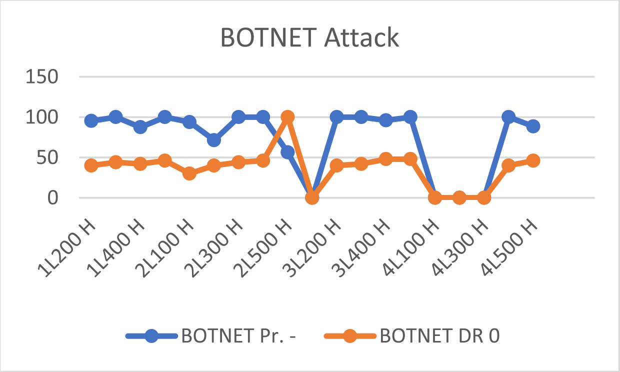


Fig. 20. Detecting BOTNET Attack.

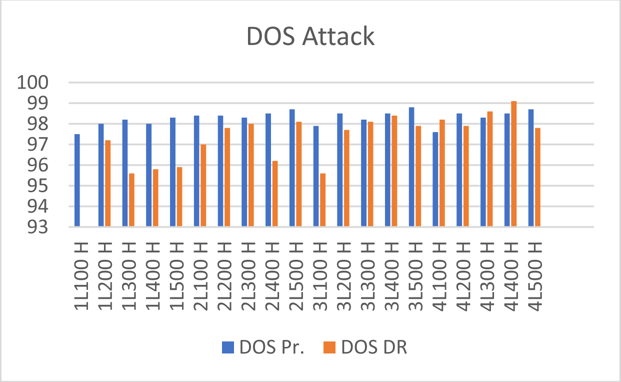


Fig. 22. Detecting DOS Attack.

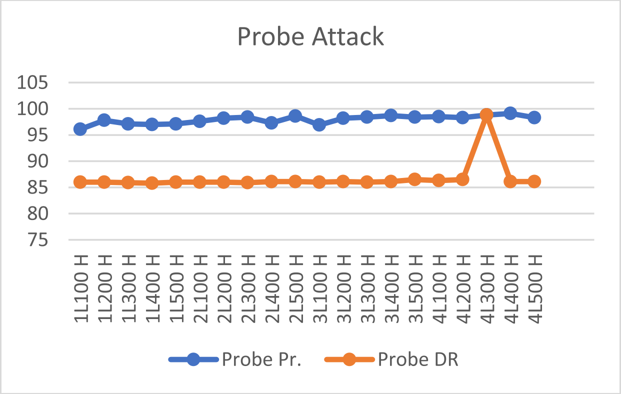


Fig. 23. Detecting Probe Attack.

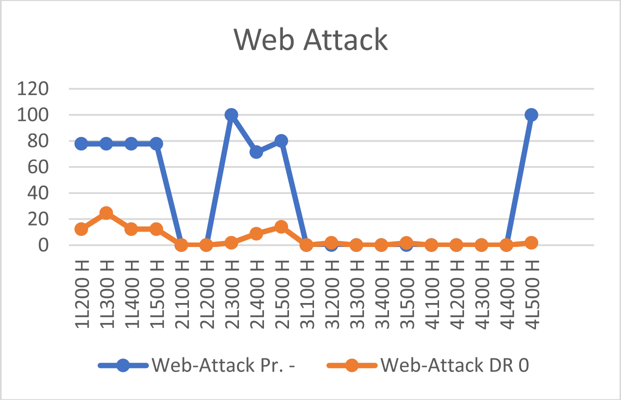


Fig. 24. Detecting Web-Attack.

Table 8
Performance comparison using ToN-IoT Database.

Technique	Performance Metrics			
	Accuracy	Precision	F1-Score	Detection Rate
Ensemble Learning [2]	96.352	90.545	95.03	99.983
SVM-IDS [2]	82.212	65.121	78.812	74.744
Health Guard [2]	88.677	60.983	83.542	82.299
SAE-IDS [2]	83.15	67.571	80.485	99.5
E-ADS [2]	96.353	90.545	95.03	99.983
Random Forest(RF) [2]	93.944	86.866	91.811	97.327
Decision Tree(DT)[1]	95.34	74.42	76.33	80
Naïve Bayes(NB) [1]	90.62	77.68	72.43	77.7
Proposed SATIDS	96.56	97.3	97.35	97.4

ROC, and 0.9845 F1-score. It has almost equal precision to CNN Model [10] with a little bit difference.

6. Conclusion and future work

Internet of Things is a powerful platform for combining users worldwide without human interference. It connects everything to the Internet via data sensing devices. Although SDN technology enhances IoT security, IoT applications still face potential security threats that needed to be reduced. This paper proposes a Secured Automatic Two-level Intrusion Detection System (SATIDS) based on improved Long Short-Term Memory (LSTM) network to differentiate between attack and benign traffic, identifies the attack category, and defines the type of sub-attack with high-performance. The proposed technique is trained and assessed using two of the latest realistic IoT datasets; ToN-IoT and InSDN. To demonstrate the

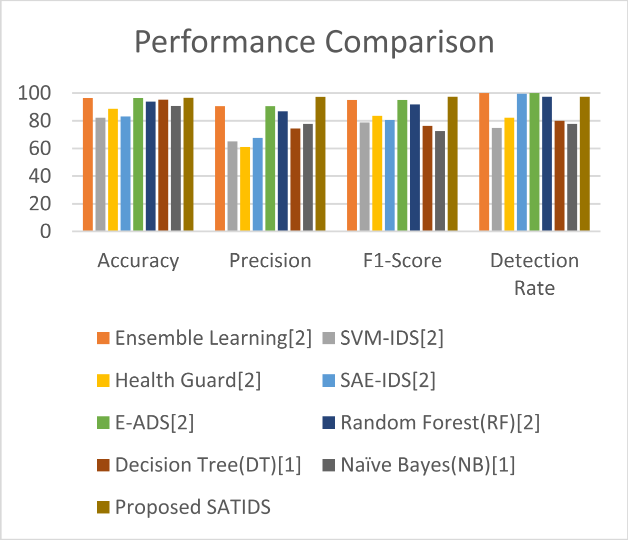


Fig. 25. Performance comparison using ToN-IoT Dataset.

Table 9
Performance comparison USING 20 features of ToN-IoT Database.

Technique	Performance Metrics			
	Accuracy	Precision	F1-Score	Detection Rate
SP2F [17]	99.64	99.94	98.87	98.88
Tp2sf (with original) [1]	97.45	96.95	94.43	92.43
TP2SF (with transform) [1]	98.84	97.23	95.28	94.03
Proposed MRMR-SATIDS	98.8	99.3	99.05	98.8

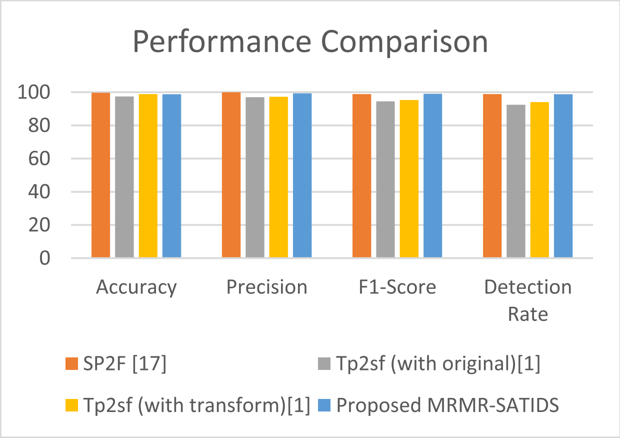


Fig. 26. Performance comparison using 20features of ToN-IoT Dataset.

Table 10
Performance comparison USING InSDN Database.

Technique	Performance Metrics				
	Accuracy	Detection Rate	Precision	F1-Score	ROC
OC-SVM [9]	87.5	93	89	91	–
LSTM Autoencoder-OC-SVM [9]	90.5	93	93	93	90.6
CNN Model [10]	93.01	86.71	98.67	93.59	92.8
Proposed SATIDS	99.39	98.4	98.5	98.45	99.64

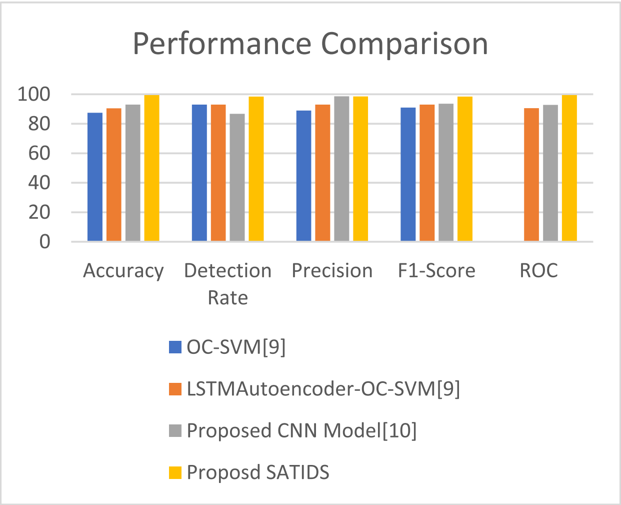


Fig. 27. Performance comparison using InSDN Dataset.

efficiency of the suggested system, its performance has been studied and compared with other IDSs. Results reveal that the suggested IDS system outperforms other IDSs with 96.35 % accuracy, 96 % detection rate, and 98.4 % precision for ToN-IoT dataset and 99.73 % accuracy, 98.6 % detection rate, and 98.9 % precision for InSDN dataset. Our future research will focus on refining the model of the proposed system by exploiting feature selection, detect zero-day attacks on IoT systems, and apply the proposed system to real-world Internet of Things networks composed of mobile devices.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Kumar P, Govind PG, Rakesh T. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. J Syst Archit 2021;115:101954.

[2] Kumar P, Prabhat GP, Gupta R. Tripathi, An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. Comput Commun 2021;166:110–24.

[3] Ashfaq Z, Rafay A, Mumtaz R, Zaidi SMH, Saleem H, Zaidi SAR, et al. A review of enabling technologies for internet of medical things (IOMT) ecosystem. Ain Shams Eng J 2022;13(4):101660.

[4] Slama SB. Prosumer in smart grids based on intelligent edge computing: a review on Artificial Intelligence Scheduling Techniques. Ain Shams Eng J 2021.

[5] Roopak M, Tian GY, Chambers J. Deep learning models for cyber security in IoT networks. In: 2019 IEEE 9th annual computing and communication workshop and conference (CCWC). p. 0452–7.

[6] Doukas C. Building Internet of Things with the ARDUINO. CreateSpace Independent Publishing Platform; 2012.

[7] da Costa KA, Papa JP, Lisboa CO, Munoz R, de Albuquerque VHC. Internet of Things: a survey on machine learning-based intrusion detection approaches. Comput Netw 2019;151:147–57.

[8] Singh S, Sharma PK, Moon SY, Moon D, Park JH. A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions. J Supercomput 2019;75(8):4543–74.

[9] Said Elsayed M, Le-Khac NA, Dev S, Jurcut AD. Network anomaly detection using LSTM based autoencoder. In: Proceedings of the 16th ACM symposium on QoS and security for wireless and mobile networks. p. 37–45.

[10] Elsayed M, Jahromi H, Nazir M, Jurcut A. The role of CNN for intrusion detection systems: an improved CNN learning approach for SDNs. In: 2020 16th IEEE international colloquium on signal processing & its applications (CSPA). IEEE; 2020. p. 29–34.

[11] Atefi K, Hashim H, Khodadadi T. A hybrid anomaly classification with deep learning (DL) and binary algorithms (BA) as optimizer in the intrusion detection system (IDS). In: Proceedings of the 16th IEEE international colloquium on signal processing & its applications (CSPA). IEEE; 2020. p. 29–34.

[12] Prasad M, Tripathi S, Dahal K. Unsupervised feature selection and cluster center initialization based arbitrary shaped clusters for intrusion detection. Comput Secur 2020;99:102062.

[13] Sabeel U, Heydari SS, Mohanka H, Bendhaou Y, Elgazzar K, El-Khatib K. Evaluation of deep learning in detecting unknown network attacks. In: Proceedings of international conference on smart applications, communications and networking (SmartNets). IEEE; 2019. p. 1–6.

[14] Zhang H, Huang L, Wu CQ, Li Z. An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset. Comput Netw 2020;177:107315.

[15] Kshirsagar D, Kumar S. An ensemble feature reduction method for web-attack detection. J Discret Math Sci Cryptogr 2020;23(1):283–91.

[16] Vinayakumar R, Alazab M, Soman K, Poornachandran P, Al-Nemrat A, Venkatraman S. Deep learning approach for intelligent intrusion detection system. IEEE Access 2019;7:41525–50.

[17] Kumar R, Kumar P, Tripathi R, Gupta GP, Gadekallu TR, Srivastava G. SP2F: a privacy-preserving framework for smart agricultural Unmanned Aerial Vehicles. Comput Netw 2021:107819.

[18] Keshk M, Turnbull B, Moustafa N, Vatsalan D, Choo K-K-R. A privacy-preserving-framework-based blockchain and deep learning for protecting smart power networks. IEEE Trans Ind Inf 2019;16(8):5110–8.

[19] Haider W, Moustafa N, Keshk M, Fernandez A, Choo K-K-R, Wahab A. FGMCHADS: Fuzzy Gaussian mixture-based correntropy models for detecting zero-day attacks from linux systems. Comput Secur 2020:101906.

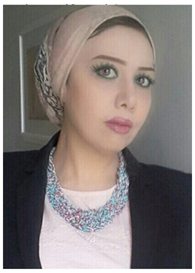
[20] Moustafa N. ToN_IoT datasets. IEEE Dataport; 2019. Online; Accessed 10-Feb-2020. doi: 10.21227/fesz-dm97.

[21] Elsayed MS, Le-Khac NA, Jurcut AD. InSDN: a novel SDN intrusion dataset. IEEE Access 2020;8:165263–84.

Rania A. Elsayed received the M.Sc. degree in electronics and communications engineering from the University of Zagazig, Egypt in 2009. She received her PhD in Electrical and Computer Engineering from the University of Zagazig in 2018. She is currently a doctor with the Department of Electronics and Communications Engineering, Faculty of Engineering, Zagazig University, Egypt.

Reem Alaa Hamada is an Teachnig Assistant at Electronics and Communications Dep., Faculty of Engineering, Zagazig University, Egypt She has received the BSc (2010) and MSc (2011) in Network Communication from the Faculty of Engineering, Zagazig University (Egypt). Her current research interests include Cyber security, Internet of things (IoT), Network Communication, Medical Imaging, and Soft Computing. She is author many research papers published at international journals, and conference proceedings.

M. I. Abdalla is a full professor in the Electronics and Communication Department, Faculty of Engineering, Zagazig University. He received his BSc degree from University of Mansoura, Egypt in 1979, and also the Master of Science degree from the same university in 1984. He received his PhD degree from Zagazig University, Egypt in 1989. He worked as a lecturer in Saudi Arabia from 1990 to 1993. He worked in a Postdoctoral research in University of Connecticut, USA in 1996. His research interests are Wireless communication, Signal processing, Image processing and Pattern Recognition. He has supervised different master and PhD theses. He has published many research papers in international conferences and journals.



Dr. Shaimaa Elsaid is an Associate Professor at Electronics and Communications Dep., Faculty of Engineering, Zagazig University, Egypt. She has received the MSc (2006) in Networks Security and PhD (2011) in Multimedia Security from the Faculty of Engineering, Zagazig University (Egypt). Her current research interests include Cyber security, Internet of things (IoT), Digital Image Processing, Medical Imaging, and Soft Computing. She is author of 2 books and many research papers published at international journals, and conference proceedings. Also, she has supervised many graduation projects, Master, and PhD theses.