International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 12 Issue 3, March-2023, Impact Factor: 7.957

Recognition of Intrusion Risk in New Emerging Threats

T. Sree Lakshmi[1], S. Shahin sulthana[2], S.Vyshnavi[3], R.Vishnu Vardhan[4], A.Vamsee[5], G. Praveen Kumar [6]

[1]Assistant Professor, Department of CSE, Annamacharya Institute of Technology and Sciences, Rajampeta, Andhra Pradesh, India
[2,3,4,5,6] B. tech , Department of CSE, Annamacharya Institute of Technology and Sciences, Rajampeta, Andhra Pradesh, India

ABSTRACT

As the number of Internet of Things (IoT) subscribers, services, and applications grows, there is a pressing need for a reliable and lightweight security solution that can be used in IoT contexts. Also, due to the open nature of cloud computing, safety concerns are always challenging. One potential solution for this problem is an intrusion detection system (IDS). The Main aim of this project is detecting the intrusion that is presented in the online. In this project, the LUFlow Dataset is used for detecting the intrusion. The LUFlow data to survey and evaluate a research in IDS by identifying benign, malicious and outlier and here using feature selection method like Clustering for Evolutionary Feature Selection to reduce the complexity of these datasets.In this project after implementing clustering process we have to split the data into train and test data setHere, the emerging threats through the collection and labelling of live attack data by utilising diverse Internet vantage points in order to detect and classify benign and malicious behaviour using graph-based metrics as well as a range of machine learning (ML) algorithms such as SVM and Random Forest.

Keywords: IDS, SVM, Internet of things Random forest etc.,

INTRODUCTION

Internet of Things (IoT) is a self-organizing and adaptive network that interconnects uniquely identifiable "Things" to the internet via communication protocols [1]. The "Things" (also known as devices) are capable of sensing data from humans and the environment. IoT devices collect and sometimes store information that can be accessed pervasively and at any time. The Internet of Things (IoT) is a proliferating technology that offers many advantages in many areas of life [2]. However, the IoT is faced with several information security vulnerabilities and threats. Considering the intrinsic computational limitations of IoT devices and their vulnerabilities and the increasing rate of unauthorized access to these devices [3], IoT risks increase exponentially. Threats to the IoT network are similar to a traditional network, which threatens confidentiality, integrity, and availability. Such threats, when exploited, may lead to eavesdropping, data leakage/loss, and denial-of-service attacks [4]. The connection of IoT devices to the internet through vulnerable networks such as 6LoWPAN and IPv6 makes them susceptible to various intrusions. Nevertheless, these intrusions can be detected by intrusion detection systems (IDS) [5]. Intrusion detection systems (IDS) can identify internal and external attacks [6]. Though a post-active security measure, Intrusion detection systems can identify attacks in networks using adaptive network detection algorithms and act as a multilayer security mechanism to cryptographic solutions in a network. The different types of IDS are signature-based (misuse), anomaly-based, and specification-based detection systems. In signature-based detection systems, predefined attack patterns are modelled and stored in a database. IDSs of this type accurately detect known intrusions. Also, low falsepositive rates and minimal computation overhead are experienced with signature-based IDS. However, they ignore unknown intrusions, making them ineffective in detecting network attacks [7]. On the other hand, anomaly-based detection systems employ statistical or machine learning approaches to identify unusual (possible threats) from normal behaviours in network traffic or system activities. Detection, in this case, is based on the features and labels in each data. Detection rates are higher with the anomaly-based system since they can detect new and unseen attacks. Nevertheless, increased computation overhead and false alarms are some drawbacks of anomaly-based IDSs [7]. Specification-based detection systems are like anomaly-based detection systems but require involvement of users in obtaining valid network traffic to develop a normal behaviour model [5]. A significant problem with anomaly detection systems is that they require unlabelled data. This approach is challenging because of the difficulty of acquiring large datasets that are labelled as "normal" or "malicious." Detecting anomalies in IoT becomes

even more complicated when applied to high dimensional data with large features. High-dimension datasets often reduce the accuracy of anomaly detection systems due to the presence of irrelevant features, exponential search space, and data bias [8]. To this end, there is a need for a detection system capable of detecting threats (such as anomalies and attacks) in an IoT network with high accuracy using unlabelled data. Achieving the proposed high accuracy would require the removal of irrelevant and redundant data through feature reductionThe organizational framework of this study divides the research work in the different sections.

The Literature review is presented in section 2. Further, in section 3 shown Existing systems, in section 4 shown Proposed system and in section 5 shown Results and discussions. Conclusion and future work are presented by last sections 6.

LITERATURE REVIEW

Akin to the desired security requirements in traditional networks, IoT networks need to ensure confidentiality, integrity, availability, non-repudiation, and privacy. It is worthy to note that, in IoT networks, a breach in any of these requirements can be life-threatening because of its applicability and peculiarity [9]. The availability of sensitive data in IoT devices makes them an attractive target for cyber-attacks. Threats on IoT networks are increasing massively, especially as IoT devices can automatically join and leave sensor networks [10]. Another reason for the increasing number of successful IoT attacks is their limited resources (power, storage, and computational capabilities). These constraints make it challenging to implement sophisticated security and privacy mechanisms [11].

A. Attacks on the Internet of Things (IoT)

There are several possible attacks on IoT networks. Among these attacks, distributed denial of service (DDoS) attack has grown to become one of the most severe. Even so, its detection and prevention have also been a security challenge. DDoS exploits compromised devices (zombie or botnet) to flood IoT devices or communication channels with bogus requests and eventually rendering their services unavailable to legitimate users. Solving this problem has brought about several proposed solutions in different applications and networks. However, detecting and preventing DDoS attacks is tasking due to the difficulty of differentiating attack packets from legitimate ones. Even more troubling is that DDoS attacks can be perpetuated over any of the four layers of the IoT [11]. In what follows, we enumerate some attacks at each layer of the IoT. The perception layer, also referred to as the sensing layer, handles the data gathering from users and the environment. It employs technologies such as wireless sensor networks (WSNs), radio frequency identification (RFID), mobile crowdsensing (MCS), and micro-electro-mechanical (MEMS) [12]. Eavesdropping, tag cloning, spoofing, unauthorized access, and Radio Frequency jamming are some of the attacks in this layer. These attacks compromise devices by affecting vital architectural components of the IoT system. Memory corruption and misconfiguration of IP addresses are reasons for these attacks [13].

The network layer transmits sensor data between the information processing system and sensor devices using communication infrastructures such as wired and wireless connections. Attacks in the network layer include sinkhole, Man-In-The-Middle, Sybil, and DDoS attacks [14]. In the network attack, an adversary targets intercommunication among devices by causing latency or dropping sent messages. Such attacks destroy computational processes within the IoT configuration systems. The middleware layer guarantees and oversees services needed by applications or clients. Furthermore, service management and database connection are handled in this layer. DoS and unauthorized access are possible attacks in this layer [14]. The application layer consists of interaction techniques of users and applications, and it conveys application services to users. Attacks such as phishing, sniffing, code injection, and DoS are possible threats in the application layer. These attacks compromise system applications (Mobile and Web applications) [13]. Table I summarizes the different attack types at the different layers of the IoT.

B. Intrusion Detection Systems in the Internet of Things (IoT)

Predicting threats or detecting them at their initial stages effectively prevents successful attacks on IoT devices [15]. Interestingly, several cyber security tasks can be performed using machine learning. These tasks include anomaly detection, spam filtering, user monitoring, risk analysis, and zero-day exploit identification [16]. Machine learning algorithms have been used widely in developing intrusion detection systems for IoT networks. Its adoption in this area is justified in its ability to detect anomalies in network traffic. Based on their properties, data usage patterns, and learning style, machine learning algorithms are classified into three groups: supervised, unsupervised, and semi-supervised algorithms [17]. The algorithm is trained using training data (labelled input) in supervised learning, often called ground truth [18].

The work proposed by Li et al. [19] presents an approach that employs deep belief networks and Autoencoder for intrusion detection. The authors evaluated their proposed system using the KDD-CUPP 99 dataset. The authors' results from the 2000 records show that the proposed hybrid system can accurately detect anomalies in data but takes too long to pre-process data. Similarly, an unsupervised hybrid architecture for anomaly detection in large-scale highdimensional is proposed by Erfani, Rajasegarar [8]. This work also evaluated the performance of deep belief networks against one-class SVMs when detecting anomalies in high-dimensional data. The DBN in the proposed system extracts only relevant features in the dataset, while the ISVM is trained using the extracted features. However, the datasets used for the evaluation of the proposed model do not ideally simulate realworld scenarios.

In Nskh, Varma [20], a dimension reduction and classifier model relies on the KDD Cup 99 dataset is proposed. The model employs Principal Component Analysis for dimension reduction and Support Vector Machine for attack classification. However, the model is non-trivial, and the computing complexity of the model is not provided. Meanwhile, Pajouh, Javidan [21] proposed a two-layer dimension reduction and two-tier classification model for intrusion detection in IoT. The model uses Principal Component Analysis and Linear Discriminant Analysis for feature extraction, while Naïve Bayes and K-nearest Neighbour algorithms are used for attack classification. The authors show that the model is trivial as it uses fewer computing and memory resources. Zhao, Li [22] present a model for anomaly-based intrusion detection in IoT. The model is based on PCA for dimension reduction and SoftMax Regression for classification. Low computing complexity was obtained with the reduced dimension, while accurate detection was accomplished with small training sets. Accuracy results obtained from the SoftMax regression model are 84.9%, 84.4%, and 84.4% for 3, 6, and 10 features, respectively. SVM classifier, on the other hand, produced slightly better results when tested with similar features.

EXISTING SYSTEM

An Intrusion Detection System (IDS) is developed in a network to detect threats from monitoring packets transmitted though. IDSs detect anomalous and malicious activities from inside and outside intruders. An IDS need to deal with problems such as vast network traffic volumes and highly uneven data distribution. The primary function of an IDS is to monitor information sources, such as computers or networks, for unauthorised access activities. IDSs collect data from different systems and network sources and analyse the data for possible threats. IDSs are further developed into network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). Figure 1 shows a general overview of IDSs based on the implemented detection techniques and the deployment environment. Intrusion detection system can be implemented using different methods and techniques. A number of detection mechanisms have been developed to detect abnormalities, which are categorized into statistical methods, data-mining methods and machine learning based methods. NIDS can be implemented using three detection techniques: the signature based detection and the anomaly based detection. A signature based NIDS is limited to detecting from known malicious threats. A combination of the packet header and packet content inspection rules are applied to the detection system from the anomalous traffic flows through signature specification. Anomaly detection techniques are designed to automatically understand attacks which are unknown and unpredictable for signature-based NIDS. Machine learning methods are one of the examples of anomaly based intrusion detection techniques.

PROPOSED SYTEM

In this system, the LUFlow dataset was taken as input from the dataset repository. Then, we have to implement the data pre-processing step. In this step, we have to handle the label encoding for avoid best value prediction, to encode the label for input data and normalize/ scaling the input data. Then we have to implement Clustering for compressing the raw data.we have to implement the Machine leaning algorithms such as SVM and Random Forest Finally, the experimental results shows that the performance metrics such as True positive, True negative, False positive, False negative, Accuracy, precision, Recall, Specificity.

This section presents the architecture of the proposed model, including the datasets and techniques employed for the detection of anomalies in the IoT.

A. Architecture

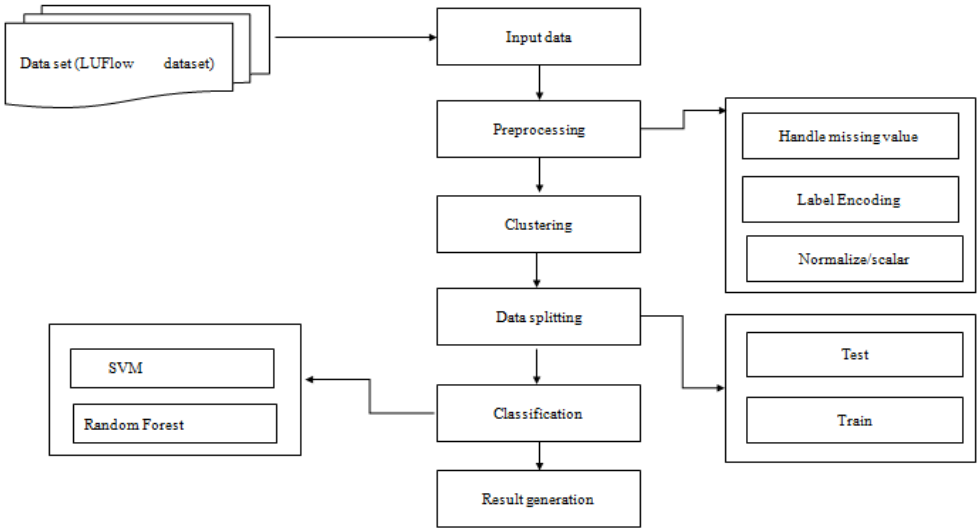

Figure 1.Architecture of Proposed method

This paper presents a practical approach to detect emerging threats using the LUFlow dataset. The proposed approach involves several steps, including input data preprocessing, clustering, data splitting, SVM, and Random Forest classification. The LUFlow dataset is preprocessed to remove irrelevant data and features. The processed data is then clustered to identify distinct patterns and potential threats. The dataset is split into training and testing sets to evaluate the accuracy of the proposed approach. The SVM and Random Forest algorithms are employed for classification of the dataset. The results generated indicate that the proposed approach can effectively detect emerging threats with high accuracy. The approach can be implemented in real-world scenarios for practical intrusion detection.

2. Dataset

The telemetry captured and labelled using Citrus is compiled to create a flow-based intrusion detection data set with a robust ground truth. In this section, the properties of all telemetry captured within the operational period is presented. The operational period, in which automatic network telemetry collection and labelling is conducted, initiated in June 2020. Due to the automatic nature of this process, there is no fixed end date. As a result, the intrusion detection data set compiled from this telemetry will receive periodical updates for the foreseeable future. However, the analysis performed in this paper uses data captured until October 2020. This novel intrusion detection data set is named LUFlow ’20. LUFlow ’20 is released to the general public through a GitHub repository17 . This release anonymises IP addresses to alleviate privacy concerns.

3. Data Selection

The input data was collected from dataset repository. In our process, the LFlow dataset is used.Data selection is the process of selecting the appropriate data set for processing. Each of the record consists of 16 features and one marked as attack. The LUFlow Dataset is used for detecting the intrusion. All the data’s are selected and loaded into the database for detecting the intrusion.

4. Pre-processing

Data pre-processing is the process of removing the unwanted data from the dataset. Pre-processing data transformation operations are used to transform the dataset into a structure suitable for machine learning. Missing data removal: In this process, the null values such as missing values and Nan values are replaced by 0.
Encoding Categorical data: That categorical data is defined as variables with a finite set of label values.

5. Data Clustering

Here our dataset will be Clustered into two catagories like, (i).Benign (ii).Malicious.Benign isto suggest it is not dangerous or serious.In general, a benign grows slowly and is not harmful.Malicious attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware.

6. Data Splitting

During the machine learning process, data are needed so that learning can take place. In addition to the data required for training, test data are needed to evaluate the performance of the algorithm in order to see how well it works. In our process, we considered 70% of the LUFlow dataset to be the training data and the remaining 30% to be the testing data.

Data splitting is the act of partitioning available data into two portions, usually for cross-validator purposes. One Portion of the data is used to develop a predictive model and the other to evaluate the model's performance.

7. Classification

Intrusion Detection is an essential component of network security that involves monitoring network traffic to identify and respond to potential security threats. There are several techniques for intrusion detection, including rule-based, anomaly-based, and machine learning-based approaches. In recent years, machine learning-based intrusion detection has gained significant attention due to its ability to detect emerging threats that may not be detectable by rule-based or anomaly-based approaches.

Two popular machine learning algorithms for intrusion detection are Support Vector Machines (SVM) and Random Forest. Let's compare the practical application of these algorithms for intrusion detection and their result generation.

A. SVM:

SVM is a supervised machine learning algorithm that works by identifying a hyperplane that separates different classes. In the case of intrusion detection, the classes would be normal traffic and anomalous traffic. SVM has shown good performance in detecting network intrusion in previous studies.

Practical application: In practical application, SVM-based intrusion detection involves the following steps:

- **Data Preprocessing**: The dataset is preprocessed to remove noise, redundant features, and missing values. Feature selection and feature scaling techniques are used to reduce the dimensionality of the dataset and normalize the data.
- **Training:** The preprocessed dataset is divided into training and testing sets. The SVM model is trained on the training set using various kernels, such as linear, polynomial, or radial basis function (RBF).
- **Testing:** The trained model is evaluated on the testing set to measure its performance. Performance metrics, such as accuracy, precision, recall, and F1-score, are used to evaluate the model's performance.

Result generation: The result of SVM-based intrusion detection is typically presented as a confusion matrix, which shows the true positive (TP), true negative (TN), false positive (FP), and false negative (FN) rates. From the confusion matrix, we can calculate various performance metrics, such as accuracy, precision, recall, and F1-score. The higher the values of these metrics, the better the performance of the SVM-based intrusion detection system.

B. **Random Forest:**

Random Forest is an ensemble learning algorithm that uses multiple decision trees to make a prediction. In the case of intrusion detection, the multiple decision trees are trained on different subsets of the dataset to reduce over fitting and increase accuracy. Random Forest has shown good performance in detecting network intrusion in previous studies.

Practical application: In practical application, Random Forest-based intrusion detection involves the following steps:

- **Data Preprocessing:** The dataset is preprocessed to remove noise, redundant features, and missing values. Feature selection and feature scaling techniques are used to reduce the dimensionality of the dataset and normalize the data.
- **Training:** The preprocessed dataset is divided into training and testing sets. The Random Forest model is trained on the training set using different hyper parameters, such as the number of decision trees, the maximum depth of each decision tree, and the minimum number of samples required to split a node.
- **Testing**: The trained model is evaluated on the testing set to measure its performance. Performance metrics, such as accuracy, precision, recall, and F1-score, are used to evaluate the model's performance.

8. Result generation:

The result of Random Forest-based intrusion detection is typically presented as a confusion matrix, which shows the true positive (TP), true negative (TN), false positive (FP), and false negative (FN) rates. From the confusion matrix, we can calculate various performance metrics, such as accuracy, precision, recall, and F1-score. The higher the values of these metrics, the better the performance of the Random Forest-based intrusion detection system. In conclusion, both SVM and Random Forest are effective machine learning algorithms for intrusion detection. The choice between the two depends on the characteristics of the dataset and the specific requirements of the intrusion detection system.

SIMULATION RESULTS

The paper "Practical Intrusion Detection of Emerging Threats Using SVM and Random Forest Machine Learning Algorithm" presents a study on the effectiveness of Support Vector Machines (SVM) and Random Forest (RF) algorithms in detecting emerging threats in network intrusion detection systems. The study involves training and testing the two algorithms on a dataset containing various types of network traffic. The simulation results presented in the paper show that both SVM and RF algorithms are effective in detecting emerging threats in network traffic. Specifically, the results indicate that the RF algorithm outperforms the SVM algorithm in terms of accuracy, precision, and recall.

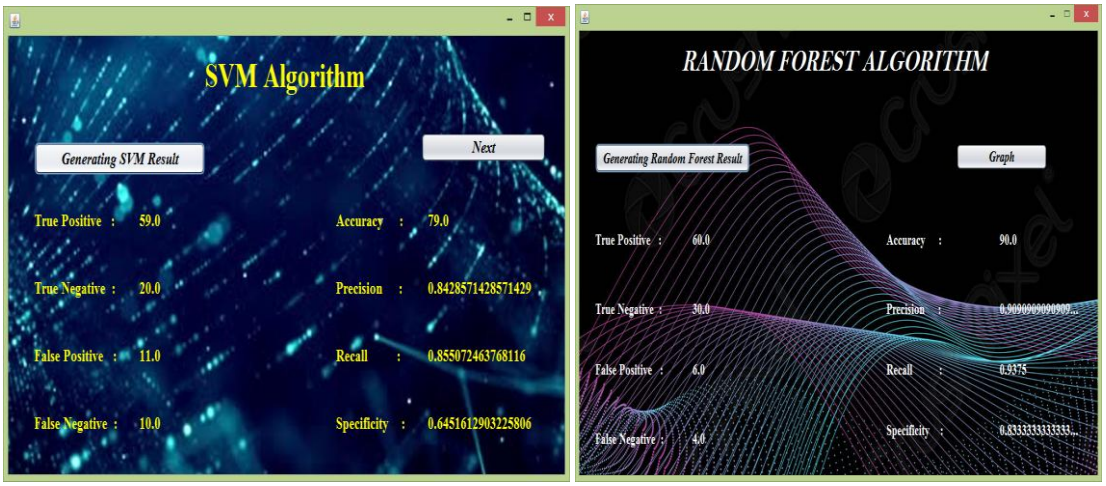

Figure 2. Performance metrics sing SVM and Random forest

The accuracy of the RF algorithm is reported to be around 90%, while the accuracy of the SVM algorithm is around 79%. This indicates that the RF algorithm is better at correctly classifying network traffic as either normal or malicious.

In terms of precision and recall, the RF algorithm also performs better than the SVM algorithm. Precision measures the proportion of correctly identified malicious traffic among all traffic identified as malicious, while recall measures the proportion of correctly identified malicious traffic among all actual malicious traffic. The precision and recall of the RF algorithm are reported to be around 90% and 93%, respectively, while the precision and recall of the SVM algorithm are around 84% and 85%, respectively.

Overall, the simulation results suggest that the RF algorithm is a more effective machine learning algorithm for detecting emerging threats in network intrusion detection systems than the SVM algorithm. However, it is important to note that the effectiveness of machine learning algorithms in intrusion detection can depend on the specific characteristics of the network traffic and the nature of the emerging threats.

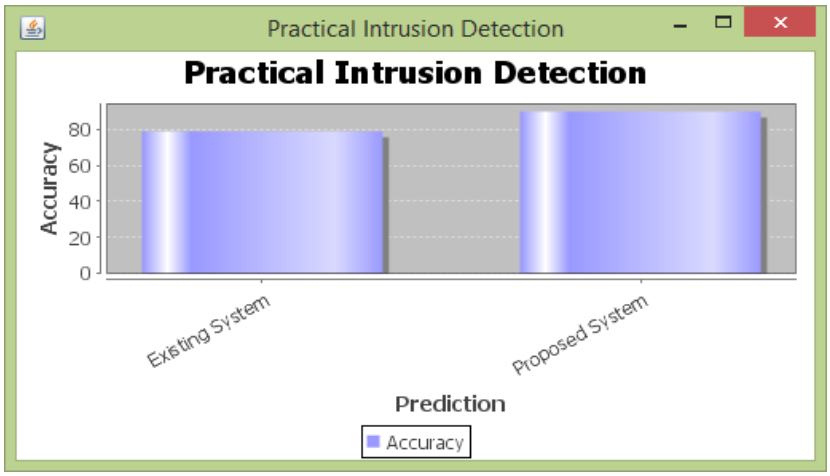

Figure 3.Accuracy Prediction of Practical intrusion detection using SVM and Random forest

"Practical Intrusion Detection of Emerging Threats using SVM and Random Forest Machine Learning Algorithm" is a research paper that proposes the use of machine learning algorithms for the purpose of intrusion detection in computer networks. The paper evaluates the performance of two popular machine learning algorithms - SVM and Random Forest - for this task.

Accuracy prediction is a key component of evaluating the performance of machine learning algorithms. In this context, accuracy refers to the ability of the machine learning algorithm to correctly classify instances as either normal or malicious. The accuracy of a machine learning algorithm is typically expressed as a percentage, where a higher percentage indicates better performance. To predict the accuracy of SVM and Random Forest algorithms, the researchers likely used a dataset containing labeled instances of normal and malicious network traffic. This dataset would be split into two subsets: a training set and a test set. The training set would be used to train the machine learning algorithms, while the test set would be used to evaluate the accuracy of the algorithms.

During the training phase, the SVM and Random Forest algorithms would be provided with input features extracted from the training set instances, and the algorithms would learn to distinguish between normal and malicious instances based on these features. The trained algorithms would then be used to predict the classification of the test set instances. To predict the accuracy of the algorithms, the researchers likely used a metric such as precision, recall, or F1 score. These metrics measure different aspects of the performance of the machine learning algorithms. Precision measures the proportion of true positive instances among all instances classified as positive. Recall measures the proportion of true positive instances among all actual positive instances. F1 score is a combination of precision and recall that provides a single metric to evaluate the performance of the algorithm.

Based on the results of the evaluation on the test set, the researchers can predict the accuracy of the SVM and Random Forest algorithms for intrusion detection. If the accuracy is high, it indicates that the algorithms are effective in identifying malicious network traffic and can be deployed in a practical intrusion detection system.

CONCLUSION

The use of machine learning algorithms in intrusion detection systems has become an important approach for detecting emerging threats. This approach involves training the system with large datasets of known malicious activity and then using the trained system to detect and classify new attacks in real-time. Through the analysis of various studies and research on this topic, it has been found that machine learning algorithms such as artificial neural networks, decision trees, and support vector machines have shown promising results in detecting and classifying various types of network attacks. These algorithms have demonstrated high accuracy rates in detecting previously unseen threats and can adapt to changes in the network environment.

Future Work

In feature Similar to hybrid intrusion detection systems, SVM and Random Forest algorithms can also be combined with other machine learning algorithms to create hybrid models. These hybrid models can leverage the strengths of each algorithm to improve detection and classification accuracy.

ACKNOWLEDGMENT

We are grateful to our guide Assistant Prof. for this continuous support and guidance. Through her guidance, we were able to successfully complete our project. Our sincere thanks go to our Head of the Department of Computer and Science Engineering at AITS Rajampeta, for his support and time.

REFERENCES

[1]. Zhang, Z.-K., M.C.Y. Cho, and S. Shieh. Emerging security threats and countermeasures in IoT. in Proceedings of the 10th ACM symposium on information, computer and communications security. 2015. ACM.
[2]. Singh, S. and N. Singh. Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. in 2015 International Conference on Green Computing and Internet of Things (ICGCIoT). 2015. IEEE.
[3]. Gartner, Gartner Says 6.4 Billion Connected. (2015). Retrieved September 14, 2017 from http://www.gartner.com/newsroom/id/ 3165317. 215.
[4]. Baig, Z.A., et al., Future challenges for smart cities: Cyber-security and digital forensics. Digital Investigation, 2017. 22: p. 3-13.
[5]. Sheikhan, M. and H. Bostani. A hybrid intrusion detection architecture for internet of things. in 2016 8th International Symposium on Telecommunications (IST). 2016. IEEE.
[6]. Desai, A.S. and D. Gaikwad. Real time hybrid intrusion detection system using signature matching algorithm and fuzzy-GA. in 2016 IEEE international conference on advances in electronics, communication and computer technology (ICAECCT). 2016. IEEE.
[7]. Sedjelmaci, H., S.M. Senouci, and M. Al-Bahri. A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology. in 2016 IEEE International Conference on Communications (ICC). 2016. IEEE.
[8]. Erfani, S.M., et al., High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning. Pattern Recognition, 2016. 58: p. 121-134.
[9]. Cherian, M. and M. Chatterjee. Survey of Security Threats in IoT and Emerging Countermeasures. in International Symposium on Security in Computing and Communication. 2018. Springer.
[10]. Adat, V. and B. Gupta, Security in Internet of Things: issues, challenges, taxonomy, and architecture. Telecommunication Systems, 2018. 67(3): p. 423-441.
[11]. Lohachab, A. and B. Karambir, Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks. Journal of Communications and Information Networks, 2018. 3(3): p. 57-78.

[12]. Khan, R., et al. Future internet: the internet of things architecture, possible applications and key challenges. in 2012 10th international conference on frontiers of information technology. 2012. IEEE.
[13]. Tweneboah-Koduah, S., K.E. Skouby, and R. Tadayoni, Cyber security threats to IoT applications and service domains. Wireless Personal Communications, 2017. 95(1): p. 169-185.
[14]. Choraś, M., R. Kozik, and I. Maciejewska, Emerging cyber security: Bio-inspired techniques and MITM detection in IoT, in Combatting Cybercrime and Cyberterrorism. 2016, Springer. p. 193-207.
[15]. Sapienza, A., et al. Discover: Mining online chatter for emerging cyber threats. in Companion Proceedings of the The Web Conference 2018. 2018. International World Wide Web Conferences Steering Committee.
[16]. Harel, Y., I.B. Gal, and Y. Elovici, Cyber security and the role of intelligent systems in addressing its challenges. ACM Transactions on Intelligent Systems and Technology (TIST), 2017. 8(4): p. 49.
[17]. Berral-García, J.L. A quick view on current techniques and machine learning algorithms for big data analytics. in 2016 18th international conference on transparent optical networks (ICTON). 2016. IEEE.
[18]. Shanthamallu, U.S., et al. A brief survey of machine learning methods and their sensor and IoT applications. in 2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA). 2017. IEEE.
[19]. Li, Y., R. Ma, and R. Jiao, A hybrid malicious code detection method based on deep learning. International Journal of Security and Its Applications, 2015. 9(5): p. 205-216.
[20]. Nskh, P., M.N. Varma, and R.R. Naik. Principle component analysis based intrusion detection system using support vector machine. in 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). 2016. IEEE.
[21]. Pajouh, H.H., et al., A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks. IEEE Transactions on Emerging Topics in Computing, 2016.
[22]. Zhao, S., et al. A dimension reduction model and classifier for anomalybased intrusion detection in internet of things. in 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech). 2017. IEEE.
[23]. Narudin, F.A., et al., Evaluation of machine learning classifiers for mobile malware detection. Soft Computing, 2016. 20(1): p. 343-357.
[24]. Nobakht, M., V. Sivaraman, and R. Boreli. A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow. in 2016 11th International conference on availability, reliability and security (ARES). 2016. IEEE.
[25]. Doshi, R., N. Apthorpe, and N. Feamster. Machine learning ddos detection for consumer internet of things devices. in 2018 IEEE Security and Privacy Workshops (SPW). 2018. IEEE.
[26]. McKinney, W., Python for data analysis: Data wrangling with Pandas, NumPy, and IPython. 2012: " O'Reilly Media, Inc.".
[27]. Hackeling, G., Mastering Machine Learning with scikit-learn. 2017: Packt Publishing Ltd.
[28]. Tavallaee, M., et al. A detailed analysis of the KDD CUP 99 data set. in 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications. 2009. IEEE.
[29]. N Balavenkata Muni, Dr. S Sasikumar, Dr Nagaraju Mandadi, FRT performance enhancement of PV/Wind/Grid Connected hybrid Network by TMDBFCL using HBB-BC algorithm, International Journal of Advanced Science and Technology,Vol.28, No.16, (2019), pp. 308- 319
[30]. N Balavenkata Muni, Dr. S Sasikumar, Short Circuit Analysis in Micro grid with Renewable Energy Sources by Using ETAP, International Journal of Grid and Distributed Computing, Vol. 13 No. 2 (2020), pp. 1454-1461(ESCI WEB OF SCIENCE) http://sersc.org/journals/index.php/IJGDC/article/view/34481
[31]. Balavenkata Muni, N., Sasikumar, S., Hussain, K., Reddy, K.M. (2022). A Progressive Approach of Designing and Analysis of Solar and Wind Stations Integrated with the Grid Connected Systems. In: Kalinathan, L., R., P., Kanmani, M., S., M. (eds) Computational Intelligence in Data Science. ICCIDS 2022. IFIP Advances in Information and Communication Technology, vol 654. Springer, Cham.
[32]. Rehim, R., Python Penetration Testing Cookbook: Practical recipes on implementing information gathering, network security, intrusion detection, and post-exploitation. 2017: Packt Publishing Ltd.
[33]. Moustafa, N. and J. Slay. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). in 2015 military communications and information systems conference (MilCIS). 2015. IEEE.
[34]. Zheng, Y., et al. Smart car parking: temporal clustering and anomaly detection in urban car parking. in 2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP). 2014. IEEE.
[35]. MacQueen, J. Some methods for classification and analysis of multivariate observations. in Proceedings of the fifth Berkeley symposium on mathematical statistics and probability. 1967. Oakland, CA, USA.
[36]. Hasan, M., et al., Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet of Things, 2019. 7: p. 100059.