scientific reports

Check for updates

OPEN

Machine learning based intrusion detection framework for detecting security attacks in internet of things

V. Kantharaju[1], H. Suresh[2], M. Niranjanamurthy[1], Syed Immamul Ansarullah[3], Farhan Amin[4]✉ & Amerah Alabrah[5]✉

The Internet of Things (IoT) consist of a network of interconnected nodes constantly communicating, exchanging, and transferring data over various network protocols. Intrusion detection systems using deep learning are a common method used for providing security in IoT. However, traditional deep learning IDS systems do not accurately classify the attack and also require high computation time. Thus, to solve this issue, herein, we propose an advance Intrusion detection framework using Self-Attention Progressive Generative Adversarial Network (SAPGAN) framework for detecting security threats in IoT networks. In our proposed framework, at first, the IoT data are gathered. Then, the data are fed to pre-processing. In pre-processing, it restored the missing value using Local least squares. Then the preprocessing output is fed to feature selection. At feature selection, the optimum features are compiled using a modified War Strategy Optimization Algorithm (WSOA). Based upon the optimum features, the intruders were categorized into two categories named Anomaly and Normal using the proposed framework. Numerous attacks are assembled, including camera-based flood, DDoS, RTSP brute force, etc. We have compared our proposed framework using state of the art model and efficiency of 23.19%, 27.55%, and 18.35% higher accuracy and 14.46%, 26.76%, and 13.65% lower computational time compared to traditional models.

Keywords Intrusion detection, Internet of things, Data acquisition, Security, WSOA

Internet of Things (IoT) provides a connectivity of physical moving things known as "Things" that are equipped with sensors, electronic chips, and other types of technology[1]. Machine learning improves Intrusion Detection System (IDS) systems by enhancing threat detection, reducing false positives, and adapting to evolving threats, which are distributed among Internet of things(IoT), devices, edge nodes, and cloud nodes. For device connection, different protocols used for providing protection susceptibility, can brunt the entire scheme in IoT systems[2]. For purchaser usage, the Internet of Things is a combination of cloud-connected embedded systems to entrance IT-relevant services by the consolidation of electronics-related things and internet protocol[3]. Due to its scarcity of elementary defense protocols, IoT devices are unprotected targets for cybercriminals and attackers[4,5]. That alludes, to IoT being hacked by botnets used to launch DDoS against entities[6]. To overcome these problems, an Intrusion Detection System (IDS) is a suitable solution. In general, the IDS consents sleuthing apprehensive or anomalous happenings which activates an alarm when an interruption transpires[7]. The enactment of IDSs for IoT is more problematic than other schemes as IoT devices are habitually premeditated to be minuscule and economical, and it does not have sufficient hardware possessions[8]. The traditional models for instance;[11–13] do not provide sufficient accuracy and it increases the computation time. To overcome this problem, Here we propose a machine learning-based intrusion detection framework that facilitates to recognition of different types of intruders[9]. At first, the IoT data are gathered via the dataset of Bot-IoT[10]. Afterward, the data are fed to pre-processing. In pre-processing, it restored the missing value utilizing the local least squares method. The preprocessing output is fed to feature selection. Here, optimum features are selected based on the War Strategy

[1]Deparment of AI&ML, BMS Institute of Technology and Management (Affiliated to Visvesvaraya Technological University, Belagavi), Bengaluru, India. [2]Department of ISE, KNS Institute of Technology, Bengaluru 560064, India. [3]Department of Management studies, University of Kashmir, North campus, Delina, India. [4]School of Computer Science and Engineering, Yeungnam University, Gyeongsan 38541, Korea. [5]Department of Information Systems, College of Computer and Information Science, King Saud University, 11543 Riyadh, Saudi Arabia. ✉email: farhanamin10@hotmail.com; aalobrah@ksu.edu.sa

Optimization Algorithm. Based on the optimum features, the intruders of IoT data are categorized into normal and anomalous data with the help of SAPGAN. The proposed SAPGAN-IDS-IoT approach is implemented in Python utilizing the dataset of Bot-IoT. The performance metrics, like accuracy, F1-score, RoC, and computational time are examined to validate the proposed efficiency. The obtained results of the proposed SAPGAN-IDS-IoT approach are analyzed with existing systems, like Design and development of a deep learning-based method for anomaly identification in IoT networks (CNN-IDS-IoT)[11]; intrusion detection scheme for IoT botnet attacks utilizing deep learning (DNN-IDS-IoT)[12] and Chronological Salp swarm algorithm based deep belief network for intrusion detection in cloud under fuzzy entropy (DBN-CSSA-IDS-IoT)[13] respectively. Industrial IoT networks lack protection against cyber threats, necessitating the development of Intrusion Detection Systems. Three models, using CNN, LSTM, and a hybrid combination, detect intrusions in IIoT networks.[25], in this article author presents a hybrid intrusion detection system utilizing a combination of CNN and LSTM for industrial IoT networks. Author introduces an autoencoder-based intrusion detection system model for detecting security anomalies in critical infrastructures, demonstrating its accuracy in attack detection using the UNSW-NB15 dataset.[26], here we proposed WSOA, Based upon the optimum features, the intruders were categorized into two categories named Anomaly and Normal using the proposed framework.

The key contributions of this manuscript are given briefly:

Herein, we propose a machine learning-based Intrusion detection framework named SAPGAN for Identifying intruders in IoT network. our proposed model classify the network traffic to normal or abnormal. Numerous attacks are assembled, including camera-based flood, DDoS, RTSP brute force, etc. Applying feature selection methods to improve the IDS performance of IoT network devices. Hence, we examined multiple ML algorithms to determine the most accurate and efficient learners for building an efficient IDS to detect attacks on IoT devices within IoT network data.

Herein, we design a framework that receive raw and preprocess data using local least square method. The key features were extracted in feature selection phase. A modified WSOA is applied. Finally the intruders were extracted. We have launched different attacks and found that proposed model is efficient.

We evaluated four supervised models using data preprocessing and feature selection methods. The performance evaluation includes accuracy, precision, recall, and F1-score metrics.

The remaining manuscript is arranged as Segment 2 analyses the literature survey, the proposed method is described in Segment 3, the outcomes and discussion are demonstrated in Segment 4, and the conclusion is presented in Segment 5.

Literature survey

Numerous research works were suggested in the literature related to deep learning-based intrusion detection in IoT; a few recent works are expressed here, In 2021, Ullah, I.et.al.,[11] suggested the design and development of a deep learning-based method for anomaly identification in Internet of Things networks. Here, the BoT-IoT dataset was taken and it was given to the pre-processing segment for retrieving the missing value. Then the pre-processed output was given a Recursive Feature Elimination (RFE)feature selection system. In which, the optimal features were selected. Then Convolutional Neural Network (CNN) classifier was utilized as IDS for detecting intruders in the IoT network. It provides high accuracy and low F-score. In 2021, Shareena, J.et.al.,[12] presented an intrusion detection scheme for IoT botnet attacks with the help of deep learning. Here, the BoT-IoT dataset was taken and it was given to the pre-processing segment for retrieving the missing value. Then the pre-processed output was given to a Deep Neural Network (DNN)) classifier, which was utilized as IDS for detecting intruders in IoT networks. It provides a high F-score with low computation time. In 2022, Karuppusamy, L.et. al.,[13] presented a Chronological salp swarm approach based deep belief network (CSSA-DBN) for intrusion detection in the cloud utilizing fuzzy entropy. Here, the BoT-IoT dataset was taken and it was given to the pre-processing segment for retrieving the missing value. Then the pre-processed output was given to the Fuzzy entropy feature selection system. In which, the optimal features were selected. Then the CSSA-DBN classifier was utilized as IDS for detecting intruders in the IoT network. It provides a high Area under curve value and low accuracy.

Table 1 discuss the existing methods for classifying IoT attacks. The literature primarily explores potential solutions based on IoT standards, technologies, architecture types, security threats, machine learning approaches, datasets, and implementation tools. Support Vector Machine (SVM) is a machine learning technique used to detect network intrusions and cyber-attacks, offering a second line of defense and alternative detection methods. Analytical study on support vector machine (SVM)-based intrusion detection techniques, involving data collection, preprocessing, training and testing, and decision-making steps in network intrusion detection systems.[17] The increasing frequency of network attacks necessitates the development of intrusion detection systems (IDS) to actively detect intrusions and attacks in networks or intranets, which can be classified as known or unknown.[18]. IDS is distributed among IoT devices, edge nodes, and cloud nodes, using lightweight detectors, Smart Data concepts, and cloud clustering. ML models detect unusual IoT activity, preventing security breaches and prompting appropriate responses.

Proposed methodology

The proposed SAPGAN-IDS-IoT framework is shown in Fig. 1. The proposed SAPGAN-IDS-IoT workflow is dived into steps. The expliantion details are given as below.

Research paper	Year	Methodology	Results	Limitations
J.P. Sheu, Y.C. Kuo et al.,[19]	2020	Decision tree	Correctness = 99.98, exactness = 97.38, recollection = 97.39, F1 = 99.98	The models require a significant amount of time to be trained
J. Zhong, C.X. Ye, Z.F. Wu et. al.[20]	2016	Self-organized ant colony networks	Correctness = 99.79 for DoS attack and accurateness = 98.55 for Probe attack	The dataset used does not accurately represent current attacks
N. Chilamkurti. Diro[21]	2017	DNN and shallow NN models	Narrow NN = 96.75% accurateness; DNN = 98.27% exactness	The NSLKDD dataset was utilized, which does not accurately represent current attacks
M. Choraś, M. Ficco et al.,[22]	2018	ELM	83% accurateness	More exercise time
L. Williams, P. Burnap et al.,[23]	2018	NB	Recollection = 97.7% Exactness = 97.7% and F-measure = 97.7%	The dataset generated does not accurately represent network behavior in a diverse environment
R. Javidan, R. Khayami et al.,[24]	2019	LDA for dimensionality reduction with NB and CF-KNN for classification of network traffic	Accurateness = 84.82% and untrue fright rate = 5.56	The detection accuracy is low, but the FP rate is high

Table 1. State of art methods for classifying IoT attacks.

Data acquisition

In this step, at first the BoT-IoT dataset is considered. This dataset is developed through a realistic IoT network environment together with 5IoT scenarios: weather station, smart fridge, smart thermostat, remotely activated, motion-activated lights. The environment incorporates is normal with botnet traffic. The dataset contains 3,668,522 samples, which comprise kinds of attacks: DDoS (HTTP, TCP, and UDP), DoS (HTTP, TCP, and UDP), OS, Service Scan, Keylogging, Data exfiltration, and normal data.

Pre-processing phase

In this section, local least squares espoused pre-processing is described. Here missing value renewal is gawked as an imperious trepidation in the BoT-IoT dataset[14]. It uses P similarity records and then it employs regression and estimation of how the P records are selected. By this, the missing value can be restored using Pearson correlation coefficients. Then, the pre-processed IoT data is fed as input for feature selection.

Feature selection

This is used to categorize and eradicate extraneous and superfluous traits as innovative feature vectors that do not contain considerable influence to augment the efficiency of an intrusion detection system. Reducing overfitting and training periods, also improving detection accuracy are the main objectives of the War Strategy Optimization Algorithm.

Figure 1 shows the proposed framework SAPGAN-IDS-IoT approach, It contains the training phase, the training phase contains data acquisition, pre-processing and feature selection method, and is connected with Intrusion detection system using self-attention based progressive generative adversarial network ant accept the testing data. The data mining and analysis tool 'Weka' is utilized as the primary tool for simulation. Weka provides a comprehensive environment for performing data analysis and ML tasks.

War Strategy Optimization Algorithm (WSOA) is a metaheuristic optimization algorithm in terms of ancient war strategy[15]. Fitness functions describe how close an architecture is to achieving an architectural aim. whale optimization with seagull algorithm (WSOA), for solving global optimization problems. Initially, the features of the BoT-IoT dataset are initialized with soldier size as 25 and maximum iteration as 500. After the initialization process, the input features of the BoT-IoT dataset are randomly created through the WSOA Algorithm. Then the Fitness function is assessed based on the following Eq. (1)

$$Fitness\ Function = Selecting\ \ optimal\ features\ of\ \text{BoT - IoT dataset} \tag{1}$$

Then select the King with the preeminent fitness and the Chief Commander with the second-best fitness. Subsequently, choosing the king and chief commander, check the iteration reached as maximum i.e., selecting the optimal features, if it reached means the process is terminated otherwise go to the next step of soldier size checking. If the soldiers' size is gratify means going to the next step of updation. The situation of soldier size is contented means and then updates the king and commander position. If it does not satisfy the condition then goes to exploitation and investigation. The exploitation phase is assessed based on the following Eq. (2)

$$z_n(x+1) = z_n(x) + 2 \times \alpha \times (AC - king) + Rdm \times (Wt_n \times king - z_n(x)) \tag{2}$$

where $z_n(x+1)$ is the new position, $z_n(x)$ is the preceding location of Army chief, $king$ represents the position of the king, Wt_n denotes weight and value is $Wt_n = 2 \times ones\,(1,\ soldiersize)$, the value of α is 0.5. Then the investigation phase is assessed based on the following Eq. (3)

$$z_n(x+1) = z_n(x) + 2 \times \alpha \times (king - x_{rdm}(x)) + Rdm \times (Wt_n \times (AC - z_n(x))) \tag{3}$$

After updation, check the fitness of each soldier based on Eq. (4), if the fitness is better than the previous one then update the weight factor based on Eq. (6), otherwise it goes to check the size of the soldier based on Eq. (5), up to best fitness found, steps are repeated.

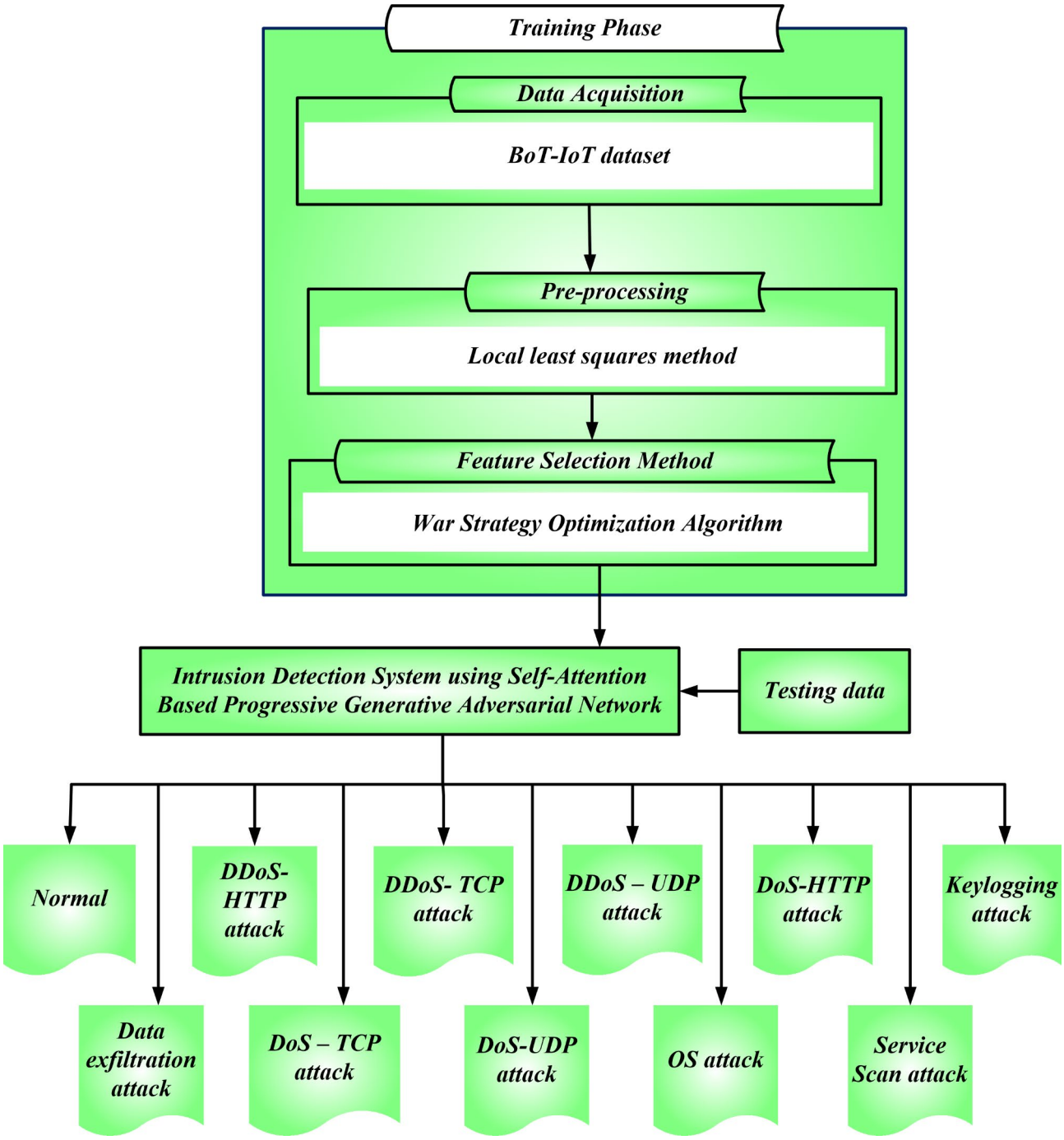

Fig. 1. Proposed framework.

$$z_n\left(x+1\right) = \left(z_n\left(x+1\right)\right) \times \left(N_{PS} \geq P_{PS}\right) + \left(z_n\left(x\right)\right) \times \left(N_{PS} < P_{PS}\right) \tag{4}$$

where N_{PS} depicts the new position of a soldier and P_{PS} depicts the previous position of a soldier. If a soldier updates successfully the position, then soldier ranks are accessed based on the following Eq. (5),

$$Rank_n = \left(Rank_n + 1\right) \times \left(N_{PS} \geq P_{PS}\right) + \left(Rank_n\right) \times \left(N_{PS} < P_{PS}\right) \tag{5}$$

where, $Rank_n$ represents the soldier's rank. By this, new weight can be determined based on the following Eq. (6)

$$Wt_n = Wt_n \times \left(1 - \frac{Rank_n}{Max\ Itrn}\right)^{\rho} \tag{6}$$

Then the replacement of weak soldier is accessed based on the following Eq. (7)

$$z_{weak}(x+1) = lb + Rdm \times (ub - lb) \tag{7}$$

The weak soldiers are replaced with new ones and the iteration is. By this, the optimal feature is selected depending on the Hybrid WSOA Algorithm iteratively repeats until fulfill $Max\ Itrn = Max\ Itrn + 1$ halting criteria. Then, the selected features are given as the input for the intrusion detection system. If all the processes are achieved it will select the accurate feature for attaining better intrusion detection of IoT. Table 2 tabulates the selected features.

The selected features are specified as the input of the Intrusion detection scheme.

Incorporation of generative adversarial network (GAN) in SAPGAN

In this subsection, we proposed SAPGAN framework. The proposed SAPGAN framework contains a generator Gnr and a discriminator $Dmtr$. The Generative Adversarial Network (GAN) design encompasses of convolution technique that is set in multi-layers to attain the order of designated features from WSOA. By this, it is knowledgeable over an arrangement of convolution procedure. Subsequently, the corporeal deceitful of convolutional filters, the IoT data crusade in CNNs is inhibited in local neighbor areas, which bound the entire classification of IoT intrusion[16]. Consequently, self-attention is exploited that accomplish appreciation for the convolution procedure. Equally, liberal training lessens the extent of training, in the meantime extra iterations are made in lesser action space, and in this the network size is miniature. Adopt the formed samples data are represented as $IoT\ D(a)$ and the original IoT data are depicted as OD. Aimed at the Z-layer discriminator $Dmtr$, the domain discrepancy (DD) is done based on the following Eq. (8)

$$L_{DD}\left[IoT\ D(a), OD\right] = \sum_{m=1}^{M} \left\| Dmtr_m(OD) - Dmtr_m\left(IoT\ D(a)\right) \right\| \tag{8}$$

where, $Dmtr_m(OD)$ describes the features from the discriminator by middle layer inspiration. Now, the ultimate mean incongruity (UMI) loss function is subjugated for domain discrepancy (DD), which actions the detachments among two probability distributions from formed IoT samples data and the reference IoT samples data. The UMI accomplishes its smallest zero if the original IoT data samples and formed IoT data samples are equal. The fitness function for the discriminator can be expressed as the following Eq. (9),

$$\begin{aligned} \max_{Dmtr} L_{Dmtr_{dd}} = {} & \mathrm{E}_{IoT\ D, IoT\ D^*}\left[Knl_{Dmtr}\left(IoT\ D, IoT\ D^*\right)\right] + \mathrm{E}_{OD, OD^*}\left[Knl_{Dmtr}\left(OD, OD^*\right)\right] \\ & -2 \times \mathrm{E}_{OD, IoT\ D}\left[Knl_{Dmtr}\left(OD, IoT\ D\right)\right] \end{aligned} \tag{9}$$

where Knl portrays the kernel, which trials the resemblance between two IoT data. Customarily, the discriminator predictable diminishes the $\mathrm{E}_{OD, IoT\ D}\left[Knl_{Dmtr}\left(OD, IoT\ D\right)\right]$, which forces the used data left from the original IoT data for deploying the loss function. In the interim, the discriminator diminishes the intra-class absurdity by prompting $\mathrm{E}_{IoT\ D, IoT\ D^*}$ and $\mathrm{E}_{OD, OD^*}\left[Knl_{Dmtr}\left(OD, OD^*\right)\right]$.

Correspondingly, the loss function for the generator is stated in the following Eq. (10)

$$\begin{aligned} \min_{Gnr} L_{Gnr_{dd}} = {} & \mathrm{E}_{IoT\ D, IoT\ D^*}\left[Knl_{Gnr}\left(IoT\ D, IoT\ D^*\right)\right] + \mathrm{E}_{OD, OD^*}\left[Knl_{Gnr}\left(OD, OD^*\right)\right] \\ & -2 \times \mathrm{E}_{OD, IoT\ D}\left[Knl_{Gnr}\left(OD, IoT\ D\right)\right] \end{aligned} \tag{10}$$

By this, ultimate mean incongruity (UMI) fostered domain discrepancy (DD) weakens the detachments among two probability deliveries from formed IoT data samples and the reference IoT data. Participating self-attention mechanism explains the Progressive Generative Adversarial Network to prominence on target networks,

SL. No	Feature	Data Type	Description
1	State	Numeric	Source–destination packets/sec
2	Mean	Numeric	Average duration of aggregated records
3	Drate	Numeric	Destination-source packets/sec
4	Seq	Numeric	Argus sequence number
5	NINConnPSrcIP total	Numeric	Count of packets per source IP
6	NINConnPDstIP total	Numeric	Count of packets per Destination IP
7	Stddev	Numeric	The standard deviation of aggregated records
8	PkSeqID	Ordinal	Row Identifier
9	Min	Numeric	Minimal duration of aggregated records
10	Max	Numeric	The maximal duration of aggregated records

Table 2. Selected feature using WSOA.

whereas, the discriminator implicitly attains to engulfun suitable data in the input IoT data. The self-attention mechanism is amalgamated erstwhile the discriminator's Down-sample layer and afterward the generator's Up-sample layer. To broaden the importance of formed IoT data (FIoTD) samples, the self-attention mechanism is dominated based on the following Eq. (11)

$$FIoTD_{SA} = \alpha \left[W_1 \times W_2^T \right] \times W_3 + IoTD \tag{11}$$

where α illustrates the updated weight functions, W_1, W_2, W_3 and describes the convolution weights with the kernel sizes of 1×1. The final loss function is dominated based on the following Eq. (12)

$$L_{total}(Dmtr, Gnr) = \max_{Dmtr} \min_{Gnr} \left[L_{Dmtr_{dd}} + L_{Gnr_{dd}} \right] \tag{12}$$

By this, the proposed SAPGAN classifier classifies the IoT data as DDoS (HTTP, TCP, UDP), DoS (HTTP, TCP, UDP), OS, Service Scan, Keylogging with Data exfiltration, and normal data.

Result and discussion

In this section, we discuss experimental results. We have used 2.50 GHz CPU, Intel Core i5, 8 GB RAM, and Windows 7 for the experiemntation. The proposed SAPGAN-IDS-IoT approach is implemented in Python utilizing the BoT-IoT dataset. The performance metrics are examined to verify the efficiency of the proposed method. The derived outcomes of the proposed SAPGAN-IDS-IoT approach are analyzed with existing systems, like CNN-IDS-IoT[11]; DNN-IDS-IoT[12], and DBN-CSSA-IDS-IoT[13] respectively.

Dataset description

The data is gathered from the dataset of BoT-IoT. It encompasses 3,668,522 archives. Out of which, 50% of data is selected for training purposes and 50% of data for testing purposes.

Performance measures

This is a significant task for best classifier selection. To examine the performance, the performance metrics, like accuracy, RoC, F1-score, and computational time are examined. To determine the performance metrics, the given confusion matrix is needed.

True Positive (TP): Count of samples wherever the predicted class labels are attacked, then a real class label is exact.
True Negative (TN): Count of samples wherever the predicted class label is normal, then a real class label is exact.
False Positive (FP): Count of instances wherever the predicted class labels are attacked, then a real class label is inexact.
False Negative (FN): count of instances wherever the predicted class label is normal, then the real class label is inexact.

Accuracy

This is computed via the following Eq. (13)

$$Accuracy = \frac{(TP + TN)}{(TP + FP + TN + FN)} \tag{13}$$

F1 score

This is determined by Eq. (14)

$$F1\,Score = \frac{TP}{\left(TP + \frac{1}{2}\left[FP + FN\right]\right)} \tag{14}$$

AUC

AUC may be computed through the aid of Eq. (15)

$$AUC = 0.5 \times \left(\frac{TP}{TP + FN} + \frac{TN}{TN + FP} \right) \tag{15}$$

Simulation and performance analysis

Figure 2 depicts the simulation results of the proposed SAPGAN-IDS-IoT method. Then, the proposed SAPGAN-IDS-IoT method is analyzed with existing CNN-IDS-IoT[11], DNN-IDS-IoT[12], and DBN-CSSA-IDS-IoT[13] respectively.

Figure 2 depicts the accuracy analysis. Here the proposed SAPGAN-IDS-IoT method attains 18.67%, 30.84% and 14.45% higher accuracy for DoS-HTTP attack; 23.47%, 11.84%, and 15.59%, higher accuracy for DoS-TCP attack; 19.38%, 18,53% and 21.56% higher accuracy for DoS-UDP attack; 25.79%, 23.15% and 16.05% higher accuracy for DDoS-HTTP attack; 19.45%, 25.45%, and 15.74%, better accuracy for DDoS-TCP attack; 15.36%, 24.65% and 29.57% higher accuracy for DDoS-UDP attack; 13.84%, 15.54% and 18.25%, higher accuracy for OS Fingerprinting attack; 17.87%, 13.98% and 23.98% higher accuracy for Server Scanning attack; 17.25%, 22.36%

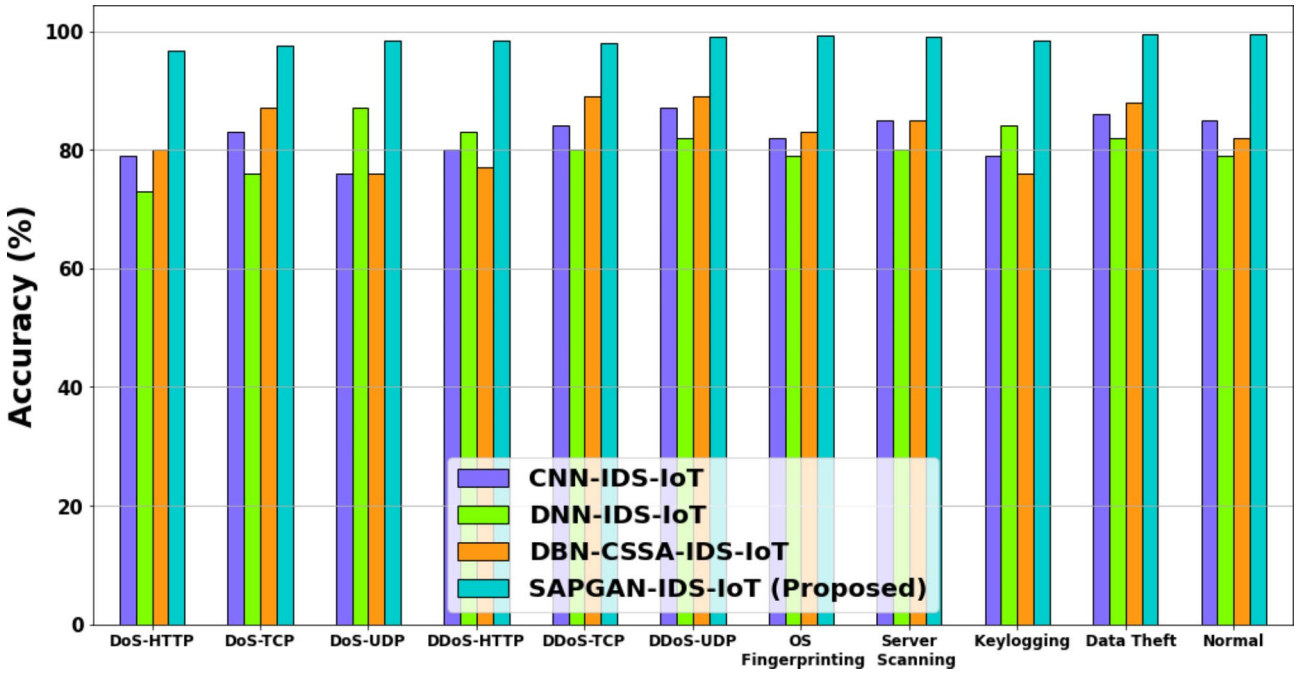

Fig. 2. Accuracy analysis.

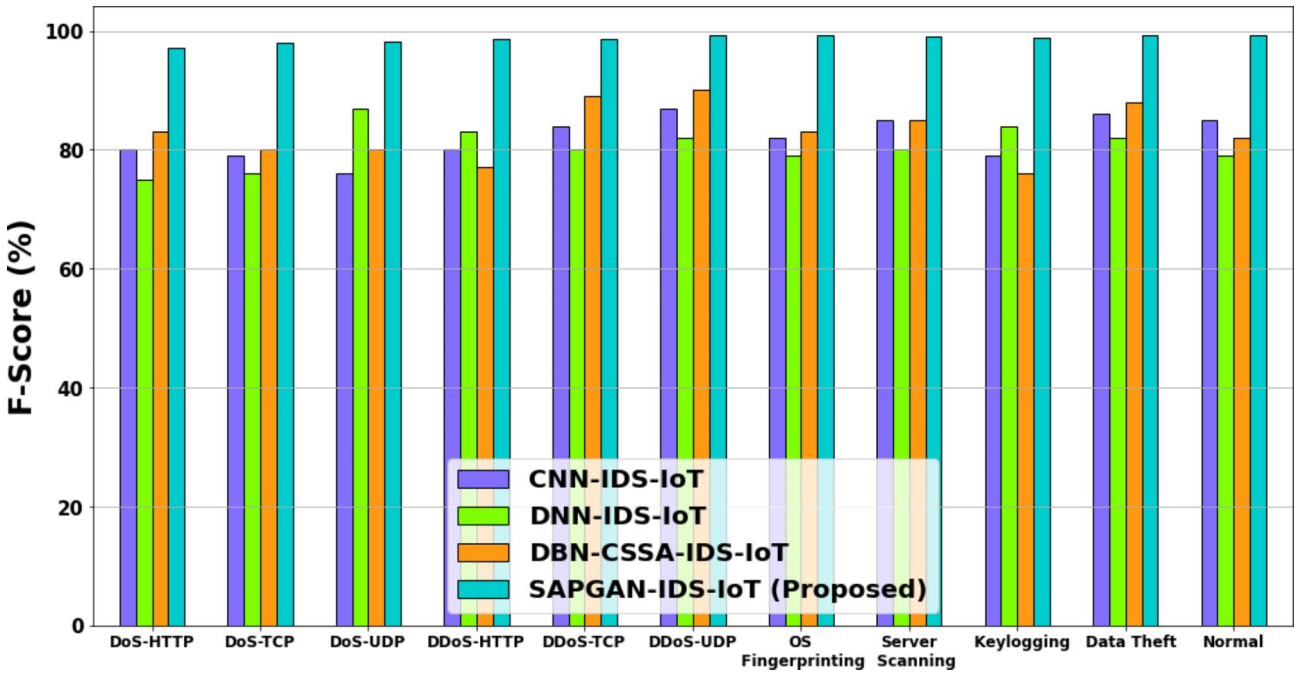

Fig. 3. F-score analysis.

and 19.56% higher accuracy for Keylogging attack; 11.83%, 19.65% and 26.54% higher accuracy for Data Theft attack; 16.98%, 19.76%, and 24.76% higher accuracy for normal compared with the existing CNN-IDS-IoT, DNN-IDS-IoT, and DBN-CSSA-IDS-IoT methods respectively.

Figure 3 depicts the F-score analysis. Here the proposed SAPGAN-IDS-IoT method attains 14.74%, 20.63% and 17.98% better F-score for DoS-HTTP attack; 16.98%, 27.45%, 17.34% better F-score for DoS-TCP attack; 13.56%,23.87%, 10.87% better F-score for DoS-UDP attack; 18.98&, 26.23% and 15.85% better F-score for DDoS-HTTP attack; 11.89%, 25.67% and 16.87% better F-score for DDoS-TCP attack; 17.98%, 14.56% and 19.45% better F-score for DDoS-UDP attack; 15.87%, 28.98%, 12.76%better F-score for OS Fingerprinting attack; 13.23%, 16.98% and 29.65% higher F-score for Server Scanning attack; 26.67%, 17.76% and 20.67% better

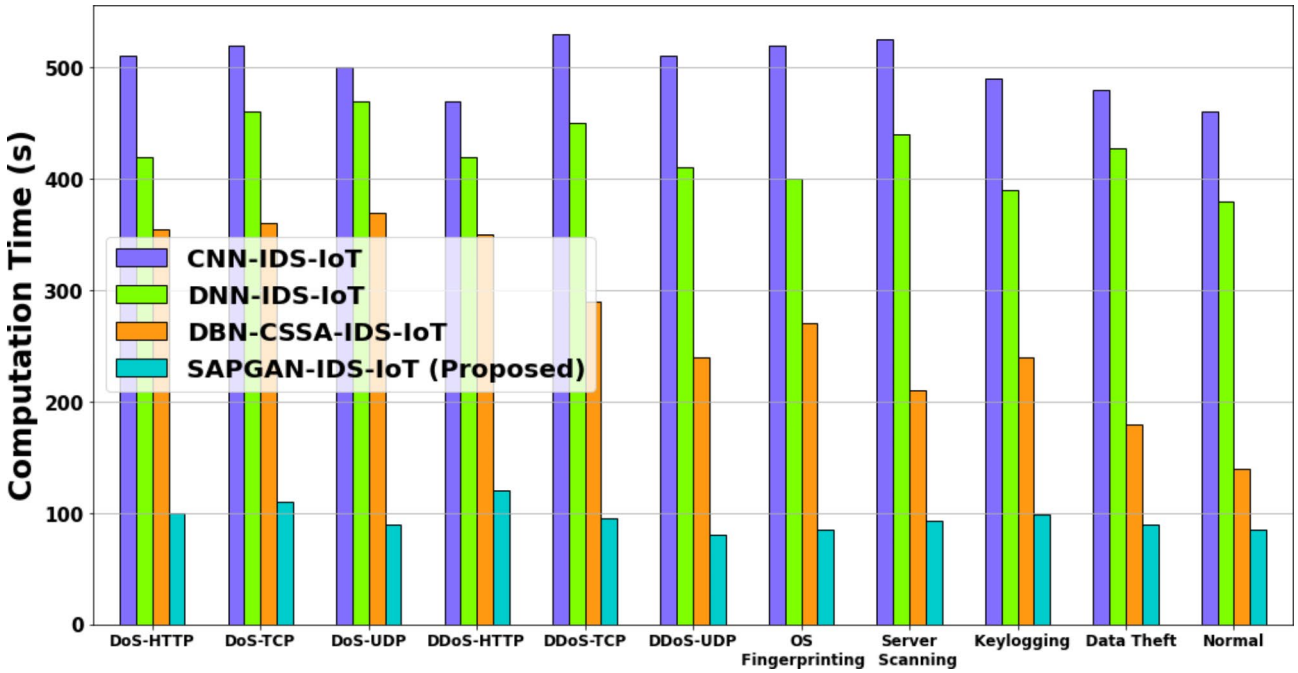

Fig. 4. Computational time analysis.

F-score for Keylogging attack; 17.65%, 24.67%, 18.67% better F-score for Data Theft attack; 25.56%, 12.56% and 27.65% better F-score for normal analyzed to the existing CNN-IDS-IoT, DNN-IDS-IoT and DBN-CSSA-IDS-IoT methods respectively.

Figure 4 depicts the computational time analysis. Here the proposed SAPGAN-IDS-IoT method attains 14.46%, 26.76%, and 13.65% lower Computational Time compared with existing methods such CNN-IDS-IoT, DNN-IDS-IoT and DBN-CSSA-IDS-IoT methods respectively. Figure 5 depicts the RoC analysis. Here the proposed SAPGAN-IDS-IoT method attains 15.45%, 21.55% and 17.79%, higher AUC estimated to the existing methods named CNN-IDS-IoT, DNN-IDS-IoT and DBN-CSSA-IDS-IoT methods respectively.

Conclusion

Herein, we propose machine learning based Intrusion detection framework named SAPGAN is for detecting security threats in IoT Networks. The proposed SAPGAN-IDS-IoT framework efficiency is assessed with certain performance metrics, like accuracy, F1-score, RoC, and computational time. Here, the performance of the proposed SAPGAN-IDS-IoT attains14.23%, 17.98%, and 22.65% higher F-score and15.45%, 21.55%, and 17.79%, higher AUC compared with existing systems as CNN-IDS-IoT, DNN-IDS-IoT, and DBN-CSSA-IDS-IoT methods respectively. The proposed framework detect IoT attacks in smart cities, homes, and healthcare devices. Future work will involve an ensemble model with a novel dataset and deep learning models to enhance this approach for the IoT environment. The BoT-IoT dataset will be used for experimental analysis and compared to the UNSWNB-15 using a deep learning model for network traffic classification.

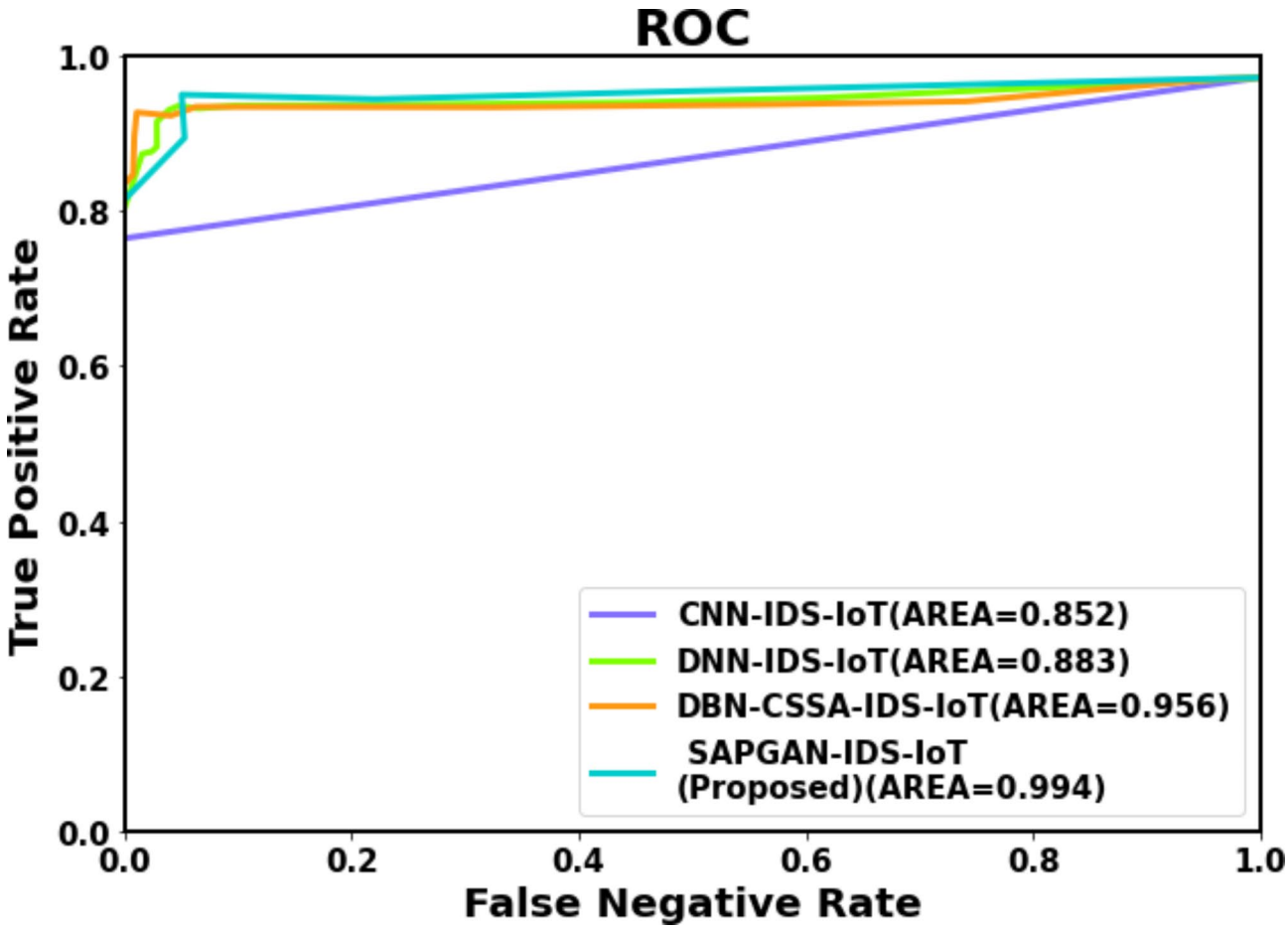

Fig. 5. RoC analysis.

Data availability

The authors confirm that the data supporting the findings of this study are available within the article.

Received: 19 September 2024; Accepted: 27 November 2024
Published online: 04 December 2024

References

1. Mehedi, S.T., Anwar, A., Rahman, Z., Ahmed, K. & Rafiqul, I. Dependable intrusion detection system for IoT: A deep transfer learning-based approach. *IEEE Trans. Indus. Inform* (2022).
2. Singh, K. P. & Kesswani, N. An anomaly-based intrusion detection system for IoT networks using trust factor. *SN Comput. Sci.* **3**(2), 1–9 (2022).
3. Zhou, Y., Cheng, G., Jiang, S. & Dai, M. Building an efficient intrusion detection system based on feature selection and ensemble classifier. *Comput. Netw.* **174**, 107247 (2020).
4. Abbas, A. et al. A new ensemble-based intrusion detection system for internet of things. *Arab. J. Sci. Eng.* **47**(2), 1805–1819 (2022).
5. Saba, T., Sadad, T., Rehman, A., Mehmood, Z. & Javaid, Q. Intrusion detection system through advance machine learning for the internet of things networks. *IT Profess.* **23**(2), 58–64 (2021).
6. Kumar, P., Gupta, G. P. & Tripathi, R. A distributed ensemble design based intrusion detection system using fog computing to protect the internet of things networks. *J. Ambient Intell. Hum. Comput.* **12**(10), 9555–9572 (2021).
7. Alhowaide, A., Alsmadi, I. & Tang, J. Ensemble detection model for IoT IDS. *Internet of Things* **16**, 100435 (2021).
8. Keserwani, P. K., Govil, M. C., Pilli, E. S. & Govil, P. A smart anomaly-based intrusion detection system for the Internet of Things (IoT) network using GWO–PSO–RF model. *J. Reliab. Intell. Environ.* **7**(1), 3–21 (2021).
9. Rahman, M. A. et al. Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. *Sustain. Cities Soc.* **61**, 102324 (2020).
10. Bot-IoT dataset. https://ieee-dataport.org/documents/bot-iot-dataset.
11. Ullah, I. & Mahmoud, Q. H. Design and development of a deep learning-based model for anomaly detection in IoT networks. *IEEE Access* **9**, 103906–103926 (2021).
12. Shareena, J., Ramdas, A. & AP, H.,. Intrusion detection system for iot botnet attacks using deep learning. *SN Comput. Sci.* **2**(3), 1–8 (2021).
13. Karuppusamy, L., Ravi, J., Dabbu, M. & Lakshmanan, S. Chronological salp swarm algorithm based deep belief network for intrusion detection in cloud using fuzzy entropy. *Int. J. Numer. Model. Electron. Netw. Dev. Fields* **35**(1), e2948 (2022).
14. Al-Janabi, S. & Alkaim, A. F. A nifty collaborative analysis to predicting a novel tool (DRFLLS) for missing values estimation. *Soft Comput.* **24**(1), 555–569 (2020).

15. Ayyarao, T. S. et al. War strategy optimization algorithm: A new effective metaheuristic algorithm for global optimization. *IEEE Access* **10**, 25073–25105 (2022).
16. Abdelhalim, I. S. A., Mohamed, M. F. & Mahdy, Y. B. Data augmentation for skin lesion using self-attention based progressive generative adversarial network. *Expert Syst. Appl.* **165**, 113922 (2021).
17. Bhati, B. S. & Rai, C. S. Analysis of support vector machine-based intrusion detection techniques. *Arab J. Sci. Eng.* **45**, 2371–2383. https://doi.org/10.1007/s13369-019-03970-z (2020).
18. Bhati, B. S. et al. An improved ensemble based intrusion detection technique using XGBoost. Trans. Emerg. Telecommun. Technol. **32**.6, e4076. https://doi.org/10.1002/ett.4076 (2021).
19. Chen, Y. W., Sheu, J. P., Kuo, Y. C. & Van Cuong, N. Design and implementation of IoT DDoS attacks detection system based on machine learning. *Eur. Conf. Netw. Commun. EuCNC* **2020**(2020), 122–127. https://doi.org/10.1109/EuCNC48522.2020.9200909 (2020).
20. Feng, Y., Zhong, J. & Ye, C. X. Clustering based on self-organizing ant colony networks with application to intrusion detection. *Proc.-ISDA Sixth Int. Conf. Intell. Syst. Des. Appl.* **2**(2006), 1077–1080. https://doi.org/10.1109/ISDA.2006.253761 (2006).
21. Diro, A.A. & Chilamkurti, N. Distributed attack detection scheme using deep learning approach for internet of things. *Futur. Gener. Comput. Syst*. **82**, 761–768. https://doi.org/10.1016/j.future.2017.08.043 (2018).
22. Kozik, R., Choraś, M., Ficco, M. & Palmieri, F. A scalable distributed machine learning approach for attack detection in edge computing environments. *J. Parallel Distrib. Comput.* **119**, 18–26 (2018). https://doi.org/10.1016/j.jpdc.2018.03.006
23. Anthi, E., Williams, L. & Burnap, P. Pulse: An adaptive intrusion detection for the internet of things. *IET Conf. Publ.* (CP740). 1–4 (2018). https://doi.org/10.1049/cp.2018.0035.
24. Pajouh, H.H., Javidan, R., Khayami, R., Dehghantanha, A. & Choo, K.-K. A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks. *IEEE Trans. Emerg. Top. Comput.* **7**(2), 314–323 (2019). https://doi.org/10.1109/TETC.2016.2633228
25. Altunay, H.C. & Albayrak, Z. A hybrid CNN+ LSTM-based intrusion detection system for industrial IoT networks. *Eng. Sci. Technol. Int. J.* **38**, 101322 (2023). https://doi.org/10.1016/j.jestch.2022.101322
26. Altunay, H.C., Zafer, A. & Çakmak, M. Autoencoder-based intrusion detection in critical infrastructures. *Curr. Trends Comput.* **2**(1), 1–12 (2024).

Acknowledgements

This research was supported by the Researchers Supporting Project number (RSP2024R476), King Saud University, Riyadh, Saudi Arabia.

Author contributions

Kantharaju V.Farhan Amin. and Suresh Niranjanamurthy M. wrote the main manuscript text and Syed Immamul Ansarullah.Amerah Alabrah. prepared figures 1-3. All authors reviewed the manuscript.

Competing interests

Authors declare that there is no conflict of interest.

Additional information

Correspondence and requests for materials should be addressed to F.A. or A.A.

Reprints and permissions information is available at www.nature.com/reprints.

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