ISSN 2278-3091
Volume 9, No.4, July – August 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse142942020.pdf
https://doi.org/10.30534/ijatcse/2020/142942020

Classification of IoT Gateway Intrusions using Machine Learning

[1]Guduri Sulakshana,[2]Kondamuri Hanumantha Rao
[1]Assistant Professor, Department of Computer Science and Engineering,
Institute of Aeronautical Engineering (IARE) College, Dundigal, Hyderabad
[2]Assistant professor, Department of Computer Science and Engineering, GITAM School of Technology,
Hyderabad Campus, India

ABSTRACT

From the several studies it has been shown that it is possible to significantly improve the classification accuracy and performance of the detection engine by carefully selecting the relevant features for the intrusion detection system. Currently, with the development of new technologies such as cloud computing and big data, a huge amount of network traffic is being generated, and the intrusion detection system needs to collect and dynamically analyze the data that is transmitted through incoming traffic. Nevertheless, not all features in a large data set reflect traffic, so to improve the accuracy and speed of the intrusion detection system, selecting a minimal set of features is required. This study proposes a feature selection mechanism that eliminates unrelated features and identifies features that help improve recognition, based on the number of points each of the features identified in the selection process determines. To accomplish this goal, a recursive feature removal procedure was used, which involved classification based on the decision tree, and the corresponding attributes were subsequently identified. This approach applies to the NSL-KDD dataset, i.e., 2017 KDD dataset used in this experiment by the machine learning library written in Python. This approach identifies relevant characteristics in the dataset and improves the level of accuracy. These results indicate that feature selection significantly improves classification performance. For identifying the appropriate functionality with relevant factors allows for a better planning of the intrusion detection system.

Key words: IoT, gateway protocols, intrusion detection system, machine learning, classification algorithms

1. INTRODUCTION

The Internet of Things aims to bring the world together. It is a concept of immense social, economic and technological importance. The big tech giants have already taken Kabbalistic business decisions to put them in the sky IoT. Telecommunications operators regard IoT as an essential part of business orientation. Cisco estimates the size of IoT devices and the financial impact of IoT on the global economy. The development of IoT is creating a new smart web for everything that fosters the next major concepts of socio-economic growth [1]. At the same time, however, IoT poses major challenges that hinder its full potential. News of Internet-connected hacking devices, cryptocurrency issues and privacy invasions have already attracted public attention. For example, IoT-based botnets have triggered the most widespread distributed denial of service (DDoS) attacks [2] in history.

Our work centers need to demonstrate a variety of Internet-related problems and develop new methodologies that can detect network anomalies and identify IoT devices that compromise the network. Our proposed method consists of two parts. The first part is based on machine learning (ML) strategies that are used to learn the general behavior of an IoT based network[3]. On the other hand, the second section is a rules-based approach that is configured and managed by the network administrator. These two components create a versatile and flexible model that ultimately allows for unusual operations and prevents security attacks.

One way to improve network security is to use Intrusion Detection Systems (IDS)[4]. IDS is one of the most productive methods to detect attacks on a network. This tool can detect network intrusions and vulnerabilities by comparing known attack patterns with current network activities. The methods used for IDS can be effective in detecting popular attacks by tracking network traffic on specific models. Interference-based detection systems detect attacks by monitoring the behavior of any system, object, or traffic and comparing it to a predetermined normal state. Machine learning techniques can be used to improve detection methods by automatically creating new rules for signature-based IDSs or following identity patterns in interference-based IDSs.

A data set must be used to create a machine learning classification. There are some popular datasets that can be used to play IDS using machine learning techniques to

detect network intrusion. IoT Network Intrusion Dataset [5] that is available at https://ieee-dataport.org/open-access/iot-network-intrusion-dataset has been used to conduct the analysis.

2. RELATED WORK

Hector et.al. [6](2019) have conducted a study on challenges in cybersecurity, especially in the area of IoT. The authors' focus was on to classify the attacks on MQTT which is one of the protocols used for IoT. They have addressed two varieties of classification of attacks, ensemble methods and deep learning models. To conduct the experiment as well to build the classification model, the authors have used the MQTT dataset. To perform the classification GRU, LSTM and XGBoost models were used. The results have shown that the model has demonstrated its efficiency with GPU implementation.

Peiyuan et.al. [7](2018) have proposed a machine learning-based model to analyse the attacker activities based on the intuition that the probability of launching temporal close attacks is more when the attackers are in the same botnet. The authors have used Multivariate Hawkes Process to create a model for temporal patterns. After clustering the attacker activities, a weighted influence matrix was developed for analysis of the attacks. The work has demonstrated the efficiency to analyse the attacks with their model.

Christos et.al. [8](2018) have attempted to establish an architecture to enhance the security issues in the IoT network. The work includes developing and installing a security wall between the Internet and Cloud Server. Through this development the authors have tried to provide a secure communication among the communication elements connected to IoT. From their work it has been proposed that heterogeneity is the major challenge for the cloud server, whereas reliability and monitoring the Internet of Things are the challenges. However, the work was concluded with a finding that cloud computing offers a green and efficient sustainable computability.

Ankur et.al. [9](2018) have discussed about the Distributed Denial of Service (DDoS) attacks on the IoT systems. In the process the authors have explored various DDoS attacks and their severity on various IoT layers. Their work has also elaborated on usage various tools to detect and overcome those attacks. Authors, after their study, have proposed their view IoT systems need to improve the techniques that are adopted to deal the DDoS attacks on IoT system.

Hezam et.al. [10](2018) have proposed a reference model based on the building blocks to deal with the attacks on IoT. Through the survey the authors have studied the surface of attacks based on four components: IoT hardware, IoT protocol stack, data, and IoT software. Subsequently, they have proposed the taxonomy of the each IoT attack and have derived the relationship between the IoT attacks and the connected security violations.

Daniel et.al.[11](2018) have proposed a security solution after studying various IoT suspicious security events. In the process, the authors have explored for various IoT security vulnerabilities as well as the unique features of the IoT devices by which they are most targeted. The entire analysis has helped to work upon proposing the security solution which understands the causes and symptoms in an effective way.

Pal et.al. [12](2017) have worked on possible security threats and the related issues that can occur while automating various IoT tasks. In the process the authors have studied the security issues that are related to the protocol stack of IoT networking layer. Attacks such as Denial of Service and Man-in-the-middle have shown their significant effect on the IoT communication. The authors have suggested that the mitigation techniques such as authorization, bidirectional link authentication, passive probing, and active firewalls would be better security measure.

Shahab et.al. [13](2017) have conducted a survey on various framework used for communication and computation for the IoT systems. The survey was focused in the IoT industry perspective, in which hardware and protocols were studied in the initial phase. Subsequently, the authors have proposed a layered framework added with the addressing of need for layered computational elements. Finally, a security system was derived on the basis of security metrics where the considered parameters were: Physical Availability, Cyber Availability, Integrity, and Confidentiality.

Jin [14](2017) has reviewed the CPSs in the context of industry 4.0, IoT and the connected service platforms. The author has found that the CPS has been established for the industries such as healthcare, transportation, manufacturing and smart grid. However, it was also found that other industries which are compliant to Industry 4.0 lack cloud-based CPS which will provide a better solution towards secured communication as well as secured storage.

Yair et.al.[15](2017) have performed a research on applying one of the machine learning algorithms, Radom Forest, for extracting the features of IoT traffic. In the process of modelling the classifiers the authors have selected 17 dissimilar IoT devices, which represent nine IoT device types. Classification was applied on twenty consecutive sessions on which majority rules was applied. The results from the experiment have demonstrated that as the number of consecutive sessions grow the accuracy of classification grows.

3. IOT COMMUNICATION AND INTRUSION THREATS

The most of the utilities we use today in our daily lives are connected to the Internet. These utilities interact with each other via a distributed network, sharing and maintaining communication for a particular task. Relatively, the Internet of Things (IoT) is a innovative concept that allows a higher level of interaction on a huge number of distributed applications.As the IoT concept includes machine-to-machine communication (M2M) [16], they have become part of smart device systems. The IoT consists of integrated systems that measure environmental conditions using sensors.For example, collecting and analyzing sensor data such as temperature and air pollution can yield significant results, such as the relationship between dimensions and expectations regarding consumer behavior and further analysis.

In such a system, hundreds of different types of devices must be connected to each other with thousands of sensors. In addition, each of these devices can be used for a different specific task requiring data rates, packet sizes, etc. different. Therefore, such a communication network becomes very different, figure 1. Specific communication protocols are required to connect the extended IoT devices to the network in a distributed manner.

Most IoT devices typically have inexpensive and restrictive resources, such as network connection, power, and processing limitations. Communication protocols are essential for managing data flows and determining how the IoT interacts with each other. Unlike simple communication protocols, IoT requires new flexible protocols for different and restrictive devices. Specifically, the holding devices are not sufficient to meet the high demands of HTTP communication. The Internet Engineering Task Force (IETF) standardizes protocols that allow light communication to reduce the need for more complex protocols for blocked devices.

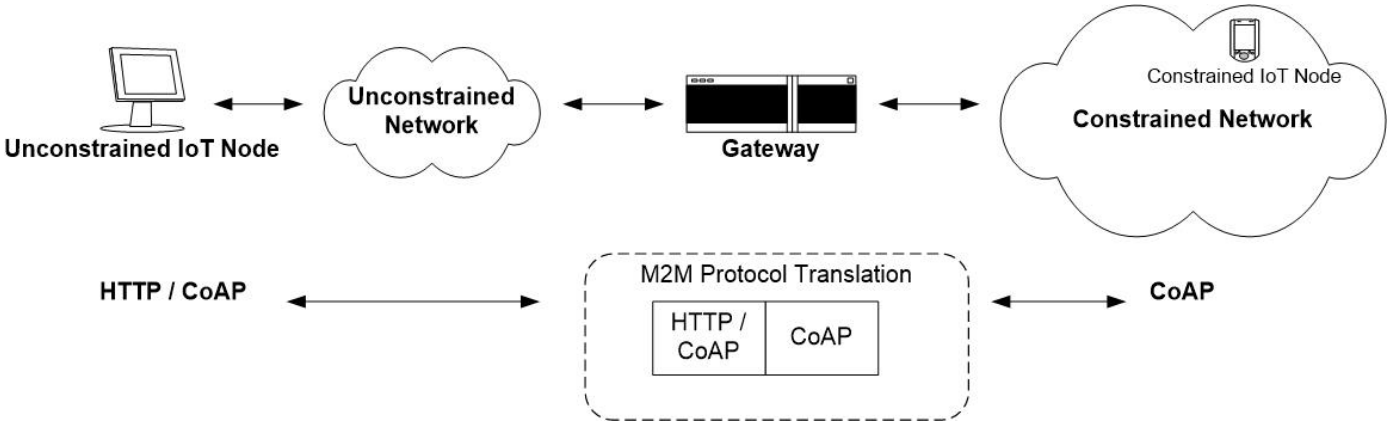

Figure 1: Communication in IoT

A. IoT Gateway Protocols

CoAP is a forwarding protocol based on a UDP layer optimized for restricted nodes and restricted networks. Since CoAP was first inspired by HTTP, the REST architecture has been used [17]. It is then standardized by an independent group called the Internet Engineering Task Force (IETF). In addition, communication between server and client is peer-to-peer. However, the server or client can respond to single and multicast requests. CoAP has four different types of messages to request resources from the server: GET, PUT, POST and DELETE.

MQTT is a lightweight M2M communication protocol for restrictive devices and untrusted networks. It has a publisher / subscriber client that manages TCP / IP. Additionally, TCP provides bidirectional connections between message reliability and nodes [18]. Nodes can publish messages with certain elements to the intermediary, and therefore different nodes can subscribe to those elements to receive messages. Communication involves a broker who controls the traffic to this message. A broker is actually server and mail traffic that customers can post / subscribe to. In addition, clients can authorize a broker by accessing their username and password. The MQTT supports three QoS levels to determine the quality of the message being sent. Message security is encrypted with SSL / TLS.

XMPP is a protocol that enables communication and transfer of files between nodes on a distributed network using XML technology [19]. Communication, such as instant messaging, group chat, collaboration, presence and other forms of data transfer such as audio and video, is based on TCP. In addition, XML stanzas support real-time communication. Allows the server to authorize specific clients to access the XMPP server and authorizes messages for these clients using XML strings. In addition, XMPP assigns a client presence index, such as online, offline, or busy. Therefore, the client notifies the server whether the mail is compatible.

B. Vulnerabilities of IoT gateway protocols

Data networks, especially wireless, are prone to a large number of attacks such as eavesdropping, spoofing, denial of service and so on. Legacy Internet systems mitigate these

attacks by relying on link layer, network layer, transport layer or application layer encryption of the underlying data. Though some of these solutions are applicable to the IoT domain, the inherently limited processing and communication capabilities of IoT devices prevent the use of full-fledged security suites.

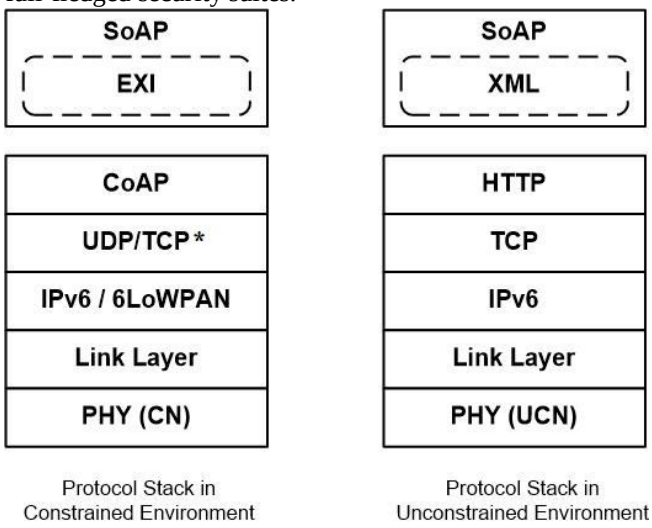

Figure 2: Protocol stack for Constrained Unconstrained environments

Figure 2 shows a possible stack of IoT device protocols based on the CoAP (left). 6LoWPAN determine how to run an IPv6 address on an IPv6 network [20]. The transport layer should use UDP, but an optimized transport solution is optional if the application requires it. In the figure 2, TCP* works as a dedicated transport protocol that is different from TCP and optimized for CN. In fact, standard TCP CNs are usually suboptimal due to significant delays, large packet loss, and their specific traffic generated by small packets of request / response pairs. SOAP (Simple Object Access Protocol) can be used to exchange structured information in an application layer based on the efficient XML Interchange (EXI).

C. Weaknesses and threats of IoT gateway protocols

CoAP

The messages are not reliable. Hence acknowledgement packets are sent to verify the messages' successful arrival at the destination. However, this does not illustrate whether or not these messages are properly decoded. CoAP has not been standardized yet. Among other protocols this is the most unstandardized [2, 12]. Unreliable messages with no proper decoding allow the intruders to manipulate the packets through injecting malicious content. Whether or not CoAP is standardized the lack of reliability is sufficient for the attacks or intrusions.

MQTT

MQTT uses TCP / IP, and TCP needs additional communication features compared to Non-UDP. The broker has limited communication capabilities [2]. All nodes are coupled to a broker. Hence, communication breakdowns when a broker fails, and becomes a single point of failure.

XMPP

XMPP server's communication capacity is limited. To authorize the client's request for the server's access, it takes longer time. Moreover, the usage of XML stanzas results into delay in the communication.

4. MACHINE LEARNING AND INTRUSION CLASSIFICATION

A. Machine Learning

In the areas of detailed analysis, prediction, automation Machine Learning has proved its efficiency in various instances. The fundamental concept of the machine learning is to scientific algorithms, and statistical models which are used to train the computer system, so that the resultant analysis would be more helpful to derive the insights. Machine learning is broader by its implementation, hence a number of branches were evolved to complement the machine learning algorithms, such as supervised, unsupervised, reinforcement learning, etc. The general approach of machine learning is to build a mathematical model from the dataset to reach the goal of the machines be able to think.

B. Role of Machine Learning in classification

In applications that manage sensitive data, it is important that the characteristic vector x and model w remain confidential to one or more parties. Intrusion detection study including a model made from private communication profiles of some machines; the model is sensitive because it releases information about machines and their processes. There are two major challenges when it comes to designing effective privacy classifications [9]. The first is that it is difficult to calculate sensitive data by some taxonomists (such as decision trees), which makes effective management difficult. The second offers a more general solution than the three classifiers: creating a unique solution for each classifier does not provide insight into how these classifiers combine or construct other classifiers.

C. Decision tree as a classifier

When there is a need for better classifier in the evolution of digital era, especially big data, decision tree algorithm has played a significant role in many diversified disciplines. Most significant feature of decision tree is its capability to capture the descriptive knowledge from the available data for a decision-making. Decision trees are computed through the training sets [15]. Based on anobject set, the decision tree is generated where objects belong to any one of classes ranging from C_1, … C_i … C_n. the process involves two steps:

- Decision tree consists of a leaf, if all the objects in the dataset belong to same class,
- Else, test partitions are created as subsets from which a specific outcome can be derived.

This process would be applied in recursion until all the objects are explored.

D. **Classification of intrusions and attacks on IoT gateway protocols using Machine Learning**

To develop the experiment methodology for the classification of intrusion attacks on the IoT gateway protocols, figure 3, it is essential that they are carried out in five steps: i) apply the dataset for cleaning and preprocessing, ii) resizing the features, iii) selection of appropriate features, and iv) building a classifier model, and v) predictive analysis and evaluation.

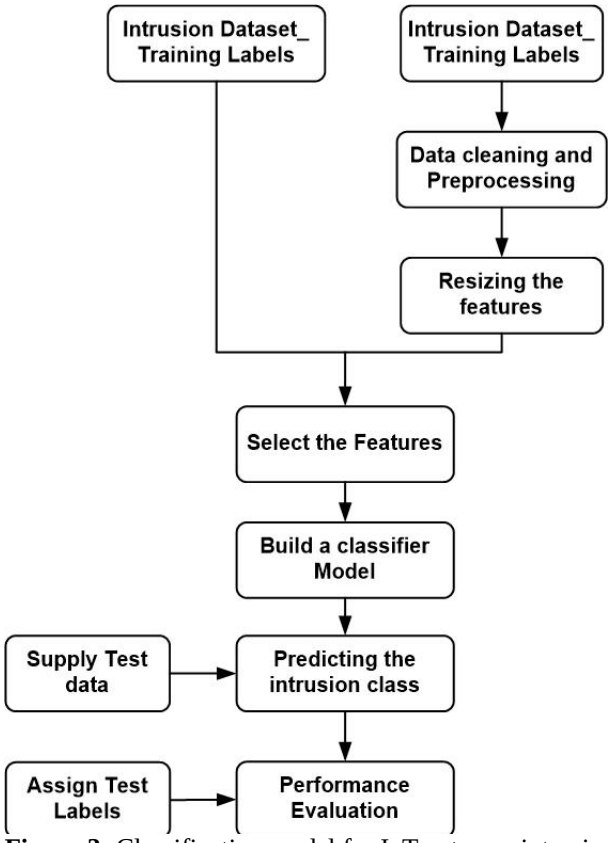

Figure 3: Classification model for IoT gateway intrusions

Basically, at this point, the data set has to go through a cleanup process to remove duplicate records, since the NSL KDD data set has already been cleaned up, this action is no longer required. The next pre-processing step is needed as the dataset contains both digital and non-digital instances. Usually, the Scikit-Learn estimator (classifier) works well with digital inputs, so a single k or one hot coding method is used to perform this transformation. This technique converts each classification attribute into m binary attributes with m possible entries, only currently active.

From the enormous set of features, appropriate features have been selected for the purpose of conducting the experiment. One of the approaches adopted to resizing the features was to avoid those features which contain large values which would create a great weight while analyzing the final results.

The next phase is selecting the features to get rid of irrelevant and redundant data. It is a technique that selects a subset of related characteristics that fully reflect a given problem with minimal reduction by distributing and analyzing the two factors to explain why feature selection is recommended: First, irrelevant attributes are more likely to reflect interactions between attributes and target classes that simply result from inadvertent and incorrect modeling of the problem. This aspect involves over-customization, usually in the Decision tree classification. Second, a large number of functions significantly increase the computation time without a corresponding classification improvement.

The entity selection process begins with a single entity selection with ANOVA-F test for entity recognition; individual entity analysis analyzes each entity individually to determine the strength of entity relationships in the sklearn.feature_selection module. The method of features selection was based on the highest score. When the best subset of functions is found, a repeated feature removal is applied that re-creates the template, overrides the feature, and then repeats the process with the remaining features until all the properties in the data set are exhausted. As such, it is a good optimization to find the best performance for your features. The idea is to use classification weights to get entity classification.

The decision tree model is designed to partition data using information mining as long as there is a single class of labels in the context of each page node. It is a simple but effective hierarchical method of supervised learning (classification or regression) that identifies a local space (area) in a small number of steps (small) at intersections. repeated. Each test uses one attribute to split a node according to the attribute values. After separation of each branch, if all selected cases belong to the same class, the compartment shall be considered complete or clean.

One possible method to measure a good partition is entropy or information retrieval. Entropy is a measure of uncertainty based on information theory, which is found in a teaching set because there are several classifications. The decision tree generation process by repartitioning the properties is equivalent to repartitioning the original format into smaller sets (i.e., all have the same example target class) until the entropy of each of these subgroups is zero.

Decision tree (DT) is the collection of nodes of internal decisions and terminal pages. The verification function is performed by each decision node with discrete results, marking the branches. As input is provided, a test is created at each node and one of the branches is considered based on the result. Here, the learning algorithm starts from the source and repeats this process until the page node is reached, at which point the value displayed on the page node is output. Each page node has a result label that is a class target in terms of classification and regression numerical value. A page node can describe a localized space or region that has the same labels for classifying instances found in this input space (area) and have a similar regression numeric value.

To perform the evaluation and classification analysis the test data was utilized. Number of settings were considered for the evaluation such as precision, accuracy score, recall, f-measure and building a confusion matrix. During the entire process a 10-fold validation was applied.

5. RESULTS AND DISCUSSION

Functional selection is used to describe redundant and irrelevant data. It is a technique for selecting a subset of relevant characteristics that fully reflects a given problem with minimal deterioration. Therefore, a small number of features would produce a better result.

A common technique to select functionality is to recover the least functionality that is able to correctly classify workout data. If the attribute is always identical to the label class (that is, it is an exact ict companion), it is sufficient to classify the data. On the other hand, if an attribute always has the same value, its expected power is reduced and much weaker. Repeat functionality is a workaround method that recreates a model, overrides an attribute, and then repeats the process with the remaining attributes until all data set properties are exhausted. The purpose of repeating functionality is to regain functionality by re-inserting small and small group attributes.

A good feature ranking criterion does not give a good subset of features. Some criteria measure the effectiveness of removing a single symptom along with the goal to be achieved. By removing several functions at the same time, they are not very optimal, which is necessary to obtain a small subset of functions. This issue can be resolved using the following repeat procedure:

- Training the classifier (optimization of the characteristic weights against the criteria).
- Ranking criteria for the entire feature set has to be computed.
- Identify those features with small ranking criteria and remove them.

First, the classification is prepared for an initial set of characteristics, and weights are assigned to each property. The absolute weight of certain entities is then removed from the current properties. The method is repeated in the pruning kit until the desired number of properties is achieved. As such, it is a good optimization to find the best performance for the features. It should be noted that RFE does not influence correlation methods as the classification criterion is calculated using information on one attribute.
After selecting the appropriate characteristics, an analysis was performed to determine the accuracy of our estimators. A significant improvement in the overall performance of the proposed model was observed when comparing the result with the performance evaluation with all selected characteristics.

To achieve a better performance of DT classifier from an exhaustive feature set, table 2, a selective feature set, table 1, has been derived. To perform this operation a one of machine learning techniques for dimensionality reduction, principal component analysis (PCA) was applied on 2017 KDD dataset.

Table 1: Performance evaluation with the limited feature set

Accuracy	Precision	Recall	F-measure	Number of features	Class	Classifier
99.92	99.71	99.81	99.76	12	DoS	DT
99.82	99.39	99.39	99.39	15	Probe	
99.90	97.42	97.43	97.42	14	R2L	
99.96	99.72	99.71	99.72	11	U2R	

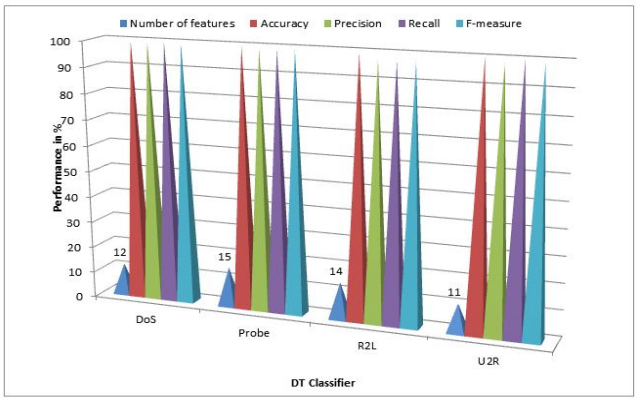

Figure 4:DT Classification performance on different attributes

Table 2: Performance evaluation with 52 features

Accuracy	Precision	Recall	F-measure	Number of features	Class	Classifier
99.68	99.52	99.73	99.63	52	DoS	DT
99.59	99.06	98.86	98.96	52	Probe	
97.05	95.85	95.61	95.73	52	R2L	
99.66	99.68	99.63	99.67	52	U2R	

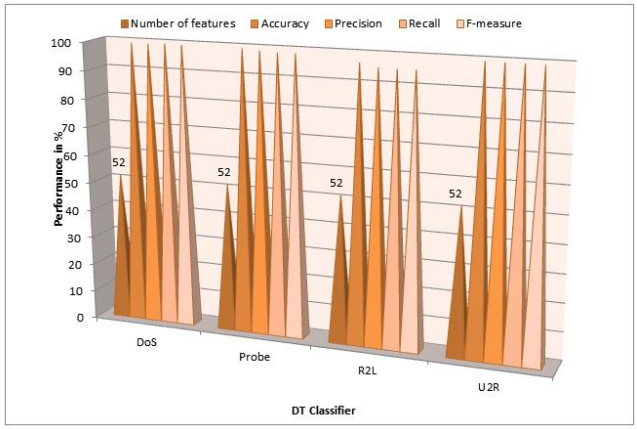

Figure 5:.DT Classification performance on fixed number of attributes

6. CONCLUSIONS AND FUTURE SCOPE

The work carried for this paper demonstrates the importance of using a set of functionalities that is associated with the corresponding classification training algorithm for IDS modeling. Demonstration and initiation of the entity selection method, which involves unique entity selection associated with redundant entity elimination, was performed using a decision tree classification to identify critical entities. This process repeatedly overrides the attribute and repeats the process with the remaining attributes until all data set properties are exhausted. The effectiveness of the method was assessed using a different classification metric, and by reducing the number of characteristics, it was shown that the accuracy of the model could be improved. The feature selection method proposed in this article has a high accuracy score, and features are identified by information acquisition and classification techniques.

REFERENCES

[1]R. Roman-Castro, J. Lopez, and S. Gritzalis, "Evolution and Trends in IoT Security," *Computer (Long. Beach. Calif).*, vol. 51, no. 7, pp. 16–25, 2018 doi: 10.1109/MC.2018.3011051.

[2] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, 2018 doi: 10.1109/JIOT.2017.2767291.

[3] S. Tweneboah-Koduah, K. E. Skouby, and R. Tadayoni, "Cyber Security Threats to IoT Applications and Service Domains," *Wirel. Pers. Commun.*, vol. 95, no. 1, pp. 169–185, 2017 doi: 10.1007/s11277-017-4434-6.

[4] Á. Asensio, Á. Marco, R. Blasco, and R. Casas, "Protocol and architecture to bring things into internet of things," *Int. J. Distrib. Sens. Networks*, vol. 2014, 2014 doi: 10.1155/2014/158252.

[5] Y. Sun, H. Song, A. J. Jara, and R. Bie, "Internet of Things and Big Data Analytics for Smart and Connected Communities," *IEEE Access*, vol. 4, pp. 766–773, 2016 doi: 10.1109/ACCESS.2016.2529723.

[6] H. Alaiz-Moreton, J. Aveleira-Mata, J. Ondicol-Garcia, A. L. Muñoz-Castañeda, I. García, and C. Benavides, "Multiclass Classification Procedure for Detecting Attacks on MQTT-IoT Protocol," *Complexity*, vol. 2019, 2019, doi: 10.1155/2019/6516253.

[7] P. Sun, J. Li, M. Z. Alam Bhuiyan, L. Wang, and B. Li, "Modeling and clustering attacker activities in IoT through machine learning techniques," *Inf. Sci. (Ny).*, vol. 479, pp. 456–471, 2019 doi: 10.1016/j.ins.2018.04.065.

[8] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT," *Sustain. Comput. Informatics Syst.*, vol. 19, pp. 174–184, 2018, doi: 10.1016/j.suscom.2018.06.003.

[9] A. Lohachab and B. Karambir, "Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks," *J. Commun. Inf. Networks*, vol. 3, no. 3, pp. 57–78, 2018, doi: 10.1007/s41650-018-0022-5.

[10] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 3, pp. 355–373, 2018, doi: 10.14569/IJACSA.2018.090349.

[11] D. Díaz López et al., "Shielding IoT against Cyber-Attacks: An Event-Based Approach Using SIEM," *Wirel. Commun. Mob. Comput.*, vol. 2018, 2018 doi: 10.1155/2018/3029638.

[12]P. Varga, S. Plosz, G. Soos, and C. Hegedus, "Security threats and issues in automation IoT," *IEEE Int. Work. Fact. Commun. Syst. - Proceedings*, WFCS, 2017 doi: 10.1109/WFCS.2017.7991968.

[13]S. Tayeb, S. Latifi, and Y. Kim, "A survey on IoT communication and computation frameworks: An industrial perspective," *2017 IEEE 7th Annu. Comput. Commun. Work. Conf. CCWC 2017*, vol. 1301726, pp. 1–6, 2017, doi: 10.1109/CCWC.2017.7868354.

[14]J. H. Kim, "A Review of Cyber-Physical System Research Relevant to the Emerging IT Trends: Industry 4.0, IoT, Big Data, and Cloud Computing," *J. Ind. Integr. Manag.*, vol. 02, no. 03, p. 1750011, 2017, doi: 10.1142/s2424862217500117.

[15]Y. Meidan et al., "Detection of Unauthorized IoT Devices Using Machine Learning Techniques," 2017.

[16] E. Ahmed et al., "The role of big data analytics in Internet of Things," *Comput. Networks*, vol. 129, pp. 459–471, 2017, doi: 10.1016/j.comnet.2017.06.013.

[17] G. Elhayatmy, N. Dey, and A. S. Ashour, Internet of Things Based Wireless Body Area Network in Healthcare. 2018.

[18] J. Roux, É. Alata, G. Auriol, V. Nicomette, and M. Kâaniche, "Toward an Intrusion Detection Approach for IoT Based on Radio Communications Profiling," *Proc. - 2017 13th Eur. Dependable Comput. Conf. EDCC 2017*, pp. 147–150, 2017 doi: 10.1109/EDCC.2017.11.

[19] J. T. Kim, "Requirement of security for IoT application based on gateway," *Int. J. Secur. its Appl.*, vol. 9, no. 10, pp. 201–208, 2015 doi: 10.14257/ijsia.2015.9.10.18.

[20] M. Abomhara and G. M. Køien, "Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks," *J. Cyber Secur. Mobil.*, vol. 4, no. 1, pp. 65–88, 2015, doi: 10.13052/jcsm2245-1439.414.