International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 9, Issue 2, 2023, PP 23-34
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
https://doi.org/10.20431/2349-4859.0902003
www.arcjournals.org

Enhanced IOT Security using Cascaded Machine Learning

FIRAS H. ZAWAIDEH[1], SALAH YOUSEF ABU BAKER[2]

[1]*Head of the Cyber Security Department, Faculty of Science and Information Technology, Irbid National University, Irbid, Jordan*
[2]*Head of Network and Cyber Security Department, Irbid electricity company, Irbid, Jordan*

Corresponding Author:** ***FIRAS H. ZAWAIDEH, *Head of the Cyber Security Department, Faculty of Science and Information Technology, Irbid National University, Irbid, Jordan*

Abstract: *The increased growing of the internet usage explodes the demand of connectivity; therefore, the number of Internet-of-Things (IOT) devices have significantly increased. According to recent figures, IOT malware attacks increased by 215.7% from 10.3 million in 2017 to 32.7 million in 2018, indicating that this deployment has raised the possibility of attacks of different kinds and demonstrates how IOT networks and devices are vulnerable and susceptible. Therefore, it is necessary to have appropriate, effective, and efficient intrusion detection method in such environments. Machine learning has become one of the significant solutions due to the massive amounts of available data for IoT devices. Thus, they have a great potential to be used in intrusion detection systems for IoT networks. For that, many researches were held to provide IOT devices with reliable, fast and effective mechanism for detecting and classifying the different types of attacks and malicious devices using the analysis of the traffic data inside the IOT networks. This research investigates the IOT traffic data and proposes best 13 features, to train cascaded Recurrent Neural Network model (RNN) combined with light GBM Machine Learning (ML) model for classifying the BOTNET attacks inside IOT networks. The proposed machine learning model solves the highly imbalanced IOT traffic problems, which lead to over fitting most of the common machine learning models. As the gradient boosted trees training behavior relies on parallel building of rules. Moreover, the reduced number of 13 used uncorrelated features increased the model generalization performance. The model was trained and tested over BOT-IOT dataset, which contains more than 3 million of IOT traffic records. The results were compared to 8 different types of other machine learning models trained over the same dataset using Knime data analysis tool. The findings showed that the proposed approach was outperformed the existing works in the literature with very high accuracy of 99.9% and a recall of 100%.*

Keywords: *LIGHTGBM, IOT, Botnet, Feature Extraction, RNN, ML.*

1. INTRODUCTION

The internet of things is new paradigm that change the IT industry. The two terms "Internet" and "Things" were combined to form the phrase "Internet of Things", which is also commonly abbreviated as "IoT." The internet is a global network that consists several interconnected computer networks like (business, academic and government networks) that use standard Internet protocol suite (TCP/IP) and serves billions of people around the world. These networks are connected by a wide range of electrical, wireless, and optical networking technologies make up this network of networks. (Tanaka et al., 2016).

However, IOT can be defined in abbreviated way as a network of physical objects, it evolves a network of devices of all types and sizes, vehicles, smartphones, household appliances, toys, cameras, medical tools and industrial systems, animals, people, and buildings, all of which are connected, all contact information and information exchange based on the protocols set forth in from For smart reorganization, positioning, tracking, safe and controlling, even real-time, online real-time monitoring, online upgrade, process control and management. Therefore, the most important thing and which attract the researcher to give this kind of technology the secure way to sending and receiving data.

Moreover, there were a great importance in increasing protection in areas related to the Internet of things, for example, IOT devices in smart home networks, which are an integral part of smart grid and promises to deliver more efficient and effective power management so, they are highly vulnerable to

multiple types of attacks included famous botnet malware attacks. So that, the researchers' study and discuss different IOT attacks and its classifying methods, its protections measures, and try to find the most prominent attacks in IOT.

The Internet of Things (IOT) raised its full potential in the early 2000s. When advancements in numerous technologies, including wireless communications, the Internet, and micro-electromechanical systems, finally caught up to its goals. The Internet of Things integrates physical items with electronics, software, and sensors to enable automatic data exchange between them or with other entities. The combination of the digital and physical aims to increase a system's effectiveness, precision, and economic worth.IOT Analytics1 estimated the amount of active IoT devices, without taking into account mobile phones, tablets, laptops, and other similar devices, in August 2018. And found that there would be 21.5 billion active IOT devices in use by 2025, as shown in Figure 1.

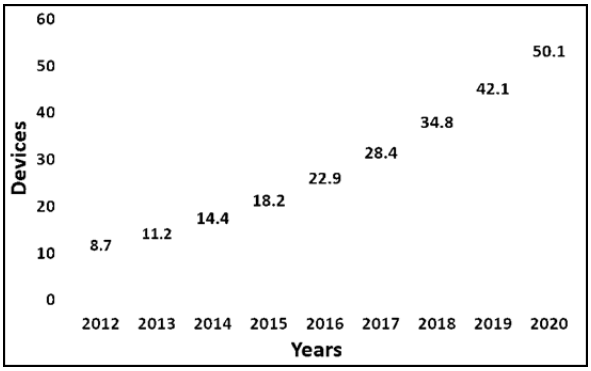


Figure1. *IOT Growth (Burhan, Rehman, Khan, & Kim, 2018)*

Though IOT solutions have great potential, they face several challenges, summarized in Figure 2 Such challenges arise while creating an IOT product, and the IOT industry must band together to try to overcome them. The challenges of resource efficiency, lifespan, and business model are covered in this section.

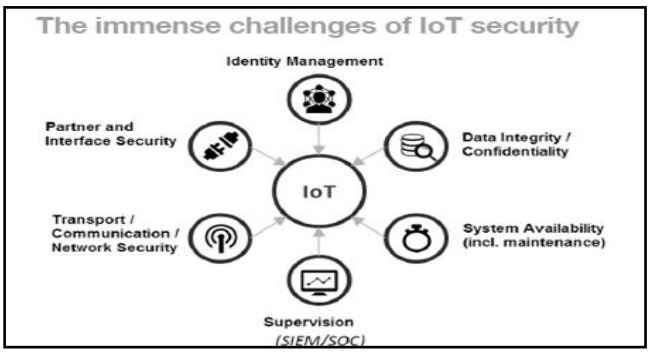


Figure2. *IOT security challenges (Raphaël, 2018)*

Any system must have authorized access as a basic component. Therefore, access control (AC), which has the goal of determining who can access what, in what way, and according to what rules, is a crucial component of a system's defence mechanism. There are two modern methods for creating an access control system for the internet of things. One can try to modify current solutions or start from scratch. In fact, there are substantial differences between the IOT paradigm and traditional systems. The first issue, like everything else in the IOT, relates to resources.

The majority of traditional access control solutions use a client-server architecture. The objects in this model are stored on a server, which is anticipated to have a substantial amount of resources at its disposal: memory to store all the client's data and access rules, possibly even a log of access requests, computational power to run the decision engine and handle concurrent client requests, and bandwidth to handle a substantial number of clients. Additionally, the server must be accessible at all times. Access requests are hosted on limited devices in IOT use cases since they are unable to fulfil the traditional server role. Requestors can also be devices themselves and are subject to the same resource limitations. Therefore, classical access control solutions cannot be used in their current state and must be adapted or abandoned entirely. Legacy solutions may become inefficient as a result of these

changes. Security can occasionally take up space that the device cannot support. In this situation, access management must be carried out outside, usually by a centralized server, which raises security concerns. Another argument occurring within the IOT access control community is where to make the decision regarding access control. The benefit of centralized systems is that they can implement legacy solutions and eliminate the majority of resource limitation problems. However, they only offer single attack point, which makes them an attractive target for attackers. Distributed systems are challenging to implement, but offer greater resilience and flexibility.

Recently, distributed access control systems have shown potential for machine learning (ML). Such a system's expressivity is still limited. While certain IOT use cases permit a bootstrap phase, they require access control only to involve local entities. This is the situation, for example, with a linked car that one can unlock using a smartphone, which should still be viable in an underground parking garage without network service. Therefore, regardless of architectural choice, the issue of offline access requires exploration.

IOT device security is a major concern for different reasons. An increasing number of gadgets are becoming smart devices, and as manufacturers launch new products more quickly. Security can be given a low priority because the focus is about the market time metrics and return on investment. Also lack of awareness among consumers and businesses is a major obstacle to safety, as the advantages of IOT technologies appear to outweigh the risks of information theft or hardware attacks. (Tanaka et al., 2016).

The research seeks to provide a security model for the IOT using ML algorithms to improve network and communication security by detecting and avoiding the malicious and infected node from spreading to other nodes in the network and infecting them. The contribution of this paper can be as the following:

a. Increase security in IOT using RNN and ML.
b. Investigate the best ML models that can be used to detect attack on IOT network devices
c. Find the best features that can describe the Bonet IOT attacks.
d. Build a secure model that can be an architecture used as one of the security models.
e. Compare the results with other researcher results.
f. Enhance the security using RNN and ML to monitor the behavior of IOT botnet attack.

2. RELATED WORK

This chapter provides an overview of previous studies that used the enhanced machine learning (ML) and deep learning models (DL) to identify IOT botnet breaches. Moreover, some studies related to IOT attack type classification were mentioned but using other algorithms such as Decision Tree (DT), Support Vector Machine (SVM), Multi-Layer Perceptron Neural Network (MLP-NN), Naive Bayes (NB), and others.(Alrashdi, et al., 2019) The authors developed an Anomaly Detection IOT (AD-IOT) algorithm to handle the IOT cyber security concerns in a smart city using Random Forest. Their approach may reliably identify compromised IOT devices at distributed fog nodes. The findings showed 99.34% accuracy score.

The authors of (Anderson, et al., 2018) provide a comprehensive reinforcement learning (RL) architecture for tackling static portable executable (PE) anti-malware engines. as shown in their study, attacks on this model seem to overcome parts of publicly hosted antivirus engines. the findings for adversarial training showed that, attack's effectiveness is decreased by 33% when the model is retrained on evasive ransomware samples. Notably, the authors provide researchers with access to an Open AI gym so they can investigate evasion rates against malware samples, ML models, and their own RL agents. This paper (Costa, et al., 2019) aims to conduct a new and comprehensive examination of significant works dealing with various intelligent approaches and their applicable intrusion detection architectures in computer networks, with a focus on IOT and ML. A wide range of subjects relevant to security in IOT systems were covered in the more than 95 articles.

This study 2019 (Dovom et al.) perform identify and categorize various malware by transform Opcodes into a vector space and by using fuzzy and fast fuzzy pattern tree methods. Particularly for the fast fuzzy pattern tree, the authors were able to maintain a high level of accuracy while still

keeping reasonable run times. the findings showed that Both employed feature extraction and fuzzy classification, worked well together to produce a more complex edge computing malware detection and categorization technique. (Ficco, 2019) The authors employed Markov chains to model the applications throughout their execution, which were then used to extract properties of the programs over time, which were essential for malware categorization. The dataset under consideration contains 22K benign programs and 24K malware, gathered from several common databases. Experiments showed that the Markov chain method outperformed alternatives based on the frequency of API requests, with malware F-measure detection rate up to 89 percent.

In this paper (Kumar & Lim, 2019), the authors proposed a model for IoT malware detection in large-scale networks prior to an attack, during the scanning and infection phase. They employ different ML models like (Nave Bayes, Random Forest KNN) and others to classify traffic of edge devices. They evaluate their model and showcase a 96% accuracy score. In 2020 (Zeadally & Tsikerdekis), the authors explore the power of ML and deploy supervised, unsupervised and RL approaches to enhance IoT security, for host-based and network-based security solutions. Also, they discussed the limitations of these models that need to be solved to deploy more effective intrusion detection models in IoT environments.(Gibert, Mateu, & Planes, 2020) The authors present a detailed overview of the methods and features used in a standard ML workflow for malware detection and classification, as well as an examination of the constraints and limits of traditional ML, as well as new research areas. The survey assists researchers in gaining a better grasp of the malware detection area.

(L. B, H. Azath et al, 2021) BOT-IOT based denial of service detection with deep learning, the authors in their paper, focused on machine learning models for the purpose of securing IOT devices data transmission. As they consider monitoring the IOT traffic packets for early malware and attacks detection, allows fast response for network recover and protect the overall network from being fraud, especially in critical IOT networks. Therefore, the authors focused on investigating and comparing different types of deep learning (DL) and Machine Learning (ML) algorithms capabilities of classifying and detecting multiple IOT attack types. In order to achieve systematic comparison between the different types of machine learning models, the authors adopted a well-defined and standardized IOT related traffic data set called BOT-IOT. Moreover, in there paper, the authors, proposed an enhanced new deep learning model for denial of service (DOS) attack detection. The proposed model were implemented and trained using Python language and some of the most common machine learning frameworks related to python (Tensor flow, and Scikit-learn). The generated model was evaluated and the results showed very high accuracy with 99.2%, which proved the model efficiency.

The authors in this paper (Injadat M, et al. 2020) developed a dynamic, efficient, and effective IoT attack detection framework based on ML model. As this approach contains extra advantage over the original knowledge-based approach which needs continues updates in order to maintain acceptable IOT data transmission security levels. While the machine learning and deep learning models are capable of classifying different patterns with same behavior leading to very high accuracy in malware attack detection. In order to classify and detect multiple IOT attacks. This paper proposed an approach to detect various IoT attacks, using optimized ML mechanism, combining decision tree (DT) and Gaussian Process (BO-GP) algorithm classification model. In order to evaluate their presented model, training and testing for the model were done based on well-defined and filtered BOT-IOT dataset released in 2018. Other machine learning models such as SVM and DT were trained and evaluated over the same dataset to compare their results with the proposed model. Evaluation results with very high accuracy of (99.9%) for the proposed model compared to 88.7%, for SVM and 99.82% for Decision tree which indicated that the model achieved very good detection efficiency. It is worth to mention that, in order to normalize the dataset, data oversampling method were utilized to overcome the regular network traffic imbalance data problem.

(Popoola et al, 2021) Stacked recurrent neural network for botnet detection in smart homes. In their paper, the authors proposed new deep learning model for classifying different types of Botnet attacks over IOT devices inside smart home networks. The proposed model implements staked layers of recurrent neural network (SRNN), which targets the highly imbalanced IOT traffic data problem, and allows for recognizing its varying hierarchal representation. Bot-IOT dataset were used to train the model and testing it. The results for the proposed model in comparison of other models and regular

RNN, showed very high capability of the RCNN of handling imbalanced dataset with lower rates of over fitting and high generalization training ability. As the model stats very high results of 100% regarding the accuracy and recall testing metrics.

3. METHODOLOGY

This section provides the methodology of this work, including, the methods used, the proposed approach and the research tools. The main purpose of the work is to recognize the malicious traffic from the normal traffic. The first subsection displays the dataset description.

3.1. Methods Used

- **Recurrent Neural Network (RNN)**

Artificial Neural Network is a self-adaptive machine learning approach, powered by non-linear data, used for classification of patterns. The biological neural network forming the human brain was somewhat inspiring for the reasoning behind ANN.

RNN is a kind of Neural Network, capable to perform sequential data analysis, in order to extract the relations on various time scales. All of the inputs and outputs in the other types of neural networks, are independent of each other. However, in some applications, such as next word prediction in a sentence, it is important to remember the previous words. Therefore, RNN is developed. With the help of the recurrent hidden states RNN save the previous information, which is the most crucial component in RNN. Also, it has an internal memory to save all the calculations information and to process various length of sequences. RNN models are mostly used in speech recognition tasks and natural language processing (NLP) (Tsoi, 1998).For RNN architecture, Simply, RNN is a collection of multiple ordered neural networks, each one of them send data to another. These networks have a memory to store the knowledge about the data. But because of the memory is short- term it cannot save the long term time-series data (Apaydin et al., 2020). RNN is trained in supervised manner, the goal is to optimize the NN weights to reduce the variations among the target and the output. Simple RNN has 3 major components which are Input layers, recurrent hidden layers, and output layers.

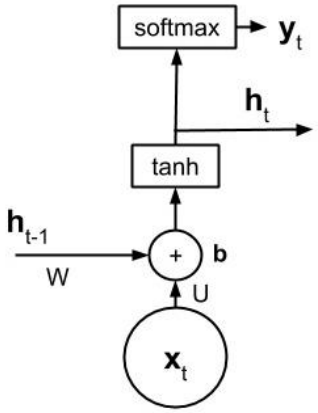


Figure3. *Simple RNN architecture*

In the h layer, x is the input vector, input is parameterized by weight matrices W and U, and b denotes to the bias. x(t) is the input at time scale t, for example, s is the input vector that represents a word in a sentence, h(t) is the memory of the network, and it is calculated depending on the previous time scale of the hidden state, and the current input through the following equation. Finally, the output is subjected to nonlinearity using activation functions.

- **Light GBM**

Traditional algorithms have found it impossible to produce results efficiently, as the scale of the data is increasingly growing day by day. Because of its processing power, LIGHTGBM is called "Light" and provides results more easily. It needs less memory to run and is able to manage vast quantities of information. The algorithm is most commonly used in Hackathons (A hackathon is an event which hosted and assembled by tech companies to work on a rapid manner to develop systems and

programs) because the purpose of the algorithm is to obtain good results accuracy and also brace GPU leaning (Graphics Processing Unit). LIGHTGBM algorithm (Light Gradient Boosting Machine) is a kind of GBDT (Gradient Boosting Decision Tree) and is generally used in the grouping, sorting, regression and efficient parallel training supports (Ke et al., 2017). At each step, the algorithm uses piece-wise constant trees and estimated loss functions with approximation of second order Taylor. This then trains a decision tree to reduce the approximation to second order, which is similar to Newton's method (Shi et al., 2018).

3.2. The Proposed Approach

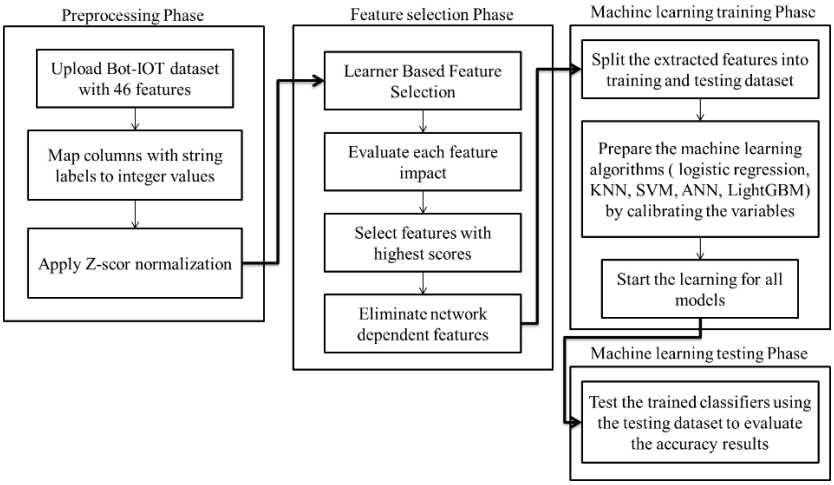


Figure4. *Proposed Approach diagram*

Figure 4 shows the whole process and steps of the proposed approach. As mentioned before the dataset used in this thesis is BOT-IOT which contains 46 features. However, in the first phase of the proposed approach, the dataset will be preprocessed by two main steps. The first one was to adapt all the features in order to make them readable by the machine learning models trainer. This was done by mapping each string labeled features to predefined integer value. The second step was related to ignore the outlier's features and reduce correlations between them, which was achieved via applying data normalization using Z-score approach. After that, The next phase, was the feature selection stage, which incorporate filtering the 46 features in the dataset resulted from the first phase in order to reduce them as much as possible, by selecting the main effective features describing the attack behavior. Moreover, ignore the correlated features that are related to each other. Since these features can be swappable, as one of them can reflect the behaviors of others. Therefore, they considered as redundant data in the original dataset.

The third phase on other hand, takes the selected features from the second phase, and split the dataset with their labels (classes) into training and testing groups, in order to start training the multiple machine learning models types (KNN, ANN, SVM, DT, Gradient boosted trees, logistic regression, and Naïve Bayes) using the training dataset. Then, evaluating the trained models using the testing dataset based on the testing metrics explained in the next section.

3.3. Research Tools

Researches tools used in our work:

- **Net using C# Language**

For the implementation of the system multi tools have been used, the major tool is Microsoft c#.net programming language which was used because of the huge built in libraries available that support machine learning process like ML.net which mainly contains the RNN algorithm which is presented in this study as main contribution. Accord.net open source library used also, it contains ready functions for machine learning like support vector machine, and many more models.

- **K-NIME**

K-NIME Analytics Platform is the free software programming proposed to make applications and administrations for information science. Instinctive, open and continuously coordinating new improvements, KNIME makes information and information science planning work processes and reusable components available to all. In this thesis the k-anime where used to learn the algorithm mentioned before and obtains the accuracy of the tested models.

In the proposed method, analysis focused in four metrics: precision, recall, sensitivity and ROC beside nfusion matrix.

3.4. Evaluation Metrics

In the proposed method, analysis focused in four metrics: precision, recall, sensitivity and ROC beside confusion matrix.

- **Confusion Matrix (CM)**

The confusion matrix should also be determined in order to judge the proposed model efficiency. This matrix provides important information about predicting the classifications generated by the different models, which in turn, will be used to test the models efficiency. Table 1 below indicates the uncertainty matrix evaluation for two groups.

Table1. *CM table.*

	Predictive Pos	**Predictive Neg**
Actual Pos	TP	FN
Actual Neg	FP	TN

The True Positive (TP) value corresponds to the quantity of True samples properly categorized by this uncertainty matrix, while the False Positive (FP) shows the sum of True samples incorrectly identified by the classifier. In the same way, False Negative (FN). implies the number of false choices identified as true, rather than False samples. However, True Negative (TN) is the quantity of false samples correctly identified by the classifier (Sokolova et al., 2006). In the following statistical tests, the success of all previous classifiers assessed based on the previous table.

- Accuracy

This metric is used to find the ratio of the correctly identified samples over the total number of samples. Accuracy is determined as following the uncertainty matrix to sum up[6].

Accuracy = (TP+TN) / (TP+TN+FP+FN)

- Precision

This metric is used to calculate the ratio of correctly identified samples as true over the total number of samples that identified as true. Accuracy is measured as follows:

Precision= TP/ (TP+FP)

- Recall or Sensitivity

This metric is used to calculate the ratio of correctly identified samples as true over the total number of true sample in the dataset .Accuracy is measured as follows:

Recall =TP / (TP + FN)

Receiver Operating Curve (ROC)

The behaviors of the formed system detected using this curve, since it shows the system's stability and normal operation. ROC distinguishes the true results obtained (true positive) versus the inaccurate results retrieved (false positive). ROC reveals the fact that, as the correctly collected findings increase, the false alarms rise. A curve with strong true positive and usual false positive values can be obtained from successful trained classification model (Nahm et al., 2022).

4. RESULTS AND DISCUSSION

This chapter highlights the result findings where an assessment of the efficiency of the recommended solution and discusses the analyses and experiments conducted in this research and elaborates the dataset used in this study as well.

4.1. Experimental Settings and Dataset

In order to complete the testing and assessment phase, a well specified and labeled IOT traffic dataset containing botnet malware packets and normal IOT traffic packets from faculty of UNSW Canberra at ADFA were used. Bot-IOT dataset was chosen as it is one of the most respected and categorized datasets since it was gathered from realistic network environment designed and implemented in the Cyber Range Lab, which has a huge number of records for many IOT malware attacks. The dataset contains DoS, OS, DDoS, Keylogging, Data exfiltration attacks, Service Scan, with the DoS and DDoS attacks further organized, based on the protocol used. The selected dataset for generating the proposed model were only 5% of the original dataset with 3 million records and approximately 1.07 GB of total size. The dataset were collected in 2018, and incorporates 46 different characteristics for each captured packet record. The dataset contains two main categories (train, and test), where each of which has two sub category (NORMAL, and Attack) based on the real IOT network record classification. Moreover, the dataset contains also the attack malware type and the protocol for the attack. However, this research tock in consideration Attack and NORMAL categories only, as they are the main focus of the proposed contribution. Train main category includes 2 million attack records, and 300000 normal records, while test main category contains 700000 records for attack and Normal.

4.2. Knime Results

The K-NIME tool allows us to test many classification algorithms such as the SVM, Decision Tree, MLP, random forests, logistic regression, and naïve Bayes. Figure 5 shows the process of training and testing the algorithms in the K-NIME tool. The researcher used the KNIME tool to implement the list of classifiers illustrated before. Figure 2 shows the classifier implementation and its different phases: Machine Learning Classifiers Implementation in K-NIME

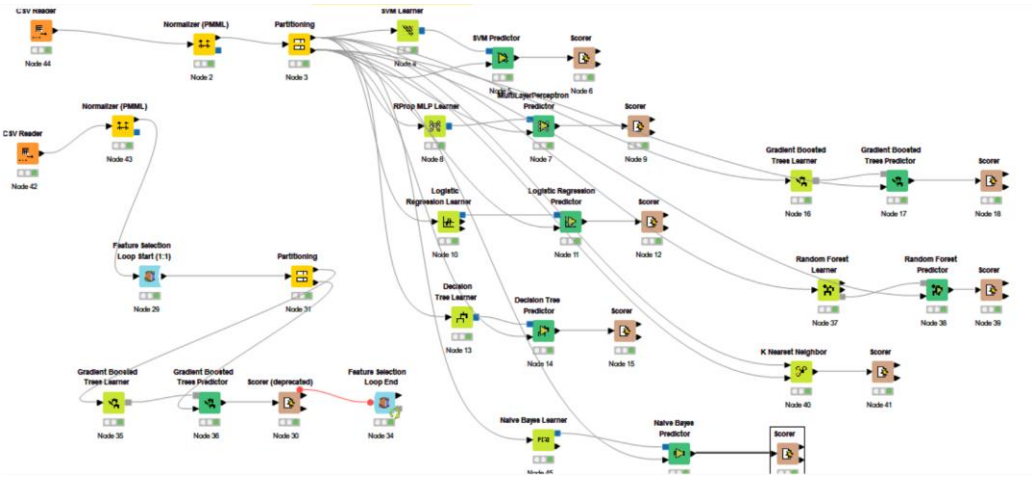


Figure5. *1Machine Learning Classifiers Implementation in K-NIME.*

As sown in figure 5 the K-NIME tool have different nodes that each of which are used for different purposes. It can be seen the "CSV reader" node that reads the dataset from a CSV file type and then using the "Normalizer" node to normalize the dataset then moving to the "partitioning" node to split the dataset into training set and test set with a specific ratio mainly 80% for training and 20%. After that, with each classification method used, the learner object presented with the training dataset. Later, in order to validate the created classification model, the trained object submitted to the predictor object. Finally, using a scorer item, the results computed. Then the matrix of uncertainty for all the models was computed.

Table1. *Results of Machine Learning Algorithms over the selected Feature only.*

Classification Method	Recall	Precision	Sensitivity	Accuracy
ANN	0.963	0.984	0.963	0.989
KNN	0.989	0.988	0.989	0.987
SVM	0.579	0.941	0.579	0.885
Decision Tree	0.855	0.854	0.855	0.853
Logistic Regression	0.482	0.461	0.482	0.507
Gradient Boosted Tree (LightGBM+RNN)	1.00	0.999	.999	0.999
Random Forest	0.960	0.993	0.960	0.997
Naïve Bayes	0.958	0.993	0.958	0.949

As shown in table 1, most of the results from all machines learning model achieved very high accuracy in terms of selected features which indicates very mature dataset feature selection and normalization. While the proposed algorithm maintained the highest accuracy results with 0.99% compared to other algorithms that use the same dataset. But not all the algorithms achieved a good accuracy compared to the other accuracies like the naïve Bayes, SVM and the Logistic Regression which were not converge to suitable accuracy level. Figure 6 illustrate and visualize the accuracies.

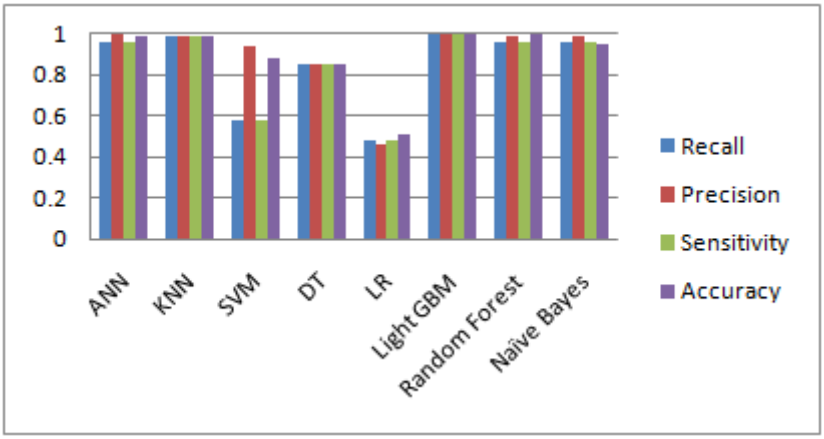


Figure6. *Result of Machine Learning Algorithms over the extracted features.*

4.3. Receiver Operating Characteristic Curve (ROC)

A sequence of tests carried out on the specified dataset for device evaluation to extract the test metrics, explained in the methodology section (Precision, Accuracy, Sensitivity, Recall, and ROC). In order to prove machine learning model effectiveness, another test (the ROC curve) conducted, as the ROC analyses true positive results with the false positive results (false alarm results).The number of false alarms increases with the rise in the number of true positive findings received, as seen in figure 7.

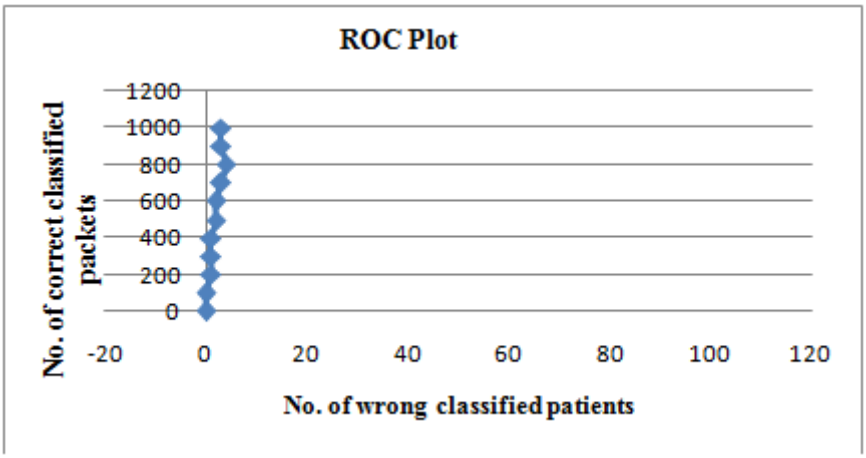


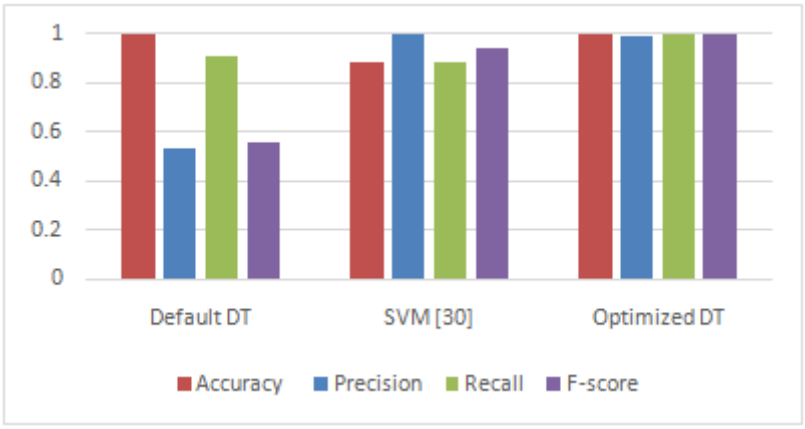
Figure7. *2ROC Curve.*

The results demonstrated that the true positive results on the Y-axis and the false positive results on the X-axis still have a significant difference. This shows that despite a large number of classified results, the system maintains its accuracy level.

In order to prove the presented model capability for detecting the malware attacks in IOT devices, performance evaluation was held between the proposed RNN –light GBM with filtered dataset and the latest related work with same dataset or same attacks types related to IOT protocols. Tables 3 to 4 below shows the evaluation results, which indicates the efficiency of the proposed contribution.

Table3. *Previous work results for the same dataset used in this thesis.*

Author & Date	**Advantage**	**Disadvantage**
Mohammad Noor et al. 2020	• Model they used easy to learn so it takes short time and it's not used a huge dataset and it take a fast tanning set • DT, Ml doesn't require huge dataset numbers perform required less time for training	• Don't make features selection, they rely on dataset recommendation features • DT model does not have ability to deal with imbalance dataset so they made data over sampling which may reduce the accuracy for new input
Proposed approach (2022)	• Model capable make handle to high imbalanced dataset • Deep learning gives high accuracy because it learns on huge dataset • Capable recognize different type patterns with high accuracy specially for new input	• Huge dataset • High time to learn • Need complex devices
Lanitha. B, et al.2021	• Single attack type classification (Poor prediction model for other attacks classes) • Used deep learning model which has strong recognition and high accuracy	• Used part of dataset with certain class (one attack class only) so any another attacks may make confused • Need huge dataset • Ignore Imbalanced dataset , relines only on deep learning model



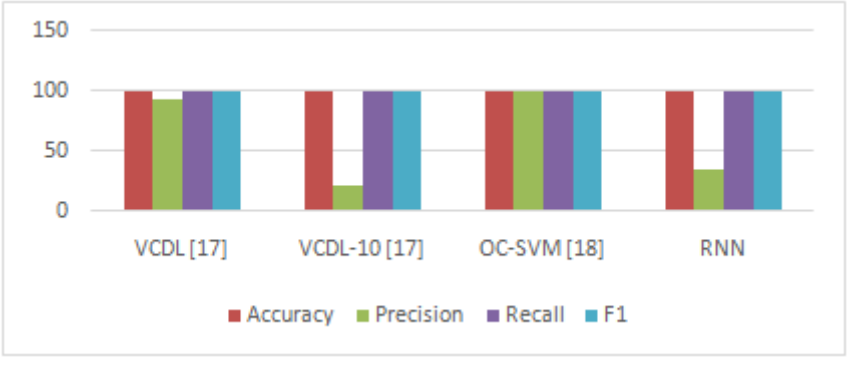


Table4. *Accuracy comparison with previous works*

Author & Date	Lanitha. B, et al.2021	MohammadNoor et al. 2020	Proposed approach (2022)
Algorithm	deep learning algorithm-based model	(BO-GP) and (DT)	LightGBM+RNN
Dataset type	BoT-IOT dataset	BoT-IOT dataset	BoT-IOT dataset
accuracy	99.2%	99.9%	99.9%

5. Conclusion and Future Work

5.1. Conclusion

In this study an automatic Botnet attack detector were proposed for IOT network devices. The detector was implemented based (RNN) algorithm and Light GBM combined with 13 selected features related to IOT network devices traffic data. The dataset used to train and test the model that was obtained, using Bot-IoTdataset. The dataset includes 46 features that describe each record. It also covers different types of attack like DDoS, DoS, OS, Service Scan, Keylogging and Data exfiltration attacks, with the DDoS and DoS attacks further organized. Unfortunately, due to the lake of high power machine that can analyze huge data (records of 7 GB and more) only 5% of the total dataset (3 million records) were used to train and test the proposed model. Furthermore, the 46 features were filtered using iterative feature selection criteria, to obtain only 13 major features that were used to generate a very solid IOT Botnet attack detection model. Furthermore, the proposed approach including (RNN +light GBM, SVM, KNN, Decision trees, Random forest, and logistic regression) models was trained on Knime application, using the same selected features. Then these models had been evaluated its robustness using confusion matrix. The results showed that the proposed approach attained the highest among all of the other models with accuracy of 99.9% and a recall of 100%.

5.2. Future Work

For the future work, other normalization methods will be tested and evaluated to select the best normalization method rather than the Z-scorer method used. Also, full data set will be used to generate more extra robust model. Moreover, deep learning model will be adopted in combination of the proposed one to enhance the overall accuracy. Also, add the attack type classification to the model. Finally, attack prevention criteria will be implemented over major IOT protocols to be combined with the proposed model to prevent the attack after being detected.

References

Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S, "IoT elements, layered architectures and security issues: A comprehensive survey. Sensors", sensors, Vol. 18,No.9, 2018, pp 27-33.

Raphaël, D. (2018, May 16). Securing the IoT: a real challenge. Orange-Business. Retrieved December 18, 2021, from https://www.orange-business.com/en/blogs/securing-IoT-real-challenge

Sultan, A., Mushtaq, M. A., & Abubakar, M. IOT security issues via blockchain: a review paper. Proceedings of the 2019 International Conference on Blockchain Technology in Pakistan,2019 ,Pp. 60-65.

Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. . Ad-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning. Annual Computing and Communication Workshop and Conference (CCWC), In 2019 IEEE 9th (Pp. 0305-0310).

Anderson, H. S., Kharkar, A., Filar, B., Evans, D., & Roth, P."Learning to evade static pe machine learning malware models via reinforcement learning", Cryptography and Security, Vol.1,No.23,2019,pp 801-811.

da Costa, K. A., Papa, J. P., Lisboa, C. O., Munoz, R., & de Albuquerque, V. H. C,"Internet of Things: A survey on machine learning-based intrusion detection approaches". Computer Networks,2019, Vol.151,No.4, pp147-157.

Dovom, E. M., Azmoodeh, A., Dehghantanha, A., Newton, D. E., Parizi, R. M., &Karimipour, H," Fuzzy pattern tree for edge malware detection and categorization in IoT". Journal of Systems Architecture,2019,Vol. 97, pp 1-7.

Ficco, M, Detecting IoT malware by Markov chain behavioral models. International Conference on Cloud Engineering (IC2E), Prague, Czech Republic,2019 (Pp. 229-234).

Guerra-Manzanares, A., Medina-Galindo, J., Bahsi, H., &Nõmm, S. MedBIoT: Generation of an IoT Botnet Dataset in a Medium-sized IoT Network. In At: Valletta, Malta ICISSP,2020 (Pp. 207-218).

Kumar, A., & Lim, T. J. EDIMA: early detection of IoT malware network activity using machine learning techniques. In Limerick, Ireland World Forum on Internet of Things (WF-IoT),2019 (Pp. 289-294).

Zeadally, S., &Tsikerdekis, M. "Securing Internet of Things (IoT) with machine learning". International Journal of Communication Systems,Vol.33,No.1,2020, pp 41-44.

Gibert, D., Mateu, C., & Planes, J. The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. Journal of Network and Computer Applications,2020, Vol.153,No.1,pp 102-111.

M. Sokolova and G. Lapalme, "A Systematic Analysis of Performance Measures for Classification Tasks," Inf. Process. Manag. Vol. 45, No. 4, Pp. 427–437, 2009.

D. Powers, "Evaluation: From Precision, Recall and F-Measure to ROC, Informedness, Markedness & Correlation," J. Mach. Learn. Technol, Vol. 2, Pp. 2229–3981, Jan. 2011.

Yang, Shengping&Berdine, Gilbert. (2017). The receiver operating characteristic (ROC) curve. The Southwest Respiratory and Critical Care Chronicles. 5. 34. 10.12746/swrccc.v5i19.391.

L. B, H. Azath, D. Beulah David, E. Chandra Blessie, A. Jayapradha and S. Sheeba Rani, "BoT-IoT based Denial of Service Detection with Deep Learning," *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2021, pp. 221-225, doi:10.1109/I-SMAC 52330.2021.9640789.

Injadat, Mohammadnoor&Moubayed, Abdallah &Shami, Abdallah. (2020). Detecting Botnet Attacks in IoT Environments: An Optimized Machine Learning Approach. 1-4. 10.1109/ICM50269.2020.9331794.

Popoola, Segun & Adebisi, Bamidele & Hammoudeh, Mohammad & Gacanin, Haris & Gui, Guan. (2021). Stacked recurrent neural network for botnet detection in smart homes. Computers & Electrical Engineering. 92. 107039. 10.1016/j.compeleceng.2021.107039.

Sokolova, M., Japkowicz, N., & Szpakowicz, S. Beyond accuracy, F-score and ROC: a family of discriminant measures for performance evaluation. In *Australasian joint conference on artificial intelligence*, 2006 , (pp. 1015-1021). Springer, Berlin, Heidelberg.

Nahm, F. S. (2022). Receiver operating characteristic curve: overview and practical use for clinicians. *Korean journal of anesthesiology*, *75*(1), 25-36.

Citation: *FIRAS H. ZAWAIDEH & SALAH YOUSEF ABU BAKER. "Enhanced IOT Security using Cascaded Machine Learning" International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), vol 9, no. 2, 2023, pp. 23-34. DOI: https://doi.org/10.20431/2349-4859.0902003.*