International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7692
***Article Received:** 06 June 2023 **Revised:** 28 July 2023 **Accepted:** 15 August 2023*

Mitigation of Attacks via Improved Network Security in IoT Network using Machine Learning

Dr. Kalaiarasi N [1*], Mr. Kadirvel A [2], Dr. Geethamahalakshmi G[3], Dr. Nageswari D [4], Mr. Hariharan N [5], Dr. Senthil Kumar S[6]
[1*]Professor, Department of Electronics and Communication Engineering
R.M.K College of Engineering and Technology, Puduvoyal
Tamil Nadu, India
Email: kalaiarasiece@rmkcet.ac.in
[2]Professor, Department of Mechanical Engineering
R.M.K. Engineering College, Kavaraipettai,Tamil Nadu, India
Email: akv.mech@rmkec.ac.in
[3]Assistant Professor, Department of Electrical and Electronics Engineering,
S.R.M Easwari Engineering College, Chennai, India
Email: geethamahalakshmi.g@eec.srmrmp.edu.in
[4]Assistant Professor, Department of Science and Humanities,
R.M.K College of Engineering and Technology, Puduvoyal, India
Email: nageswari@rmkcet.ac.in
[5]Assistant Professor, Department of Science and Humanities,
R.M.K College of Engineering and Technology, Puduvoyal, India
Email: hariharan@rmkcet.ac.in
[6]Professor**,** Department of Mechanical Engineering, R.M.K College of Engineering and Technology,
Puduvoyal, India
Email: sskrb55@gmail.com

Abstract— In this paper, we develop a support vector machine (SVM) based attack mitigation technique from the IoT network. The SVM aims to classify the features related to the attacks based on pre-processed and feature extracted information. The simulation is conducted in terms of accuracy, precision, recall and f-measure over KDD datasets. The results show that the proposed SVM classifier obtains high grade of classification accuracy in both training and testing datasets.

Keywords- support vector machine, attack mitigation, IoT, KDD datasets.

I. INTRODUCTION

Recent developments in the internet of things point to a fundamental shift in the communication infrastructure that now exists around the world [1]. A greater interoperability of smart communication technologies has a substantial impact on many aspects of urban life in smart cities [2].

Internet of Thing (IoT) are starting to become apparent as more intelligent computing devices like wristbands, smartphones, sensors, and actuators are incorporated into IoT infrastructure [3]. These applications make use of the significant computational resources and data processing capabilities that are managed by human users and take advantage of such capabilities.

It is now possible for many internet-oriented applications of IoT to be employed in smart city environments thanks to the smooth integration of the 5G network, which in turn maximizes the production of IoT devices. Recent security investigations, on the other hand, have suggested that hackers are effectively hacking devices that are only moderately protected by the internet of things [4].

Because it is populated by thousands of relatively unprotected devices, the IoT network is an appealing target for denial-of-service (DoS), distributed denial-of-service (DDoS), brute-force, and transmission control protocol (TCP), flooding attacks. Millions of IoT devices might have their safety compromised if they were subjected to a DDoS attack [5], which is becoming increasingly common as a result of the expansion of botnets.

A high level of technical competence on the part of an attacker is now necessary to breach the security of a network since attackers have progressed to the point where they possess such expertise. They can modify the information that is contained within the packet header and carry out valid, comprehensive service requests on certain workstations or servers [6] for distributed networks that have been constructed in line with the best practices that have been established. To enhance their respective detection

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7692
***Article Received:** 06 June 2023 **Revised:** 28 July 2023 **Accepted:** 15 August 2023*

and prevention capabilities, intrusion detection systems (IDS) have lately begun implementing classifier strategies that are derived from machine learning [7].

The system makes use of approaches based on machine learning to differentiate between anonymous network traffic and conventional network traffic [8]. This contributes to the system intelligence being raised to a higher level. Using adaptive machine learning frameworks, one can categories the many different types of cybercrime. Despite these efforts, a centralized reconfiguration mechanism is necessary for these frameworks to successfully design a mitigation system for the online network traffic generated by the IoT [9].

Machine learning (ML) is a technique that does not require computing systems to be explicitly programmed for them to learn from data and apply algorithms to carry out tasks. Computing systems are now able to learn from data and apply algorithms to complete tasks. The artificial intelligence (AI) contains the subfield of machine learning (ML), of which deep learning is a subset (DL) [10]. The fundamental building blocks of DL are complex algorithms that are modelled after the processes that occur in the human brain.

The processing of text as well as several other kinds of unstructured data is now feasible. ML is the process of teaching a computer to think and act independently, without the participation of a human instructor. DL often requires a less consistent level of participation from humans. It performs significantly better than more conventional machine learning algorithms when it comes to analyzing visual content and other forms of unstructured data [11].

In this research, we offer an attack mitigation strategy based on a support vector machine (SVM) for the Internet of Things network. The purpose of the SVM is to categories the characteristics that are associated with the attacks using information that has been preprocessed and feature extracted.

II. RELATED WORKS

Kumar et al. [12] proposed a strategy for boosting the capacities of IoT devices to detect intrusions that combines the benefits of machine learning models and Blockchain technology. This approach is a way for enhancing the security of IoT devices. They carried it out in stages, first clustering the information, then moving on to classifying it, and finally utilizing Blockchain technology as the concluding step. By utilizing techniques for clustering and classification, machine learning was able to automatically extract information relevant to malware, and this information has been posted on the Blockchain.

Lei et al. [13] referred to their concept for a security system as Eve Droid, in contrast to others, makes direct use of event groups to describe app activities, which may capture a higher degree of semantics for the detection process. This is because their method describes app activities. This is since their strategy characterizes activities within the app in terms of event groups.

Su et al. [14] developed an idea for a simple method that has the potential to identify DDoS malware in IoT contexts. They started by retrieving the contaminated images, and then they fed the shots into a lightweight convolutional neural network to classify the images.

Jagielski et al. [15] was demonstrated to be quite resilient to the many various kinds that are investigated during their research. They put a limit on the potentially destructive capacity of poisoning attacks and gave formal guarantees concerning the convergence of the method.

Chen et al. [16] developed a method of defense against poisoning attacks that is not specific to any one type of attack. To protect users from the effects of poison, De-Pois was created. The training of a mimic was the central concept that boosted their overall strategy. They have accomplished this by trying to replicate the movements of the model [17].

Liu et al. [18] that the way of defense against backdoor attacks is the use of a firewall. There are a total of three backdoor attacks devised, and they are used to test the efficacy of two promising defensive measures, namely pruning and fine-tuning.

Chen et al. [19] achieved the finest results in the field of ML about cyber security. Additional study paths have been provided to facilitate the participation of other academics in the quest to find solutions to the problems that have been brought to light. The amount of time and effort that you engage in learning is directly proportional to the level of profit that you gain from that investment in the long run. In addition, if we wish to implement a higher level of safety, we will have to make a greater financial investment in the system underlying resources.

III. PROPOSED METHOD

In this section of the essay, we will investigate how the suggested method achieves security-based intrusion detection by utilizing a unique attack prediction and mitigation mechanism that is based on machine learning. A flowchart illustration of the approach is provided in Figure 1.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7692
***Article Received:** 06 June 2023 **Revised:** 28 July 2023 **Accepted:** 15 August 2023*

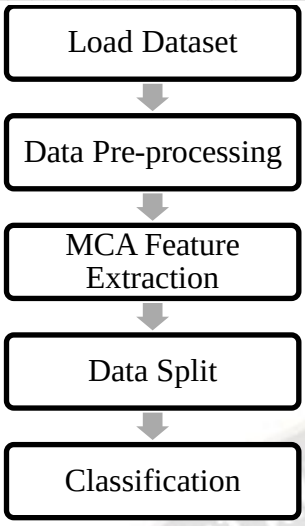

Figure 1. Proposed Framework

A. Pre-processing

Using the pre-processing, the input KDD-CUP IDS dataset is first subjected to the suggested method, which then continues with the normalization stage. The process will start here with this initial stage. The raw data are handled in a stage called pre-processing to make the management of the raw data simpler and the utilization of the raw data in the subsequent processing steps to be more effective.

B. Feature extraction

Multilinear component analysis (MCA), a popular method for feature extraction, can be improved with the help of several different search method. The MCA places a high weight not only on the fact that certain qualities overlap with one another but also on the fact that every single one has its own distinct potential for extrapolation.

C. SVM Classifier

SVM is an approach for a supervised classifier that is hyper plane-based, discriminative, and parametric. SVM are only able to tackle binary classification problems; their hyper plane-based classification skills do not extend to multi-class classification tasks.

To find a hyper plane that has the greatest margin feasible, it is strongly suggested that an algorithm be utilized in conjunction with the smallest number of points as is possible. It is important to minimize the amount of time spent travelling whenever it is at all possible $w*$

$$w*=\text{argwmax}[\min_n dH(\phi(x_n))] \quad (1)$$

where

$dH(\phi(x_n)$ - distance of a hyper plane.

$$w^T(\phi(x))+b>0 \quad (2)$$

We obtain a negative number when we plug the predictions.

$$w^T(\phi(x))+b<0 \quad (3)$$

These hyper plane-based classifiers can perform traditional classification thanks to the application of maximized margin iterative perceptron learning, Fisher linear discriminant analysis, and least-squares optimization. These three techniques are used in combination. When it comes to protecting internet of things networks from DDoS attacks, we utilize SVM classifiers that are constructed on hyper planes. The SVM classifier training method often makes use of several kernel functions of polynomial functions, which are sometimes referred to as radial basis functions. These functions are used to train the model.

In the traditional implementation of SVM, the training data points are frequently represented in a space, mapped onto categories, and then partitioned along hyper planes. This is done to facilitate the classification process. The decision threshold is raised until it reaches its maximum value, and after that, fresh data points are added to the clusters that are the most appropriate for them according to the characteristics of those clusters. SVM algorithm has a high degree of accuracy in differentiating between normal traffic flows and DDoS traffic flows in terms of the amount of traffic they generate.

IV. RESULTS AND DISCUSSIONS

Both testing and measuring could be done with the help of this dataset. In addition to examples from the standard class, the KDD-99 dataset also includes examples from the DoS class, the R2L class, the Probe class, and the U2R class. An important component to consider during a DoS attack is the total number of samples that are utilized, in addition to the sample size, the U2R, and any other relevant factors.

A possible attack can be any activity that is made to build a connection to a network. This includes additional features and functionalities, such as connection learning (TCP/IP), friendly features, and traffic. The KDD CUP is one of the most extensive and up-to-date databases for the detection of intrusions that is currently available. It is not a flow because it does not adhere to the structure of a typical data packet, and it is not a flow because it does not adhere to the structure of a flow.

Both requirements must be met for something to be considered a flow. Even if the basic characteristics of TCP connections and aggregate information like the total number of failed login attempts are included in the dataset, IP addresses are not included in it. This is even though the dataset contains everything else related to TCP connections.

The findings of the RF, MLP, and CNN algorithms are modelled using goal functions so that they could arrive at their respective conclusions. On the same dataset, three distinct machine learning algorithms are tested, and after being put through their paces, their overall performance was

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7692
***Article Received:** 06 June 2023 **Revised:** 28 July 2023 **Accepted:** 15 August 2023*

compared. This performance can be assessed using a variety of criteria, such as accuracy, the true positive rate, and the false negative rate, amongst others.

After putting together a confusion matrix, one can then arrive at a performance matrix using this method. One method that might be used to evaluate how well a test classification algorithm worked in relation to the actual classification was to look at the algorithm confusion matrix.

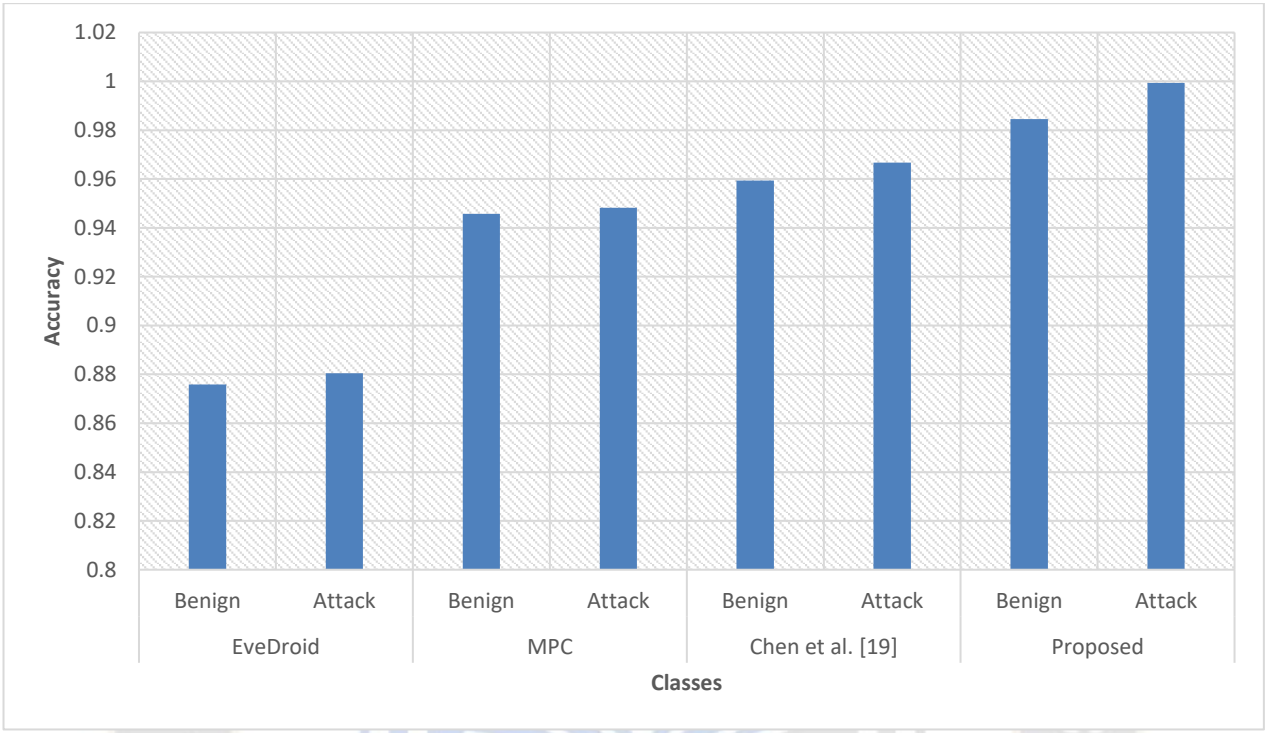

Figure 2. Accuracy

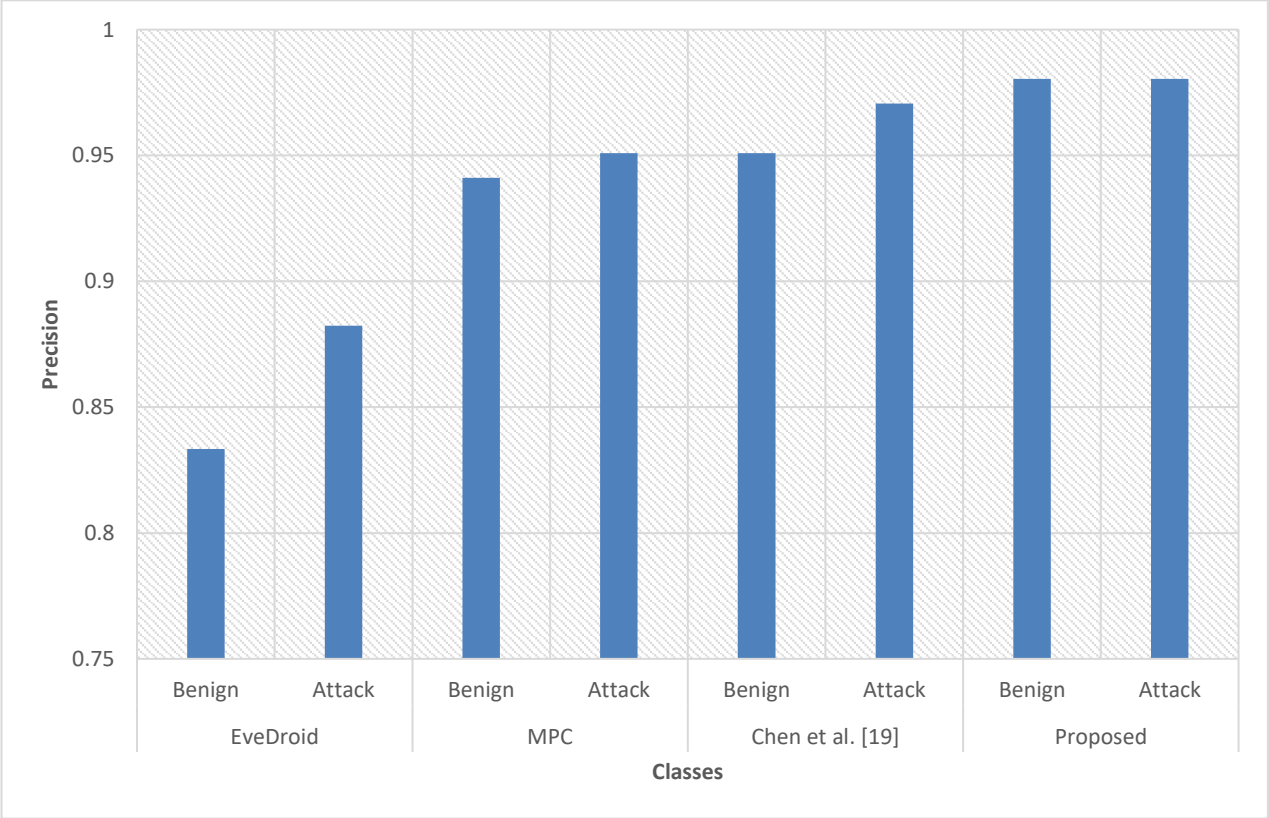

Figure 3. Precision

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7692
***Article Received:** 06 June 2023 **Revised:** 28 July 2023 **Accepted:** 15 August 2023*

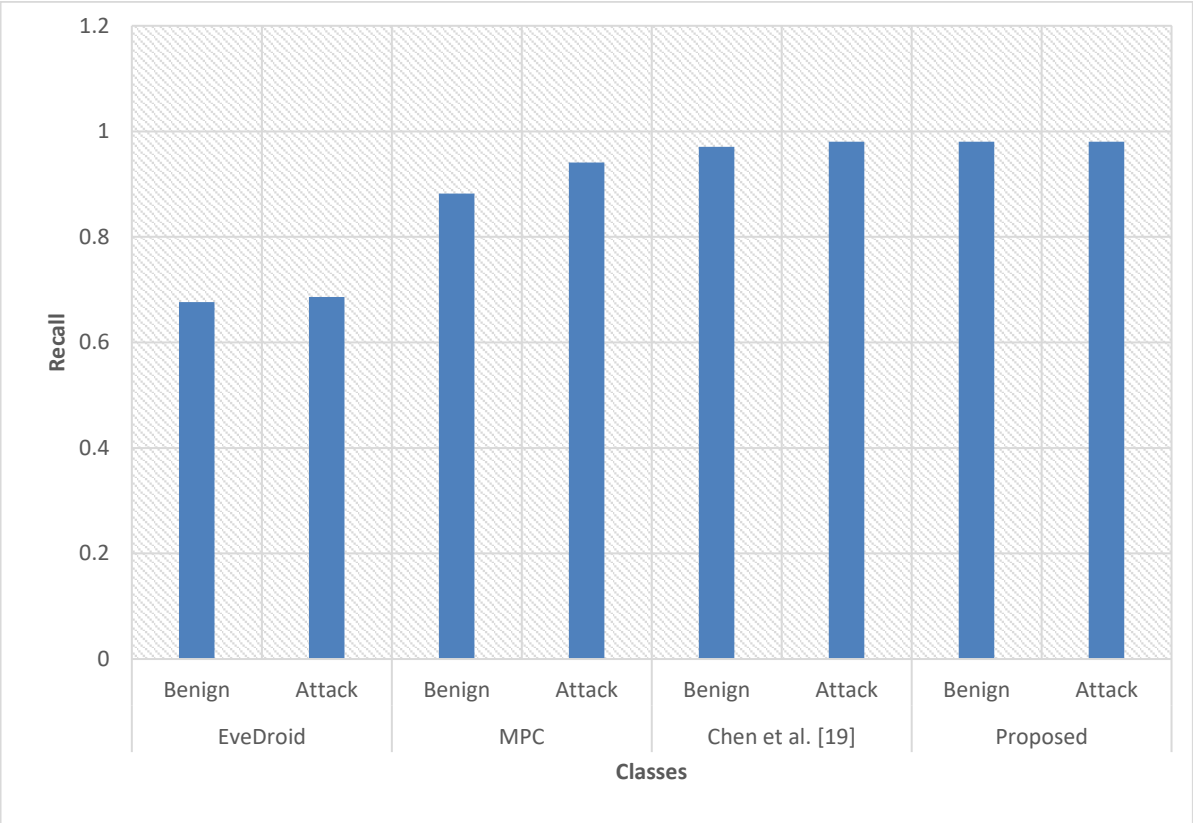

Figure 4. Recall

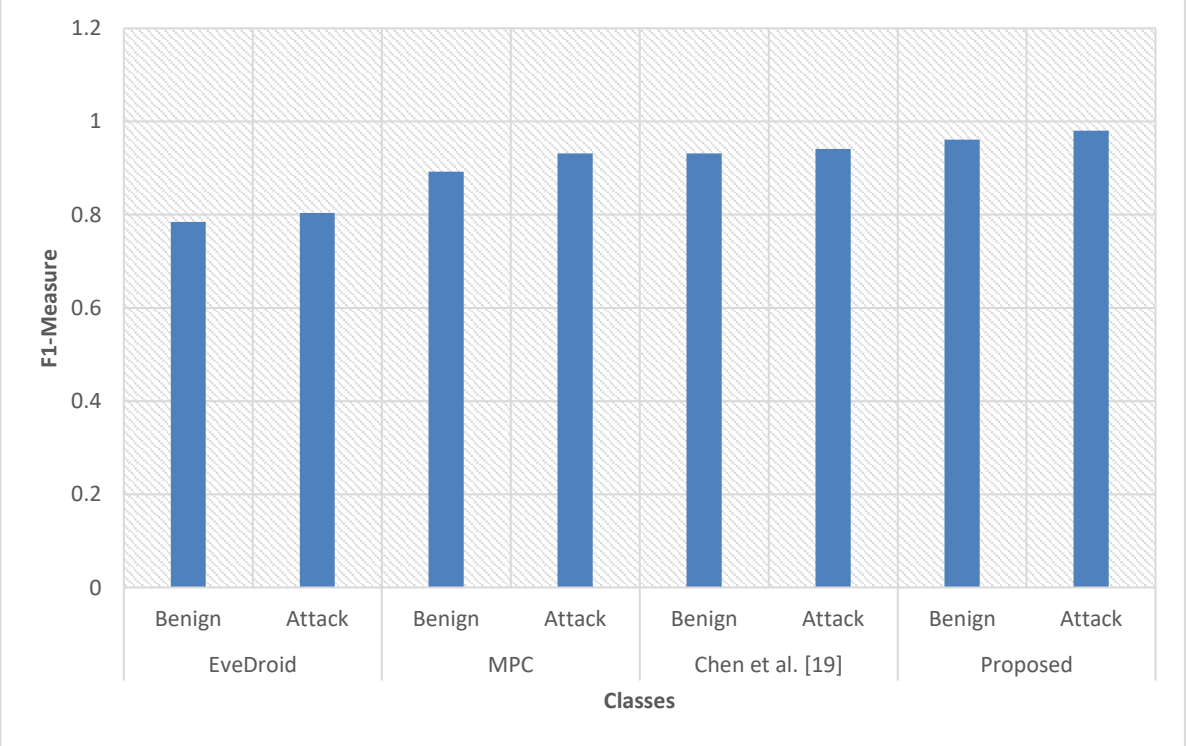

Figure 5. F-Measure

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7692
***Article Received:** 06 June 2023 **Revised:** 28 July 2023 **Accepted:** 15 August 2023*

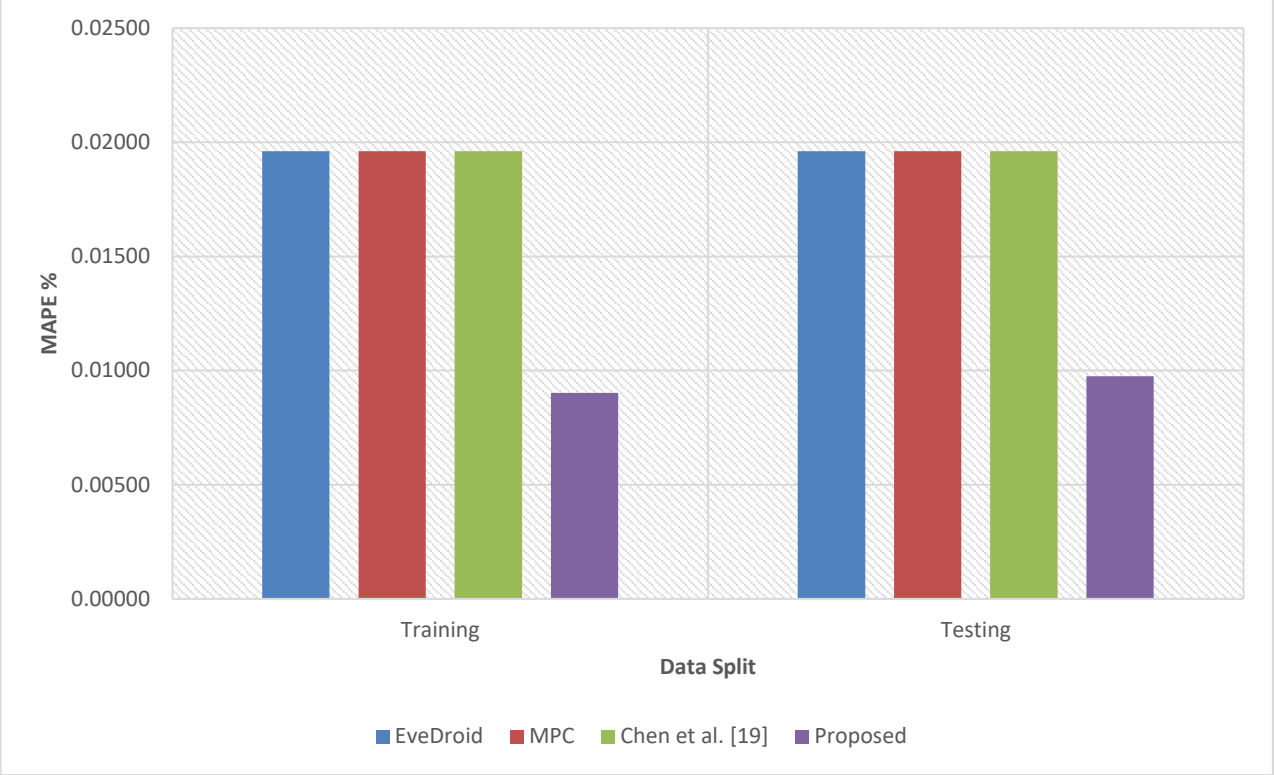

Figure 6. MAPE

From the results of simulation, it is found that the proposed SVM classifier achieves higher rate of accuracy in detecting the attack while an intruder is trying to get into the network. The other classifier shows a near optimal performance as in Figure 2 - 6.

V. CONCLUSIONS

In this research, we offer an attack mitigation strategy based on a SVM for the Internet of Things network. The purpose of the SVM is to categories the characteristics that are associated with the attacks using information that has been pre-processed and feature extracted. Over KDD datasets, the python simulation achieves high levels of accuracy, precision, recall, and f-measure. According to the findings, the SVM classifier can achieve a high level of classification accuracy in both the training and testing datasets.

REFERENCES

[1] A. Mpatziakas, A. Drosou, S. Papadopoulos, and D. Tzovaras, "IoT threat mitigation engine empowered by artificial intelligence multi-objective optimization." Journal of Network and Computer Applications, vol.203, pp.103398. 2022.

[2] O. D. Okey, S. S. Maidin, P. Adasme, R. Lopes Rosa, M. Saadi, D. Carrillo Melgarejo, and D. Zegarra Rodríguez, BoostedEnML: "Efficient Technique for Detecting Cyberattacks in IoT Systems Using Boosted Ensemble Machine Learning". Sensors, vol.22, no.19, pp.7409. 2022.

[3] N. Mahajan, A. Chauhan, H. Kumar, S. Kaushal, and A.K. Sangaiah, "A Deep Learning Approach to Detection and Mitigation of Distributed Denial of Service Attacks in High Availability Intelligent Transport Systems". Mobile Networks and Applications, pp.1-21. 2022.

[4] V. Ravi, R. Chaganti, and M.Alazab, "Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system." Computers and Electrical Engineering, vol.102, pp.108156. 2022.

[5] Asim, A. ., & Cada, M. . (2023). Enhancement of Physical Layer Security in Flying Ad-hoc Networks by Intelligent Reflecting Metasurfaces. International Journal of Intelligent Systems and Applications in Engineering, 11(1s), 46–50. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2475

[6] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems": Past, present and future. Electric Power Systems Research, vol.215, pp.108975. 2023.

[7] Mr. Dharmesh Dhabliya, Mr. Rahul Sharma. (2012). Efficient Cluster Formation Protocol in WSN. International Journal of New Practices in Management and Engineering, 1(03), 08 - 17. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/7

[8] B. B. Behera, R. K. Mohanty, and B. K. Pattanayak, Attack Detection and Mitigation in Industrial IoT: "An Optimized Ensemble Approach". Specialusis Ugdymas, vol.1, no.43, pp.879-905. 2022.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7692
***Article Received:** 06 June 2023 **Revised:** 28 July 2023 **Accepted:** 15 August 2023*

[9] Z. Abou El Houda, B. Brik, and L. Khoukhi, "Why Should I Trust Your IDS?": "An Explainable Deep Learning Framework for Intrusion Detection Systems in Internet of Things Networks". IEEE Open Journal of the Communications Society, vol.3, pp.1164-1176. 2022.

[10] R. Amrish, K. Bavapriyan, V. Gopinaath, A. Jawahar, and C. V. Kumar, "DDoS Detection using Machine Learning Techniques". Journal of IoT in Social, Mobile, Analytics, and Cloud, vol.4, no.1, pp.24-32. 2022.

[11] Rodriguez, L., Rodríguez, D., Martinez, J., Perez, A., & Ólafur, J. Leveraging Machine Learning for Adaptive Learning Systems in Engineering Education. Kuwait Journal of Machine Learning, 1(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/103

[12] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model". Computers and Electrical Engineering, vol.99, pp.107810. 2022.

[13] T. Berghout, M. Benbouzid, and S. M. Muyeen, "Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects". International Journal of Critical Infrastructure Protection, pp.100547. 2022

[14] U. Islam, A. Muhammad, R. Mansoor,M. S. Hossain, I. Ahmad, E. T. Eldin, and M.Shafiq, "Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models". Sustainability, vol.14, no.14, pp.8374. 2022.

[15] R. Kumar, X. Zhang, W. Wang, R. U. Khan, J. Kumar, and A. Sharif, "A multimodal malware detection technique for Android IoT devices using various features". IEEE access, vol.7, pp.64411-64430. 2019.

[16] T. Lei, Z. Qin, Z. Wang, Q. Li, and D.Ye, "EveDroid: Event-aware Android malware detection against model degrading for IoT devices". IEEE Internet of Things Journal, vol.6, no.4, pp.6668-6680. 2019.

[17] J. Su, D. V. Vasconcellos, S. Prasad, D. Sgandurra, Y. Feng, and K. Sakurai, "Lightweight classification of IoT malware based on image recognition". In 2018 IEEE 42Nd annual computer software and applications conference (COMPSAC) (Vol. 2, pp. 664-669). IEEE. 2018.

[18] Dhabliya, D. (2021). Feature Selection Intrusion Detection System for The Attack Classification with Data Summarization. Machine Learning Applications in Engineering Education and Management, 1(1), 20–25. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/8

[19] M. Jagielski, A. Oprea, B. Biggio, C. Liu, C. Nita-Rotaru, and B.Li, "Manipulating machine learning: Poisoning attacks and countermeasures for regression learning". In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 19-35). IEEE. 2018.

[20] J. Chen, X. Zhang, R. Zhang, C. Wang, and L.Liu, "De-pois: An attack-agnostic defense against data poisoning attacks." IEEE Transactions on Information Forensics and Security, vol.16, pp.3412-3425. 2021.

[21] P. Mohassel, and Y.Zhang, "Secureml: A system for scalable privacy-preserving machine learning" In 2017 IEEE symposium on security and privacy (SP) (pp. 19-38). IEEE. 2017.

[22] K. Liu, B. Dolan-Gavitt, and S. Garg, "Fine-pruning: Defending against backdooring attacks on deep neural networks." In International Symposium on Research in Attacks, Intrusions, and Defenses (pp. 273-294). Springer, Cham. 2018.

[23] B. Chen, W. Carvalho, N. Baracaldo, H. Ludwig, B. Edwards, T. Lee, and B. Srivastava, "Detecting backdoor attacks on deep neural networks by activation clustering." arXiv preprint arXiv:1811.03728. 2018.