BioGecko Vol 12 Issue 03 2023

ISSN NO: 2230-5807

A Novel Framework for detecting IoT-based botnet DDoS attacks using machine learning

Dr.M.Rajaiah 1 , Dean Academics & HOD, Dept of CSE, Audisankara College of Engineering & Technology, Gudur.
Mr.PVRK MURTY 2 , Associate Professor ,Dept of CSE, Audisankara College of Engineering &Technology, Gudur.
Mr. Jandrajupalli Ramesh Babu 3 , Dept of Computer science and engineering, Audisankara College of Engineering& Technology, Gudur.
Mr. Guntamadugu Rupesh 4, Dept of Computer science and engineering,Audisankara College of Engineering& Technology, Gudur.

ABSTACT_ IoT security has emerged as one of the most pressing issues in the world of network security as a result of the enormous growth of IoT botnet DDoS attacks in recent years. Numerous security strategies have been put forth in the field, but they still fall short when it comes to addressing newly emerging IoT malware strains known as Zero-Day Attacks.in this In this paper author is applying Machine Learning algorithms such as SVM, KNN, Random Forest, Decision Tree and Neural Network to detect DDOS attacks from IoT networks. IoT are small devices deployed in any environment such as battle fields, agriculture fields, healthcare hospitals etc to sense data and then send that sense data to destination server using internet connection.

1.INTRODUCTION

Without human intervention, the Internet of Things (IoT) is a network of networked objects that has suddenly turned into a source of DDoS attacks [1]. Compared to desktop PCs, IoT devices are more susceptible to compromise. As a result, IoT-based botnet assaults have significantly increased in frequency [7]. Malware infestations in an IoT network lead to the creation of the so-called botnet, also known as a network of bots (compromised IoT devices) [2].Over 6 billion Internet of Things (IoT) devices are reportedly present on the planet; with so many potentially vulnerable devices, cybercriminals cannot easily go unnoticed. About half of the thousands of malware samples found in prior years were found in 2017 alone [5]. As the name implies, a honeypot is designed to attract attackers so that you may see and study how they initiate an attack by gathering data on the attacking agent, such as malware for a DDoS attack [9].It is a gadget with the capacity to compromise the main server by simulating any vulnerability that an attacker may easily exploit. IP addresses, MAC addresses, port numbers, the types of devices it targets, malware executables and their orders, etc. are just a few of the pieces of information it can gather by keeping an eye on interactions between the attacker and itself [27]. In the past few years, honeypots have been proven to be a valuable resource for learning about different malware and its variations in the field of computer security.It first came into actuality in the late 1990s as ‘ The Deception Toolkit ’ which was developed by Fred Cohen in 1998(28) and latterly came publically and commercially available especially to attack with the tone-replicating programs called worms. currently, there are different types of Honeypots available to be used by colorful operations. It can be classified depending on the position of commerce it allows with the bushwhacker. The position of commerce depends upon the quantum of data that needs to be get collected. thus, it's distributed into Low commerce honeypots and High commerce honeypots(9). It can also be classified on the base of ideal it wants to attaini.e either they can be used for carrying out any exploration to get knowledge of possible pitfalls and failings in the system called as Research Honeypots, or they can be used for guarding the companies means from the attacks in real time to ameliorate the overall security called as product Honeypots. therefore, honeypots are relatively effective in dealing with Zero- Day DDoS Attacks without compromising IoT bias(29).

2.LITERTURE SUREVY

2.1 Atzori, L., Iera, A., Morabito, G. (2010). The Internet ofThings: A survey. Computer Network, 54(15): 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

This paper addresses the Internet of Things. Main enabling factor of this promising paradigm is the integration of several technologies and communications solutions. Identification and tracking technologies, wired and wireless sensor and actuator networks, enhanced communication protocols (shared with the Next Generation Internet), and distributed intelligence for smart objects are just the most relevant. As one can easily imagine, any serious contribution to the advance of the Internet of Things must necessarily be the result of synergetic activities conducted in different fields of knowledge, such as telecommunications, informatics, electronics and social science. In such a complex scenario, this survey is directed to those who want to approach this complex discipline and contribute to its development. Different visions of this Internet of Things paradigm are reported and enabling technologies reviewed. What emerges is that still major issues shall be faced by the research community. The most relevant among them are addressed in details.

2.2**Sedjelmaci, H., Senouci, S.M., Al-Bahri, M. (2016).Lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology.IEEE ICC - Mobile and Wireless NetworkingSymposium. https://doi.org/10.1109/ICC.2016.7510811**

In the Internet of Things (IoT), resources' constrained tiny sensors and devices could be connected to unreliable and untrusted networks. Nevertheless, securing IoT technology is mandatory, due to the relevant data handled by these devices. Intrusion Detection System (IDS) is the most efficient technique to detect the attackers with a high accuracy when cryptography is broken. This is achieved by combining the advantages of anomaly and signature detection, which are high detection and low false positive rates, respectively. To achieve a high detection rate, the anomaly detection technique relies on a learning algorithm to model the normal behavior of a node and when a new attack pattern (often known as signature) is detected, it will be modeled with a set of rules. This latter is used by the signature detection technique for attack confirmation. However, the activation of anomaly detection for low-resource IoT devices could generate a high-energy consumption, specifically when this technique is activated all the time.

2.3 Summerville, D.H., Zach, K.M., Chen, Y. (2015). Ultralightweight deep packet anomaly detection for Internet of Things devices. 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC). https://doi.org/10.1109/PCCC.2015.7410342

As we race toward the Internet of Things (IoT), small embedded devices are increasingly becoming network-enabled. Often, these devices can't meet the computational requirements of current intrusion prevention mechanisms or designers prioritize additional features and services over security; as a result, many IoT devices are vulnerable to attack. We have developed an ultra-lightweight deep packet anomaly detection approach that is feasible to run on resource constrained IoT devices yet provides good discrimination between normal and abnormal payloads. Feature selection uses efficient bit-pattern matching, requiring only a bitwise AND operation followed by a conditional counter increment. The discrimination function is implemented as a lookup-table, allowing both fast evaluation and flexible feature space representation. Due to its simplicity, the approach can be efficiently implemented in either hardware or software and can be deployed in network appliances, interfaces, or in the protocol stack of a device. We demonstrate near perfect payload discrimination for data captured from off the shelf IoT devices

3.PROPOSED SYSTEM

In this paper author is applying Machine Learning algorithms such as SVM, KNN, Random Forest, Decision Tree and Neural Network to detect DDOS attacks from IoT networks. IoT are small devices deployed in any environment such as battle fields, agriculture fields, healthcare hospitals etc to sense data and then send that sense data to destination server using internet connection. IoT are small devices and can be attacked by attacker to sense and send corrupted data and to provide security from such attacks heavy security algorithms cannot be installed on IoT devices so author is deploying

Honeypot server which can run between centralized server and IoT networks and whenever user send any request then honeypot server will process that request and if request is genuine then it will forward that request to centralized server or IOT networks. If user send malicious request by giving wrong username and password then honeypot will server dummy response to user and try to extract more information such as IP address, mac address and then inform to centralized server and IOT network to be aware of such IP address and mac address.

In existing technique honeypot using signature based attack detection which is not efficient so author is deploying machine learning framework at honeypot server to predict whether request is normal or contains attack signature. In propose technique ML algorithms will be trained with previous data and then this trained model can be used to detect attacks from old or new request signature and this detection will solved ZERO-DAY Distributed Denial of service (DDOS) attacks.

In propose work author using honeypot server and IOT devices to capture data and this data will be used to train ML algorithms but we don't have any IOT devices so we are using IOT dataset to trained ML algorithms. In propose work we are using SVM, Random Forest, K-Nearest Neighbours, Decision Tree and Neural Networks. In all algorithms SVM, KNN and Neural network is giving best performance.

3.1 DATASET INFORMATION

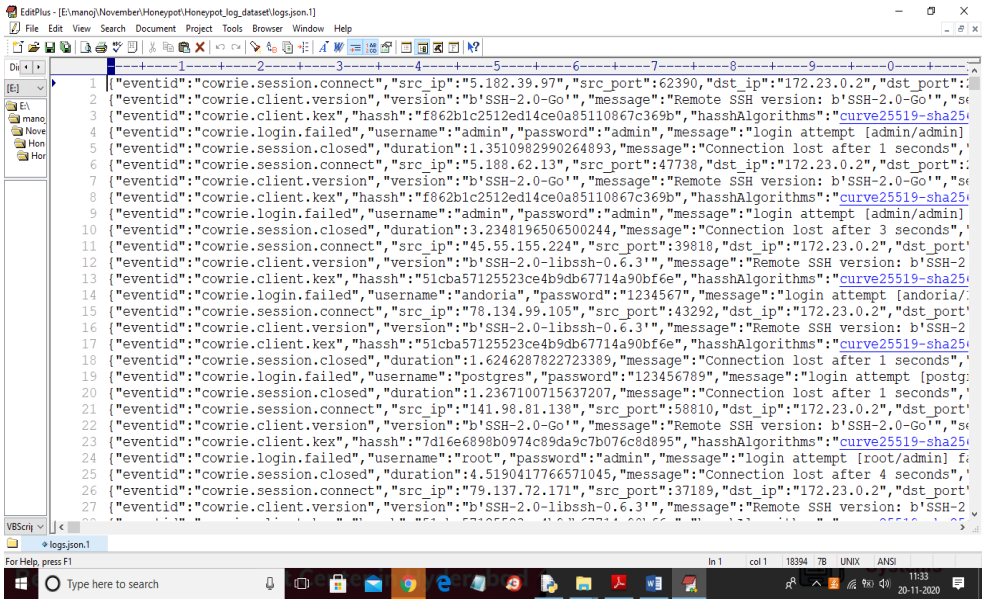

Fig 1:In above Honeypot IOT log dataset we have complete details such as event id, sender IP, port no, destination IP and many other signatures and using above dataset we will train machine learning algorithms. In above dataset we can see we have some request with login failed which will consider as attack and if in new request such commands appear then ML predict it as attack. After training ML with above dataset then we will upload new test data and then ML will predict whether new data contains normal or attack signature. Above dataset cannot be used to train ML so we will pre-process dataset to convert it into features. Above dataset you can see inside 'Honeypot_log_dataset' folder

3.2 IMPLEMENTATION

Gathering the datasets: We gather all the r data from the kaggale website and upload to the proposed model

Generate Train & Test Model: We have to preprocess the gathered data and then we have to split the data into two parts training data with 80% and test data with 20%

Run Algorithms: For prediction apply the machine learning models on the dataset by splitting the datasets in to 70 to 80 % of training with these models and 30 t0 20 % of testing for predicting

Obtain the accuracy: In this module we will get accuracies

Predict output:In this module we will predict output . ML analyse each request and then mark that request signature as normal or DDOS attack. At each request line after equals to symbol we can see ML detection result.

4.RESULTS AND DISCUSSION

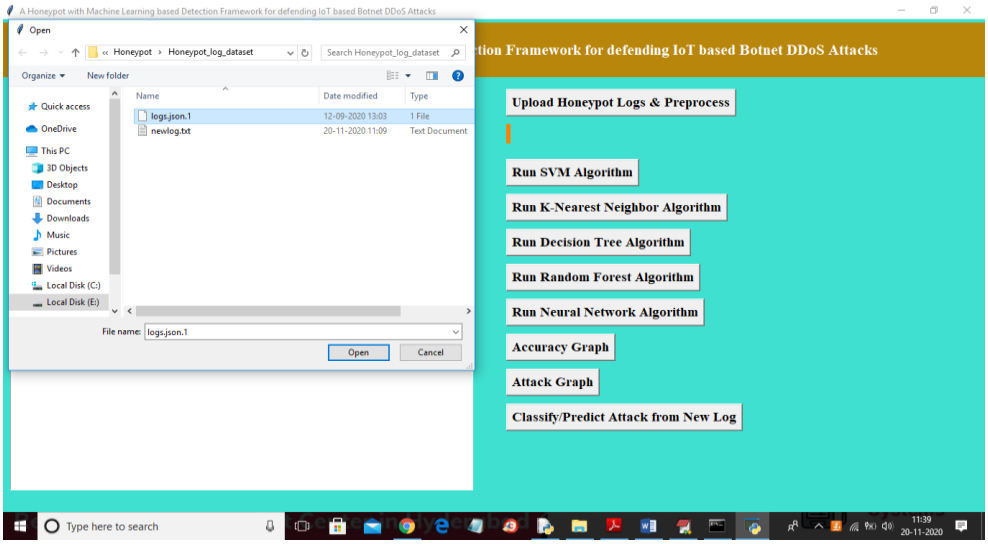

Fig 2:In above screen uploading 'logs.json.1' log file and then click on 'Open' button to load dataset and to get below screen

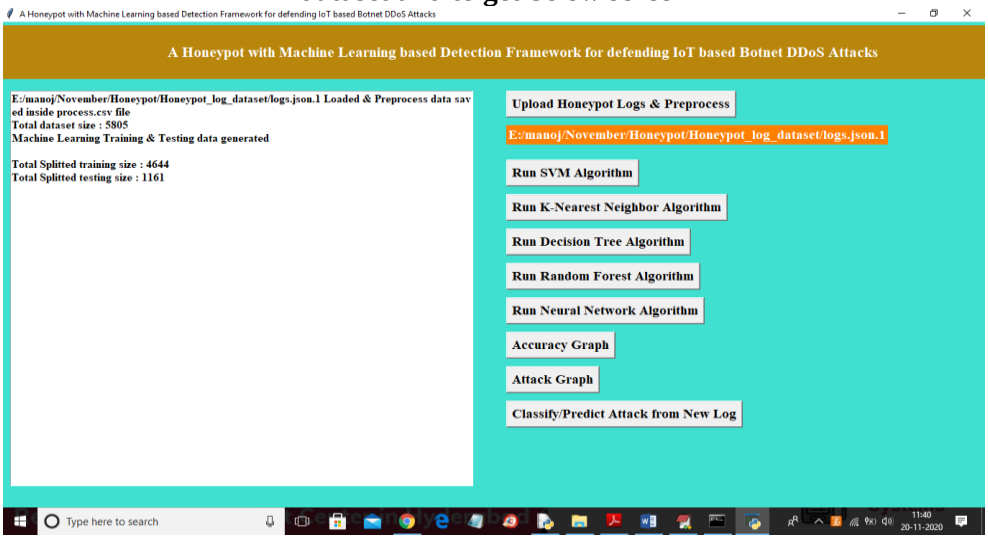

Fig 3:In above screen we can see dataset contains 5805 records and application split that data into train and test part and application using 4644 (80% dataset records) for training and 1161 (20% dataset records) for testing. After building model on 80% records then ML apply 20% data on trained 80% model to predict request type as normal or attack. From 20% if ML predict 18% records correctly then 18/20*100 will give ML prediction accuracy performance. Now in above screen both train and test data is ready and now click on 'Run SVM Algorithm' button to train SVM model and calculate its accuracy

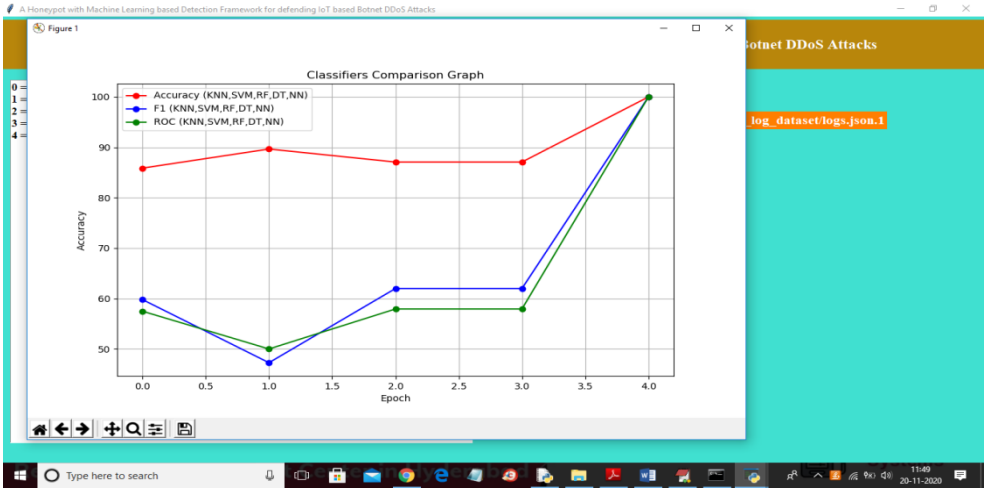

Fig 4:In above graph x-axis represents algorithms as KNN, SVM, RF, DT and NN and y-axis represents accuracy and in above graph red line refers to accuracy and blue line for FSCORE and green line for ROC value. In above graph each point refers value for one algorithm and last point is for NN which is having high performance. Now click on 'Attack Graph' button to get below graph

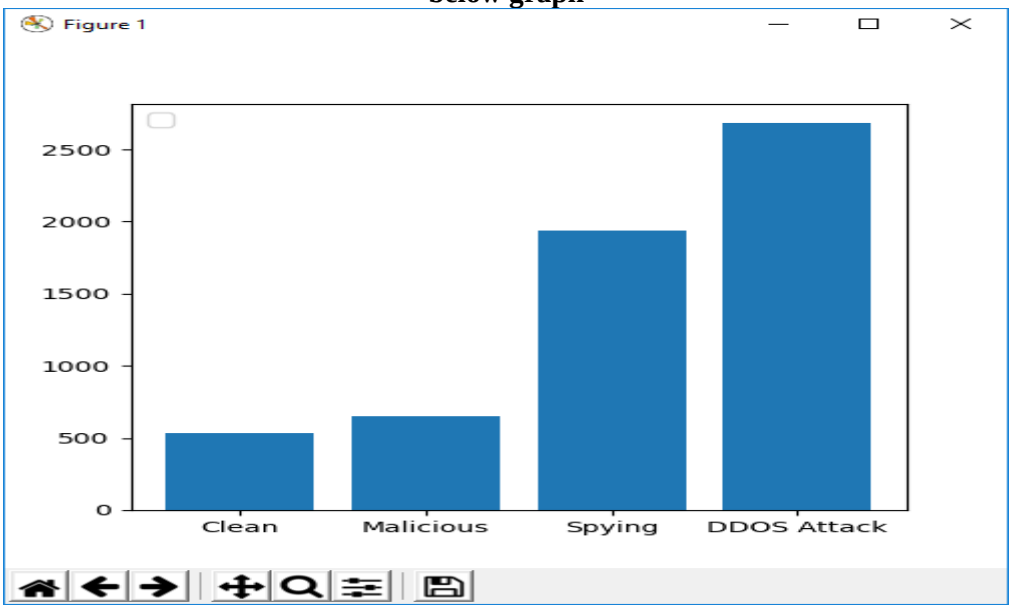

Fig 5:Above graph x-axis contains request type and y-axis contains count and this attack graph obtained from honeypot log dataset. From all request honey pot received more number of DDOs attacks. Now click on 'Classify/Predict Attack from New Log' button to upload new log dataset and then ML will apply on new log dataset to predict whether new log contains attack or normal request

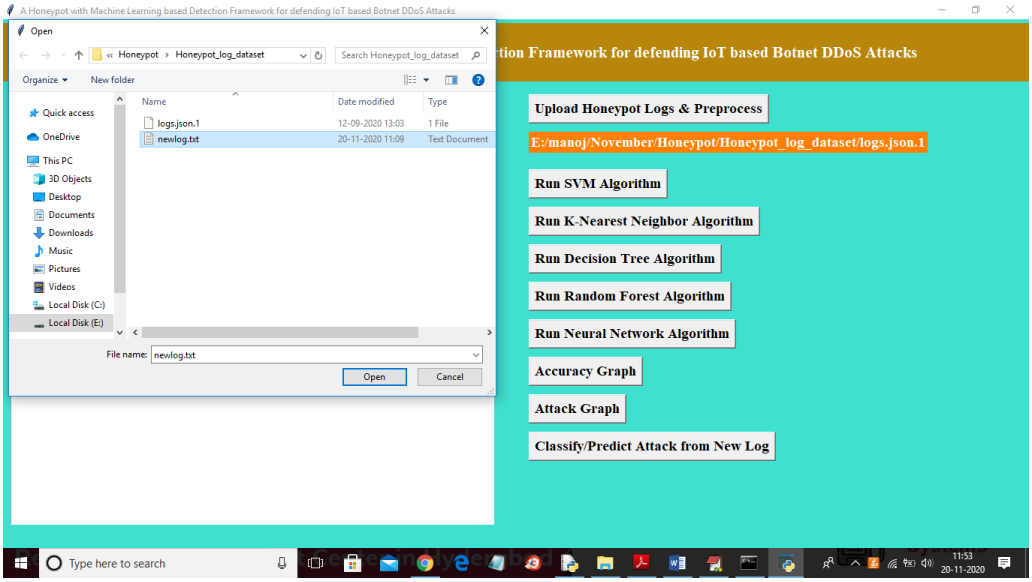

Fig 6:In above screen uploading 'newlog.txt' file and then click on 'Open' button to get below prediction result

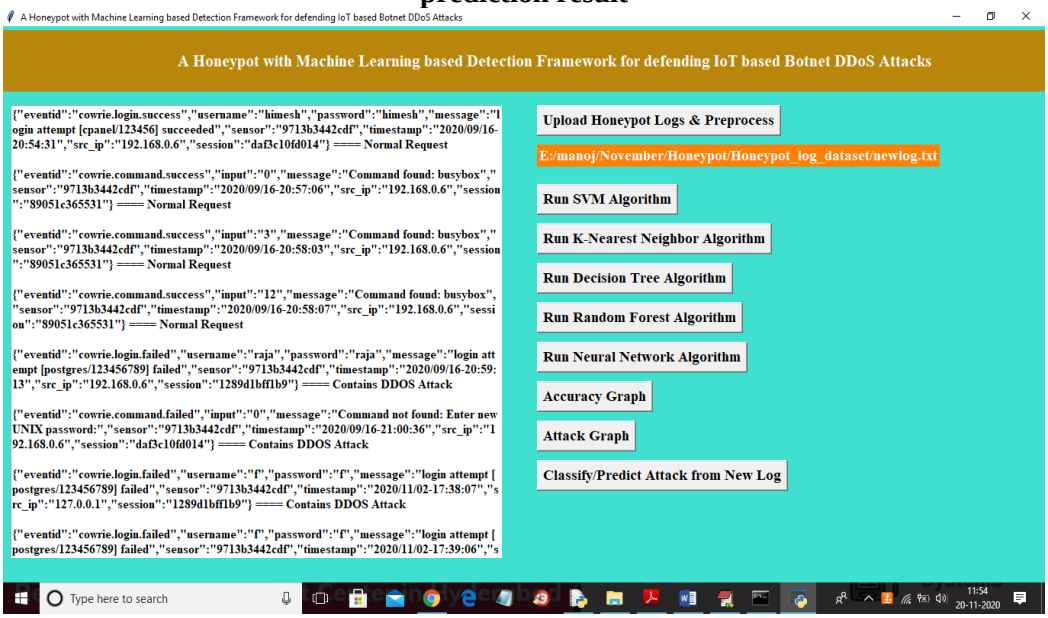

Fig 7:In above screen ML analyse each request and then mark that request signature as normal or DDOS attack. At each request line after equals to symbol we can see ML detection result. In above screen scroll down to view all request result

5.CONCLUSION

The primary driver of the real world's technological modernization is the internet of things. However, it is also the primary cause of the rise in cyberattacks, particularly DDoS attacks. Because of this, protecting against attacks that employ IoT as a means of compromising network security has emerged as the main issue in the field of internet security. To render the IoT network immune to such attacks, a variety of protection methods have been presented in the relevant sector, but they become unable to handle new variations of IoT botnet attacks.For the DDoS detection, we developed a honeypot-based solution that makes use of a real-time machine learning detection framework. The use of honeypots will ensure the logging of newly emerging malware traits, which ML-based detection framework will use to efficiently train their classifiers.

REFERENCES

[1] K. Chen, S. Zhang, Z. Li,Yi Zhang, Q.Deng, Sandip Ray, YierJin, “Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice” Journal of Hardware and Systems Security, vol. 2, Issue 2, pp. 97–110, (2018).
[2] W. Zhou, Y. Jia, A. Peng, Y. Zhang and P. Liu, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved," IEEE Internet of Things Journal. 2018.
[3] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142 (2017).
[4] Honeypots and the Internet of Things. Available at https://securelist.com/honeypots-and-the-internet-of-things/78751.
[5] Hastie, T., Tibshirani, R., & Friedman, J. Unsupervised learning. In The elements of statistical learning (pp. 485-585). Springer, New York, NY (2009).
[6] C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," in Computer, vol. 50, no. 7, pp. 80-84 (2017).
[7] Dougherty, J., Kohavi, R., &Sahami, M. Supervised and unsupervised discretization of continuous features. In Machine Learning Proceedings 1995, pp.194-202 (1995).
[8] Sommer, R., & Paxson, V. (2010, May). Outside the closed world: On using machine learning for network intrusion detection. In Security and Privacy (SP), IEEE Symposium on (pp. 305-316). IEEE (2010).
[9] M. Anirudh, S. A. Thileeban And D. J. Nallathambi, "Use of Honeypots for Mitigating DoS Attack Targeted on IoT Networks," 2017 International Conference On Computer, Communication And Signal Processing (ICCCSP), Chennai, Pp. 1-4, (2017).
[10] Rieck, K., Holz, T., Willems, C., Düssel, P., &Laskov, P. (2008, July). Learning and classification of malware behavior. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 108-125). Springer, Berlin, Heidelberg.
[11] Bailey, M., Oberheide, J., Andersen, J., Mao, Z. M., Jahanian, F., & Nazario, J. Automated classification and analysis of internet malware. In International Workshop on Recent Advances in Intrusion Detection Springer, Berlin, Heidelberg, pp. 178-197 (2007). [12] Binkley, J. R., & Singh, S. An Algorithm for Anomaly-based Botnet Detection. SRUTI, 6, 7-7. (2006).
[13] Song, Y., Keromytis, A. D., &Stolfo, S. J. U.S. Patent No. 8,844,033. Washington, DC: U.S. Patent and Trademark Office. (2014).
[14] The New Threat: The IoT DDoS Invasion. https://www.a10networks.com/sites/default/files/resource-files/A10-TPS-GR-The_New_Threat_The_IoT_DDoS_Invasion.pdf.
[15] Zammit, DA machine learning based approach for intrusion prevention using honeypot interaction patterns as training data. University of Malta, 1-55 (2016).
[16] Pa, Y. M. P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T., &Rossow, C. IoTPOT: analysing the rise of IoT compromises. EMU, 9, 1(2015).
[17] Doshi, R., Apthorpe, N., &Feamster, N. Machine Learning DDoS Detection for Consumer Internet of Things Devices, arXiv preprint arXiv:1804.04159 (2018).
[18] Pa, Y. M. P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T., &Rossow, C., IoTPot: A novel honeypot for revealing current IoT threats. Journal of Information Processing, 24(3), 522-533 (2016).
[19] Musca, C., Mirica, E., &Deaconescu, R. Detecting and analyzingzeroday attacks using honeypots. In Control Systems and Computer Science (CSCS), 2013 19th International Conference on (pp. 543-548). IEEE. (2013).

AUTHOR PROFILES

Dr.M.Rajaiah , Currently working as an Dean Academics & HOD in the department of CSE at ASCET (Autonomous), Gudur, Tirupathi(DT).He has published more than 35 papers in, Web of Science, Scopus Indexing, UGC Journals.

Prof. PVRKMURTY , He completed his Masters of Technology in Computer Science and Engineering . Pursuing Ph.D in CSE at Saveetha school of engineering, Chennai. Currently working as an Associate Professor in the department of CSE at ASCET (Autonomous), Gudur, Tirupathi(DT). His areas of interest include, Data Mining, Cloud Computing and MachineLearning

Mr. Jandrajupalli Ramesh Babu, as M.Tech student in the department of CSE at Audisankara College of Engineering and Technology, Gudur, Tirupathi(DT). He has completed BTech in Mechanical Engineering from SRI VENKATESWARA UNIVERSITY. His areas of interests are Networks, Big Data, Data warehousing, Data Mining, Machine Learning, Cloud Computing & Blockchain Technology

ISSN NO: 2230-5807

Mr. Guntamadugu Rupesh, as M.Tech student in the department of CSE at Audisankara College of Engineering and Technology, Gudur. He has completed BE in Computer Science and Engineering from Audisankara College of Engineering and Technology (Autonomous). His areas of interests are Networks, Mobile Wireless Networks, Big Data, Data warehousing and Data Mining and Deep Learning