International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.48047/INTJECSE/V15I4.65 ISSN: 1308-5581 Vol 15, Issue 04 2023

CYBER RISK IN INTERNET OF THINGS WORLD

1Mrs.A.DIVYA,
Assistant Professor, Department of CSE, Sreyas Institute of Engineering and Technology,Telangana, India,
divya.a@sreyas.ac.in
2 Maduguri Aashritha,
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India,
aashrithamaduguri001@gmail.com
3Nimmala Chandana Priya,
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana,India,
priyanimmala17@gmail.com
4 Amanaganti Bhanu Prakash,
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana,India,
bp666670@gmail.com
5 Kondam Madhavendra Goud,
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India,
kondammadhvendragoud@gmail.com

ABSTRACT
Internet of Things (IoT) is an emerging technology which has revolutionized the network in the global world. It is estimated that about 38.5 billion IoT devices will be connected by 2020. These devices are used in every part of life. Large number of data are collected by these IoT devices and transmitted from one device to another and from devices to enterprise systems. As large numbers of devices are connected with each other and to the world network and the number is increasing every day, there is a major risk of security threat, vulnerabilities, data manipulation, stealing, identity, device manipulation, and hacking. Due to the ease of automation and digitization, these devices bring with them numerous security issues. Poor security of these devices can provide an entry point for cyberattacks which may compromise sensitive data, threaten users' privacy and weaponize the device. The IoT ecosystem needs proper security at device level, application level, and network level. Different vendors with diverse goals but inadequate cybersecurity expertise manufacture these devices. The purpose of this paper is to identify the current security and privacy issues in IoT devices and propose recommendations for the solution of Cyber security issues in IoT devices.

INTRODUCTION
The importance of Internet of Things (IoT) comes from its final objective which is enabling direct integration between the physical world and digital one. The physical world is represented by the word (thing) such as appliances used in medical field for monitoring hearts, chips used in GPS enabled applications for transportation, biochips utilized to track animals in biology, and devices employed to build smart homes or cities. The digital world is represented by the computer-based systems installed in the devices to enable full remote control via the Internet in terms of communication and data exchange.That IoT results in improved efficiency, accuracy, and economic benefit. One report showed the estimation of the impact of the IoT on the economy up to the year 2025 in various fields in which IoT is employed. The estimation showed that the IoT can contribute from $ 3.9 trillion to 11.1 trillion. In spite of its valuable benefits, the IoT is not without risks. We will now look at some of its darker sides. As shown in Fig. 2, this risk has two aspects: security and privacy. To provide convenience, IoT devices configure the surroundings of users as a connected environment. A single vulnerable point can be a security challenge for IoT devices as most of these devices are connected to the Internet all the time. Confidential and personal information on IoT devices can be used unauthorizedly and stolen by any malicious attackers. The attacker may monitor the user's life as well. Therefore, risk identification, assessment, and measurement should be implemented in IoT devices so that the unauthorized access and control may be identified and counter-measured.

As the number of IoT devices is increasing every day, there is a major risk of security threats, vulnerabilities, data manipulation, stealing, identity, device manipulation, and hacking. Poor security of these devices can provide an entry point for cyberattacks which may compromise sensitive data, threaten users' privacy and weaponize the device. The paper aims to identify the current security and privacy issues in IoT devices and propose recommendations for the solution of cybersecurity issues in IoT devices.

This article aims to comprehensively examine the landscape of cyber risks within the Internet of Things (IoT) realm. By delving into the intricate interconnections of IoT devices, it seeks to uncover potential vulnerabilities and threats that could compromise data security and user privacy. The objective is to provide a detailed analysis of these risks, coupled with real-world examples, highlighting the urgency for robust cybersecurity measures. Furthermore, the article intends to offer practical insights and strategies that individuals, businesses, and policymakers can adopt to effectively manage and mitigate cyber risks in the dynamic and rapidly evolving IoT world, fostering a safer and more secure digital environment.

LITERATURE SURVEY

The Internet of Things Promises New Benefits and Risks: A Systematic Analysis of Adoption Dynamics of IoT Products: Cyber risk for buyers is a major obstacle to broad adoption of the Internet of Things (IoT). Using a system dynamics approach, we conducted a case study of a connected lighting product to understand how cybersecurity influences IoT adoption.

Internet of Things: A survey on the security of IoT frameworks: The Internet of Things (IoT) is heavily affecting our daily lives in many domains, ranging from tiny wearable devices to large industrial systems. Consequently, a wide variety of IoT applications have been developed and deployed using different IoT frameworks. An IoT framework is a set of guiding rules, protocols, and standards which simplify the implementation of IoT applications. The success of these applications mainly depends on the ecosystem characteristics of the IoT framework, with the emphasis on the security mechanisms employed in it, where issues related to security and privacy are pivotal. In this paper, we survey the security of the main IoT frameworks, a total of 8 frameworks are considered. For each framework, we clarify the proposed architecture, the essentials of developing third-party smart apps, the compatible hardware, and the security features. Comparing security architectures shows that the same standards used for securing communications, whereas different methodologies followed for providing other security properties.

The Internet of Things vision: Key features, applications and open issues: The Internet of Things (IoT) is a new paradigm that combines aspects and technologies coming from different approaches. Ubiquitous computing, pervasive computing, Internet Protocol, sensing technologies, communication technologies, and embedded devices are merged together in order to form a system where the real and digital worlds meet and are continuously in symbiotic interaction. The smart object is the building block of the IoT vision. By putting intelligence into everyday objects, they are turned into smart objects able not only to collect information from the environment and interact/control the physical world, but also to be interconnected, to each other, through Internet to exchange data and information. The expected huge number of interconnected devices and the significant amount of available data open new opportunities to create services that will bring tangible benefits to the society, environment, economy and individual citizens. In this paper we present the key features and the driver technologies of IoT. In addition to identifying the application scenarios and the correspondent potential applications, we focus on research challenges and open issues to be faced for the IoT realization in the real world.

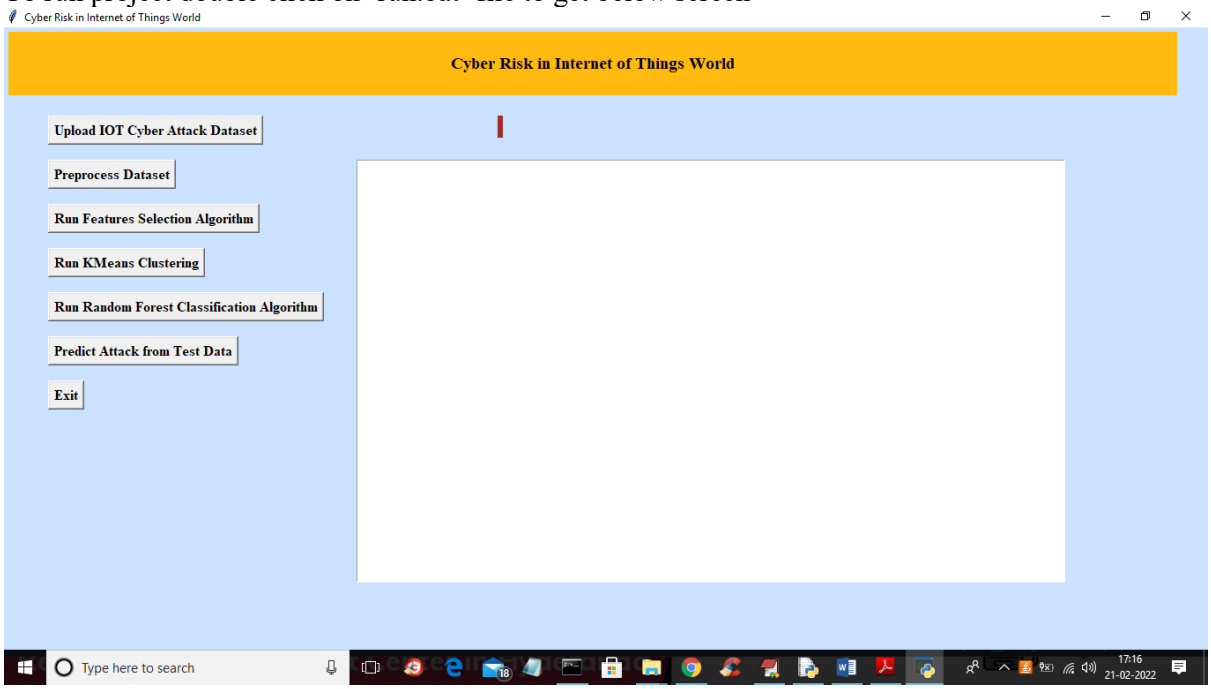
Cyber Risk Management for the Internet of Things: The Internet-of-Things (IoT) enables enterprises to obtain profits from data but triggers data protection questions and new types of cyber risk. Cyber risk regulations for the IoT however do not exist. The IoT risk is not included in the cyber security assessment standards, hence, often not visible to cyber security experts. This is concerning, because companies integrating IoT devices and services need to perform a self-assessment of its IoT cyber security posture. The outcome of such self-assessment need to define a current and target state, prior to creating a transformation roadmap outlining tasks to achieve the stated target state. In this article, a comparative empirical analysis is performed of multiple cyber risk assessment approaches,

to define a high-level potential target state for company integrating IoT devices and/or services. Defining a high-level potential target state represent is followed by a high-level transformation roadmap, describing how company can achieve their target state, based on their current state. The transformation roadmap is used to adapt IoT risk impact assessment with a Goal-Oriented Approach and the Internet of Things Micro Mart model. The main contributions from this paper represent a transformation roadmap for standardisation of IoT risk impact assessment; and transformation design imperatives describing how IoT companies can achieve their target state based on their current state with a Goal-Oriented approach. Verified by epistemological analysis defining a unified cyber risk assessment approach. These can be used for calculating the economic impact of cyber risk; for international cyber risk assessment approach; for quantifying cyber risk; and for planning for impact of cyber-attacks, e.g. cyber insurance. The new methods presented in this paper for applying the roadmap include: IoT Risk Analysis through Functional Dependency; Network-based Linear Dependency Modelling; IoT risk impact assessment with a Goal-Oriented Approach; and a correlation between the Goal-Oriented Approach and the IoTMM model.

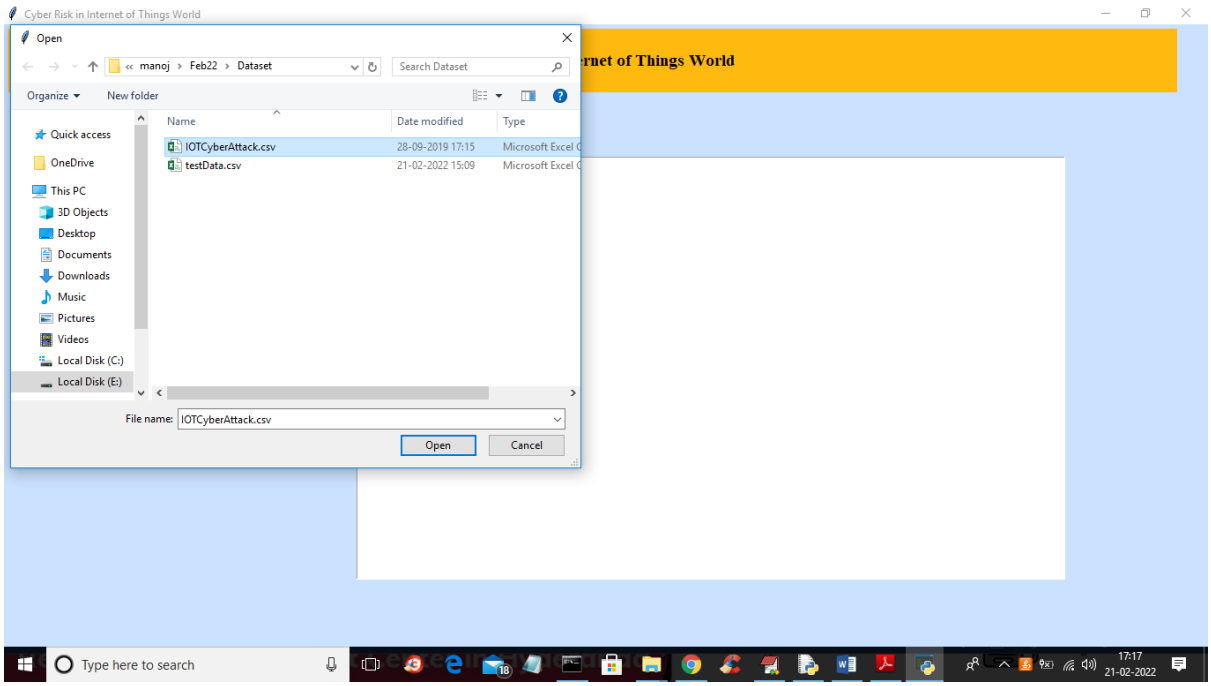
PROPOSED SYSTEM

The IoT ecosystem needs proper security at device level, application level, and network level. Different vendors with diverse goals but inadequate cybersecurity expertise manufacture these devices. The purpose of this paper is to identify the current security and privacy issues in IoT devices and propose recommendations for the solution of Cyber security issues in IoT devices.

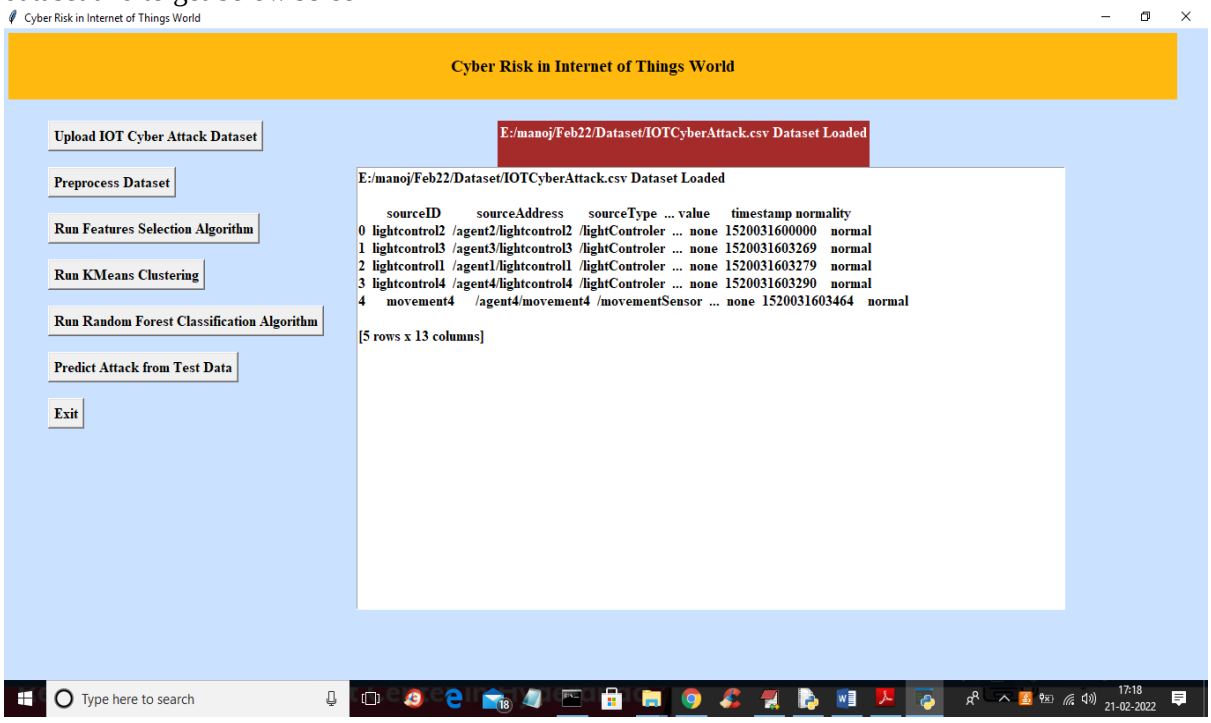
To run project double click on 'run.bat' file to get below screen



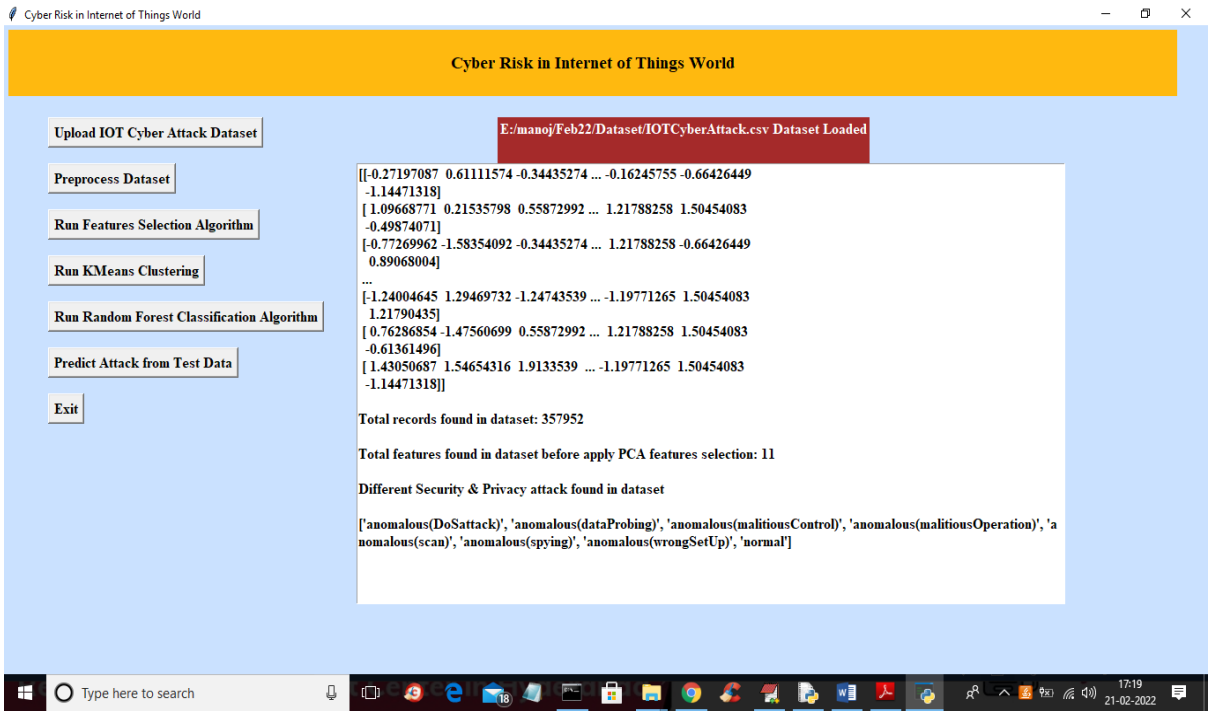
In above screen click on 'Upload IOT Cyber Attack Dataset' button to upload dataset and to get below screen



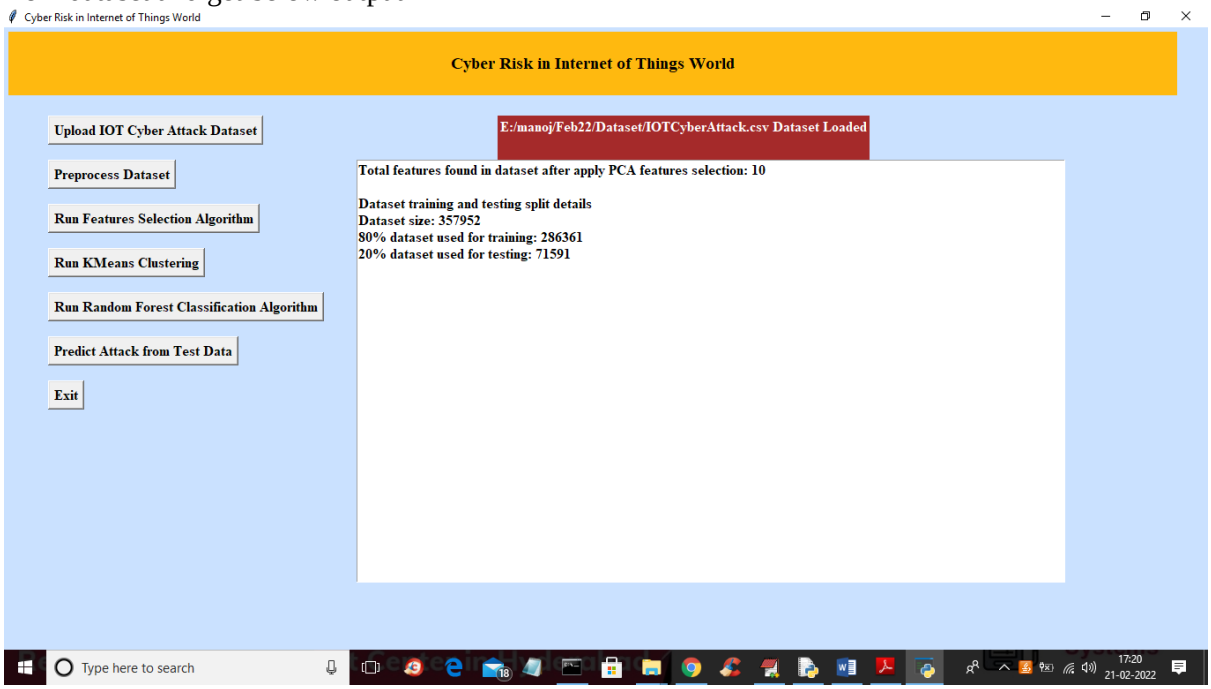
In above screen select and upload 'IOTCyberAttack.csv' file and then click on 'Open' button to load dataset and to get below screen



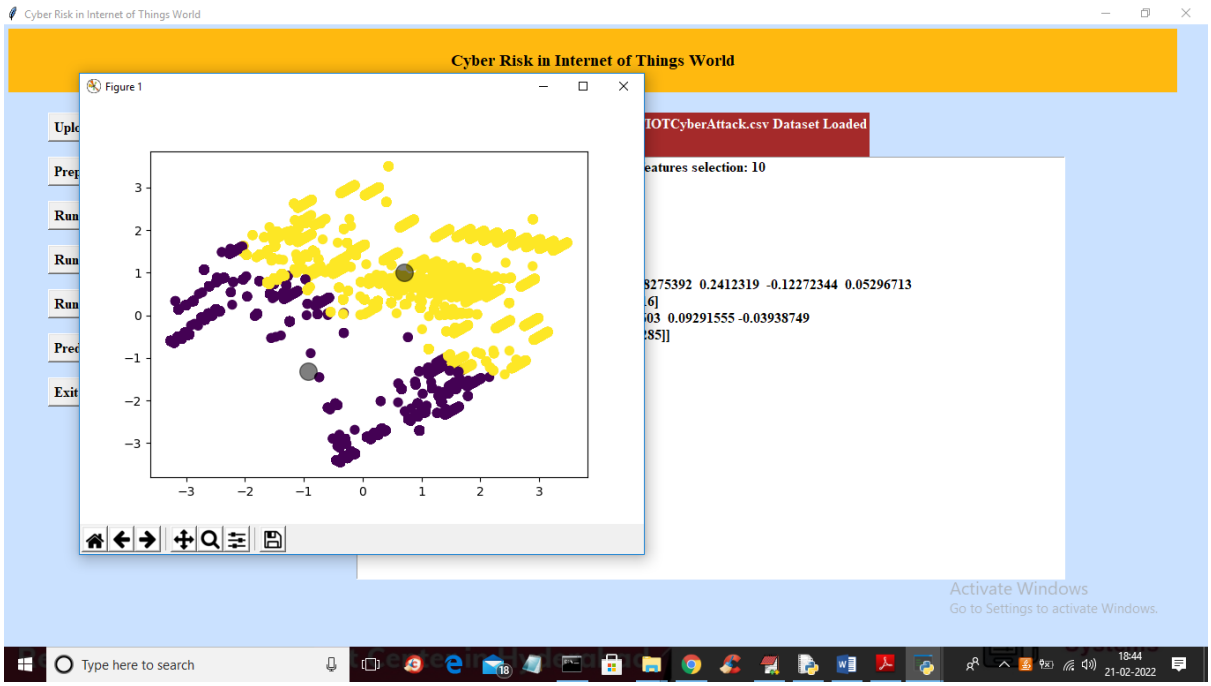
In above screen dataset loaded but all values are non-numeric and we need to convert to numeric so click on 'Preprocess Dataset' button to assign numeric ID to each values and to get below screen



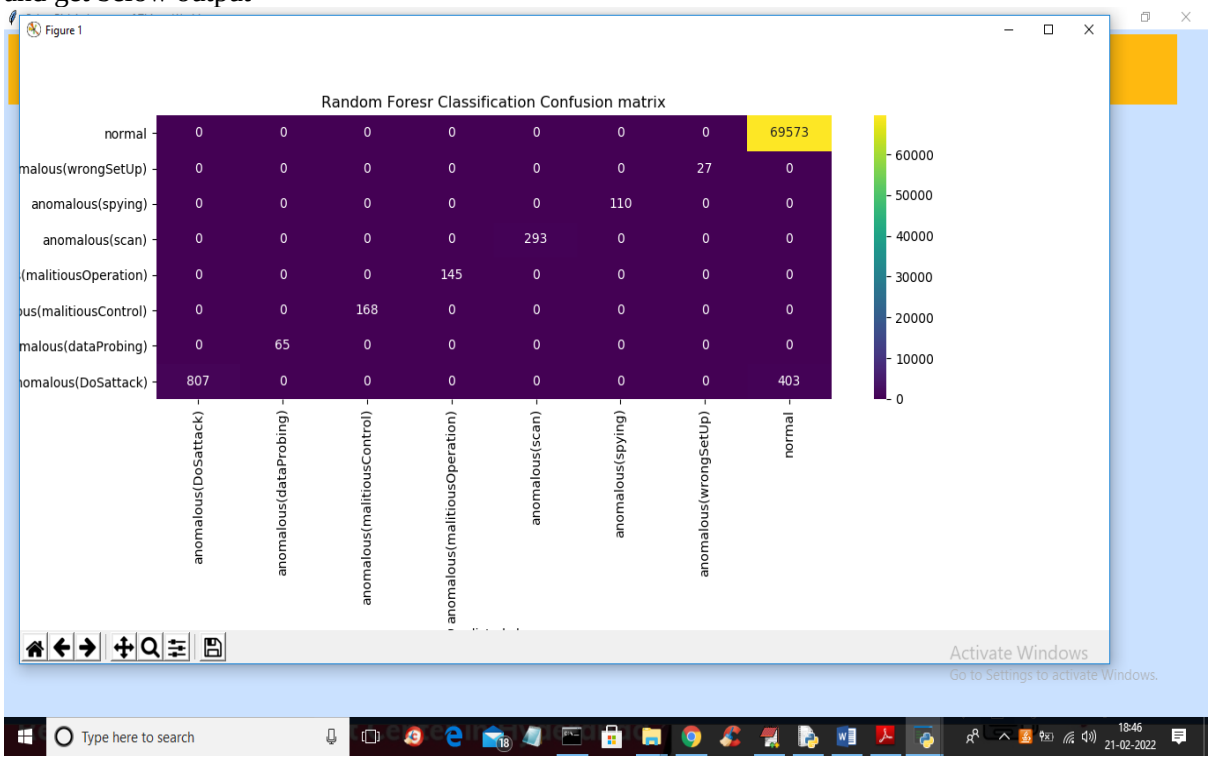
In above screen we can see all values are converted to numeric and in last line we can see before applying PCA features selection algorithm dataset contains 11 features and we can see different attack names found in dataset and now click on 'Run Features Selection Algorithm' button to select features from dataset and get below output



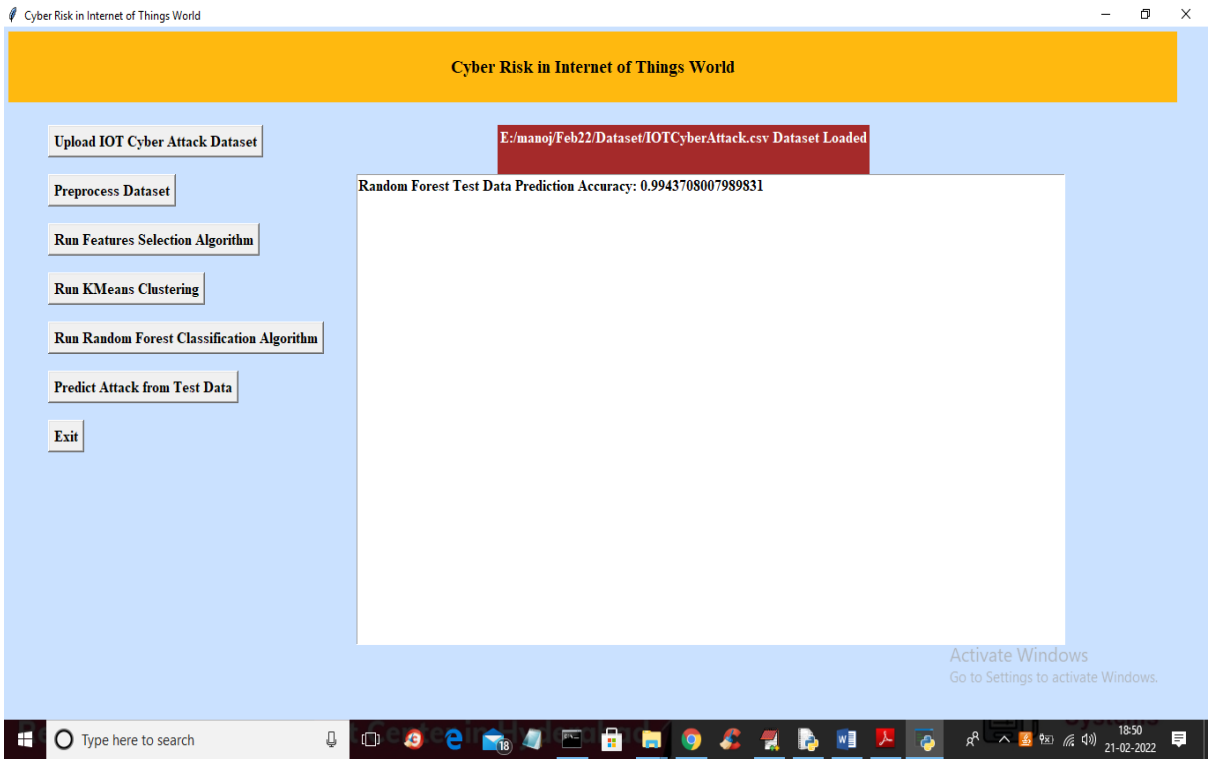
In above screen we can see after applying features selection algorithm we got 10 important features out of 11 and we can see total dataset with training and testing size. Now process dataset is ready with train and test data and now click on 'Run KMeans Clustering' button to group data into different clusters and get below output



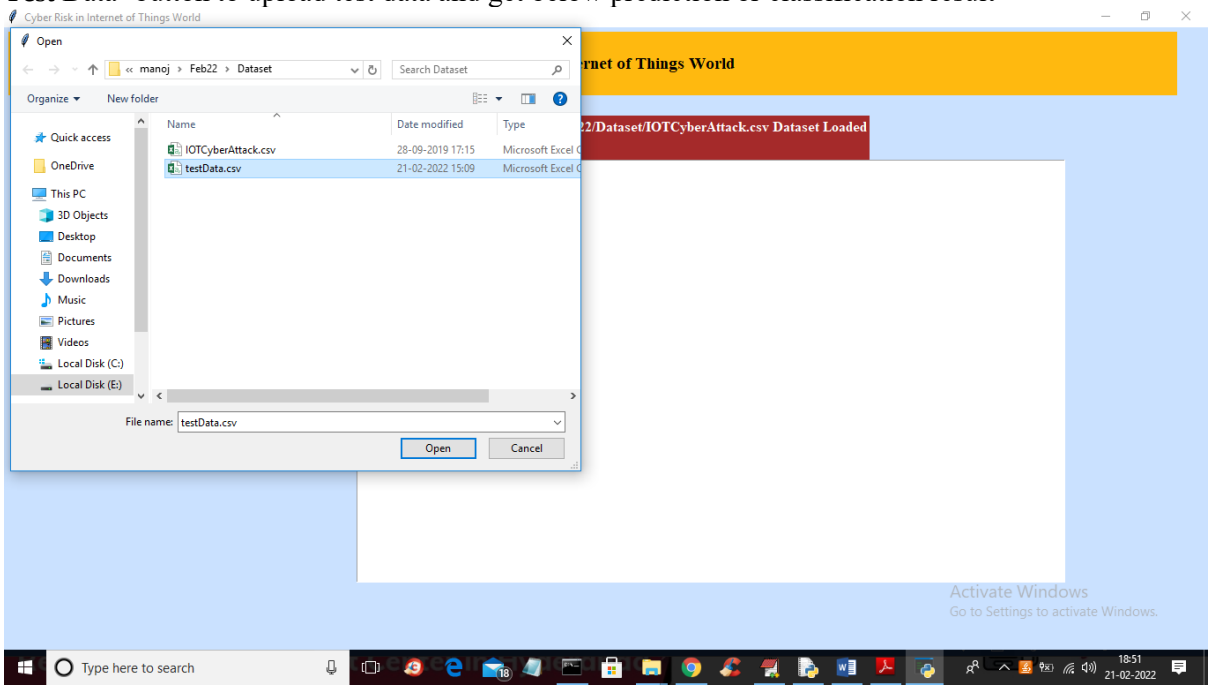
In above graph we can see same data are group into same cluster with same dots and different data is group into different clusters so in above screen we got two colours dots where one colour dot contains normal traffic and other colour dot contains attack traffic and now close above graph and then click on 'Run Random Forest Classification Algorithm' button to train dataset with random forest algorithm and get below output



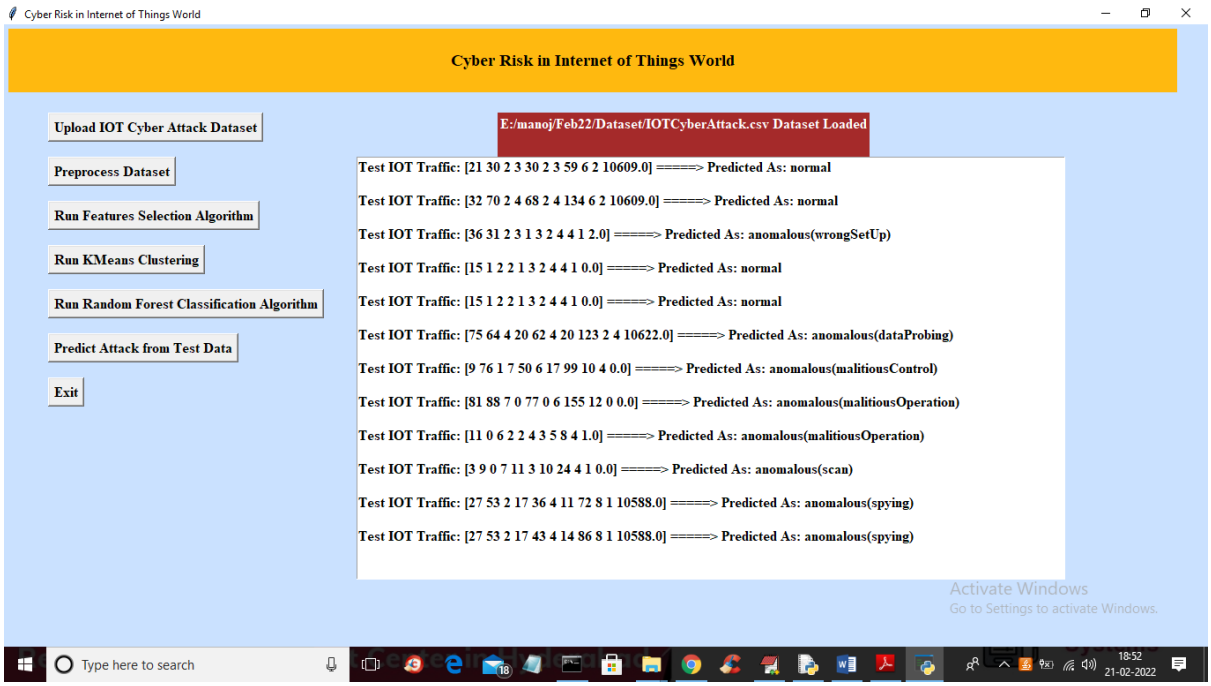
In above classification confusion matrix x-axis represents PREDICTED classes and y-axis represents TRUE TEST classes and we can see that in both X and y-axis we can see values > 0 which means TEST and predicted classes are correct and now close above graph to get below output



In above screen with Random Forest we got 0.99% accuracy and now click on 'Predict Attack from Test Data' button to upload test data and get below prediction or classification result



In above screen selecting and uploading 'testData.csv' file and then click on 'Open' button to load test data and get below output



In above screen in square bracket we can see test data and after square bracket we can see predicted traffic as NORMAL or attack names. So with this model we can predict or classify attack from IOT traffic.

CONCLUSION

The wide spectrum of IoT-based systems leads to convenience, speed, and satisfaction regarding tasks performed by users. This attracts more and more users. However, cyber risk is tightly coupled with

IoT systems. The main two aspects of it are security and privacy. The research gap associated with these aspects is related to deal with advanced attacks in the light of increasing the ability of attackers. The third aspect related to ensure safety is presented and discussed in this work. An intelligent-based framework is presented in this work to enable dealing with the aspect of cyber risk.

REFERENCES

[1] Jalali, M.S., Kaiser, J.P., Siegel, M., & Madnick, S. (2019). The Internet of Things Promises New Benefits and Risks: A Systematic Analysis of Adoption Dynamics of IoT Products. IEEE Security & Privacy, 17(2), pp.39-48.

[2] Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, pp.8-27.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. Computer Communications, 54, pp.1-31.

[4] Radanliev, P., Charles De Roure, D., R.C. Nurse, J., Burnap, P., Anthi, E., Uchenna, A., Maddox, L., Santos, O. and Mantilla Montalvo, R. (2019). Cyber Risk Management for the Internet of Things. [online] Available at: https://www.preprints.org/manuscript/201904.0133/v1 [Accessed Dec. 2019].

[5] Ali, B., & Awad, A. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. Sensors, 18(3), p.817.K. Elissa, “Title of paper if known,” unpublished.

[6] Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet of Things Journal, pp.1–1.

[7] Park, M., Oh, H., & Lee, K. (2019). Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective. Sensors, 19(9), p.2148.

[8] Hara, T., Suzuki, A., Iwata, M., Arase, Y., & Xie, X., (2016). Dummybased user location anonymization under real-world constraints. IEEE Access, 4, pp.673-687.

[9] Niu, B., Li, Q., Zhu, X., Cao, G. and Li, H., 2015, April. Enhancing privacy through caching in location-based services. In 2015 IEEE conference on computer communications (INFOCOM) (pp. 1017- 1025). IEEE.

[10] Bagga, P. & Hans, R. (2017). Mobile agents system security: a systematic survey. ACM Computing Surveys (CSUR), 50(5), p.65.