CYBER ATTACK DETECTION MODEL FOR WIRELESS SENSOR NETWORK

Dr. T PremChander[1], Nishat Fathima[2] , Bushra Mohiuddin[3], Sumaiya Qureshi[4],

Associate Professor[1], UG Scholar[2,3,4],

Department of Information Technology, ISL Engineering College, Hyderabad, Telangana.

ABSTRACT - Cyber crime is proliferating everywhere exploiting every kind of vulnerability to the computing environment. Ethical Hackers pay more attention towards assessing vulnerabilities and recommending mitigation methodologies. The development of effective techniques has been urgent demand in the field of the cyber security community. Our main goal is that the task of finding attacks is fundamentally different from these other applications making it significantly harder for the intrusion detection community to employ effectively. Detection of local attacks needs just a little amount of information. Hence efficient adaptive method like various techniques of machine learning can result in higher detection rates lower false alarm rates and reasonable computation and communication cost.

Keywords - *Detection of Cyber Attacks · machine learning · Django-analysis-microgrids*

I. INTRODUCTION

Microgrids provide a number of benefits over traditional electricity grids, including lower costs and more flexibility. Because of their regional production and compatibility with a wide range ofrenewable sources, they guarantee high-quality, low-loss electrical power transmission DC and AC microgrids are made up of a network of small, autonomous units. Generators, storage and loads(DGU). Microgrids powered by DC As a significant section of the population, (DCmGs) have a lot of potential. DC loads have received a lot of attention in the field of electrical engineering .Microgrids must have a steady and efficient operation to guarantee their long term viability a hierarchical control architecture is used First and foremost controls local authority in a decentralised manner electrical properties such as voltage, current, and frequency. Secondary andtertiary levels power quality control, load sharing and DGU are all handled by the layers. co- ordination, microgrid synchronisation and optimization enforcing system rules and regulations. As exemplified, Secondary and tertiary aims in are outlined in detail. However, hostile attacks and data compromises may occur as information travels over communication channels [9]. [10] and [11] are two examples of this. As a result of these assaults, people's lives are disrupted the functioningof a microgrid and may have negative effects as well as harm to key loads, blackouts, and voltageinstability. Therefore, spotting and preventing assaults is essential in order to take correctivemeasures.

In this paper, we present a strategy for counterattack approach that is able to distinguish between differenttypes of disease security measures in place to protect the communications network a supplementary control for current sharing based on consensus in the form of DCMGs. It has beendiscovered that a new estimator is based on the use of UIOs. The idea that has been floated using just the information provided, the estimator may determine if output measures are includedin the DCmG model as a whole data-injection has tainted the data it receives from its neighbours whether or not to engage in a fight presents preliminary findings. The use of local UIOs for estimation in the condition of DGUs in close proximity. Limits of detection (LOD) are systems have been created to prevent false alerts. To This is the first publication of its kind, as faras the writers can tell developing a DC microgrid attack detection framework.

Unfortunately, the analysis is limited to the DC microgrid and the method is not smart enough to detect different attack severities. In addition, the high complexity and nonlinearity of microgrid Local consumers (residential, industrial or agricultural) make it impossible to reach all points for comparison. This paper proposes a new intelligent framework to deal with the data integrity attackin microgrids and defend them against these malicious activities. The proposed framework can detect cyber attacks with different severities (let's call attack strength) by measuring specific features of the microgrid and learning their behavior during the normal operation.

II. PROPOSED SYSTEM

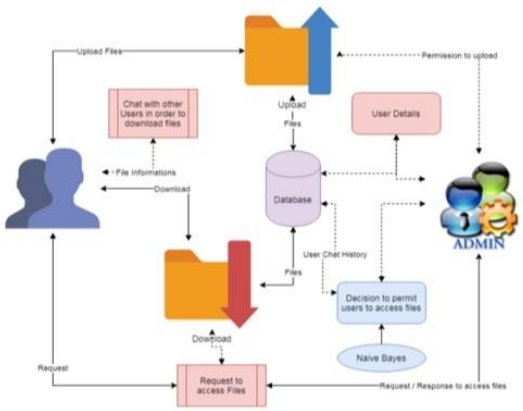
The proposed framework can detect cyber attacks with different severities (let's call attack strength) by measuring specific features of the microgrid and learning their behavior during the normal operation. The proposed cyber resilient model is constructed on Django framework and NNP methodology. We explore the suitability of ensemble learning methods as a means

of detecting power system cyber-attack. We evaluate various ensemble learning methods as cyber-attack detectors and discuss the practical implications for deploying ensemble learning methods as an enhancement to existing power system architectures.

III. LITERATURE SURVEY

The nature of the system breaches and the attacks on the system affects the state of operation and working of the system. A system may incur active or passive attack which makes the whole system collapse. When a system is attacked, the data security is breached and all the information contained in the system are hacked or obtained by the hacker in the successful attack. When a system is underattack and if the access to the system is granted, all the potential information will be lost or damaged depending on the intention of the attacker.

Block Diagram



Modules

Upload Data

The data resource to database can be uploaded by both administrator and authorized user. The data can be uploaded with key in order to maintain the secrecy of the data that isnot released without knowledge of user. The users are authorized based on their details thatare shared to admin and admin can authorize each user. Only Authorized users are allowedto access the system and upload or request for files.

User Details

The access of data from the database can be given by administrators. Uploaded data aremanaged by admin and admin is the only person to provide the rights to process the accessing details and approve or unapproved users based on their details.

User Permissions

The data from any resources are allowed to access the data with only permission fromadministrator. Prior to access data, users are allowed by admin to share their data and verify the details which are provided by user. If user is access the data with wrong attempts then, users are blocked accordingly. If user is requested to unblock them, based on the requests andprevious activities admin is unblock users.

Data Analysis

Data analyses are done with the help of graph. The collected data are applied to graph in order to get the best analysis and prediction of dataset and given data policies. The dataset can be analyzed through this pictorial representation in order to better understand of the data details.

IV. RESULT AND CONCLUSIONS

In this paper, we present a systematic review of cybersecurity detection attacks in the IoT using Django framework. Due to their rapid development in the various domains, large amounts of data are constantly being generated, which requires an increased focus on privacy and security. If these attacks succeed, IoT performance can be compromised in many ways such as giving false information. While in the past, traditional methods have been used for improving IoT security, due to the rapid evolution of cyber threats. As a result, the Django approach can be considered one of the most promising framework. We summarized, categorized, and mapped the existing literature on Django framework for the detection of cybersecurity attacks in IoT environments using formulated research questions.

V. REFERENCES

[1]. W.R. Issa, A.H. El Khateb, M.A. Abusara, T.K. Mallick, "Control Strategy for UninterruptedMicrogrid Mode Transfer During Unintentional Islanding Scenarios", IEEE Trans. Industrial Electronics, vol. 65, no. 6, pp. 4831 –4839, 2018.

[2]. M. Dab, A. Kavousi-Fard, S. Mehraeen, "Effective Scheduling of Reconfigurable MicrogridsWith Dynamic Thermal Line Rating", IEEE Trans. Industrial Electronics, vol. 66 , no. 2, pp. 1552– 1564, 2019.

[3]. K.W. Hu ; C.M. Liaw, "Incorporated Operation Control of DC Microgrid and Electric Vehicle", IEEE Trans. Industrial Electronics, vol. 63, no. 1, pp. 202-2015, 2016.

[4]. Greentech Media reports, 2018. Online: https://www.utilitydive.com Pagliery, J. (2014) Hackers Attacked the U.S. Energy Grid 79 Times This Year, (accessed10 March 2017). http://money.cnn.com/2014/11/18/technology/security/energy-gridhack/

[5]. R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon", IEEE Security & Privacy, vol. 9, no. 3, pp. 49-51, 2011.

[6]. R. Rashed Mohassel, A. Fung, F. Mohammadi, K. Raahemifar,

"survey on Advanced Metering Infrastructure", International Journal of Electrical Power & Energy Systems, vol. 63, pp. 473-484,2014.

[7]. O. Kosut; L. Jia; R.J. Thomas ; L. Tong, "Malicious Data Attacks on the Smart Grid", IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 645 – 658, 2011.

[8]. X. Yang; P. Zhao; X. Zhang; J. Lin; W. Yu, "Toward a Gaussian-Mixture Model-Based Detection Scheme Against Data Integrity Attacks in the Smart Grid", IEEE Internet of Things Journal, vol. 4, no. 1, pp. 147 – 161, 2017.

[9]. J. Duan; W. Zeng ; M.Y. Chow, "Resilient Distributed DC Optimal Power Flow Against Data Integrity Attack", IEEE Trans. Smart Grid, vol. 9, no. 4, pp. 3543 – 3552, 2018.

[10]. Q. Yang, D. Li ; W. Yu ; Y. Liu ; D. An ; X. Yang ; J. Lin, "Toward Data Integrity Attacks Against Optimal Power Flow in Smart Grid", IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1726 – 1738, 2017.