Kepes
http://scholopress.com/kepes-journal

2023 Volume 21 Issue 3 pp. 490-504

Evaluation on Bot-IoT Dataset Enabled Reducing False Alarm Rate for IoT Threats

Umar Audi Isma'ila [1], ***Kamaluddeen Usman Danyaro** [1], **Mohd Fadzil Hassan** [1], **M.S. Liew** [2], **Umar Danjuma Maiwada** [1,3], **Aminu Aminu Muazu** [1,3]

[1]Computer and Information Sciences Department, Faculty of Science and Information Technology, Universiti Teknologi PETRONAS, Perak 32610, Malaysia

[2]Civil and Environmental Engineering Department, Faculty of Engineering, Universiti Teknologi PETRONAS, Perak 32610, Malaysia

[3]Computer Sciences Department, Faculty of Natural and Applied Science, Umaru Musa Yar'adua University Katsina, Nigeria

Abstract

The growth of Internet of Things (IoT) devices has been increasing day by day. Its widespread adoption is significantly simplifying our daily tasks. However, the increasing number of these interconnected IoT devices has led to a many insecurity vulnerabilities, resulting in higher operational expenses. Consequently, IoT devices are experiencing a notable rise in False Alarm Rate (FAR). Therefore, this study intends to explore the application of Anomaly-based Intrusion Detection System (A-IDS), specifically focusing on the utilization of Bot-IoT dataset. First, we deliver a description of the Bot-IoT dataset and evaluate its potential in A-IDS enabled reducing FAR. We introduce a new model termed *TrigFAR Model*. In which TrigFAR utilized lightGBM classifier and trained on two sets of Bot-IoT dataset, namely 10-best features set and full features set. This is to enable the reduction of high FAR for IoT threats. The results obtained demonstrate that TrigFAR on Bot-IoT dataset overcome the performance of other publicly and real-world A-IDS datasets. While in terms of reducing FAR for IoT we achieved the highest accuracy in detecting attacks of 100% with 0% FAR on the full features set. Whereas achieving 99% accuracy and 0.42% of FAR on 10-best features set. Lastly, we discuss the results and identify areas for future study on IoT threats while maintaining the minimum FAR.

Keywords: False alarm rate, Bot-IoT dataset evaluation, Anomaly-based intrusion detection, LightGBM classifier, IoT device threats

1. Introduction

Significant emphasis is placed on the information derived from IoT devices. These IoT devices are data-driven insights, which drive our personalized experiences, smart cities, industrial efficiency, healthcare improvements, and environmental monitoring. This leads to the ongoing progression and widespread use of IoT devices by individuals and firms across the globe (Rejeb et al., 2022; Zohourian et al., 2023). Because of this, the number of attacks on IoT devices has hypothetically increased (Otoum, Liu, & Nayak, 2022). This is intensified by the fact that many IoT devices are designed to be always connected to the internet, which means that they are constantly transmitting data and potentially exposing themselves to IoT attacks.

*Corresponding author

DOI https://doi.org/10.5281/zenodo.7936583#107

Meanwhile, cybersecurity has extensively utilized Machine Learning (ML), particularly in the development of anomaly-based intrusion detection systems (A-IDS) (Sivanantham et al., 2019). These systems employ classification techniques to predict discrete values, such as normal or anomalous outcomes by analyzing legitimate user behavior data using statistical tests (Jamil & Rahman, 2022). Additionally, network traffic generated by Smart IoT devices flows in both directions (Otoum et al., 2022), from the data collection device to the cloud server then to authorized entities over the internet (Sultan et al., 2019). For instance, a smart home security system collects data from sensors and then sends it to the cloud for A-IDS analysis.

On the other hand, in this cloud processing environment, by verifying each connection of the IoT device it can be resource-intensive, leading to higher operational costs, especially when the number of connections increases (Martins et al., 2022). So, this process incurs excessive costs and poor performance of attacks detection model, thus could result to high false alarm rate (FAR) (Khraisat et al., 2019). Meanwhile, given the severity and volume of data shared by these smart devices in IoT scenarios, the performance of the detection model can severely be affected to report many FAR (Khraisat & Alazab, 2021). Therefore, to address the issue of high FAR for these IoT threats. Firstly, on the publicly known datasets for A-IDS highlight specific limitations (Yang et al., 2022). These limitations involve a limited dataset size and lack of diversity to IoT scene. Therefore, we will examine the statistical analysis of Bot-IoT dataset (Koroniotis et al., 2019) and justify its adequacy in training A-IDS model while specifically considering it to be the right potent for reducing the high FAR for IoT devices. Although several works (Faysal et al., 2022; Saba et al., 2022; Saif et al., 2022) have demonstrated remarkable effectiveness for A-IDS model for IoT devices, there are still certain aspects of high FAR in this context that require further attention in academics. According to the literature available, no previous research has considered using this Bot-IoT dataset in enabling reducing the high FAR for IoT. So, the following are specifically the primary contributions of this article.

- To analyze Bot-IoT dataset, while evaluating the consistency of employing of Bot-IoT dataset on creating A-IDS model for IoT threats.
- To experiment on Bot-IoT dataset in developing new A-IDS model, while aiming on reducing the high FAR for IoT threats.
- To establish a reference point for evaluating its performance in comparison to earlier studies available in the present literature. We will consider studies with different diverse datasets and determine whether our study's performance is significant in reducing the FAR for IoT or not.

The remaining sections of this study are organized in the following manner. Section 2 provides a brief background of study and related works. Section 3 provides analysis of Bot-IoT dataset on creating A-IDS model for IoT threats and proposed approach of reducing FAR for IoT devices. Section 4 presents the experimental result and discussion of result. Finally, some concluding remarks are introduced in Section 5.

2. Related Works

In this section, we provide an overview of relevant literature regarding IoT threats, A-IDS methods, and the influence of A-IDS for FAR on IoT devices.

2.1 IoT Devices Threats

The fundamental components of the IoT ecosystem consist of IoT devices (S. Bansal & Kumar, 2020). IoT-edge devices refers to Internet-connected devices located at the periphery of a network often nearer the data source (Wang et al., 2018). Moreover, these devices are commonly utilized to collect, process, and transmit data from sensors and actuators in real-time. They are often lightweight, low-power devices that can be quickly placed in a variety of settings. Moreover, they are also capable of carrying out activities including data analysis, storage, and interaction with some other devices (Abreha et al., 2022). This allows the devices to

form decisions and actions on the data they collect (Al Mogbil et al., 2020). However, IoT device come in a varied range of examples such as smart thermostats, smart homes devices, industrial control systems, smart agriculture devices, and smart transportation devices (Huh et al., 2017; Manab et al., 2021).

Meanwhile, IoT-edge devices continue to produce more data, as these devices are increasing in our daily life, they becoming more essentials (Shahab et al., 2022). Nevertheless, these devices are exposed to many cyber threats, the exposures not only have the potential to compromise the data collected by the devices, but also to destroy the physical systems, causing economic loss, harm to individuals, and even environmental degradation. Moreover, the top seven most frequent attacks are all DoS attacks, with DDoS attacks coming in first. After that, there were attacks such as Traffic Analysis, Man-in-the-Middle, Sybil, Spoofing, and Routing (Albalawi et al., 2022; Khan et al., 2022).

Consequently, it can be observed that there is a notable absence of built-in security contributions in the design of these devices (Atlam et al., 2020; Buja et al., 2022). This is primarily because many of them exhibit a similar approach, utilize common connection, and network protocols, and share certain distinctive attributes such as sensing, self-configuration, connectivity, and heterogeneity (Patel, Patel, & Scholar, 2016). These factors collectively render the devices vulnerable to various forms of attacks. However, to address these challenges, the strong protection key that is particularly made for IoT-edge devices, is keeping track of the data produced by the devices while consistently checking them for unusual activity, in which is widely accomplished by intrusion detection system (IDS).

2.2 A-IDS Method

An Intrusion Detection System (IDS) is a security tool that detects malicious activities and violations of rules in a network (Bhattacharya et al., 2020; Fernandes et al., 2019). Among the types of IDS, there is the anomaly-based IDS (A-IDS) (Agrawal et al., 2022), which uses ML techniques to identify unusual activity, while the signature-based IDS is limited to a specific set of signatures (Agrawal et al., 2022; Khraisat et al., 2019). A-IDS can detect both known and unknown attacks. Moreover, the A-IDS method collects data on normal user behavior and applies statistical tests to determine whether a behavior is acceptable or not, making it effective in detecting new attacks.

Meanwhile, there are numerous ways that A-IDS models can operate. Certain models employ unsupervised learning techniques to detect intrusions that deviate from normal behavior (Chatterjee & Ahmed, 2022), while other models utilize supervised learning methods to identify well-known attack patterns (Alsoufi et al., 2021). Furthermore, there are models that leverage techniques such as neural networks (NN) or clustering (Fernandes et al., 2019). However, A-IDS still pose challenges for both industry and academia in determining which of the techniques to adopt.

2.3 Impact of A-IDS for High FAR on IoT Devices

It is determined to learn that researchers have successfully deployed and verified the effectiveness of the A-IDS model using various methods. In this regard, to ensure the validity of the model, the modeling algorithm employed plays a crucial role in combining model updates. Though, choosing the right algorithm is vital as it impacts the trade-off between model accuracy. Moreover, determining the accuracy of the model is an essential metric that helps assess its performance. It is also vital to understand the value of FAR as this can provide insights into its strengths and limitations, as well as how it can be improved for new models. Therefore, we are determined to consider the mentioned approaches in summarizing the A-IDS models. Thus, the following authors deployed models that are developed for A-IDS models to IoT threats.

Firstly, (Khraisat et al., 2019) conducted their study using the Bot-IoT dataset and employed the one-class SVM modeling algorithm. With an impressive accuracy of 99.97%, their contribution involved presenting a stacking ensemble method to improve the detection accuracy. This method enhanced the model's ability to

identify and classify IoT botnet attacks. However, the specific FAR was not provided. While (Saba et al., 2022) focused their research on the NID dataset and proposed a CNN-based model to study traffic across the IoT. This results with an accuracy of 95.5% and their model aimed to predict possible intrusions behaviors. Thus, in leveraging convolutional neural networks, the model effectively analyzed IoT traffic data, which enables the detection of potential security threats. However, a FAR was not provided.

Meanwhile, (Ge et al., 2019) worked with the Bot-IoT dataset and utilized feed-forward neural networks as the modeling algorithm, achieving an accuracy of 99%. However, their contribution involved proposing an intelligent binary and multiclass classification scheme. This scheme, implemented via feed-forward neural networks, facilitated accurate classification of distinct types of IoT traffic and the identification of potential anomalies activities. The FAR was not provided. Moreover, (Saif et al., 2022) focused on the NSL-KDD dataset and utilized a hybrid approach combining K-Nearest Neighbors (K-NN) and Decision Trees (DT) modeling algorithms. Their aim was to achieve maximum accuracy while using the least number of features. Thus, achieves an accuracy of 99.88%. This hybrid approach improved the efficiency of IDS in accurately identifying potential threats. In which the specific FAR value was not provided also.

Another sensational work (Sivanantham et al., 2019), propose a hybrid IDS that combines classification and boosting methods. The efficiency of the proposed method is evaluated using various datasets, including the Intrusion Detection Kaggle Dataset. Through extensive analysis, they observed that the Random Tree classifier yields the best average accuracy rate of approximately 99.98% while maintaining a minimal FAR of 0.12. Lastly, (Otoum et al., 2022) in their research with the NSL-KDD dataset, employed a combination of modeling algorithms including SMO, SDPN, and Deep Learning (DL) for their proposed IDS model. While the specific FAR value was not provided. Their extensive analysis demonstrated that the DL-IDS outperformed other approaches in terms of accuracy, precision, recall, and F-score. This highlighted the effectiveness of their proposed DL-IDS in emphasizing its superior performance.

One of the common limitations observed across these studies is the high FAR. However, in the context of IoT, the high FAR was due to the lack of diverse datasets for developing the model (Khraisat & Alazab, 2021; Khraisat et al., 2019). Thus, because IoT devices operate in a wide range of environments and encounter several types of network conditions and attacks. Without a diverse dataset that reflects these real-world scenes, A-IDS models for IoT may struggle to effectively detect attacks and may produce high FAR. Therefore, to improve the performance of A-IDS model in IoT, it is vital to utilize large and diverse datasets that cover the scene of IoT ecosystem. This approach would enable the A-IDS models to enhance the overall security and consistency of IoT systems.

3. Proposed System and Methodology

3.1 Evaluation Dataset

The Bot-IoT dataset (Koroniotis et al., 2019) is a publicly available dataset that simulates IoT-based botnet attacks. Moreover, it contains network traffic data generated from a simulated IoT environment that is infected with the Mirai botnet, which is a malware that targets IoT devices. Thus, the dataset was created to facilitate research on IoT-based botnet attacks and to evaluate the effectiveness of various detection and mitigation techniques (Koroniotis et al., 2019).

According to (Peterson, Leevy, & Khoshgoftaar, 2021), the dataset consists of two sets and two subsets that have distinct file format, dimension, and features. Thus, raw set and full set, then 5 percent subset and 10-best subset, respectively. All the subsets are extracted from the full set which contains roughly 73 million counts of instances (Peterson et al., 2021). Overall, it includes traffic data captured from both the botnet infected devices and the network traffic that the devices generate (Koroniotis et al., 2019). It also includes a variety of transactional network protocols, such as HTTP, TCP, and UDP, where each comprises certain attacks

count as Fig. 1 and Fig. 2 depicts. Moreover, service scanning covers some counts, as well as information theft attacks category of such keylogging and data exfiltration.

Additionally, while analyzing the dataset, the dataset is divided into several into three according to features available (Peterson et al., 2021). That is dependent features, independent features, and invalid features. However, dependent features are features that are subjective by other features in the dataset, this includes two category, and subcategory and attack features presented in Table 1. While independent features as also presented which are not subjective by other features. These are divided into standard features, standardized to have a zero mean besides unit variance, typically used to ensure consistency in modeling. For example *"sport"* and *"dport"* are standard categorical features that signify an exclusive port number series from 1 to 65,535. Secondly, calculated features which are derived from existing features through mathematical operations to capture additional patterns. For instance, *"Pkts_P_State_P_Protocol_P_DestIP"* and *"Pkts_P_State_P_Protocol_P_SrcIP"* features signify the sum of total packets for sessions in the similar connection state that have the similar source or destination IP address. Lastly, invalid features which are attributes in a dataset that are irrelevant for modelling are often removed or treated separately during data preprocessing. *"pkSeqID"* and *"seq"* are row identifiers that only comprise ordinal information.

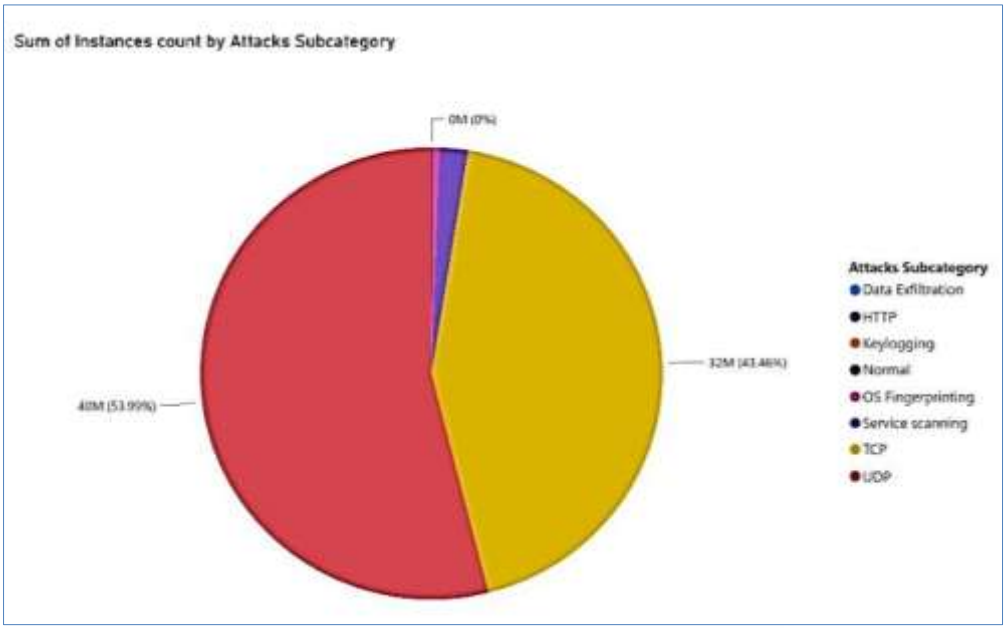

Fig. 1 Bot-IoT Dataset Subcategories Attacks Division

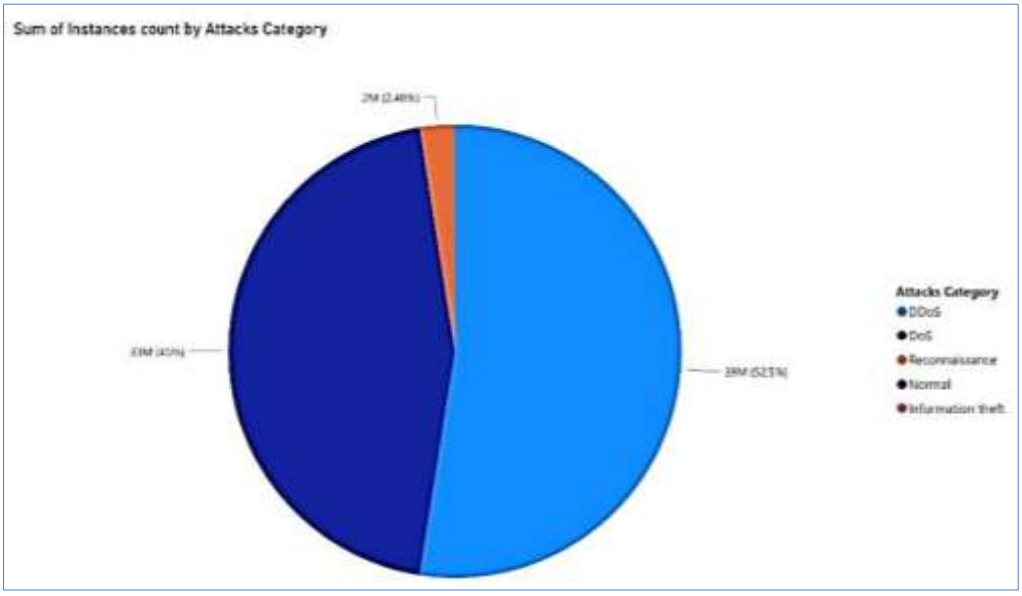

Fig. 2 Bot-IoT Dataset Categories Attacks Division

Table 1 Features Analysis of the Bot-IoT dataset

Dependent features	Category, Subcategory and Attack	
	Standard	**Calculated**
Independent features	flgs, proto, state, flgs number, proto number, state number, sport, dport, pkts, bytes, dur, spkts, dpkts, sbytes, dbytes, rate, srate, drate, mean, stddev, sum, min, and max	TnBPSrcIP, TnBPDstIP, TnP_PSrcIP, TnP_PDstIP, TnP_PerProto, TnP_Per_Dport, N_IN_Conn_P_DstIP, N_IN_Conn_P_SrcIP, Pkts_P_State_P_Protocol_P_DestIP, Pkts_P_State_P_Protocol_P_SrcIP, AR_P_Proto_P_SrcIP, AR_P_Proto_P_DstIP, AR_P_Proto_P_Sport, and AR_P_Proto_P_Dport. pkSeqID, seq, stime, ltime, saddr, and daddr.

However, Bot-IoT dataset has been used in various research studies to evaluate the effectiveness of ML algorithms in detecting internet intruders, to develop new techniques for botnet detection and to evaluate the performance of various network security solutions of such reducing FAR. Hence, Bot-IoT dataset serves as a motivating resource to explore and address this research problem of IoT device security.

3.2 Proposed TrigFAR Model

The provided pseudocode in Algorithm 1 presents a process for data preprocessing, anomaly detection using a LightGBM classifier (Ke et al., 2017) and triggering FAR. It involves steps of cleaning the data by removing irrelevant instances and filling missing values. Additionally, transforming categorical values into numeric form using LabelEncoder, then selecting relevant features in our evaluation dataset and passing the preprocessed data to the LightGBM classifier for anomaly detection. Meanwhile, we performed some actions based on the anomaly predictions of triggering an alarm and logging the anomaly event with a timestamp if the anomaly score exceeds a predefined threshold.

Algorithm 1: TrigFAR Model

Input*: TrainingSample D, LightGBM_Classifier (lgbm_model)*
Output*: A-IDS_Model*
Step 1: Data Cleaning
For each dataset Di, the following steps are performed:
Remove irrelevant, redundant, and less useful instances.
Fill missing values with either 0 or a relevant value.
Step 2: Data Transformation
If there are non-numeric or null values in the dataset:
Transform categorical features. This step is performed for all features that are in string or non-numeric form.
Apply the fit_transform() function to the LabelEncoder to transform the categorical features.
Reshape the transformed features to synchronize them with other features.
Step 3: Feature Selection
If any irrelevant or less useful features are identified within the feature set (F), they are explicitly removed from the dataset.
Step 4: Pass the preprocessed data to the lgbm_model for anomaly detection
Step 5: Get the anomaly prediction result from the lgbm_model
If anomaly score exceeds a predefined threshold:
- Trigger an alarm
- Log the anomaly event with timestamp
End

Furthermore, the high-level view of our proposed model for reducing the high FAR and detecting IoT threats was developed which includes the data preprocessing, fitting the model into lightGBM classifier and check the performance for whether the proposed model reduced high FAR before considering positive, as illustrated in Fig. 3. To prepare the Bot-IoT dataset for model development, several tasks were carried out in the preprocessing phase, such as data exploration, data cleaning, feature selection, and data splitting.

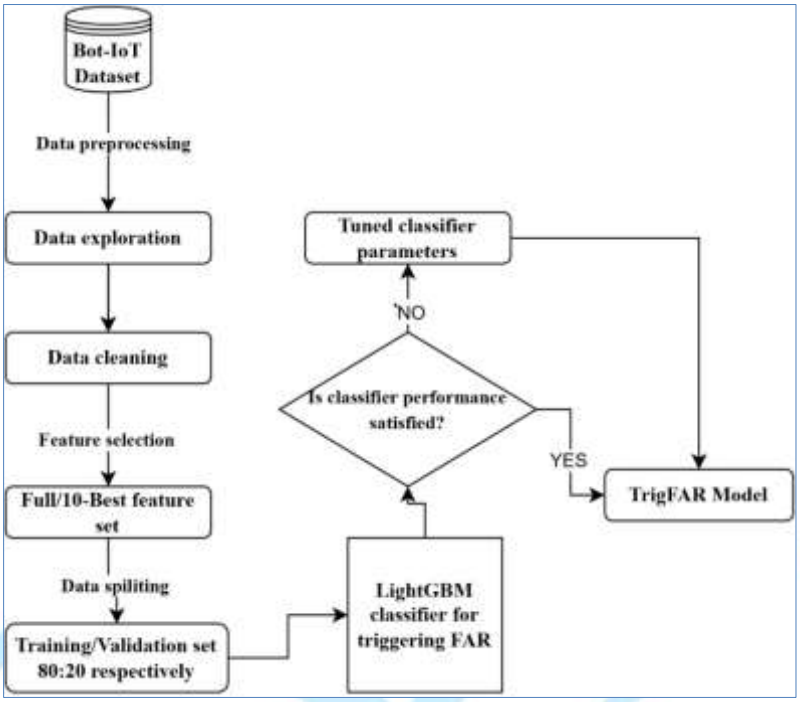

Fig. 3 Flow for the Development of TrigFAR Model

3.2.1 LightGBM classifier

LightGBM classifier (Ke et al., 2017) is proposed in this work. The fundamental concept of LightGBM is to combine multiple 'weak' learners to create a 'strong' learner. This approach is driven by two main reasons. Firstly, training 'weak' learners is easy. Secondly, combining multiple learners tends to have better generalization performance. Meaning, it can perform well on unseen data beyond the training dataset. This combination of 'weak' learners into an integrated model is a key principle behind the design of LightGBM algorithms.

The LightGBM strategies of Exclusive Feature Bundling (EFB) and gradient-based one-side sampling (GOSS), enable efficient training of large-scale data without sacrificing attack detection performance (Ke et al., 2017). Moreover, LightGBM also supports categorical features in training process, eliminating the need for complex data preprocessing tasks. The leaf-wise tree growth strategy as illustrated in Fig. 4 further enhances decision-making efficiency (Bansal & Kaur, 2018; Ke et al., 2017). Considering these benefits, we find LightGBM to be highly competitive and adopt it in evaluation of Bot-IoT dataset in reducing FAR for IoT threats.

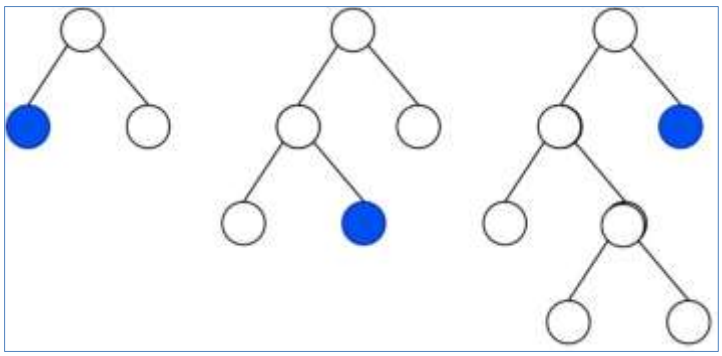

Fig. 4 Leaf-wise Tree Growth Strategy

3.3 Performance Measure

Confusion matrix is used in this work to determine evaluation metrics such accuracy, precision, recall, and F1 score. Meanwhile, (Saranya et al., 2020) studied that A-IDS could also be evaluated based FAR. Hence, the metrics for amount of True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN) predictions built by the classifier are computed using equations in Table 2. In which TP denotes instances correctly predicted as attack, TN denotes instances correctly predicted as normal, FP denotes instances falsely predicted as attack when they are actually normal; and lastly FN donates instances falsely predicted as normal when they are actually attack.

Table 2 Performance Measures

Metrics	Formula
Accuracy	$(TP + TN)/(TP + TN + FP + FN)$
Precision (Detection rate)	$TP/(TP + FP)$
Recall	$TP/(TP + FN)$
F-score	$2 * (Precision * Recall)/Precision + Recall$
False Alarm Rate (FAR)	$FP/(FN + TN)$

4. Experimental Result and Discussion

Our experiment was carried out using the Pycaret framework in the google Colab IDE. The experiments were performed on an Intel(R) Xeon(R) of 2.80GHz CPU, 64-bit OS with an 8GB RAM. In our experiments, we justified the use of 5% subset of the Bot-IoT dataset and made use of 10-best features subset and full features set for training and validation, and split it into 80% and 20% instances, respectively. Thus, it allows efficient simulation within available resource limitations while keeping a representative instance of the original data. While we set other hyperparameters of our LightGBM as boosting_type='gbdt', learning_rate=0.1, max_depth=-1, min_child_samples=20, min_child_weight=0.001, n_estimators=100, num_leaves=31. The subsection below presents the performance results of the proposed model using different schemes, followed by a detailed discussion.

4.1 Results

In this section, we explore the performance results of the proposed model, evaluated using statistical measures mentioned. These performance outcomes are presented to offer a comprehensive understanding of the model's capabilities and limitations. Thus, allowed us to gain valuable insights into how the Bot-IoT dataset performs under proposed model of enabling reducing FAR in IoT threats. We embark on an in-depth discussion, wherein we carefully analyze and interpret the findings. Moreover, we explore any potential areas for improvement and discuss potential future research in this study.

4.1.1 Features ranking on TrigFAR model for the Bot-IoT dataset

In the TrigFAR model using LightGBM classifier with the 10-best features set and full features set of Bot-IoT, feature ranking is achieved through the feature importance attribute as illustrated in Fig. 5 and Fig. 6

respectively. These attribute provides insights into the importance of each feature, aiding in identifying the most influential variables for accurate classification.

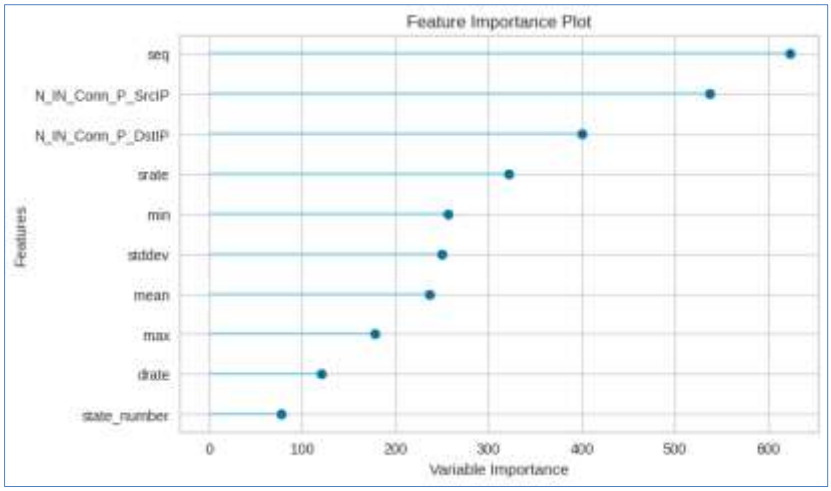

Fig. 5 Feature ranking based on information gain for 10-best features set

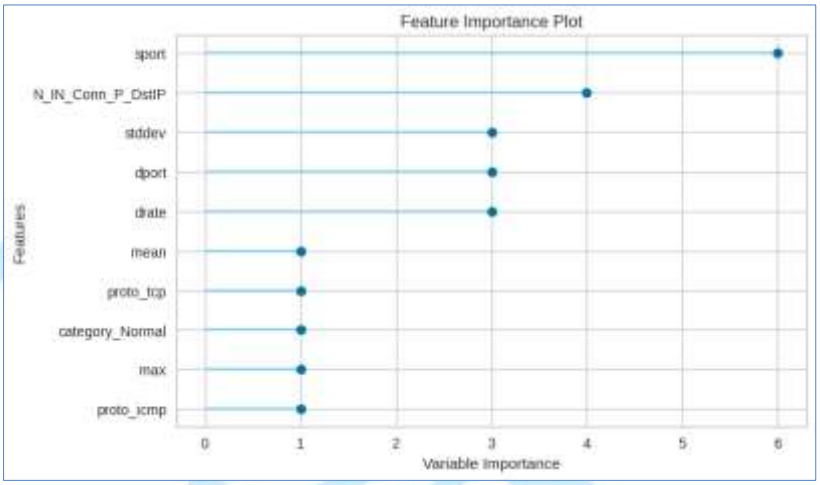

Fig. 6 Feature ranking based on information gain for full features set

4.1.2 Classification Report for TrigFAR Model

The classification report for the "attack" feature, using the 10-best features set of Bot-IoT with LightGBM classifier, shows promising results. The model achieves high precision, recall, and F1-score, indicating accurate identification of attacks as illustrated in Fig. 7 and Fig. 8 respectively for 10-best features set and full features set of Bot-IoT dataset. This performance indicates a robust ability to distinguish between normal and malicious activities.

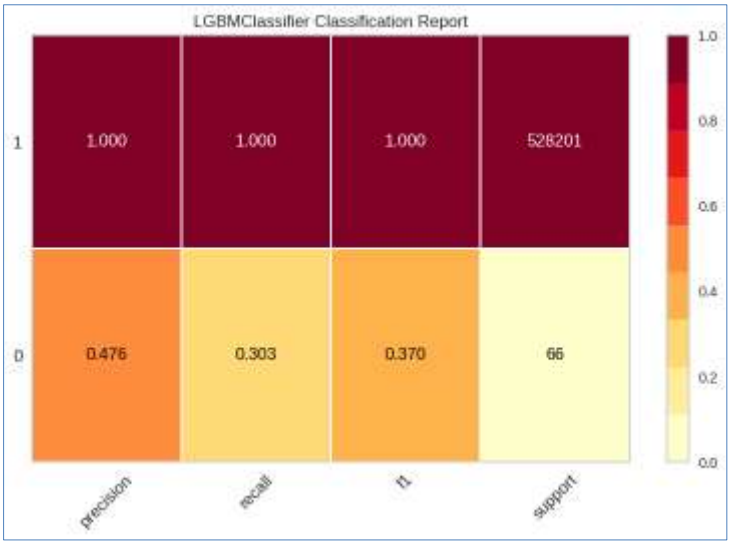

Fig. 7 Classification report of target feature for 10-best features set

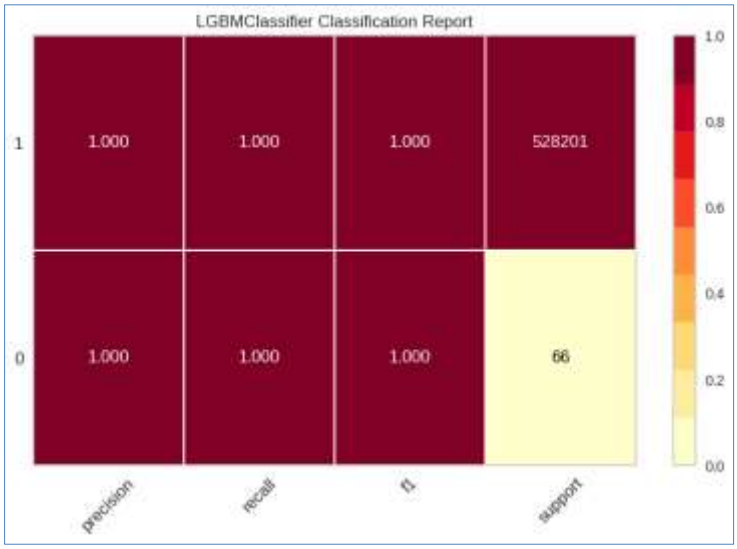

Fig. 8 Classification report of target feature for full set features

4.1.3 TrigFAR Model Performance

The TrigFAR model has been tested on LightGBM classifier, using Bot-IoT dataset with 10-best features set and full features set. Table 3 displays the results obtained so far, while Figure 10 and 10 illustrate the confusion matrix on the Bot-IoT dataset with 10-best features set and full features set, respectively. Using the top 10 feature sets, the FAR is 0.0042%, indicating a low rate of incorrectly identifying threats in IoT. While when using the full feature set, the FAR is 0.0000%, signifying that the system makes no FAR with all features in Bot-IoT dataset.

Table 3 Performance analysis with LightGBM on BoT-IoT dataset

Algorithm	**LightGBM**	
Dataset version	**10-best feature**	**Full feature**
Accuracy	0.9990	1.0000
Precision (Detection rate)	0.9994	1.0000
Recall	1.0000	1.0000
F-score	0.9995	1.0000
False Alarm Rate (FAR)	0.0042%	0.0000%

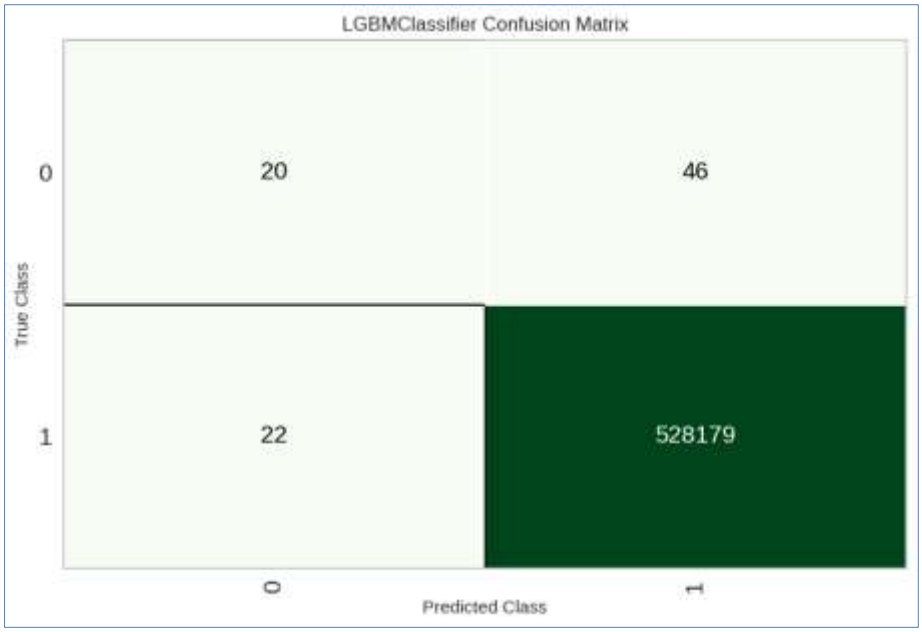

Fig. 9 Confusion matrix on 10-best features set

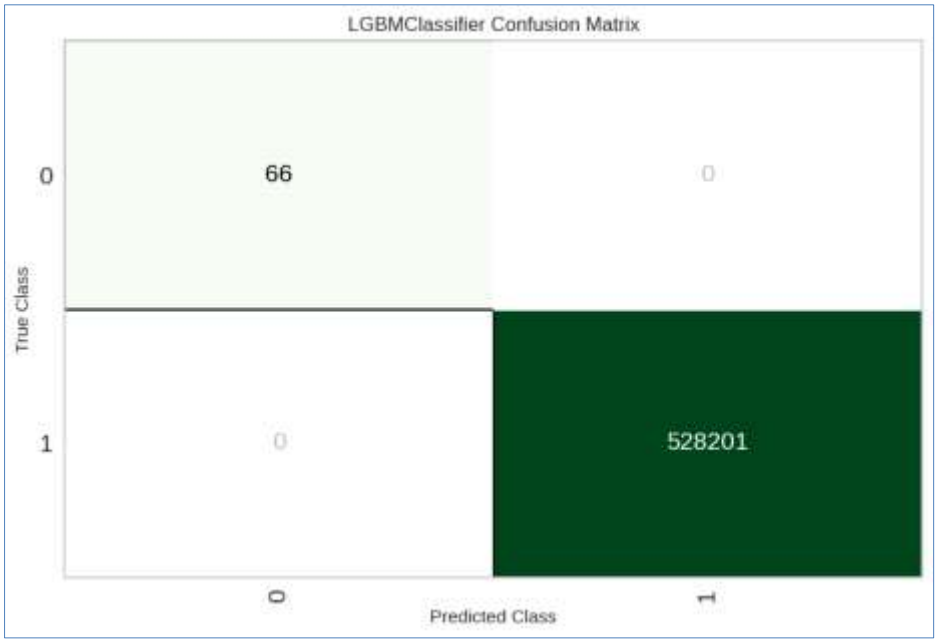

Fig. 10 Confusion matrix on full feature set

4.2 Justification with ROC Curve

The information in Table 3 reveals that our proposed TrigFAR model correctly classified the attacks available on Bot-IoT dataset, thus enabled the reducing the high of FAR in IoT environment. As a result, we have constructed a receiver operating characteristic curve (ROC) for TrigFAR on 10-best feature set and full features set in Fig. 11 and Fig. 12, respectively. Moreover, the TrigFAR model exhibits promising performance based on the evaluation results. Specifically, the ROC curves for class 0 and class 1 achieved an AUC of 0.64. Though, the micro-average ROC curve attained an ideal AUC of 1.0, suggesting perfect overall classification accuracy across the attack classes of 10-best features set. Nevertheless, the macro-average ROC curve mirrored the individual class AUC values at 0.64.

Meanwhile, the proposed TrigFAR model demonstrates outstanding performance on the full set of features, achieving an AUC of 1.0 for both class 0 and class 1 ROC curves, as well as for the micro-average and macro-average ROC curves. This suggests that the model excels in accurately distinguishing instances attacks on full features set, and its overall classification accuracy is perfect across all classes. However, from the AUC values alone, the model's discriminatory ability is better when using the full set of features since all the AUC values are 1.0. An AUC of 1.0 suggests perfect classification performance, which means the model can perfectly separate positive and negative instances, achieving no zero FAR for TrigFAR model.

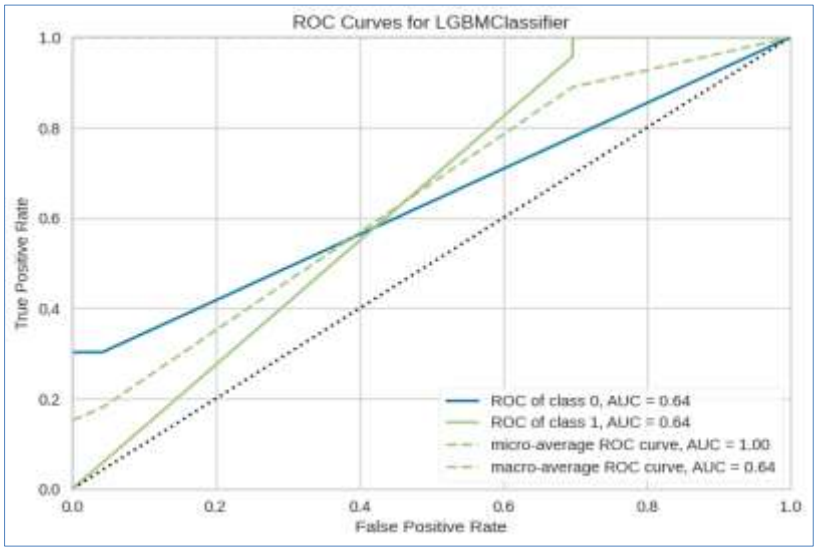

Fig. 11 ROC Curve for TrigFAR on 10-best features set

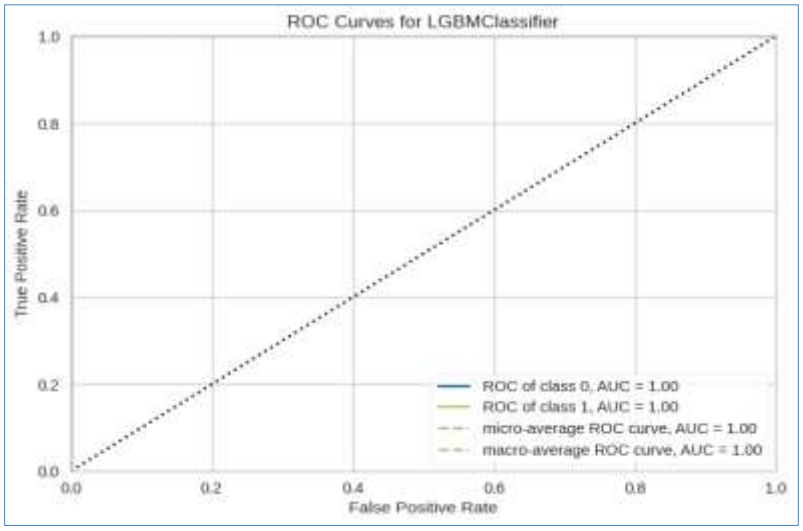

Fig. 12 ROC Curve for TrigFAR on full features set

4.3 Performance Comparison with Other Related Works

We compare our proposed model with previously published works using the similar validation means and complete feature set on each dataset. Tables 4 demonstrate the effectiveness of our TrigFAR model, outperforming other approaches. Notably, our TrigFAR significantly reduces the FAR by 0.0000% on the full features set of Bot-IoT dataset. On the 10-best features set, reduced the high FAR in IoT environment by 0.0042% our method performs well in all performance metrics.

Table 4 Performance comparison with other related works

Author	Dataset	Modeling Algorithm	Accuracy	Detection Rate	FAR
Logeswari et al., 2023	NSL-kDD	HFS-LGBM	0.9872	0.9745	-
Saba et al., 2022	NID	CNN	95.5	-	-
Ge et al., 2019	Bot-IoT	NN	0.99	0.99	-
Saif et al., 2022	NSL-kDD	K-NN and DT	99.88	-	-
Fatani et al., 2021	Bot-IoT (10-best features set)	CNN	99.99	99.99	-
Otoum et al., 2022	NSL-KDD	SDPN	99.02	99.38	-
Sivanantham et al., 2019	IDS Kaggle Dataset	ADA-RT	99.91	93.04	0.079
This study	Bot-IoT (10-best features set)	LightGBM	0.9990	0.9999	0.0042
	Bot-IoT (full features set)		1.0	1.0	0.0000

4.4 Discussions

One of the key advantages of the Bot-IoT dataset is that it comprises IoT network traces, which allows this study to address the specific challenges of securing IoT devices while reducing the high FAR. Moreover, it covers a wide range of attack types, including various forms of DoS and DDoS attacks, occurring across different transactional protocols. This attack diversity ensures that the proposed TrigFAR model can be carefully evaluated under accurate scenes. Although, (Peterson et al., 2021) provides a broad description and analysis of the Bot-IoT dataset, but not checking the consistency of the data in an application of specific security concern, rather provides only information referring to dataset. However, since Bot-IoT dataset is real-world data from various sources, this reflects the actual challenges faced when it comes reducing high FAR for IoT devices. Based on this fact, it can be recommended that the Bot-IoT dataset is actively gathered and aligned with the developments of A-IDS model for IoT, making it suitable for conducting these experiments and validating our proposed model.

Upon inspecting the results, it becomes evident that the proposed TrigFAR with lightGBM classifier of A-IDS model on Bot-IoT dataset outperforms other methods like (Logeswari et al., 2023; Otoum et al., 2022).

This superiority stems from the numerous advantages offered by Bot-IoT dataset and lightGBM classifier, making them more suitable for A-IDS, more specifically in reducing high FAR for IoT. Apart from the qualities of the dataset mentioned earlier, LightGBM possess several qualities, including the utilization strategies like EFB and GOSS, enabling efficient training on large-scale data without compromising attack detection performance. Concisely, LightGBM strikes a balance between performance and efficiency when training a model. Making it an excellent choice for tackling high FAR for IoT, where accuracy and speed are crucial factors for successful A-IDS models.

Meanwhile, reducing high FAR for IoT based on A-IDS is challenging especially when assessing the classifier performance. Though, it is almost impossible to completely avoid FAR on A-IDS models (Fernandes et al., 2019). While, when it comes to reducing high FAR, our proposed TrigFAR model achieved significant enhancement over present works such as (Logeswari et al., 2023; Sivanantham et al., 2019) among others on different dataset. Although most of the related works did not provide the exact FAR value they obtained. But when computing the FAR value with metrics value they present, it will produce a higher value than the value we obtained. For instance, (Saba et al., 2022) obtained FP of 16, FN of 9 and TN of 2317, thus could provide us with 0.0069 FAR value, which is higher than our FAR value. Meanwhile, not providing the FAR value does not undermine their model but highlights the gap of not prioritizing high FAR for IoT which can rise when deploying their model.

To sum it up, despite the success of our TrigFAR model on Bot-IoT dataset when reducing high FAR for IoT, it is observed that it requires a deep understanding of the underlying concepts. For Instance, the IoT device privacy, model privacy and data leakage can be among the security and privacy concerns with A-IDS models. Notably, IoT devices gather sensitive data, including personal data, which raises questions about how well it will be protected. Additionally, models are trained in central entity, which means that all participating device contributes its own local data to the model, disclosing classified data like device fingerprints and other attack patterns. Therefore, A-IDS models of any specific concern like high FAR for IoT should be designed using privacy preserving methods such of federated learning (FL) and go through frequent security evaluations to overcome these problems.

5. Conclusion

This paper presents an evaluation on Bot-IoT dataset with a proposed TrigFAR model that enabled reducing of high FAR on IoT devices. The Bot-IoT dataset was a freely available dataset that simulates large botnet attacks. This leads us to carefully examine the dataset in enabling reducing FAR for IoT. And we found that it comprises IoT network traces with diverse attack types of different transactional protocols. Meanwhile, the proposed TrigFAR model is evaluated on Bot-IoT dataset with lightGBM classifiers to support the A-IDS model. The results obtained demonstrate the practical achievability of TrigFAR on Bot-IoT dataset, as it achieves recommendable performance to the reducing of FAR with 0% and accuracy 100% on full feature set of the dataset. In other cases, TrigFAR outperforms other related works, as seen from the evaluation results. Importantly, TrigFAR model on Bot-IoT dataset maintains minimum FAR for IoT systems. However, our proposed future work will focus on improving the model performance on detecting modern attacks and maintaining the minimum FAR for IoT threats, while also prioritizing data privacy of the IoT devices.

Acknowledgment

The authors wish to acknowledge the support in part by Universiti Teknologi PETRONAS (UTP) and the Yayasan Universiti Teknologi PETRONAS-Fundamental Research Grant (YUTP-FRG) for the funding of project titled: Fundamental study of supervised machine learning techniques for autonomous defect mapping of offshore structures (cost centre: 015LC0-373).

Funding Information

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of Conflict

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

References

1. Abreha, H. G., Hayajneh, M., & Serhani, M. A. (2022). Federated learning in edge computing: a systematic survey. *Sensors, 22*(2), 450.
2. Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Alazab, M., . . . Gadekallu, T. R. (2022). Federated learning for intrusion detection system: Concepts, challenges and future directions. *Computer Communications*.
3. Al Mogbil, R., AL Asqah, M., & El Khediri, S. (2020). *Iot: Security challenges and issues of smart homes/cities.* Paper presented at the 2020 International Conference on Computing and Information Technology (ICCIT-1441).
4. Albalawi, A. M., & Almaiah, M. A. (2022). Assessing and Reviewing of Cyber-security Threats, Attacks, Mitigation Techniques in IoT Environment. *Journal of Theoretical and Applied Information Technology, 100*(9).
5. Alsoufi, M. A., Razak, S., Siraj, M. M., Nafea, I., Ghaleb, F. A., Saeed, F., & Nasser, M. (2021). Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review. *Applied Sciences, 11*(18), 8383.
6. Atlam, H. F., Alenezi, A., Alassafi, M. O., Alshdadi, A. A., & Wills, G. B. (2020). Security, cybercrime and digital forensics for IoT. In *Principles of internet of things (IoT) ecosystem: Insight paradigm* (pp. 551-577): Springer.
7. Bansal, A., & Kaur, S. (2018). *Extreme gradient boosting based tuning for classification in intrusion detection systems.* Paper presented at the Advances in Computing and Data Sciences: Second International Conference, ICACDS 2018, Dehradun, India, April 20-21, 2018, Revised Selected Papers, Part I 2.
8. Bansal, S., & Kumar, D. (2020). IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication. *International Journal of Wireless Information Networks, 27*(3), 340-364.
9. Bhattacharya, S., Maddikunta, P. K. R., Kaluri, R., Singh, S., Gadekallu, T. R., Alazab, M., & Tariq, U. (2020). A novel PCA-firefly based XGBoost classification model for intrusion detection in networks using GPU. *Electronics, 9*(2), 219.
10. Buja, A., Apostolova, M., Luma, A., & Januzaj, Y. (2022). *Cyber Security Standards for the Industrial Internet of Things (IIoT)–A Systematic Review.* Paper presented at the 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA).
11. Chatterjee, A., & Ahmed, B. S. (2022). IoT anomaly detection methods and applications: A survey. *Internet of Things, 19*, 100568. doi:https://doi.org/10.1016/j.iot.2022.100568
12. Fatani, A., Abd Elaziz, M., Dahou, A., Al-Qaness, M. A., & Lu, S. (2021). IoT intrusion detection system using deep learning and enhanced transient search optimization. *IEEE Access, 9*, 123448-123464.
13. Faysal, J. A., Mostafa, S. T., Tamanna, J. S., Mumenin, K. M., Arifin, M. M., Awal, M. A., . . . Mostafa, S. S. (2022). *XGB-RF: A hybrid machine learning approach for IoT intrusion detection.* Paper presented at the Telecom.
14. Fernandes, G., Rodrigues, J. J., Carvalho, L. F., Al-Muhtadi, J. F., & Proença, M. L. (2019). A comprehensive survey on network anomaly detection. *Telecommunication Systems, 70*, 447-489.
15. Ge, M., Fu, X., Syed, N., Baig, Z., Teo, G., & Robles-Kelly, A. (2019). *Deep learning-based intrusion detection for IoT networks.* Paper presented at the 2019 IEEE 24th pacific rim international symposium on dependable computing (PRDC).
16. Huh, S., Cho, S., & Kim, S. (2017). *Managing IoT devices using blockchain platform.* Paper presented at the 2017 19th international conference on advanced communication technology (ICACT).
17. Jamil, S., & Rahman, M. (2022). A Comprehensive Survey of Digital Twins and Federated Learning for Industrial Internet of Things (IIoT), Internet of Vehicles (IoV) and Internet of Drones (IoD). *Applied System Innovation, 5*(3), 56.

18. Ke, G., Meng, Q., Finley, T., Wang, T., Chen, W., Ma, W., . . . Liu, T.-Y. (2017). Lightgbm: A highly efficient gradient boosting decision tree. *Advances in neural information processing systems, 30*.
19. Khan, Z. A., Naz, S., Teo, J., Ghani, A., & Almaiah, M. A. (2022). A Neighborhood and Machine Learning-Enabled Information Fusion Approach for the WSNs and Internet of Medical Things. *Computational Intelligence and Neuroscience, 2022*.
20. Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity, 4*(1), 1-27.
21. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity, 2*(1), 1-22.
22. Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., & Alazab, A. (2019). A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks. *Electronics, 8*(11), 1210.
23. Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Generation Computer Systems, 100*, 779-796.
24. Logeswari, G., Bose, S., & Anitha, T. (2023). An intrusion detection system for sdn using machine learning. *Intelligent Automation & Soft Computing, 35*(1), 867-880.
25. Manab, A. C., Jamwal, A., & Saha, P. S. (2021). A Summary of Current Smart Farming Practices in an Indian Perspective. *Kepes, 19*(1), 19-27. doi:10.5281/zenodo.7936583-20
26. Martins, I., Resende, J. S., Sousa, P. R., Silva, S., Antunes, L., & Gama, J. (2022). Host-based IDS: A review and open issues of an anomaly detection system in IoT. *Future Generation Computer Systems, 133*, 95-113.
27. Otoum, Y., Liu, D., & Nayak, A. (2022). DL-IDS: a deep learning–based intrusion detection framework for securing IoT. *Transactions on Emerging Telecommunications Technologies, 33*. doi:10.1002/ett.3803
28. Patel, K. K., Patel, S. M., & Scholar, P. (2016). Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. *International journal of engineering science and computing, 6*(5).
29. Peterson, J. M., Leevy, J. L., & Khoshgoftaar, T. M. (2021). *A review and analysis of the bot-iot dataset.* Paper presented at the 2021 IEEE International Conference on Service-Oriented System Engineering (SOSE).
30. Rejeb, A., Rejeb, K., Simske, S., Treiblmaier, H., & Zailani, S. (2022). The big picture on the internet of things and the smart city: a review of what we know and what we need to know. *Internet of Things, 19*, 100565.
31. Saba, T., Rehman, A., Sadad, T., Kolivand, H., & Bahaj, S. A. (2022). Anomaly-based intrusion detection system for IoT networks through deep learning model. *Computers and Electrical Engineering, 99*, 107810.
32. Saif, S., Das, P., Biswas, S., Khari, M., & Shanmuganathan, V. (2022). HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare. *Microprocessors and Microsystems*, 104622.
33. Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. A. (2020). Performance analysis of machine learning algorithms in intrusion detection system: A review. *Procedia Computer Science, 171*, 1251-1260.
34. Shahab, S., Agarwal, P., Mufti, T., & Obaid, A. J. (2022). SIoT (Social Internet of Things): A Review. *ICT Analysis and Applications*, 289-297.
35. Sivanantham, S., Abirami, R., & Gowsalya, R. (2019). *Comparing the performance of adaptive boosted classifiers in anomaly based intrusion detection system for networks.* Paper presented at the 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN).
36. Sultan, A., Mushtaq, M. A., & Abubakar, M. (2019). *IOT security issues via blockchain: a review paper.* Paper presented at the Proceedings of the 2019 International Conference on Blockchain Technology.
37. Wang, S., Tuor, T., Salonidis, T., Leung, K. K., Makaya, C., He, T., & Chan, K. (2018). *When edge meets learning: Adaptive control for resource-constrained distributed machine learning.* Paper presented at the IEEE INFOCOM 2018-IEEE conference on computer communications.
38. Yang, Z., Liu, X., Li, T., Wu, D., Wang, J., Zhao, Y., & Han, H. (2022). A systematic literature review of methods and datasets for anomaly-based network intrusion detection. *Computers & Security, 116*, 102675.
39. Zohourian, A., Dadkhah, S., Neto, E. C. P., Mahdikhani, H., Danso, P. K., Molyneaux, H., & Ghorbani, A. A. (2023). IoT Zigbee device security: A comprehensive review. *Internet of Things*, 100791.