Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 6, 7466-7472

A Viable Methodology Of Defending Smart Iot Devices Cyberattacks With Notification Using ML

R.Jaya Bharathi[1] , S.Anitha Rajathi[2] , M.A.Berlin[3] , Josephin Sharmila[4] , P.Shobha Rani[5]

[1]Assistant Professor, Department of Computer Science and Engineering, RMK College of Engineering and Technology, Chennai. TamilNadu, India , jayabharathicse@rmkcet.ac.in
[2]Assistant Professor, Department of Computer Science and Business, Systems, R.M.D Engineering College, Chennai. TamilNadu, India, anitha.csbs@rmd.ac.in
[3]Professor, Department of Computer Science and Engineering, R.M.D Engineering College, Chennai. TamilNadu, India, mab.cse@rmd.ac.in
[4]Department of Electronics and Communication, RMK College of Engineering and Technology, Chennai. TamilNadu, India , blossomshermi@gmail.com
[5]Associate Professor, Department of Computer Science and Engineering, R.M.D. Engineering College, Chennai. TamilNadu, India, psr.cse@rmd.ac.in

Abstract - Vulnerabilities in smart home (IoT) platforms make it possible for intruders to perform attacks in a variety of settings, including home automation, industrial automation, and sophisticated health systems. Research has developed a variety of comprehensive security technologies to get around this cyber-attack obstacle. Machine Learning (ML), which is being deployed, has been identified as the most viable method. Consequently, the majority of ML approaches solely concentrate on researching suitable learning models in order to increase the recognition rate. However, a lack of suitable identification characteristics frequently contributes to the limits in terms of recognition rate in a variety of assaults. The present approaches, however, are inadequate to cover the comprehensive security spectral range of IoT environments due to the distinctive characteristics of IoT nodes. Furthermore, the majority of previous efforts lacked implementation structures and methods for defending against cyber-attacks. As a result, in this research, we examine the characteristics of several smart home security threats as well as the value of the information that may be extracted and used in Ml techniques to effectively identify any of these cyberattacks. Due to the increase in internet traffic, it is more difficult to identify cyberattacks in the IoT as well as identify fraudulent traffic in its initial stages. SVM, RF, LR, and decision tree algorithms were successfully used in machine learning systems to determine and alert users of smart IoT devices to potential threats. A methodology for the identification of malicious cyber activity is suggested in this paper.

Keywords: IoT, Drones, Remote Sensing, GPS, Deforestation.

I. INTRODUCTION

IoT is characterized as a dispersed, linked network of integrated devices that communicate via wireless connection methods. IoT devices produce a staggering quantity of data, so conventional methods for gathering data, storing, and analytics might not even be effective at this level. This massive amount of data can be used to identify correlations, behaviors, predict outcomes, and perform assessments. This capacity of a smart device to change or regulate a condition or behavior based on experience is regarded to be a key component of an IoT application and can enable machinery with smart devices to derive relevant information using user facts.

The Internet of Things' primary goal is to link networks, green infrastructure, tools, platforms, and devices so that they can communicate, share data, and be controlled. This Internet of Things is intended to make our livelihoods and modernity work more efficiently. Our everyday lives are being impacted by the IoT. It's all online, including intelligent sensors, smartphone health apps, thermometers, photovoltaic systems, coolers, and household appliances. As a result of the IoT technology's

fast evolution, it is far more difficult to safeguard IoT data from intruders, cybercriminals, malicious access, and harmful traffic. In order to safeguard data, several methods are accomplished and more methods are being created and put into use in IoT networks and platforms. Machine learning has been employed more for many purposes in the security industry, as its usage in attack detection difficulties has become a strongly discussed subject. Only a small number of studies have been done on effective diagnostic strategies appropriate in IoT contexts, despite the fact that much literature has employed Ml methods to identify the best methods to find assaults. Through analyzing the effectiveness of machine learning on such a relevant IoT set, the response to these threats in IoT is improved. In this regard, machine learning is among the most efficient analytical models to deliver embedding knowledge as in the IoT environment. For a wide range of network security tasks, including network monitoring and intrusion prevention, machine learning approaches were deployed.

IoT security concerns are more complex due to IoT devices' quick expansion and widespread usage. That highlights the necessity for p2p security mechanisms. Although contemporary technologies are effective in detecting cyber intrusions, it is difficult to uncover every one of these attacks. As malicious activities and the volume of data available on networking increased, faster and more accurate techniques for detecting intrusions were required. There are still many continuing approaches to enhance network infrastructure. Confidentiality is a major IoT concern that requires emphasis and additional investigation. IoT cyber security attack identification utilising Ml has significantly improved. The IoT's biggest fear, meanwhile, is with limiting factors that prevent the usage of modern security mechanisms that are still on the market in IoT. In particular, IoT systems might require new varieties of efficient cryptography as well as other techniques to handle safety and confidentiality owing to computing limits. IoT safety concerns will be addressed by the establishment of innovative, sophisticated, resilient, adaptive, and adaptable methods along with recommendations from current security measures. The IoT faces a significant problem in mitigating assaults conducted by smart malware attacks since these cyberattacks automatically scan and scan its networks in search of significant vulnerabilities before launching numerous attacks, including powerful DDoS attacks. In order to ensure safety, IoT devices must be shielded from both public and private security breaches. Organizations' physical assets, data, and transit at rest and storage should all be protected by cybersecurity.

A major issue with IoT products or services is user privacy. This ability of the IoT system to confirm that an entity has authorization to view the resource is required. After identity, permission means establishing if the user or IOT device is allowed to use a resource. Managing access to information involves utilising a range of indicators to allow or prohibit use. Authentication and access control are crucial to being able to link various technologies and applications securely. Those assaults consist of traffic monitoring, protocol assaults, side-channel threats, impersonation attacks, and MAN threats. Certain such assaults have been covered. Attacks using network analysis involve passively monitoring the data even as intruders seek to make meaning of it. So, because sender and receiver are frequently unaware when their traffic has been intercepted, such assaults are exceedingly difficult to counteract. Mostly in internet traffic, cyber intruders search for intriguing data, including user private details, application logic specifics, passwords, and other data that could be useful to the intruder. Additionally, with the IoT, file transfer integrity is of the utmost significance. The Iot generates information that is used for decision-making; thus, it is crucial to ensure the data quality.

Due to the omnipresent nature of the IoT ecosystem, confidentiality is indeed a crucial concern in IoT environments. Due to the connection of entities as well as the communication and interchange of data across the network, privacy protection is a sensitive issue in several study efforts. There are still unanswered important questions about data protection and information sharing, including confidentiality during data gathering. Security flaws are flaws in a system's functionality or architecture that let an outsider run programmers, get access to confidential data, or launch denial-of-service (DoS) assaults. As in the IoT network, flaws may be located in many different places. In particular, these could be flaws in the firmware of the network, flaws within regulations and procedures that are implemented by the scheme, and mostly flaws in system user behavior. Threats involve acts performed to damage a system or obstruct operational capabilities through utilising different methods and solutions to compromise the security. Intruders initiate assaults to accomplish objectives, whether for their own gratification or to receive retribution. Assault value seems to be an assessment of the level of work that will be done by an attack, represented in-depth knowledge, assets, and purpose. Attacking actors would be those who pose a risk to the online environment. Close-range threats; anonymous source manipulation; network device threats that supervise non-encrypted traffic while searching for

sensitive data; passive strikes that monitor undefended connectivity channels in order to decipher poorly encoded traffic; and so on. IoT vulnerabilities and security threats have increased as a result of the IoT's rapid expansion. Most of these threats were caused by hardware flaws brought on by criminal extortion and inappropriate device asset utilization. So, IoT must be designed in a way that makes convenient and effective use management possible. For users to benefit greatly from the IoT as well as minimize confidentiality threats, they must have the ability to do so. As previously stated, all IoT device services were vulnerable to a wide range of common threats, including malware and denial-of-service attacks. Easy precautions won't be enough to protect against these dangers and address the potential for error; instead, it's important to ensure that policies are implemented smoothly and are backed by reliable processes.

This vast number of IoT devices makes it extremely difficult to meet the necessary security requirements of cloud-based IoT. Additionally, while IoT technologies are created with a specific Iot ecosystem in view, they need not cover the full spectrum of other domains, which might provide adequate levels of such an area. IoT employs a wide variety of different technologies using different criteria, methods, and protection. Both underpinning apps and infrastructures must be taken into consideration in order to concentrate on IoT security considerations since these set us up for appropriate solutions. The main drawback of core machine learning approaches is that they often require large datasets for model development. Implementations for the Internet of Things combine a variety of computing resources, including ultra-low-power end devices through highly efficient cloud storage. Such diverse gadgets necessitate more robust safeguards and superior ML capability. Innovative IoT systems like drone attacks, smart watches, and driverless cars need improved reliability and functionality while using fewer resources. Additionally, because IoT systems are energy-constrained, it is necessary to build and create extremely low-cost circuitry as well as lightweight cryptography algorithms. This infrastructure would face severe consequences when IoT nodes are compromised and identities are assumed, since this will allow attackers to execute causes by malicious operations, in which bogus nodes trick the main network into assuming that actual nodes are sharing data. Such behaviors can spread phoney information over the internet and send bogus information to apps. Any decision support system that depends on incoming information might be readily subverted by malicious nodes. In conclusion, the different network threat vectors prey upon the IoT's communication-related features and take advantage of resource limitations and the absence of comprehensive identification and permission protocols.

II. LITERATURE REVIEW

P. Illy [1] the author, investigated lack of adequate detecting characteristics is frequently to blame for the limits of classification accuracy in different assaults. Additionally, installation strategies and intrusion prevention methods are absent from the bulk of earlier efforts. As a result, in this research, we examine the characteristics of several smart security assaults as well as the value of the services that may be extracted and used in MLM techniques to effectively identify each of these attacks. This study suggests installing intrusion in wired networks using networking and robust invasion prevention strategies. Various feature subsets and ML algorithms are used in practical assessments of the proper approach. Upcoming engineering and technological projects on intrusion for IoT would be improved by the inputs and developments highlighted throughout this paper.

Inayat, [2] introduced a paper in The IoT technology is a key development which makes it simple and advantageous to share data with other devices across wireless or internet connections. IoT devices are prone to intrusions that might result in hostile incursions given the changes and advances in the IoT ecosystem. The effects of such breaches may result in material and financial losses. The IoT scheme, the IoT having to learn approaches, as well as the obstacles encountered by IoT equipment and systems following an attack are the key points of this research. Various attacks, including DoS, DDoS, sniffing, malware assault, phishing, and MITM cyber-attacks, will be used to examine learning algorithm methodologies. Several machine learning methods are described and examined in connection to the identification of intrusions in IoT networks using learning approaches. To provide a clear understanding of many advancements throughout this field, a thorough inventory of all publications that have been made in recent years in the field is incorporated. This study also includes ideas for further investigation.

According to Mohamed [3], the industry 4.0, which began in recent decades, is marked by the increasing growth of IoT, cloud technology, information assurance, and cybercrime. IoT internet-enabled devices are rapidly evolving, resulting in large datasets that require strict privacy and authorization. Among the most recent

alternatives for combating cyber risk and ensuring safety is part of AI. We categorise, analyze, and assess the published evidence on AI methods being used to identify security assaults mostly in the IoT environment inside this report's systematic review, which we provide. The above scope covers a thorough analysis of the majority of AI trends for defence and cutting-edge technologies. Therefore, in this research, the overall usefulness of machine learning and deep learning approaches for IoT was examined. To address the current privacy risks, various research has suggested integrating smart architecture platforms and sophisticated security devices with AI. Support vector machines and random forests are two of the most popular techniques, which is likely because of their excellent detection performance. Affordable storage could also play a role. Additionally, alternative approaches with enhanced quality include rnn, neural nets, and exceptional XGBoost. This investigation also sheds light on the AI strategy for identifying dangers depending on the types of attacks. We conclude by offering suggestions regarding prospective future research. Z. Trabelsi [4] introduced a paper The Internet of Things (IoT) is now extensively applied across many industries. Users are increasingly embracing IoT technologies, for instance, to build innovative households. Such Internet of Things gadgets allow customers to control and safeguard their simulated environment while also collecting information. Nevertheless, harmful people and actions target IoT systems. As a result, security is crucial for Internet-of-things home automation. The study intends to empirically assess the endurance and durability of another class of IoT systems, referred to as home surveillance systems, against a number of prevalent attacks. This Kali Linux operating system, which has a variety of pen testing and internet appropriate cases, serves as the attacking foundation.

Tarek Gaber [5] introduced a paper One IoT platform that is expanding quickly is smart cities. WSNs are mostly used in smart cities to link all of their various parts simultaneously. The vast IoT infrastructure of interconnected devices is needed because urban areas depend on the convergence of IoT with 5G technology. About 80% of overall data flow over the present Internet of Things infrastructure comes through domestic wireless connections. Data security and privacy are a top worry for thousands of Internet-of-things connected devices as urban areas and their apps proliferate. Another explanation for this might be that the designers of IoT systems fail to address safety issues that allow hackers to use such devices' weaknesses in such a variety of ways. Another method for identifying and reducing the danger of these assaults is unauthorised access. An intrusion prevention approach was put forth in research to identify software vulnerabilities in IoT networks. Numerous machine learning classifications evaluated two different sorts of feature extraction strategies throughout this strategy. The T-Test has been used to examine the efficacy of all these suggested characteristic decision models. Our findings using publicly available data AWID revealed that a decision tree could identify injecting assaults with a 99 percent accuracy using only 8 characteristics chosen using a suggested feature search strategy. Some benefits of the suggested idss were further demonstrated by comparing them with more pertinent research.

According to 6.M. Anwer [6], Numerous experts have now investigated the dangers that IoT devices offer to major corporations and transport systems. Smart methods that can identify suspect activity on IoT devices linked to local stations were required given the growing integration of IoT, its nature, intrinsic portability, and standardisation restrictions. Overall, the bandwidth of online traffic increased as there were more IoT devices connected via the internet. As a result of this development, intrusion detection systems using conventional approaches and outdated information techniques have become ineffective. Because of the rapid increase in the volume of network activity, identifying attacks within this IoT and detecting malicious traffic early on appears to be a difficult task. A methodology for the identification of fraudulent internet traffic was suggested in this study.

Vitorino [7] suggested an approach on Privacy in the technological age is a major concern. The increasing frequency of cyberattacks on Internet of Things systems emphasises the need for highly reliable detection of hostile connectivity. Throughout this study, 9 infection grabs from IoT-23 data were subjected to a comparative examination of supervised and unsupervised learning, including reinforcement learning. Several binary and multi-class classifying situations were taken into account. SVM, XGBoost, and a Deep Reinforcement Learning system based on DDQIN, all of which were customised for intrusion prevention settings, were advanced concepts. The light-enabled gradient boosting method delivered the performance that could be trusted the most. According to Hussain [8], IoT devices (IoT) will have a significant impact on our activities, primarily in the future at the economic, economic, and societal levels. IoT system components are frequently assets, which makes them prime targets for assaults. Throughout this context, significant attempts were made, largely using

conventional encryption methods, to solve fundamental privacy risks in networks. Most present methods, though, are inadequate to cover the complete security range of IoT networks due to the distinctive qualities of IoT. To deal with various security threats, deep learning and machine learning approaches that may incorporate knowledge from IoT devices are used. Within that study, we comprehensively examine the necessities, attack surfaces, including available security mechanisms in networks. Key holes in such security mechanisms that demand ML and DL strategies are therefore highlighted. Finally, we go into great detail about the ML and DL technologies that are now being used to solve IoT security challenges. We additionally go over a number of potentials lies in the following with ML and DL-based IoT security studies.

III. PROPOSED METHODOLOGY

3.1 Data Collection

A device's user is able to receive service as required. IoT environments' many systems and applications should be durable throughout in order to continue to function, often in the midst of malevolent attackers or challenging circumstances. Different systems use different needs for reliability. In contrast, surveillance devices for disasters or medical conditions will probably need more reliability than detectors monitoring distorted noise.

Such organisations frequently serve their objectives through vengeance, stealing of proprietary information, corporate espionage, and attacks on the state infrastructure. The motivations of such organisations are fairly varied. It may entail providing personal information, including financial records, to terrorists, corporations, as well as other organised criminals. Several of these threats are caused by hardware flaws brought about by hacking extortion and inappropriate device asset utilization. This IoT must be made in a manner that makes simple and secure use management possible. For users to benefit greatly from the IoT and minimise user privacy threats, they must have the trust to do so. As was previously said, the bulk of IoT devices and services are vulnerable to a variety of typical dangers, including malware and DOS assaults. Precautions won't be enough to protect against such dangers and address the potential for error; instead, it's important to ensure that policies are implemented smoothly and are backed by reliable processes.

3.2 Threat Models in IOT

Persistent manipulation of a device inside an Iot is typically correlated with flaws, which frequently result from a major weakness in a system. To create a precise evaluation of the system overall, it is essential to study such vulnerabilities. In order to give a clear view of the origin of vulnerability in an IoT context and to underline the relevance of eliminating such flaws, we examined the weaknesses only at the gadget level. Iot systems have to be protected since vulnerabilities in security might possibly diminish the value of the device. In every IoT area, the increasing devaluation of sensors owing to inherent flaws might result in varying levels of damage.

3.3 Security Challenges

Weak security protocols raise the risk of data loss as well as other dangers. Owing to insufficient security procedures and regulations, the majority of experts perceive the IoT as a source of vulnerability for cybersecurity threats. Many safeguards have been created to safeguard IoT systems against intrusions; however, safety protocols really aren't properly documented. Nevertheless, because of the widespread use of smart devices that share and integrate data, many organisations are now very concerned about privacy or security breaches since they disrupt work processes, daily operations, and core networks. Experts are required to address such security issues, create thorough security policies and procedures to safeguard their corporate resources, and guarantee the continuation and reliability of their operations.

3.4 ML solutions in IoT

The implementation of IoT typically consists of a collection of comparable or pretty similar equipment with shared traits. Every vulnerability that seems to have a major impact on a few of those gets amplified by this commonality. Other organisations have developed instructions for conducting risk assessments based on this. Such action indicates there are probably an unparalleled number of linkages connecting IoT technologies. It is evident that even a large number of such gadgets have the chance to empathise with and speak informally and spontaneously with certain other gadgets. They demand that the analysis and assessment, approaches, and strategies linked to Iot be taken into account. The purpose of a recent study is to examine sophisticated assaults that might have been largely based on breaches of corporate security policies. When finished, an attacker is enabled to prey on people who link unapproved Internet of Things types to smart municipalities. Because of their high detecting precision and low false alarm rate, the preceding methods were widely used. They are unable to intercept new strikes, though. Outlier detection, on either hand, cannot accurately identify emerging assaults but does identify them. Traditional ML research has been

increasingly utilised for both processes. Modern gadgets that learn algorithms are unable to recognise sophisticated security breaches.

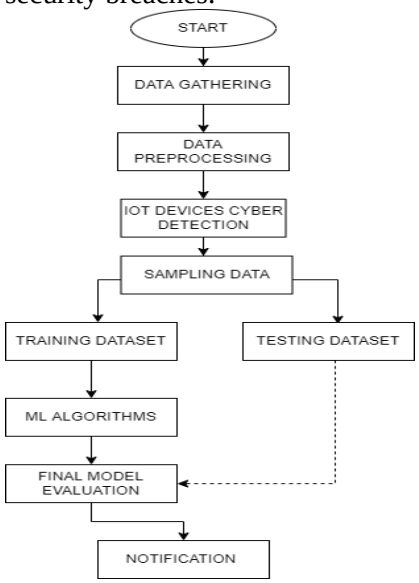

Figure 1. Flow Representation

IV. DESIGN AND IMPLEMENTATION

4.1 Dataset

The IoT device market is expanding exponentially, giving hackers a larger system of vulnerabilities from which to conduct increasingly damaging cyber-attacks. This attacker wanted to use suspicious attacks to use up all of the bandwidth on the targeted network infrastructure. Iot's methodologies and detecting techniques necessitated well planned data. The most popular method in automated data analysis is categorization. The goal of categorization would be to build models using classified elements to predicate things. Assessment of contemporary intrusion prevention methodologies needs fresh, comprehensive data. The goal of categorization would be to build models using classified elements to predicate entities.

4.2 IOT Security Attacks

As IoT employs an information system comparable to the old network design for the interaction of many objects, it carries over the shortcomings of conventional system architecture. The Internet of Things has led to the creation of several threat vectors that aim to circumvent Internet of things safety. Efforts have been made to put up many defences against such assaults. Unfortunately, putting most of these safeguards and procedures into practise at once uses up gadget power consumption or processing power, which is unacceptable with IoT technology or its gadgets. Hence the need for a security feature that addresses all security vulnerabilities. It must be portable and strong enough to work with Iot. Numerous IoT threats have been explored and categorised here.

4.3 Machine Learning Algorithms

Similarly, to providing a model with numerous samples of documents to determine whether they are malicious software, all information must be labelled throughout. This algorithm might choose to include more information acquired here on data labelling. Another name for this is the task-driven method. Throughout this section, the issues with detecting attacks are investigated through the statistical categorization of measures utilising ML. Cybersecurity's search function isolates malware from various telecommunication services. Spam appears to be the most popular ML technique used in data security. In categorization, the training data labelling approach is typically utilised. The main drawback of core machine learning approaches is that they often require large datasets for model development.

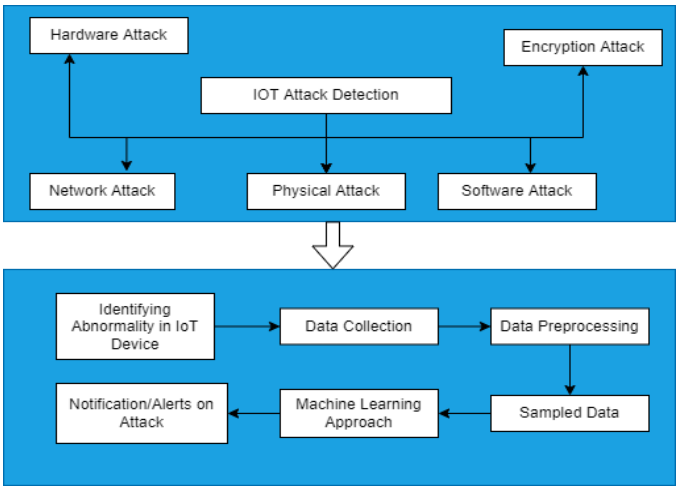

Figure 2. IoT Attack Detection Mechanism Approach Using ML Techniques

VI. CONCLUSION

IoT confidentiality is still of utmost significance and is crucial to the development of the IoT market. This changing dynamic of Iot presents a variety of challenges for conventional confidentiality approaches. Through analysing statistics and environmental data, such training methods can promote self-organizing operations and increase the quality system efficiency. Every technology becomes more complicated whenever its capabilities cannot be reused or applied for multiple situations. Moreover, basic activities in complicated processes need several phases. SVM, RF, LR, and decision tree

algorithms were successfully used in machine learning systems to determine and alert users of smart IoT devices to potential threats.

VII. REFERENCES

1. P. Illy, G. Kaddoum, K. Kaur and S. Garg, "ML-Based IDPS Enhancement with Complementary Features for Home IoT Networks," in IEEE Transactions on Network and Service Management, vol. 19, no. 2, pp. 772-783, June 2022, doi: 10.1109/TNSM.2022.3141942.
2. Inayat, Usman, et al. "Learning-Based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects." Electronics 11.9 (2022): 1502.
3. Mohamed, Yahia & Abdullahi, Mujaheed & Alhussian, Hitham & Alwadain, Ayed & Aziz, NorShakirah & Jadid Abdulkadir, Said. (2022). electronics Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics. 11. 1-27. 10.3390/electronics11020198.
4. Z. Trabelsi, "Investigating the Robustness of IoT Security Cameras against Cyber Attacks*," 2022 5th Conference on Cloud and Internet of Things (CIoT), 2022, pp. 17-23, doi: 10.1109/CIoT53061.2022.9766814.
5. Tarek Gaber, Amir El-Ghamry, Aboul Ella Hassanien, Injection attack detection using machine learning for smart IoT applications, Physical Communication, Volume 52,2022,101685, ISSN 1874-4907, https://doi.org/10.1016/j.phycom.2022.101685.
6. M. Anwer, S. M. Khan, M. U. Farooq, and Waseemullah, "Attack Detection in IoT using Machine Learning", Eng. Technol. Appl. Sci. Res., vol. 11, no. 3, pp. 7273–7278, Jun. 2021.
7. Vitorino, J., Andrade, R., Praça, I., Sousa, O., Maia, E. (2022). A Comparative Analysis of Machine Learning Techniques for IoT Intrusion Detection. In: Aïmeur, E., Laurent, M., Yaich, R., Dupont, B., Garcia-Alfaro, J. (eds) Foundations and Practice of Security. FPS 2021. Lecture Notes in Computer Science, vol 13291. Springer, Cham. https://doi.org/10.1007/978-3-031-08147-7_13
8. Hussain, Fatima & Hussain, Rasheed & Hassan, Syed & Hossain, Ekram. (2020). Machine Learning in IoT Security: Current Solutions and Future Challenges. IEEE Communications Surveys & Tutorials. PP. 10.1109/COMST.2020.2986444.
9. K. Lounis and M. Zulkernine, "Attacks and Defenses in Short-Range Wireless Technologies for IoT," in IEEE Access, vol. 8, pp. 88892-88932, 2020, doi: 10.1109/ACCESS.2020.2993553.
10. Jadel Alsamiri and Khalid Alsubhi, "Internet of Things Cyber Attacks Detection using Machine Learning" International Journal of Advanced Computer Science and Applications (IJACSA), 2019.https://dx.doi.org/10.14569/IJACSA.2019.0101280
11. Prasanna Srinivasan.V, Balasubadra.K, Saravanan.K, Arjun.V.S and Malarkodi.S, (2021), "Multi Label Deep Learning classification approach for False Data Injection Attacks in Smart Grid", KSII Transactions on Internet and Information Systems, Vol. 15, No. 6.
12. A. Roukounaki, S. Efremidis, J. Soldatos, J. Neises, T. Walloschke and N. Kefalakis, "Scalable and Configurable End-to-End Collection and Analysis of IoT Security Data: Towards End-to-End Security in IoT Systems," 2019 Global IoT Summit (GIoTS), 2019, pp. 1-6, doi: 10.1109/GIOTS.2019.8766407.
13. A. Djenna and D. Eddine Saïdouni, "Cyber Attacks Classification in IoT-Based-Healthcare Infrastructure," 2018 2nd Cyber Security in Networking Conference (CSNet), 2018, pp. 1-4, doi: 10.1109/CSNET.2018.8602974.
14. I. You, K. Yim, V. Sharma, G. Choudhary, I. -R. Chen and J. -H. Cho, "On IoT Misbehavior Detection in Cyber Physical Systems," 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), 2018, pp. 189-190, doi: 10.1109/PRDC.2018.00033.
15. Abomhara, Mohamed and Geir M. Køien. "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks." J. Cyber Security. Mobil. 4 (2015): 65-88.