Expert Systems With Applications 282 (2025) 127414

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

Deciphering TON-IoT threats: Meta-heuristic and deep learning for attack classification

Yifan Fang [a], Yingwei Jia [b,*], Guozheng Bai [b], Rao Hong [c], Xia Linglin [c], Ghulam Mohi-ud-din [c,*], Chen Ai [c], Muhammad Asim [d], Zhou Li [e]

[a] Huawei Technologies Co., Ltd., Xian, PR China
[b] Shaanxi Polytechnic Institute, Xianyang, PR China
[c] School of Software, Nanchang University, Nanchang, PR China
[d] School of Software, Northwestern Polytechnical University, Xian, PR China
[e] Department of Basic Education and Research, Jiangxi Police College, Nanchang, PR China

ARTICLE INFO

Keywords:
Attack detection
TON-IoT dataset
Intrusion detection
Attention Mechanism
Feature selection
Deep learning
Attack classification

ABSTRACT

In recent times, Internet of things (IoT) has a dynamic performance in the technological sector and the applications are highly susceptible to the malicious attacks and practices to their network traffic, which is considered as challenges for the security domain. Nevertheless, the Intrusion Detection System (IDS) prevents cyber-attacks in IoT enabled networks, which contains multiple features for designing a fast and effective IDS, the procedure of feature selection is used to remove the redundant features from the data. Though several approaches tend to perform feature selection and attack classification some of the pitfalls such as model complexity, higher convergence rate and redundant feature election has lead the model incomplete. This is done using the Improved Genetic Algorithm (IGA), which increases the search capabilities under feature space to identify the relevant features for classification. This is followed by the procedure of attack classification using hybrid DL models such as Convolutional Neural Network (CNN) and Bi-Directional Long short Term Memory (Bi-LSTM) with Attention Mechanism (AM) for performing the attack classification, which is named as ACBSLTM. Here, CNN framework identifies spatial features from the input data, successfully recognizing patterns that signal various types of attacks. The Bi-LSTM then processes these features in a sequential manner, moving both forward and backward, which enables it to understand temporal dependencies and contextual information in the data stream and it is validated through performance metrics. The model performing the classification of attack in the data are evaluated by comparing the existing models performing the attack detection and classification upon the data.

1. Introduction

IoT networks are connected to the objects that interacts with one among the other and with humans, the communication are held wireless, using some of the cellular networks. The data being collected are stored, analyzed and processed in the cloud. This in turn improve accuracy and the efficacy of the data by taking the appropriate measurements based on the gathered data. These IoT devices subsidize to the interconnection among the real-world and the smart systems for generating valuable insights for decision making and in improving quality of life (Sadhwani, Manibalan, Muthalagu, & Pawar, 2023). Protecting data from any of the attack is one of the essential tasks in securing any of the systems, which can enhance the attack type and prediction which can be done using various AI approaches (Jarjis, Al Zubaidi, & Pehlivanoglu, 2023). Thus, the IoT is significantly used by various business, due to their volume and capacity of the IoT, nevertheless the security issued and the IDS systems, which ensures both the security posture and the defense against data. The primary concerns upon the existing approaches for the intrusion and attack detection are the security frameworks and the inadequate capabilities, lower significant latency rates and their longer processing time (Moustafa, Koroniotis, Keshk, Zomaya, & Tari, 2023).

These results in an undesirable attack and non-availability of integrity upon the data. The self-configured form of nodes which are used in creating devices upon various innovative applications such as the automation, home control and the data analysis. According to reports, about 8.3 of the population rely on the IoT during the year

* Corresponding authors.
E-mail addresses: jiayingwei@sxpi.edu.cn (Y. Jia), mohiuddin@ncu.edu.cn (G. Mohi-ud-din).

https://doi.org/10.1016/j.eswa.2025.127414
Received 15 March 2024; Received in revised form 17 March 2025; Accepted 23 March 2025
Available online 8 April 2025
0957-4174/© 2025 Elsevier Ltd. All rights are reserved, including those for text and data mining, AI training, and similar technologies.

of 2025 (Chaganti, Suliman, Ravi, & Dua, 2023). Thus, the extensive use of the internet are one of the unavoidable concern. Correspondingly, one of the main difficulty is the maintenance of security in the IoT nodes using limited resources. Thus, various forms of attack are prone to occur in the data (Madhu, Venu Gopala Chari, Vankdothu, Silivery, & Aerranagula, 2023). Thus, with a deep apprehension to these issues, several approaches have been carried out in making an essential perspectives of securing and inhibiting data prone to attacks. The suggested approach intends to perform IDS in the IoT based using the stacking of DL models. This is done by combining several applicable DL models, into the Fully Connected (FC) layer, for making a stand-alone model. This is done using TON-IoT 17 dataset for the attack detection and classification. The outcomes from the model were comparatively notable and are with lower false positive rates (Lazzarini, Tianfield, & Charissis, 2023).

Correspondingly, the state-of-art approach intends in performing ID, which are based upon the combination of PCA and the May fly Optimization algorithm. This is achieved using data balancing technique and the LSTM model for performing the attack classification. This is done using various dataset such as TID20, Ton-IoT dataset based on CIC and are evaluated using various performance metrics (Karamollaoğlu, Yücedağ, & Doğru, 2022). Since, IDS play a significant and crucial role in the detection and in the prevention of IoT attacks, the suitable comparative approach intends to perform both feature selection and the attack type classification using Mutual Information technique and the Pearson's Correlation Coefficient known as PCC. This suggested filter-based approach is used in the employment of ranking the features according to the initialization of the guided population initiation. About 13 important features were extracted from 43 features (Dey, Gupta, & Sahu, 2023). Concurrently, the suggested approach involves in performing the DDoS-attack detection in the IoT environment. Many such applicable light-weight IDS systems have been employed for the intrusion detection using the BOT-IoT and TON-IoT dataset. From the outcomes, the attack in the both the dataset are highly imbalanced. Smote technique have been used in the balancing approach upon the BOT-IoT dataset (Khanday, Fatima, & Rakesh, 2023).

Though, several approaches intends to Perform attack detection and classification, as the size and the ability to handle the large number of devices upon IoT due to data flow are one of the crucial tasks. This can be further made to optimized data and parallel processing can be followed. Exploring the techniques and the process of data sharing and processing can enhance the ensuring of data privacy (Mahalingam et al., 2023).

As IoT devices become more widespread, they face increasing risks from various cyber threats, such as Denial-of-Service (DoS) attacks and data breaches. Intrusion Detection Systems (IDS) play a crucial role by continuously monitoring network traffic and device behavior, which allows for the real-time detection of anomalies and potential intrusions. With the help of machine learning algorithms, modern IDS can learn from past attack patterns, enhancing their ability to recognize new and complex threats while reducing false positives. However, this study focuses on the limitations of traditional IDS in addressing the unique features of IoT environments, including limited computational resources, diverse device types, and the necessity for real-time processing.

Thus, to overcome these pitfalls and laybacks, the proposed study endures both the feature selection and the attack detection model for ensuring the data effectiveness and the data availability using TON-IoT. This in turn ensures a safer data state and attack less data upon the IoT and their applications. This is achieved in the proposed study by performing both the feature selection using meta-heuristic algorithm and classification using the DL based models comprising the Bi-LSTM with CNN model with AM. The model capable of performing the attack detection and classification using the DL based approaches are evaluated using the probabilistic metrics for the model performing the attack detection and classification. Moreover, the aim of the study is to create an efficient IDS framework capable of autonomously detecting cyber threats in IoT networks while tackling challenges such as resource limitations, privacy issues related to data collection, and the incorporation of advanced ML techniques to improve detection accuracy.

1.1. Motivation of the study

The IoT systems and the devices having limited resources, the attackers are less sophisticated with the wide range of initiatives and the strategies for in filtering them. The certain resistant solutions for making the IoT for the attack identification are the primary intentions. This is done to enhance the state of success in the detection of threats occurring against the overall IoT architecture. Moreover, due to the inconsistency of the increased network intrusion and attack due to data traffic, many such vague data packets are generated in the security of IoT and the IIoT. Some of the crucial pitfalls associated with the attacks are due to the lack in information about recent attacks, and insufficient rates of feature detection form the large datasets (Liu, Wang, Lin, & Liu, 2020). Thus, data availability are less reliable and appropriate approaches are tend to be identified. There is a limited work on implementing deep learning models with multiclass classification on various new network intrusion systems (Almarshdi, Nassef, Fadel, & Alowidi, 2023). The accuracy range of threat classification in IoT networks in Ding, Abdel-Basset, and Mohamed (2023) is 90.5%. Though, it has a considerable accuracy value, there is a possibility of threat detection. Thus, motivated by these factors and significant concern for the attack detection, the proposed study is enabled to perform both attack detection and classification using TON-IoT dataset. The proposed model follows the procedure of attack classification using hybrid DL models such as by combining the Convolutional Neural Network (CNN) and Bi-Directional Long short Term Memory, known as Bi-LSTM with the Attention Mechanism (AM) for performing the attack classification.

1.2. Aim and objective

The main aim of the study intends in performing the attack classification of the TON-IoT dataset, especially to the Network TON-IoT dataset, using the objectives as constructed

- To perform data pre-processing, by checking missing values and perform categorical encoding to TON-IoT dataset in aspects of reducing the bias and complexity of the model.
- To perform feature selection using the IGA for selecting only the optimal features from the dataset to reduce the model training and validation time.
- To perform classification of attack occurring in the TON-IoT dataset using ACBSLTM model for attack detection and classification to reduce the attack rates and complexity due to attack in data.
- To evaluate the model performance using measurable metrics encompassing accuracy ranges, recall rates, F1-score rates and the Precision ranges for affirming model capability upon attack classification.

1.3. Paper organization

The rest of the paper is categorized into four various sections. Where, Section 2 deliberates some of the existing models used in the analyzing intrusion and the attack detection, classification upon TON-IoT and various data using various approaches. Section 3 deliberates the comprehensive methodology adapted of the entire study with their corresponding algorithms. Followed by Section 4 deliberates the overall results and the outcomes obtained after the implementation. Finally Section 5 briefing a conclusion and adaptable future work for the proposed study.

2. Literature review

Some of the existing approaches dealing with intrusion attack detection and classification using various AI approaches and their outcomes are deliberated in the corresponding section.

The identification of the centralized model performing the attack detection using the ML technique has been carried out in the suggested approach. Because of inconsistent also increases network traffic, generation of vague packet affects IoT security. One of the exhaustive and a diversified form of data have been used in the suggested approach for attack detection and classification using the Adaboost and the RUS boost approach. Effectiveness of the model is validated using various probabilistic metrics (Chishti & Rathee, 2023). Concurrently, the state-of-art approach lies in performing the attack detection and classification in both the IoT and SDN networks. A two-leveled security approach has been used in the detection of intrusion, which have been done based on LSTM. Besides, the functionality to compel the dataset for parallel processing to gather the range of routines and cyber-attack events. The model intends to perform the classification among the attack and the benign traffic occurring in the network. Moreover, the identification of the attack category using the TON-IoT dataset. The overall model is concerned with the 96% of accurate detection rate and it is not exploit towards the feature selection and zero-day detect attacks on IoT systems (Elsayed, Hamada, Abdalla, & Elsaid, 2023). The approach of extreme drift latency has been done in the suggested study using the Stream Classification algorithm for effectively dealing with EVL scenarios. These are vitally carried in the non-stationary environments, in IoT domains.

Real-time IoT dataset have been used upon the study for the sophisticated detection of attack in IoT. The key problems in GPC is it performs with the CD variants and utilize offline training classifiers that leads to the efficiency deprivation in online learning (Shyaa et al., 2023). Whereas, the suggested approach have been a two-step form of ensemble approach used in the detection and in the identification of the IOT and the fog environments prone to attacks. This have been done using the RF, and DNN under various dataset (De Souza, Westphall, & Machado, 2022). Transfer Learning based models have been used in the suggested approach using TON-IIoT dataset upon various IoT devices. The implementation of the GRU model for the enhancement in accuracy rates have shown effective results. The existing model is not deployed of the fog nodes, which are attacked to various IoT devices (Poonkuzhali, Shobana, & Jeyalakshm, 2023).

A multi-step CNN with the LSTM have been used in the suggested approach for performing the attack detection in IoT, based in the healthcare applications. LSO algorithm has been used in the Optimization. Where, Activation function has been used in compiling the best selected features. This has been done in approach of increasing the data adaptiveness and in lowering the computational complexity (Thulasi & Sivamohan, 2023). Whereas, the suggested approach combines six various AI based approaches for the attack detection and classification upon the IoT. This has been done using PCA and the Gini based approach for the attack detection upon various IoT datasets. The generalizability of the algorithm has to be improved (Alhanaya & Hamdi Ateyeh Al-Shqeerat, 2023). Correspondingly, the suggested approach have been used with the DeepAK-IoT dataset for the detection of cyber-attacks in the IoT environment. This has been considered as one of the effective model in the attack detection and threat classification in IoT networks with an accuracy range of 90.5%. Moreover, the vanishing and exploding gradient problem has to be minimized (Ding et al., 2023). Sparse Capsule based encoder model have been used in the suggested approach for the feature selection and mapping. Attention based GRU have been implemented for the attack detection (Kethineni & Gera, 2023).

The attack detection upon the IoT based on 6G have been deliberated in the suggested approach using digital and twin computing approach. This have been Implemented for the monitoring of real-time and enhancing the security of the attack detection performance and it has certain limitations in detecting the performance with the online learning module (Yigit, Chrysoulas, Yurdakul, Maglaras, & Canberk, 2023). Similarly, the suggested approach has been intended for the detection of IoT and their security challenges using three various supervised forms of algorithms. XG-boost is one of the models achieving the higher accuracy rates for the intrusion detection by adversarial training and using security based approaches. However, there is an increase in the threat and then the defense strategies have to be improved (Vitorino, Praça, & Maia, 2023). Correspondingly, the suggested approach has been intended for the attack detection using hybrid CNN and IDS methods, where, Krill Herd algorithm for the enhancement of encryption standard have been used in the suggested approach. The weights of these HCNN have a significant impact on the classification results and it has certain limitations to find unidentified traffic (Akshaya, Mandala, Anilkumar, Vishnuraja, & Aarthi, 2023).

The anomaly detection in the IIoT environment have been intended in the suggested approach encompassing various approaches. The traffic data upon network have been converted to a graph based representation and are provided as input to the learning ML models. Besides, to know about the interaction among the graph theory and network for better performance (Alwasel, Aldribi, Alreshoodi, Alsukayti, & Alsuhaibani, 2023). KNN, SVM and the ANN models have been used in the state-of-art approaches for performing IDS. These have been implemented for performing the differences among 15 types of varying intrusions in the network. SMOTE technique have been used in the process of normalizing the imbalanced dataset and for performing feature selection. The model cannot identify the phishing attack that is considered as a attack (Othman & Abdullah, 2023). CNN and Bi-LSTM have been combined in the suggested approach for the attack detection and have been compared with some of the other DL based models for the classification of attack and normal attacks over the data. The CNN model have achieved an overall accuracy rate of 89.9%. It is not implemented in the multi-class classification on various networks (Almarshdi et al., 2023).

ML based models and Optimization based upon the arithmetic algorithm have been carried out in the suggested approach using RF. The features have been reduced to enhance the prediction time of the attack, where NIDS dataset have been used in the suggested model (Fraihat, Makhadmeh, Awad, Al-Betar, & Al-Redhaei, 2023). Whereas, ensuring the network security upon a robust form of IDS using ensemble form of ML models have been used in the suggested approach. This model can be used in affiliating the safety of the networks against cyber-attacks in networks and has the limitations of intrusion detection system and give a structure verified with various datasets (Hossain & Islam, 2023). Anomaly detection upon the malicious forms of data in the IoT networks have been carried out in the suggested approach. This have been carried out using DL based model and de-noising based Autoencoders approaches for obtaining the optimal features, upon the real-time IoT dataset. This has been carried out in the heterogeneous environment for ensuring the effectiveness of the model (Abusitta et al., 2023).

Both the RF and XG-boost classifier have been used in the suggested approach for the detection of attack in IoT using the UNSW15 dataset, with an 10-fold cross validation, an overall accuracy have been notably higher than the other models (Srivastav & Srivastava, 2023). The IoT for a malware detection have been carried out in the comparative approach makes use of adversarial evasion strategy for the attack detection in IoT, using SIMBIoTA-ML model. Which can be used for both the original malware and the adversarial samples for attack detection. Moreover, the convergence speed and stability of the algorithm can be improved (Sándor, Nagy, & Buttyán, 2023). Though, the suggested models tend to perform better in aspects of attack detection and classification, some of the core laybacks and pitfalls are deliberated in the following sub-section.

The methodology employs CNNs and RNNs that are trained on a variety of datasets to ensure precise threat detection. However, there are limitations, including high computational complexity, scalability challenges in extensive IoT networks, dependence on diverse training data, difficulties in interpretability, and the necessity for regular updates to keep pace with evolving threats (Kumar & Neduncheliyan, 2024). Similarly, The IDS employs a modified Arithmetic Optimization Algorithm for feature selection and utilizes machine learning for intrusion detection in IoT NetFlow networks. However, it encounters challenges such as high computational complexity, scalability issues, data dependency, interpretability, and the need to adapt to evolving threats (Fraihat et al., 2023). The hybrid meta-heuristics algorithm integrates feature selection with XGBoost to enhance intrusion detection in IoT networks, utilizing gradient boosting for precise classification. Nonetheless, it encounters several limitations, including significant computational requirements, scalability challenges, and reliance on high-quality data, difficulties in interpretability, and the necessity for regular updates to tackle emerging threats (S. Bajpai & Chaurasia, 2024).

2.1. Problem identification

Some of the core apprehensions and the pitfalls of the state-of-art approaches are discussed in the respective section.

- Though the suggested model is capable of performing better attack detection and classification, with higher accuracy rates, the statistical and the non-statistical data regarding the dataset are less procured by the suggested model (Alwasel et al., 2023).
- The suggested model capable of performing the comprehensive evaluation of the model. The algorithm, in aspects of network scenarios and the dataset used in the model has to be designed even more efficient. This should be done for making them applicable to various network settings and applications (Thulasi & Sivamohan, 2023).
- The model suggested in Kethineni and Gera (2023) has to be optimally tuned its hyper parameters with focus on the categorization and early detection time analysis of many cyber-malware in complex systems.
- The suggested model in Vitorino et al. (2023) is efficient in IoT intrusion detection and classification, whereas defense strategies have to be improved for the reliable and robust IoT network intrusion detection and cyber-attack classification, when the threat of adversarial attacks increases.
- The model suggested in the study has to be dealt with different ways to prepare the data, extract important features, and use machine learning techniques in order to improve the classification process and better performance (Alwasel et al., 2023).

3. Proposed methodology

AI approaches is extensively adapted for the accurate detection of network intrusion. However, the users of these Network Intrusion Detection (NID) systems are unable to understand the correct and incorrect forms of decisions. These are due to the complexity and the black-box nature of AI approaches. Thus, to overcome these laybacks, the proposed study initiates DL based and Meta-heuristic approaches for the feature selection and classification of the attack and non-attack occurring in the TON-IoT dataset. Besides, CNN model has the limitations, which includes problems like challenges in sequential data handling and high computational requirements. Whereas, Bi-LSTM approach is limited with challenges such as increased computational complexity, potential overfitting with large datasets, and challenges in capturing dependencies beyond a certain range in sequential data. Hence, the hybrid approach is used to overcome these challenges.

Here, the proposed model uses hybrid approach due to its strengths combination, improved generalization, and enhanced robustness. Also it reduces computational complexities like training time, inference times, resource utilization and scalability. Hybrid approach confers the enhanced robustness to different types of attacks or variations in input data. For these reasons, the proposed model uses hybrid approach rather than other approaches. Moreover, the raw forms of data comprising many of duplicate values and non-readable forms of data are converted to model readable data and editable forms of data using the data pre-processing techniques. These techniques are used in the conversion of raw data to be understandable to obtain approximate outcomes from the model. Because of hybrid model, the missing values are checked and process of categorical encoding. The non-checking of missing values, can result in increased bias rate of the model. The process of categorical encoding is done for transforming the integer forms of data to the categorical forms of data. This can make the model to bring out enhanced forms of outcomes upon the model performing classification. The following process of feature selection and classification are discussed in the following sub-sections. The overall flow of the projected model is figured in Fig. 1.

3.1. Data-preprocessing

The ToN IoT Dataset goes through thorough pre-processing to get the raw data ready for analysis and machine learning tasks. This process includes cleaning the data to eliminate errors, duplicates, and missing values, which helps maintain the dataset's integrity. Normalization is used to scale feature values consistently, avoiding biases that can arise from different data ranges. Feature extraction focuses on identifying and transforming the most relevant attributes from the raw data, while dimensionality reduction techniques, such as Principal Component Analysis (PCA), help decrease the number of features while keeping essential information intact. These steps are crucial for enhancing data quality, minimizing computational complexity, and facilitating accurate and efficient analysis of IoT network behaviors.

3.2. Feature selection using modified GA

GA is one of the global optimum searching algorithm. The algorithm is simple and are with strong robustness property, which are widely adapted under many fields. The speed of convergence is comparatively low for a conventional GA., where the process of local ability searching is optimally low in quality. Moreover, the phenomena of premature convergence is higher. In aspects of changing the standard disabilities of the GA, many such improved methods have been adapted including the Adaptive GA. The GA, follows sequence of steps such as initialization of the population, fitness value computation, applying crossover, mutation, selection etc. The proposed algorithm involves initializing the heuristic data and the artificial pheromone. Finally, overall population will be generated. Finally, the end population of GA will be considered. Once the final population is generated, heuristic data and artificial pheromone are initialized. In the following step, when the iteration for the final step is unsatisfied, local is considered and pheromones are updated. Termination occurs only when the Local Best Path (LP) is better than the Global Best path (GP). Moreover, for ensuring the stakeholders insights and trustworthiness transparency is needed and for feature selection in Improved GA fitness convergence curve is presented.

Improved GA

In the proposed study the Improved GA is employed for selecting the features for enhancing the efficiency of the model with reduced complexity. Further, its objective is to identify the relevant and features that are related to the dataset and reduces the dimensionality and enhances the efficacy of the classification model. In feature section process, the feature subsets are randomly generated for the initial population, where every individuals are represented in features. In

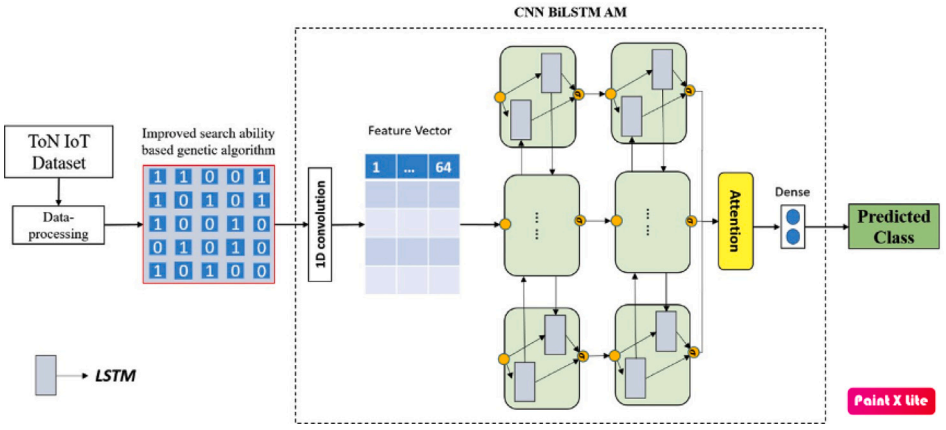

Fig. 1. Overall flow of the proposed study.

the fitness evaluation, the features are evaluated by using a fitness function where, the selected features are optimized the data gained when minimizing redundancy. Then, it is calculated by the contribution of feature subset to achieve an accuracy for the entire dataset variance. Through fitness-proportionate selection, crossover, and mutation operations, IGA promotes diversity and helps avoid premature convergence while effectively exploring the search space. The incorporation of adaptive mutation probabilities, pheromone-based updates, and a two-generation competitive strategy further improves both the speed of convergence and the quality of solutions. By reducing dimensionality and eliminating redundant features, IGA simplifies models, decreases computational demands, and minimizes the risk of overfitting, leading to better generalization. Moreover, it boosts performance by enhancing accuracy, scalability to large datasets, and the interpretability of results. For these factors the improved GA is implemented and it is discussed below.

Each of the methods involved in improving the GA in several aspects, and have procured several better outcomes. Nevertheless, the behavior of convergence is dependent on many varying factors. The complete working of the GA pseudocode is deliberated in Algorithm 1.

Algorithm 1 GA

```
parameter(s): S - blocksin set are considered as input
output: S superstring is received
t ← 0
Pt is Initializes to random set of individuals from S* EVALUATE-FITNESS-GA(S,Pt)
while condition for termination not met do
    individuals are Selected from Pt ( overall fitness proportionate)
    individuals are Recombined
    each of individuals are Mutate
    FITNESS is EVALUATED–GA(S,modified individuals)
    Pt+1 ← individuals are newly created
    t←t+1
end while
return (superstring retrieved from best individual in Pt)
procedure FITNESS ɪs EVALUATED(GA(S,P))
S-set of blocks
P-population of individuals
    for each individual i ∈ P do
        derived string s are generated (i)
        m←all blocks from S that are not covered by s(i)
        s} (i)←concatenation of s(i)and m
        fitness value← 1/‖S'(i)‖2 (i)
    end for
end procedure
```

In the proposed study the Improved GA is employed for selecting the features for enhancing the efficiency of the model with reduced complexity. Further, its objective is to identify the relevant and features that are related to the dataset and reduces the dimensionality and enhances the efficacy of the classification model. In feature section process, the feature subsets are randomly generated for the initial population, where every individuals are represented in features. In the fitness evaluation, the features are evaluated by using a fitness function where, the selected features are optimized the data gained when minimizing redundancy. Then, it is calculated by the contribution of feature subset to achieve an accuracy for the entire dataset variance. Through fitness-proportionate selection, crossover, and mutation operations, IGA promotes diversity and helps avoid premature convergence while effectively exploring the search space. The incorporation of adaptive mutation probabilities, pheromone-based updates, and a two-generation competitive strategy further improves both the speed of convergence and the quality of solutions. By reducing dimensionality and eliminating redundant features, IGA simplifies models, decreases computational demands, and minimizes the risk of overfitting, leading to better generalization. Moreover, it boosts performance by enhancing accuracy, scalability to large datasets, and the interpretability of results. For these factors the improved GA is implemented and it is discussed below.

Moreover, the mutation regions, overdue the phenomena of premature and enhances the ability of local optimum values. The enhancement in the premature convergence is done by adding all of the older father generation to the new father chromosome, this the fitness value of the new generation is increased.

This is given by,

$$IGA(k) = (Fit_{Val_{max}} - Fit_{Val_{min}}) + (Fit_{Val_{aver1}} - Fit_{Val_{aver2}}) \tag{1}$$

The new chromosome of the respective generation, having the chromosome fitness value, with distributing condition is demonstrated using the fitness distribution function. This is given using,

$$Fit_{Val_d} = \frac{(F_{max} - F_{min})}{F_{aver}} \tag{2}$$

Whereas, on the other aspect the enhancement in the methods of probability of mutation is confirmed by the father generation and the fitness due to the crossover probability having $P_c ross$ value of 1 is given using,

$$\mathrm{Per_{mut}} = \mathrm{Per_{mut}}\ 0\left(1 + \frac{4}{1+\mathrm{F_d}} + \left(\frac{5}{(1+\mathrm{IGA(K)})}\right)\mathrm{Per_{mut}} \le 10 * \mathrm{Per_{mut}}\ 0\right) \tag{3}$$

Here, Per_{mut} is defined as the current probability of the mutation, Per_{mut} 0 represents the primary probability of mutation.

When the process of adaptive adjusting the overall operation range is changed corresponding to the binary system, the ith solution of

vector equals to the solution of the vector size, provided using,

$$R_{\text{size}} = \frac{2^{k-1}}{2^n - 1} * \left(X_r - X_l\right) \tag{4}$$

The operation of mutation searching performance is varied according to the length such as the point mutation and in case of many point mutation, position of mutation is given by,

$$\frac{2^{\text{Mpoint i-1}}}{2^{n-1}} * \left(X_r - X_l\right) < \frac{2^{\text{Mpoint j-1}}}{2^n - 1} * \left(X_r - X_l\right) \tag{5}$$

Whereas, the performance of cross-over operations for each of the searching step length is given using,

$$\text{cros}_{\text{size}} = \frac{2^{k-1}}{2^{n-1}} * \left(X_r - X_1\right) \tag{6}$$

When, the value of K is higher, the searching procedure of the cross over length are also greater. Similarly, when K becomes smaller, the searching step also diminishes.

The operation of scale transforming is given using,

$$\text{Fit}_{\text{Val}}\ (x, y) = \frac{\alpha}{\alpha + (1 - f(x, y))} \tag{7}$$

Where, α=0.1 The phenomena of avoiding the sticking to small difference among the optimum function optimum and the function of sub-optimum. This is provided by, Rosenbrock function

$$(x, y) = 100\left(y - x^2\right)^2 + (1 - x)^2 \tag{8}$$

This is one of the minimal problems, where the global minimum position is (1,1), which transforms the object function to the fitness function, resulting in finding the maximal values and the scale using,

$$it_{Val}(x, y) = \frac{a}{(\alpha + f(x, y))} \tag{9}$$

Based on the IGA, the process of finding the selected features of X_{feat} is proceeded and are passed to the ACBSLTM.

3.3. Data split

The raw data from the dataset which is pre-processed upon various approaches such as missing values check and the categorical encoding are proceeded for the optimal feature selection is done for data split based on train and test data. The data is split as to 80:20 for the train and test data respectively.

Training: This model is to be trained, because it is essential to provide it with a labeled dataset. However, it allows the model to learn patterns and set weights or parameters that reduce prediction errors. Generally, around 80% of the available data is used for this training phase. During this process, the model receives the data and adjusts its weights using optimization methods like back propagation to boost its performance. Hence, the iterative approach helps the model enhance its grasp of the essential interactions in the data, ultimately leading to better predictions on new, unseen data.

Testing: During evaluation, remaining 20% of the dataset, the so-called test or validation set, is used to generalize to previously unknown data. The main goal is to evaluate the model's performance by measuring various metrics such as accuracy, precision and recall. In this process, the trained model is applied to the test dataset, predictions are generated and compared with the actual results. By computing these performance metrics provides insight into the effectiveness and robustness of the model in making accurate predictions on new data and ensures that the model not only fits the training set but also effectively handles real-world scenarios.

Data split with evaluation protocols: The datasets are typically separated into three parts namely, training set (70%–80%) for model training, and test set (10%–15%) for final validation. This framework split enables unbiased assessment for the model's performance on unknown data. Moreover, main evaluation metrics comprise accuracy, which measures complete correctness, while precision is the ratio of correctly predicted positives to total predicted positives. Whereas, recall is the proportion among the predicted and the actual positives. Then, f1-score that balances precision and recall. Additionally, a confusion matrix provides understandings between True Positive (TP), False Positives (FP), True Negatives (TN) and False Negatives (FN), which ensures a completes evaluation of the model's generalization capabilities.

3.4. Classification using ACBSLTM

CNN and Bi-LSTM

CNN is one of the reputed DL network, present in a neural form, where 1D CNN is used in the proposed study as these convolutional kernels, can scan along the depth of the logging curves. The CNN comprises the Convolutional Layer (CL), Pooling Layer (PL) and the Fully Connected (FC) layer. The CNN is used for capturing the implicit features, from the data provided as the input, using the convolutional operations with the pooling operations. The features which are extracted are fed into the FC layer and some of the activation function are used in reducing the mom-linearity among the neuron. Whereas the CL manipulates the kernels used in capturing the hidden features, forming feature maps. The Fig. 2 shows the CNN architecture, initially input layer is bidirectional, which has input size of (8, 2, 2), then it is loaded to the bidirectional LSTM where the (8, 2, 2) is given as input and has the output of (1,128) and it send to the dropout layer. It is a significant layer during the training process because it predict over-fitting at training data and it has achieved the output of (1,128). Finally, dense layer is a simple layer where the input with (8, 128) receives all the data of the previous layer and gives the (1, 1) as the output.

Whereas, Bi-LSTM is one of the most adapted DL models, adapted due to their inherited capability of resolving the issues related to gradient explosion and vanishing. The structure of Bi-LSTM operates in an interactive manner. The Bi-LSTM compiles the Input and Output from each of the layers in both the forward and the backward layer. In aspects of training the sequence, both forward and the backward layer acts sequentially. Both the forward and the backward networks are connected to the same output layer in aspects of providing a complete context of information obtained at each of the sequence point. The Bi-LSTM model is accurate to perform classification, as they take up the advantage of both the past information and the reverse information for predicting the right fault and the location of the fault. The outcomes from the Bi-LSTM model are accurate than the uni-directional LSTM. From Fig. 3 it is observed that input layer has (8, 2, 2) as the input, where the Bi-LSTM layer procedures the embedded sequences in forward and backward motions. Then it is fed to the conv1D layer, where the one dimensional data are processed and obtained the output (1, 2,128). The bidirectional processing allows the proposed model to capture the input sequence of (8, 2,128) and obtained the output of (1, 2,128). Lastly, the batch normalization assists in mitigating inner-covariate shift through normalizing the activation in every batch in training process and obtained the output of (1, 2,128).

ACBSLTM for classification

In order to perform classification, the proposed model makes use of CNN and the Bi-LSTM with the AM for classification the attack and non-attack among the TON-IoT dataset. The CNN is used in the classification model which has an inherited ability to perform classification over the network data attack. The ability of the CNN model having local perception and weight sharing, are prompt to enhance the efficacy of learning ability of the model. CNN comprising Convolutional layer, Pooling and the Fully Connected layer are with convolutional kernel operation acts better upon the classification process. The features extracted are with higher dimension, which are reduced by the pooling layer present in the CNN model.

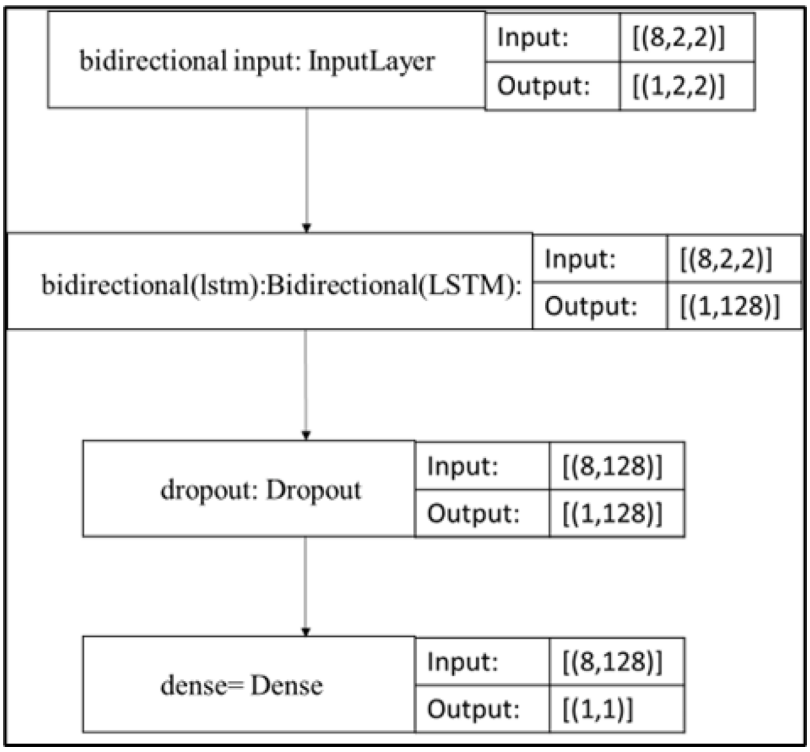

Fig. 2. Architectural design of CNN.

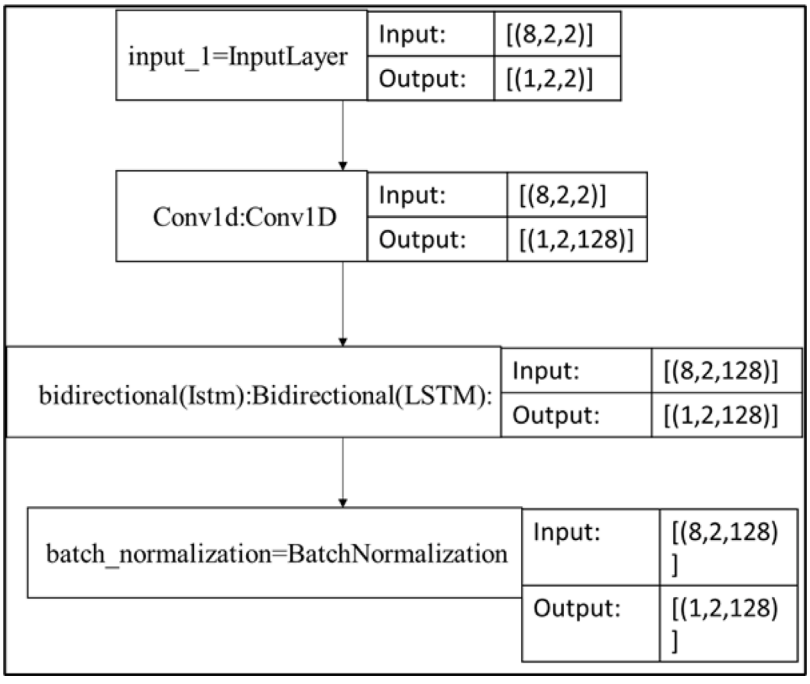

Fig. 3. Bi-LSTM architectural design.

Moreover, pooling layers in CNNs has the main function in reducing the spatial dimensionality of feature maps while retaining important features, simplifying the model and reducing computational complexity. Besides, down sampling is achieved by aggregating values from local regions, such as max pooling, which preserves the maximum value, or average pooling, which calculates the average value within a defined window. This process not only helps extract more abstract and invariant features, but also improves the robustness of the model to small changes in the input values and makes it less susceptible to changes in position, rotation, scaling, etc. In addition, pooling layers reduce the risk of overfitting by reducing the number of parameters, especially in deep networks. The complete algorithm of Bi-LSTM training is provided in Algorithm 2.

Followed by the extracted features are fed into the Bi-LSTM as input. This makes the model to be complex and increases the overall cost of training the network. Thus, to resolve the problem, the pooling layer

Algorithm 2 BiLSTM

Input:
Features: each data point are used from set of features.
Labels: label set for each data point.
K: total number of folds in the K-fold cross-validation.
Output:
BiLSTM is completely trained .
Each test set are performed for classification.
Steps:
dataset is loaded.
data point for training and test sets are validated:
features are extracted (fet).
labels are extracted (lab).
For each of the feature in fet:
encoding is done when the values are numerical using Keras library.
Scale the features using $Z' = \frac{fet - fet_{min}}{fet_{max} - fet_{min}}$
For i from 1 to n:
Initiate with K=10.
Divide the training modules into K-groups.
Load into the BiLSTM .
model is fit using K-1 groups.
model is validated using the rest of Kth group.
Repeat until all K-groups are used as validation sets.
Test the model on the test set (Ton IoT Test).
trained BiLSTM model and the classifications of test set is obtained.

involved in reducing the dimensions of features are done using,

$$\text{Out}_t = \tanh\left(X_{\text{feat}} * \text{Weg}_t + \text{bis}_t\right) \tag{10}$$

The output features from the CNN are estimated using the hidden layer present in the Bi-LSTM layer, and the final output are obtained. The Bi-LSTM layer is used in adding key features to the certain areas for extraction of more precise and required information. This, further avoids the un-necessary information and simultaneously assigns significance to each data. The output of the final moment and input of current time are provided to the forget gate. This is given using,

$$f_t = \sigma\left(\text{Weg}_t \cdot \left[h_{t-1}, X_{\text{feat}}\right] + bi_t\right) \tag{11}$$

The output value and the candidate cell of the current input are provided by,

$$\text{Out}_t = \sigma\left(Weg_t \cdot \left[h_{t-1}, X_{\text{feat}}\right] + bi_t\right) \tag{12}$$

$$\tilde{C}_t = \tanh\left(Weg_c \cdot \left[h_{t-1}, X_{\text{feat}}\right] + bi_t\right) \tag{13}$$

The current cell state which is updated are provided using, the

$$C_t = f_t * C_{t-1} + \text{Out}_t * \tilde{C}_t \tag{14}$$

The overall output value from the output gate is obtained using,

$$o_t = \sigma\left(We_t \cdot \left[h_{t-1}, X_{\text{feat}}\right] + bi_o\right) \tag{15}$$

Thus, the overall output from the LSTM is obtained by estimating the output from the cell state and the output gate using,

$$h_t = o_t * \tanh\left(C_t\right) \tag{16}$$

The CNN and Bi-LSTM is one of the DL models, applied for resolving the issues such as gradient explosion and gradient vanishing. The structure of Bi-LSTM operates in an interactive manner. The Bi-LSTM structure composing the Input, Output and the forget gate in each of the layer in both the forward and the backward layer. For each of the training sequence, both forward and the backward layer acts sequentially. Both these networks are associated to the identical output layer in aspects of providing a complete framework of information to each of the sequence point. Moreover, the Bi-LSTM model is precise than the other DL models namely SVM, as they take up the benefit of previous and the reverse information for the future information. As, Bi-LSTM considers both the past and the future, the final prediction made by the model is exact than a unidirectional LSTM does. The similarity and the correlation among the query and the key feature is estimated using,

$$\text{Sim}_t = \tanh\left(\text{Weg}_t h_t + bi_t\right) \tag{17}$$

The AM improves classification accuracy by dynamically assigning importance to features, allowing the model to focus on relevant information while minimizing noise and redundancy. It calculates an attention score to weight features based on their relevance, ensuring that important features contribute more to decision making. It identifies complex patterns in high-dimensional IoT data by capturing contextual dependencies, simplifying the model without compromising accuracy. This improves performance metrics such as accuracy, precision, and recall, and improves interpretability by highlighting important features. This makes the model more robust and effective for real-time IoT applications that require fast and accurate decision making.

The source of initial stage is normalized and the overall softmax function, which is employed in converting the attention score is

$$att_t = \frac{\exp\left(\text{Sim}_t \text{ v}\right)}{\sum \exp\left(\text{Sim}_t^{\text{T}} \text{ v}\right)'} \tag{18}$$

Here, v refers to the value of attention

On context to the weight coefficient, the overall attention value is gained using the weighted summation of each of the value, using

$$\text{sim} = \sum_t att_t h_t \tag{19}$$

Thus, a gap is produced in the input data, which makes the model training to suppress. Thus, to overcome the issue and better train the model, the standardization of the method which is adapted to the input is provided by the standardization of the input data provided is done for better training of the model where the standardization of the Z-score is adapted for the process of standardizing the input data using,

$$y_t = \frac{\left(X_{\text{feat}} - \bar{X}\right)}{\text{sim}} \tag{20}$$

Here, y refers to the value being standardized, x_{feat} is the provided input data and $\overline{X}$ indicates the average of the provided input data and sim refers the standard deviation of the input data. The illustration of ACBSLTM is depicted in Fig. 4.

The Fig. 4 shows that the ACBLSTM architecture, where the dropout layer predict the over-fitting and it randomly neutralizes some layers, thus nullifying the contribution towards the output. Hence, it is output of the CNN is given as the input for Bi-LSTM. Using the permute operation, the given input data is flattened and it has accomplished (1, 2,128) as the output. By the usage of dense layer the activation argument is passed to the activation function and obtained an output of (1, 2,128).

In this model, the process starts with the Ton IoT dataset that gathers telemetry data in IoT devices, enduring preprocessing to clean and arrange the data for analysis. Next, an improved search ability-based GA is applied to enhance feature selection, signified using a binary values matrix. Moreover, the enhanced data is then managed over a 1D convolution layer, extracting patterns then generating a feature vector by 64 features for succeeding layers. Then, the core of the model contains CNN that captures spatial features, monitored by a BiLSTM network that analyzes sequential dependences in the data, improved by an AM to select significant structures. Besides, the output from the AM is provide to a dense layer, which plots the features to classification outputs. Finally, the model produces a predicted class, to identify IoT device types or perceiving variances in the dataset.

For enhancing the resistance of model to attacks and it utilizes a variety of balanced datasets during training. To boost resilience, we

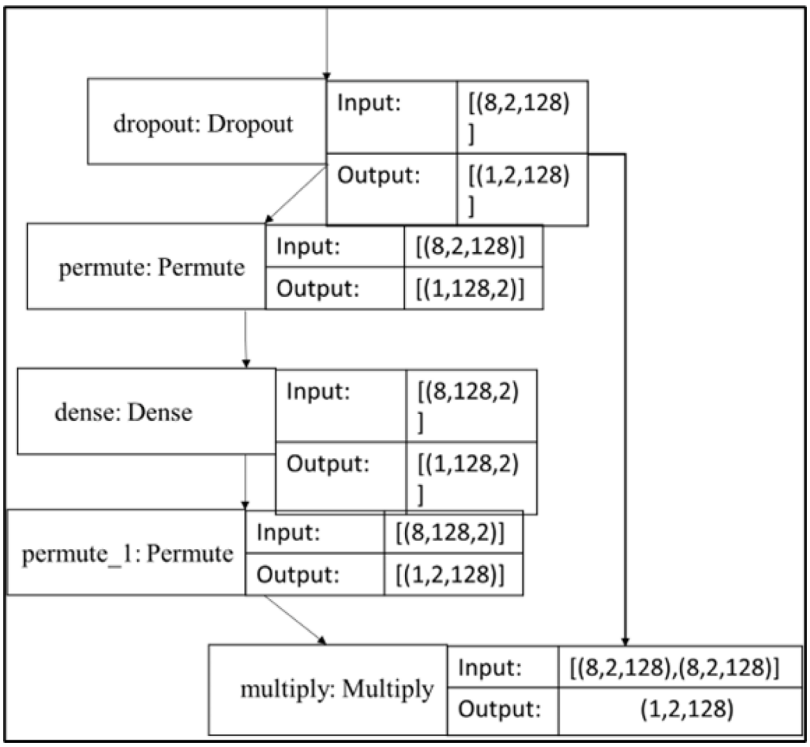

Fig. 4. Working architecture of ACBSLTM.

incorporate regularization methods like dropout, weight decay, and batch normalization. It also employ feature masking and preprocessing techniques to minimize our model's sensitivity to minor alterations. Defensive distillation is applied to develop a more resilient version of the model. Additionally, input gradient are introduced for regularization to limit the gradient in the presence of perturbations. It is important to use robust evaluation metrics to assess model performance in attack scenarios. Then, the secure deployment practices also implemented which, includes model versioning, secure communication, and monitoring systems to identify and address potential threats in real time. The further outcomes provided by the model in connected to other performance and their outperformed on comparing to the other existing approaches are deliberated in the following section.

4. Results and discussions

The overall outcomes of the proposed model performing attack detection and classification over the network data is discussed in the respective and following sub-sections. The study is pondered in each of the section with their suitable data and link for reference. The overall working of the model is related with state-of-art models for affirming the proposed method efficacy.

4.1. Dataset description

The TON-IoT dataset are used in evaluating the fidelity and the efficacy of the various cyber security applications which are based on AI and it contains 2,233,921 records. Moreover, dataset have features (44) that is extracted from Bro-IDS (Zeek). Furthermore, dataset having 795,380 (3.56%) is normal flows and 21,542,641 (96.44%) is malicious. They are designed for use in intrusion detection applications, Models such as threat intelligence, adversarial ML, and privacy preserving. These datasets were named as 'ToN IoT' as it contain diverse data sources that have been collected from Telemetry dataset of different origins. Moreover, Windows operating systems and IoT sensor data. TLS, and Network. Traffic datasets. Then, a realistic approach was used to obtain the datasets. A tested network of significant scale was developed at the IoT Lab of Google. Several virtual machines are being linked by UNSW Canberra Cyber. The physical systems, hacking platforms, and cloud-based fogging. The scalability and complexity of IoT sensors are comparable. IIoT and Industry 4.0 networks. The proposed study makes use of network datasets, which are collected in the packet capture formats, sometimes in log files and in the CSV file formats. The dataset are used for various applications such as the fraud and intrusion detection, digital forensics and in adversarial ML.

Moreover, the proposed model can increase its training time with fine-tuning through the recommended hardware such as CPU, GPU and required memory to provide a better outcomes for the fine-tuning process.

Table 1
Computational requirements.

Model	Specification
Processor	Multi Core Intel i5 Processor
RAM	16
SSD	500
NVIDIA GPU	RTX 3060
Software	Matlab 2022

4.2. Computational requirements

The proposed model's computational requirements are depict in 1

4.3. Exploratory data analysis (EDA)

EDA is used in prospects of estimating the data using various visualization approaches. In case, EDA is applied in defining the patterns or to authorize the assumptions. These are done using either a graphical representations or using a statistical summaries. Furthermore, EDA compromises the data which is used in understanding the entire dataset.

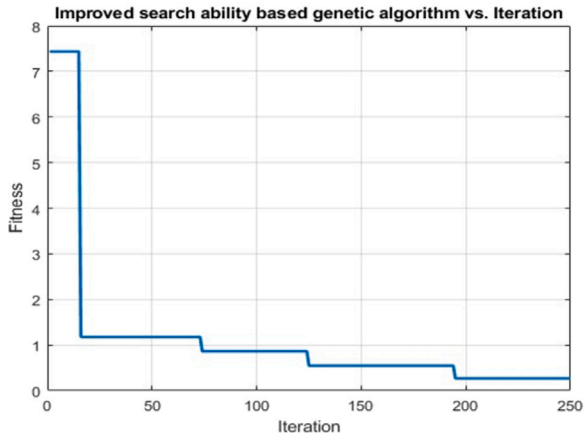

Fig. 5. Feature Selection ability of the proposed IGA with respect to iteration.

Fig. 5, indicting the performance of the IGA in context to the minimization of fitness ranges and the iteration rages of the proposed algorithm. The effective performance of the IGA aids in effectual setting of the lower and the upper boundaries for the attack classification occurring in the TON-IoT dataset. Further, the efficacy of the model are unveiled by comparing them with the state-of-art approaches and are deliberated in the following sub-section. Fig. 6, Indicates the training graph of the model proposed in the study. This is indicated with respect to the number of epoch. Hence, the proposed model is executed with 10 epochs. Then, the initial learning rate is selected based on the grid search or hyperparameter tuning method. After that the learning rate is saturated. Both the accuracy and the loss plot are depicted in of the proposed model.

Fig. 7, Indicates the overall performance metrics outcomes of the proposed model in terms of their accuracy, precision and the overall recall rates. This is used in evidencing the performance of the model behavior in terms of classifying the attack and non-attack occurring in the TON-IoT dataset.

The statistical results is given below.

ADF Statistic: 3.1451856893067296

n_lags: 1.0

p-value: 1.0

Critical Values: 1%, −3.465620397124192

This shows that the critical value is 1% and ADF statistics is 3.1451856893067296.

Fig. 8, indicating the unique values which are predicting by the proposed model in terms of performing binary classification as 0 and 1 indicating the attack and the non-attack present in the TON-IoT dataset. Whereas, Fig. 7. Indicates the performance metrics plot of the proposed model such as Accuracy rates, precision and the recall ranges of the proposed model. The outcomes from the model depicted the effective working of the model showing an overall accuracy range of 99.80%. Moreover, the overall recall and range of the model has been higher with a range of 99% and 99.4% correspondingly.

From, Fig. 9, indicating the overall performance of the model in aspects of several performance metrics such as the accuracy rates, precision and the overall F1-score rates are depicted using bar graph.

4.4. Performance metrics

While assessing the DL models for classification, then confusion matrix oriented metrics are typically intricate. Furthermore, the confusion matrix provides the relation among the prediction of class labels of the given input image and also provides the true class label for the image. Moreover, in AI-based classifications, several conditions can ascend at the output layer of the model. Further, these conditions are captured by four metrics such as TP, TN, FP and FN.

Correspondingly, estimation of an image classifier can be achieved through performance metrics namely accuracy, recall, precision and F1 score. Moreover, the accuracy is the ratio of precise predictions done by the model and it is evaluated as the degree of exact prediction by the entire amount of predictions. Then, the recall is a degree that is used to calculate the ability of model to identify entire positive samples and it is evaluated as the quantity of true positive predictions by actual positive samples. One more metrics is precision, where the ability of the model is measured to detect positive instances and it is obtained by dividing the degree of positive predictions to the aggregated positive predictions. The fourth metrics is F1 score, where the harmonic mean of recall combined with precision is utilized in balancing precision and recall at the time of conflict. Then, the arithmetical representation of these measures are expressed and it is as follows:

$$Accuracy(A) = \frac{TP + TN}{(TP + FP + FN + TN)} \tag{21}$$

$$Recall(R) = \frac{TP}{TP + FN} \tag{22}$$

$$Precision(P) = \frac{TP}{TP + FN} \tag{23}$$

$$F - 1\ Score = \frac{2 * (Precision * Recall)}{Precision + Recall} \tag{24}$$

Table 2
Comparison of ACBSLTM model with and without IGA.

	With Improved Genetic Algorithm (IGA)	Without Improved Genetic Algorithm (IGA)
ACBSLTM model	99.82	80.2

4.5. Performance analysis

The performance analysis of the proposed model are calculated by confusion matrix of FNR (False Negative Rate) and FPR (False Positive Rate). Confusion matrix refers to the table, which is used to define the performance of classification algorithm. Fig. 8 shows the confusion matrix of the proposed model.

From Fig. 10, the actual and predicted labels have values of false negative, false positive, true positive and true negative. The value of FNR is 0.0238 and the value of FPR is 0.0196. When compared with existing models, FNR and FPR values have resulted better performance.

In existing studies, several models have been proposed with the inclusion of CNN, Bi-STM and AM. Also, ACBSLTM model has been proposed in existing studies without the inclusion of IGA that have resulted in less accuracy. But, the proposed model has the combination of CNN, Bi-STM and AM with the inclusion of IGA. This results better performance when compared to the other existing models. The comparison of ACBSLTM model with and without IGA is described in the Table 2.

Fig. 11 shows the comparison of ACBSLTM model with and without IG algorithm. The above figure clearly shows that the ACBSLTM model shows better performance while it is combined with improved genetic algorithm than without improved genetic algorithm. This proves that the proposed model confers better accuracy.

4.6. Comparative analysis

Some of the suitable existing approaches have been compares to the projected model for validating their outperformance in aspects of unveiling the proposed model efficacy are discussed in the respective section.

From Fig. 12, The comparison of various DL based models have been considered and are compared in context to the various performance

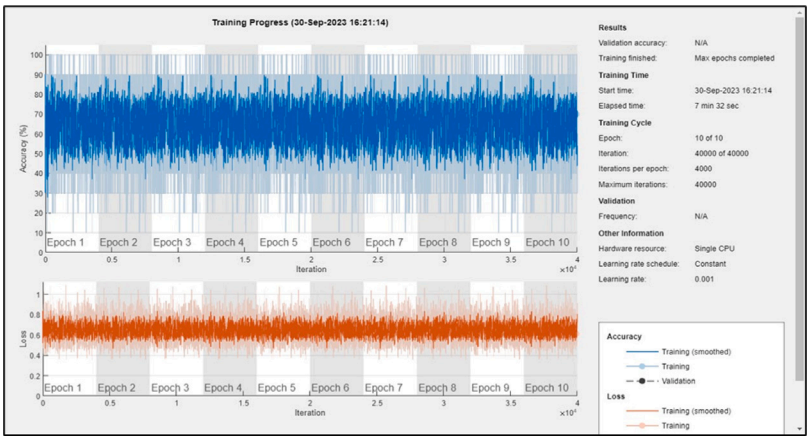

Fig. 6. Training and loss plot in context to epochs.

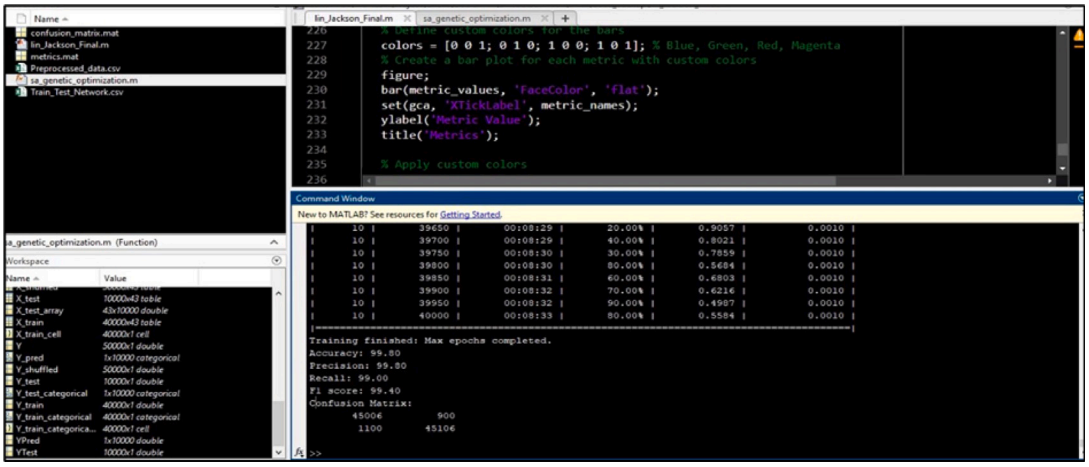

Fig. 7. Overall Performance metrics outcome of the proposed model.

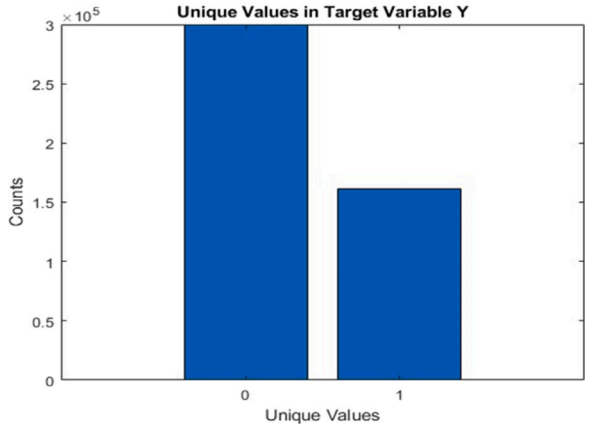

Fig. 8. Target variable selection using the proposed model.

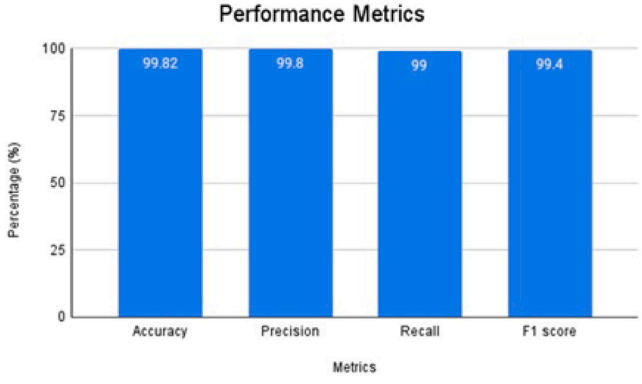

Fig. 9. Outcome Plots for the proposed model upon attack detection in TON-IoT dataset.

measuring metrics. Though, the KNN Model have been comparatively better in producing effective results in performing the attack detection and classification, the model is unable to make an effective attack detection and classification once if the model is elevated and when used with complex dataset. The model is able to perform well only using the baseline models and dataset approaches. This unveils the effectiveness of the proposed approach showing an overall accuracy and the precision rate of 99.8 and with a recall rate of 99

Concurrently, from the Fig. 13, the accuracy ranges are compared with the suggested model where, the proposed model has achieved higher accuracy rates. Over the comparison of accuracy ranges, the KNN model tends to be better performing than the other DL based models, which are even considered as better model for performing the attack detection and classification. Though, the proposed model is 0.7 times comparatively higher than the KNN model.

From, the Fig. 14, Which is compared with the model performing the standardization and the heterogeneity of the attack types in the IoT,

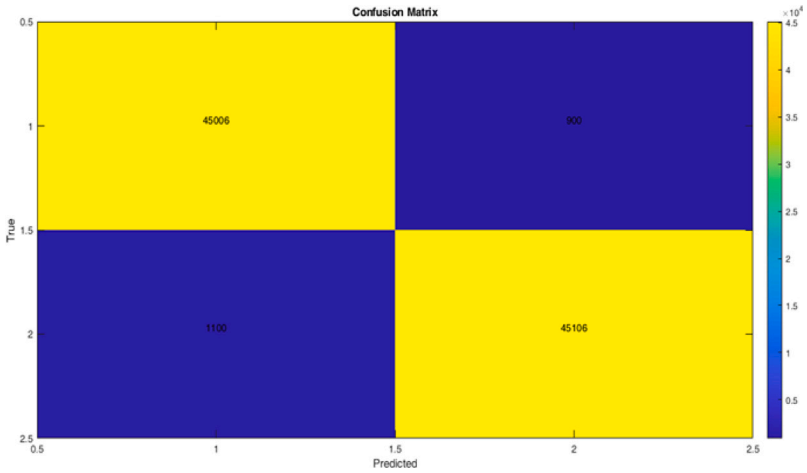

Fig. 10. Confusion matrix for existing model vs. proposed model.

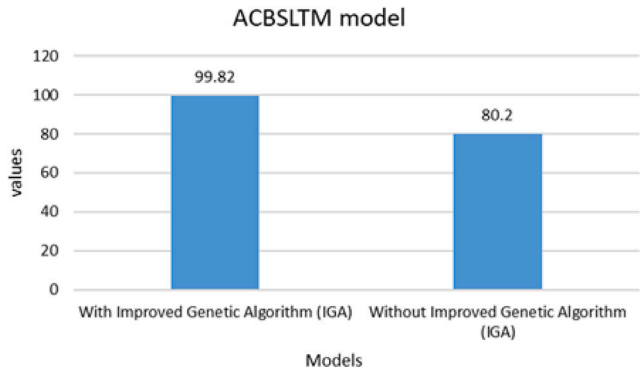

Fig. 11. Comparison of ACBSLTM model with and without IGA — Graphical Representation.

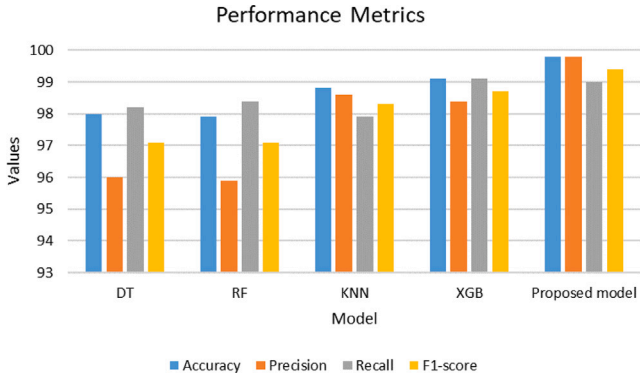

Fig. 12. Comparison of Proposed model and state-of-art approaches in context to performance metrics (Gad et al. 2022).

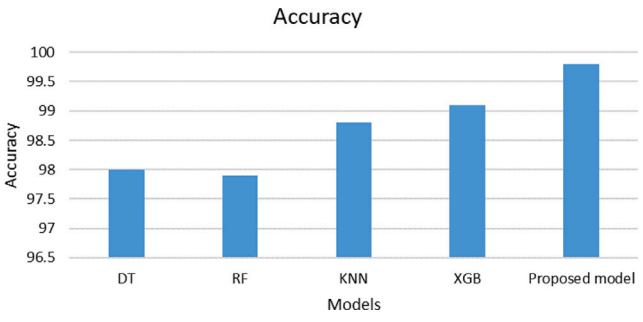

Fig. 13. Comparison of proposed an existing approach in terms of accuracy rates. (Gad et al. 2022).

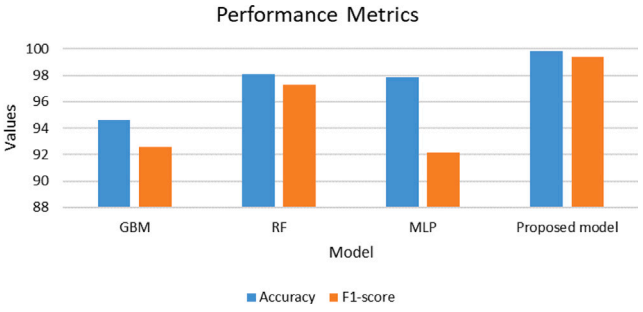

Fig. 14. Comparison of Proposed model and state-of-art approaches in context to Accuracy and F1-score (Booij et al. 2021).

with the proposed approach, the comparison have been done based on both the accuracy and the F1-score rates, though, the model compared with RF having higher ability to achieve increased rates of accuracy and he F1-score rates, and GBM model being a lower performing approach achieving an overall accuracy rate of 94.6% and 92.5% only. Thus, when compared to other DL models the proposed model achieved an overall increased ranges in scales of 4.2–1.2% higher than the other suggested models.

The model comparison have been done using the network intrusion detection and the classification which are used upon the heterogeneous and hybrid-forms of meta-heuristic data, for the detection of the cyber-attacks in the IoT environments. The comparison have been done based on the feature selection mechanism from the dataset for an accurate intrusion detection from the data as shown in Fig. 15. Though, the SVM model is capable for performing the higher ranges of feature selection, the proposed model is comparatively higher and are well-performing in aspects of feature selection using the improved GA algorithm achieving the accuracy range of 99.8%, with an overall feature selection count of only 13. This is all due to the limited convergence capability of the proposed IGA, which has better searching ability of features within specified and limited number of iteration due to the addition of weights in the conventional GA algorithm. This made the algorithm to search and find the appropriate features from the model for a better working and classification.

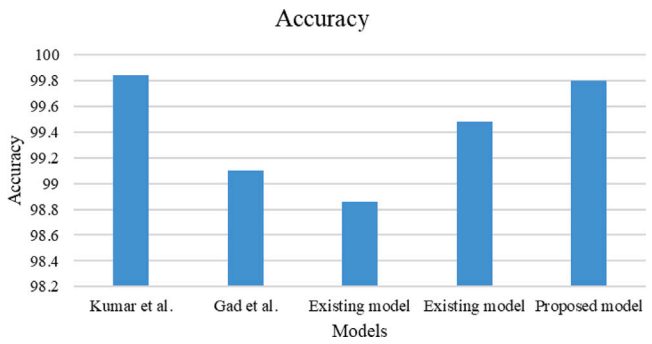

Fig. 15. Comparison of Proposed model and existing approaches in terms of Accuracy (Dey et al. 2023b).

Discussion

The IoT is collection of things, where common forms of physical things and communication using the synthetized data are connected to internet. The IoT networks are prone to increased vulnerability and security breaches, as the population growth intensifies. The security attacks and threat to the data ate popular to the severe dangers provided by the IoT security. Many researchers though intended in detecting and in classifying the attack occurring in the data, these approaches laid back in providing the appropriate classification of the dataset attack rather them providing only the attack detection. Thus, the proposed study makes use of meta-heuristic approaches which are improved and DL models for the feature selection and classification of the attack occurring on the data. The proposed model has achieved and overall accuracy and precision rate of 99.8%, which is one of the markable outcomes from the model performing attack classification. The proposed model outperformed the other ML and DL approaches participating in the attack detection involved in detecting the cyber-attacks to the data, in the IoT networks. Though the standardization of the features and the detection of attack with their types are classified in the existing approaches, the proposed study has outperformed the models and achieved about 2.1–0.8 times greater than the existing models in terms of accuracy. Whereas, in terms of F1-score rates the proposed model is comparatively 3.3–2.3 times higher than the existing models. Moreover, the proposed model is compared with the advanced transformer model like BERT, GPT or the variants that have exposed imposing performance in classification model. However, the transformer models have the possibility to capture long-term dependencies and related data progressively, but its efficiency is less when compared with the proposed model. n addition to that model can significantly enhance the security for IoT devices by enabling real-world anomaly findings, contextual security and unified integration with prevailing systems. It aids in identifying the anomalous patterns, dynamically adapt security measures and ensure secure data processing. With a focus on scalability and resources effectiveness, the proposed model provides an effective performance in IoT networks and reduces risks like unauthorized access with data breaches.

In addition to that deploying the ML models in IoT have latency, scalability and integration issues. Where, low latency is required for real-time implementation and achieves a lightweight computations and optimizations like multi-threading or acceleration in GPU. On the other hand, scalability is critical to manage data generated by IoT systems, needs the models to scale components such as feature extraction and also classification separately. However, integration issues involves ensuring interoperability and compatibility over various IoT eco-systems and enables interrupted communication and incorporation in resource-constrained situations.

5. Conclusion

DL networks is powerful tools in various domains, such as intrusion and attack detection and classification. Despite their exceptional performance, the models have shown quite notable enhancements to the inputs and the attack occurring to various data under various aspects. DL based models such as CNN and Bi-LSTM are highly adapted in the current practical systems which are more advantageous in detecting and in classifying the attack occurring in the network data. Combining CNN and Bi-LSTM with Attention Mechanism can leverage the strengths of different deep learning architectures. CNNs are excellent for feature extraction from structured data, while Bi-LSTM with attention can capture temporal dependencies in sequential data. Hence, the proposed system used Meta-heuristic approach for the process of feature selection to measurable enhance the accuracy and the detection rates of the model. Followed by, the classification of the attack and non-attack over the data are achieved by the hybrid ACBSLTM model. The proposed model when estimated for their performance using the probabilistic metrics, the outcomes were more effective towards the attack classification. The overall accuracy rates of the model were comparatively higher than the other state-of-art approaches intended in performing attack detection and attack type classification. The overall outcomes such as the accuracy and the precision rates are markable in ranges of 99.8%, where the recall and the F1-score are also in the ranges of 0.99 and 99.4% respectively. Nevertheless, the proposed model has an additional advantage such as less model complexity, less training time of the model and higher accuracy of detection rates. Thus, on a real time application, the model can also be applied to higher volume dataset. Moreover, the model can be used to detect the real time data intrusion and attack occurring on the network and other data.

Limitation

Though, the model is with several advantages, some of the limitations have been encountered to the respective model. The property of attack detection to the heterogeneous forms of data makes the model to enhance time for both the model training and for model validation. Ideally using the heterogeneous forms of datasets, the unsupervised models for the attack selection and the classification makes the model to be less developed and behave when applied to real time environment. The performance of the baseline techniques can be improved by advanced parameter optimization approaches. This can result in further Optimization of the model and in obtaining superior outcomes. Moreover, the proposed model fails to perform better in cases of applying them to the other network dataset and other higher forms of meta-heuristic techniques. In future, the proposed model can be combined with other transformer models to control the corresponding efficiency and improves the performance of attack classification model. The implementation of incremental IDS for batch learning problems.

The proposed hybrid model remains effectual but it has some limitations, containing its reliance on the TON-IoT dataset that can limit scalability and generalizability. In addition to that complexity can obstruct interpretability for end-users. In future, it is to optimize computational efficacy, endorse the model with various datasets and it can be combined with Explainable AI (XAI) methods to enhance the interpretability and overall utilization.

CRediT authorship contribution statement

Yifan Fang: Methodology, Data curation. **Yingwei Jia:** Methodology, Data curation, Software. **Guozheng Bai:** Writing – review & editing. **Rao Hong:** Formal analysis, Validation, Writing – original draft. **Xia Linglin:** Supervision, Conceptualization, Project administration. **Ghulam Mohi-ud-din:** Formal analysis, Validation, Writing – original draft. **Chen Ai:** Software, Writing – original draft. **Muhammad**

Asim: Software, Writing – review & editing. **Zhou Li:** Software, Writing – review & editing.

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.

Data availability

No data was used for the research described in the article.

References

Abusitta, A., Silva De Carvalho, G., Abdel Wahab, O., Halabi, T., Fung, B., & Al Mamoori, S. (2023). Deep learning-enabled anomaly detection for IoT systems. *SSRN Electronic Journal*, *21*, Article 100656. http://dx.doi.org/10.2139/ssrn.4258930.

Akshaya, V., Mandala, V., Anilkumar, C., Vishnuraja, P., & Aarthi, R. (2023). Security enhancement and attack detection using optimized hybrid deep learning and improved encryption algorithm over Internet of Things. Article 100917.

Alhanaya, M., & Hamdi Ateyeh Al-Shqeerat, K. (2023). Performance analysis of intrusion detection system in the IoT environment using feature selection technique. *Intelligent Automation & Soft Computing*, *36*(3), 3709–3724. http://dx.doi.org/10.32604/iasc.2023.036856.

Almarshdi, R., Nassef, L., Fadel, E., & Alowidi, N. (2023). Hybrid deep learning based attack detection for imbalanced data classification. *Intelligent Automation & Soft Computing*, *35*(1), 297–320. http://dx.doi.org/10.32604/iasc.2023.026799.

Alwasel, B., Aldribi, A., Alreshoodi, M., Alsukayti, I., & Alsuhaibani, M. (2023). Leveraging graph-based representations to enhance machine learning performance in IIoT network security and attack detection. *Applied Sciences*, *13*(13), 7774. http://dx.doi.org/10.3390/app13137774.

Chaganti, R., Suliman, W., Ravi, V., & Dua, A. (2023). Deep learning approach for SDN-enabled intrusion detection system in IoT networks. *Information*, *14*(1), 41. http://dx.doi.org/10.3390/info14010041.

Chishti, F., & Rathee, G. (2023). ToN-IOT set: Classification and prediction for DDoS attacks using AdaBoost and rUSBoost. In *2023 3rd international conference on advance computing and innovative technologies in engineering* (pp. 2842–2847). IEEE, http://dx.doi.org/10.1109/icacite57410.2023.10183100.

De Souza, C., Westphall, C., & Machado, R. (2022). Two-step ensemble approach for intrusion detection and identification in IoT and fog computing environments. *Computers & Electrical Engineering*, *98*, Article 107694. http://dx.doi.org/10.1016/j.compeleceng.2022.107694.

Dey, A., Gupta, G., & Sahu, S. (2023). Hybrid meta-heuristic based feature selection mechanism for cyber-attack detection in IoT-enabled networks. *Procedia Computer Science*, *218*, 318–327. http://dx.doi.org/10.1016/j.procs.2023.01.014.

Ding, W., Abdel-Basset, M., & Mohamed, R. (2023). DeepAK-IoT: An effective deep learning model for cyberattack detection in IoT networks. *Information Sciences*, *634*, 157–171. http://dx.doi.org/10.1016/j.ins.2023.03.052.

Elsayed, R., Hamada, R., Abdalla, M., & Elsaid, S. (2023). Securing IoT and SDN systems using deep-learning based automatic intrusion detection. *Ain Shams Engineering Journal*, *14*(10), Article 102211. http://dx.doi.org/10.1016/j.asej.2023.102211.

Fraihat, S., Makhadmeh, S., Awad, M., Al-Betar, M., & Al-Redhaei, A. (2023). Intrusion detection system for large-scale IoT NetFlow networks using machine learning with modified Arithmetic Optimization Algorithm. *Internet of Things*, *22*, Article 100819. http://dx.doi.org/10.1016/j.iot.2023.100819.

Hossain, M., & Islam, M. (2023). Ensuring network security with a robust intrusion detection system using ensemble-based machine learning. *Array*, *19*, Article 100306. http://dx.doi.org/10.1016/j.array.2023.100306.

Jarjis, A., Al Zubaidi, N., & Pehlivanoglu, M. (2023). *Cyber attacks classification on enriching IoT datasets, vol. 9*.

Karamollaoğlu, H., Yücedağ, İ., & Doğru, İ. (2022). *A hybrid PCA-MAO Based LSTM model for intrusion detection in IoT environments*. Research Square Platform LLC, http://dx.doi.org/10.21203/rs.3.rs-2357212/v1.

Kethineni, K., & Gera, P. (2023). Iot-based privacy-preserving anomaly detection model for smart agriculture. *Systems*, *11*(6), 304. http://dx.doi.org/10.3390/systems11060304.

Khanday, S., Fatima, H., & Rakesh, N. (2023). Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks. *Expert Systems with Applications*, *215*, Article 119330. http://dx.doi.org/10.1016/j.eswa.2022.119330.

Kumar, P. J., & Neduncheliyan, S. (2024). A shark inspired ensemble deep learning stacks for ensuring the security in internet of things (iot)-based smart city infrastructure. *International Journal of Computational Intelligence Systems*, *17*, 243.

Lazzarini, R., Tianfield, H., & Charissis, P. (2023). *A stacking ensemble of deep learning models for IoT network intrusion detection*. Elsevier BV, http://dx.doi.org/10.2139/ssrn.4412746.

Liu, L., Wang, P., Lin, J., & Liu, L. (2020). Intrusion detection of imbalanced network traffic based on machine learning and deep learning. *IEEE Access*, *9*, 7550–7563. http://dx.doi.org/10.1109/access.2020.3048198.

Madhu, B., Venu Gopala Chari, M., Vankdothu, R., Silivery, A., & Aerranagula, V. (2023). Intrusion detection models for IOT networks via deep learning approaches. *Measurement: Sensors*, *25*, Article 100641. http://dx.doi.org/10.1016/j.measen.2022.100641.

Mahalingam, A., Perumal, G., Subburayalu, G., Albathan, M., Altameem, A., Almakki, R., et al. (2023). ROAST-IoT: A novel range-optimized attention convolutional scattered technique for intrusion detection in IoT networks. *Sensors*, *23*(19), 8044. http://dx.doi.org/10.3390/s23198044.

Moustafa, N., Koroniotis, N., Keshk, M., Zomaya, A., & Tari, Z. (2023). Explainable intrusion detection for cyber defences in the Internet of Things: Opportunities and solutions. *IEEE Communications Surveys & Tutorials*, *25*(3), 1775–1807. http://dx.doi.org/10.1109/comst.2023.3280465.

Othman, T., & Abdullah, S. (2023). An intelligent intrusion detection system for internet of things attack detection and identification using machine learning. *ARO-the Scientific Journal of Koya University*, *11*(1), 126–137. http://dx.doi.org/10.14500/aro.11124.

Poonkuzhali, S., Shobana, M., & Jeyalakshm, J. (2023). A deep transfer learning approach for IOT/IIOT cyber attack detection using telemetry data.

S. Bajpai, K. S., & Chaurasia, B. K. (2024). A hybrid meta-heuristics algorithm: Xgboost-based approach for ids in iot. *SN Computer Science*, *5*, 1–16.

Sadhwani, S., Manibalan, B., Muthalagu, R., & Pawar, P. (2023). A lightweight model for DDoS attack detection using machine learning techniques. *Applied Sciences*, *13*(17), 9937. http://dx.doi.org/10.3390/app13179937.

Sándor, J., Nagy, R., & Buttyán, L. (2023). Increasing the robustness of a machine learning-based IoT malware detection method with adversarial training. In *Proceedings of the 2023 ACM workshop on wireless security and machine learning*. ACM, http://dx.doi.org/10.1145/3586209.3591401.

Shyaa, M., Zainol, Z., Abdullah, R., Anbar, M., Alzubaidi, L., & Santamaría, J. (2023). Enhanced intrusion detection with data stream classification and concept drift guided by the incremental learning genetic programming combiner. *Sensors*, *23*(7), 3736. http://dx.doi.org/10.3390/s23073736.

Srivastav, D., & Srivastava, P. (2023). A two-tier hybrid ensemble learning pipeline for intrusion detection systems in IoT networks. *Journal of Ambient Intelligence and Humanized Computing*, *14*(4), 3913–3927. http://dx.doi.org/10.1007/s12652-022-04461-0.

Thulasi, T., & Sivamohan, K. (2023). LSO-CSL: Light spectrum optimizer-based convolutional stacked long short term memory for attack detection in IoT-based healthcare applications. *Expert Systems with Applications*, *232*, Article 120772. http://dx.doi.org/10.1016/j.eswa.2023.120772.

Vitorino, J., Praça, I., & Maia, E. (2023). Towards adversarial realism and robust learning for IoT intrusion detection and classification. *Annals of Telecommunications*, *78*(7–8), 401–412. http://dx.doi.org/10.1007/s12243-023-00953-y.

Yigit, Y., Chrysoulas, C., Yurdakul, G., Maglaras, L., & Canberk, B. (2023). Digital twin-empowered smart attack detection system for 6G edge of things networks. In *2023 IEEE globecom workshops (GC wkshps)*. IEEE, http://dx.doi.org/10.1109/gcwkshps58843.2023.10465218.