An Examination of Security and Privacy Challenges in Internet of Things

Aditya Harbola, Shivani, Deepti Negi, Aditya Joshi

Abstract- The Internet of Things (IoT) has been growing to market from the past several years with great potential. Many several devices have been now available in the market based on IoT, which enables it to connect with your smart phones or with any other kind of smart resources, and then that device is ready to perform smart work via the Internet. With the help of IoT, we are now able to make our devices connect with the internet and then can be operated from anywhere from the geo location as well as it can store and retrieve a large amount of data for better communication between the end-user and the device. IoT also has a wide range of applications that are being used on many platforms. However, this great technology also has to face many problems and among all the problems the main issue arises with its security aspects. The major concern on using IoT security is the hacker wants to enter into the large network system using a particular device as all the devices are connected over the network. Not only this, many other security threats and malware are also a major concern in IoT. So taking these security aspects as a major concern this research paper reviews several security issues and challenges that occur in IoT. As there in every field when it comes to cyber security for any kind of data, we need to follow CIA Security Triangle i.e., Confidentiality, Integrity, and Availability of data. CIA security triangle is the most important concept in terms of security and also must be taken into consideration in the IoT domain. Therefore, considering all these facts and reviewing some of the latest documents as well as researches in the field of IoT, this paper has been based on all the facts related to IoT security issues and its desirable solution which is needed to be done and should follow the security triangle to an extent.

Keywords- Internet of Things, Security Threats, CIA Security Triangle, Solution

I. INTRODUCTION

Internet of Things firstly came in existence around 1999 by the vision of Kevin Ashton and if we see our future going to be in several years, is the future of the Internet of Things where we all are going to see Smart devices with built-in-sensor in every home to reduce human efforts. So if we talk about the Internet of Things, here "thing" is any device or object with built-in-sensor which can smartly perform many several tasks with the ability to collect data and also to transfer data such that it connects all the devices to internet and let them communicate with each other over the internet.

IoT is a giant network of connected devices where the huge amounts of data are being transferred which is based on a smooth message exchange mechanism between systems through different networks for end-to-end communication (Interoperable Communication Protocols) over its global network infrastructure. According to the European Research Cluster on the Internet of Things (IERC), IoT is defined as:" a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocol where physical and virtual things have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network" [13].

IoT has a wide range of application like commerce, smart healthcare, smart agriculture, utilities, energy, smart transportation, industrial control, buildings, etc and also many big vendors like Amazon (AWS IoT), Cisco (Jasper), IBM (Watson), Apple(HomeKit), Google (Brillo), Microsoft (Azure IoT), and Qualcomm (AllJoyn) have also rapidly growing in the IoT market from the few past years. Not only this IoT will also be going to be seen in the education field such that students can experience real-time learning via the Internet. IoT has a lot of benefits that attract a lot of people, some of them are Product Personalization, Faster time to market, responsive service support in decision making, the potential for efficiency, energy efficiency, and many more at present to be coming in future.

Every year we see a huge improvement in many technologies; like in Mobile Communication, Radio Frequency Identification (RFID) innovation, and Wireless Sensor Networks (WSNs) which makes IoT devices communicate at any time, place and form in a better way with better performance. With the increase in the use of IoT devices, several security issues has raised rapidly. As mentioned above, IoT devices and things are becoming the part of internet infrastructure therefore they should be highlighted and need to be addressed because everything which is connected to the Internet.

A study conducted by Hewlett Packard revealed that 70% of the most commonly used IoT devices contain serious vulnerabilities. IoT devices are vulnerable to security threats due to their design by lacking certain security features such as insecure communication medium, insufficient authentication, and authorization configurations [3]. Since the market of IoT is growing day by day from an individual to an organization, all are going to use it and then security concerns will be going to affect all among them.

Revised Manuscript Received on April 25, 2019.

Aditya Harbola, School of computing, Graphic Era Hill University Dehradun, Uttarakhand, India. E-mail: aharbola@gehu.ac.in

Shivani, School of computing, Graphic Era Hill University Dehradun, Uttarakhand, India. E-mail: shivanisemwal1816@gmail.com

Deepti Negi, School of computing, Graphic Era Hill University Dehradun, Uttarakhand, India. E-mail: dnegi@gehu.ac.in

Aditya Joshi, Department of CSE, Graphic Era University Dehradun, Uttarakhand, India. E-mail: adi.joshi@geuac.in

So to make its acceptance in the market among the people to use IoT based devices we have to enhance the security model for IoT by giving proper training to our designers and developers to manage all the security-related issues and which follows our CIA Security Triangle where our data should remain confidential, integrity should remain such that no outsider can manipulate it and our data should be available to us at any seconds and all this should be done in a proper environment such that only authorized person can look after their data and after all this security aspect keeping in mind, integrates them into IoT Products. This will build trust in users and also encourage them to use IoT products without any hesitation because of the security features which will give them their privacy and make them feel to be in a safe environment. Therefore, this paper has been created to enlighten some of the security issues associated with IoT and then some of the major steps to be taken in consideration for solving that particular problem in the very first phase of its, which in its design phase.

II. SECURITY AND PRIVACY ISSUES

IoT is a huge network where a large number of sensor-built-in devices are connected in a smart environment such that they can communicate through the Internet. From the past several years we have seen a huge growth in the domain of IoT and it is making its place in between the people with a good response until it comes to the matter of its security issues which has also raised the concern for its security among the developers. Using IoT in a smaller development scale work is not much vulnerable to security but using it in the development for a large scale it leaves behind a major concern for its security issues and thereafter may also lead in the fall down in the adaptation of IoT based products among the people. Since IoT has limited resources therefore it is not able to utilize complete security suites (used in typical networks). So this becomes a challenge whether to create a new unique security framework or to use the existing ones in IoT.

Everything we put in the world of the Internet needs to have some security algorithms to make it secure and safe from the outer world so we need to do in the field of IoT. In IoT, we work in a largely connected device area over the Internet which leads it to establish an insecure communication between the devices. Not only this, if we take a look at the security and privacy issues related to IoT we come with a long-handed list of problems.

2.1 Security and Privacy Issues

Since the list of security's problems are very long and creates its device limitation, but according to research some of them are:

a) Botnets- The term Botnet means the number of internet- connected devices such that they all are running on one or more bots. This is mainly used by hackers by performing DDoS attacks to steal data, send spam, allows the hacker to have access to the devices, and many more. From the past several years it has been come to notice that there is an increase of Botnet among the IoT based devices to steal user's data and use it illegally for their purpose without any user's knowledge. According to a site, Botnet controllers increased by 140% in 2017 [9].

b) Usage of More IoT Devices- It has been come to notice that from the past several years there is an increase in the usage number of IoT devices all around the world. A few years back the security professionals only have to focus on the protection of mobiles and computers from the malware but now it has become

c) a major problem for them to also protect the IoT devices as their usage has been increasing day by day in the market. According to a site, there have been 7 billion devices are being used all over the world and this number is going to make an increase of 20 billion by 2020 [5]. That means the more we use IoT devices the more it leads to security issues and will also going to create a challenge for the security professionals.

d) Lack In Encryption- In terms of security encryption is the most powerful weapon which works as the shield for data and makes it safe from the outer world such that it is not easy for anyone to manipulate with the data. Encryption is also the major problem that is mostly being faced by the IoT security challenge. IoT based devices lack in the Encryption Techniques which increase attacks done by the hackers and because of the poor security-based algorithms used in the IoT system it becomes easy for them to crack it and use data illegally.

e) Outdated Legacy Security- Due to IoT's interconnected legacy the system that means that it has been superseded but is difficult to replace because of its wide use and because of this it lacks security as compare to modern security standards.

f) Passwords- Many IoT devices come with their default password which is a weak default password; although we all know it is recommended to change your passwords firstly once you get the default password. So a weak password is easy to guess and crack by the hackers as well as leads to a brute force attack. According to a site, this issue becomes so prevalent that California banned default passwords in 2018 [6].

g) Threat Detection- In the Internet World we all are familiar with the term data breaching which simply means stealing of the data but our experts have numerous methods to detect all this data breaching by their many security protocols. Due to the increase in the number of IoT devices usage and the complexity present in every device, it makes it tough to indicate a normal threat and even makes it more challenging.

h) Small Scale Attacks- Mostly we all focus on the large scale attacks and performs all necessary precaution to prevent this kind of attack but the actual reality is that the small scale attacks are more serious especially in terms of IoT security and makes it more challenging to be handle.

Small scale attacks are difficult to detect and can make a huge damage without anybody's knowledge. Hackers can manipulate with data and even can use IoT devices as their tool to steal information and can control whole your IoT device as well.

i) Phishing Attacks- As we know Phishing is a cyber attack and mainly uses emails as a weapon to target and it is already a major security concern all over the IT field and this attack is now have been seeing in IoT devices as well. Here hacker sends a signal to the device that generates numerous complications. Phishing attacks are a common type of security attack but here in IoT devices it is new and it can be stopped just by giving training to the developers about the latest phishing threats.

j) Fail to Predict Threats- In every IT field, the security professional must be proactive and should be prepared for any kind of attack before they occur and start breaching our data. But some enterprises lack behind in the management system for security and do not take precautions like time to time activity monitoring which afterward leads in the huge data breaching.

k) Slow Updates- When we create software maintenance is the last phase of a software life cycle and it should be done from time to time. Frequent Updates make software fresh and bug-free and also ensures that our system is secure. But in the case of IoT devices, it lacks behind in the software updates, and enterprises also struggle to provide proper security updates to IoT devices.

l) Financial Breaches- Now a day's many agencies are using IoT devices for electronic payments and due to lack of security purposes, there are always some clouds of risk in between the payment such that hackers can steal money and information as well of a particular individual.According to a site, some organizations are integrating machine learning [7] or blockchain [8] to stop IoT related financial fraud or breach before it happens to an internet-connected device. But much other organization is still hasn't tried this idea.

m) User Privacy- In the IT field-based organizations the first most priority is always the protection of the data at anyhow whether it is internal user data or external user data. IoT based enterprises make IoT based devices and sell them to the market. Not only in the market, but these devices are also used by their employees. But due to lack in security aspect and high risk in data breaching, it not only leads to the external user to suffer from their private data breaching but as well as the company staff also have to suffer a lot and company itself have to compromise a big loss in data breaching and also have to face a big hit in the company's reputation. This is the most security challenge have to face by many enterprises . These are only some of the privacy and security issues that have been reported yet, with this increase in technology no one knows how many more issues have to come in the future. There are many more security concerns like DoS/DDoS Attacks, Man-in-the-middle attack, heterogeneous network issues, application risk of IPv6, WLAN Application conflicts that also hinders the deployment of IoT security, and many more.

2.2 Confidentiality, Cyber Security and Access

If we talk about the core technology that enables IoT networks includes RFID, NFC, WSN, low-energy Bluetooth, low-energy wireless, low-energy radio protocols, LTE-A, and WiFi-Direct. But these technologies only support specific security functionality and network functionality as compare to the standard uniform network of the common system.

Radio-Frequency Identification (RFID) and Near Field Communication (NFC) are used in IoT to provide simple, low energy, and adaptable options for identity and access token. This RFID Technology enables the IoT objects to work smartly by their smart chips such that the objects can sense information and also compute them and hence to communicate with other objects as well as human beings. And this all makes it possible by the RFID 2-way radio transmitter-receivers Technology to identify and track the tags associated with the objects. Whereas the NFC supports the communication between the objects in a small distance few in centimetres and consists of some communication protocol for electronic devices. But these both technologies are also prone to many cyberattacks as the RFID Technology

component is highly prone to DoS attacks, eavesdropping, skimming, relay, and side-channel attacks that create a matter of concern for security purposes. And the NFC Technology also has to face cyber attacks like phishing, user tracking, relay, and data forging attacks.

WSNs are used to gather information and also support the remote sensing application and this technology is most preferred in IoT devices because of its low cost in the market, they are efficient, consume low power, also preferred intelligent and have good processing capabilities. But this technology is also susceptible to many cyber attacks like wormhole, neighbor discovery, ICMP, ping flood, flood and syn flood attacks. The cybersecurity revolves around the CIA Triangle which is confidentiality, integrity, and availability. The term Confidentiality refers to ensure that the data should remain confidential or the data should be kept private such that it protects the data from unauthorized users and only the authorized person should have access to the data. On the other hand, the term integrity means that the data should be protected in such a manner that no unauthorized user can manipulate with the data and also provides the assurance of the completeness of data without any alteration. The term Availability refers that the data should be available all the time among its authorized users. It also ensures that the data should deliver in time and without any kind of interrupt access to the system.

So, by this concept, we can provide trustworthy confidence among the users but giving them proper means of security such as only verified user can have access to the data and information, there is no tampering of data in between the transmission and should be delivered to the receiver in its pure form as send by sender or author.

III. CHALLENGES

Evolving features and technology in the IoT has led it to specific privacy and security issues. Everything we are using in the IoT domain we are simply connecting it to the Internet. As we know there is a huge increase in the number of usage of IoT devices because of its effective communication between its objects, its automated things, save time and cost, and hence have many other benefits as well. But having all this cool stuff like smart homes, self-driven cars, and smart cities, etc., still, one thing which is making IoT devices to more challenging rather than to trust that is its IoT security issues.

As technology is growing day by day problems are also coming out with their new way, which is creating a more challenging problem among the developers and Security Professionals. As discussed in the security and privacy issues section, all these security problems are becoming challenges, and if we talk about them there a many in the queue.

Outdated hardware and software, use of weak and default credentials, malware and ransom ware, difficult to find if a device is affected or not, data protection and security challenges, the security of autonomous vehicles, and many more. Furthermore, identification concerning the risk associating with an identifier such as an address with the data is also the major concern that has seen as the challenge in security and privacy issues. Here the main challenge is with the identity of a particular context that violates an individual's privacy and it is all done by providing the identifying information to the entities. And the other one case of localizing and tracking is also becoming a challenge in which a person's cross space and time have been recorded, and this entire

thing makes itself possible by means such as Internet traffic and mobile GPS Location. This is not all done all yet, many more challenging problems like Profiling and Authentication where profiling methods used in e-commerce for internal targeting an individual based on customer interest and another one is Lifecycle Transitions and Inventory Attacks here user's private information is collected during IoT device's lifetime such that there is a violation in the sensitive data of the user.

This is not end here all, these all are the present time challenges that are being faced but in the future, we have to face many more if it is going to be so long. For future aspects we have to start working on this matter right now, otherwise, the burden will go on so long and can cause huge damage in the market of IoT such that people will not be going to buy all the IoT based devices in the fear of security issues among the people because security is the main concern in everybody's life, everyone loves to live in their privacy without any interruption in-between. Not only this, but the reputation of the organization will also have to pay a high cost for this issue.

Since some researchers and organization are giving their best to solve these problems and trying to make things get better and perfect, but there is still a lot to be done.

IV. SOLUTION TO PRIVACY AND SECURITY ISSUES

For the solution to this concern, it requires a proper management approach for successfully implementing the IoT devices. IoT device security also depends on various elements such as sensitive data information, mitigating costs of security vulnerabilities. One of the security solutions is proposed by the Dynamic Prime Number Based Security Verification (DPBSV) for the big data stream. It requires less processing time and also protects from the malicious attack on big data stream as it uses the concept sharing of a common key which is updated timely by giving a synchronized pair of prime numbers for real-time security verification on the big data stream [11]. Rather than this, Physical Unclonable Functions (PUFS) can also be used in IoT devices as it is low cost primitive, used for secure key generation, and helps in to authenticate the IoT objects, protects from cyber attacks like man-in-middle, protects from stealing of data and tempering of data. And PUF based protocol also leads to secure communication in IoT networks [12]. Updates and patches in the software is also a concern as already mentioned above, all the IoT based organization should give their updates time to time for this concern with new security features and with more enhancement than the previous version. These challenge can be addressed by giving proper training to our developer, designers and security professionals regarding security solutions and also to be prepared for any type of danger that will harm the system with all possibilities and after that integrating those solutions into the IoT devices or object, this will also motivate the users and encourage them to buy IoT based stuff will full confidence and trust.If we can't do things on a larger scale at least we can make a lightweight security solution for Security Issue to make our IoT devices secure and do not lack behind in its performance.

V. CONCLUSION

This study aims to provide a view on the Security and Privacy Issues and the challenges involved in the Internet of Things.

Many challenges are related to security issues in the IoT devices domain at present and can't be estimated for the future. For the safety of IoT devices and their related security issues, developer and security professionals have to take a prior action as soon as possible. Besides, this paper has covered some of the major security problems related to IoT based devices and some of its solutions such as Physical Unclonable Functions (PUFS) [12] and

the solution which is proposed by the Dynamic Prime Number Based Security Verification (DPBSV) for the big data stream [11]. These solutions will help in resolving some of the security problems like cyber attacks, data breaching, and many more as mentioned above and this problem has to be resolve as soon as possible because of the increasing number of users in IoT devices. Furthermore, Confidentiality of data, the integrity of data, and the availability of data that covers all the security-related issues should be considered and addressed at the very first design stage. In conclusion, there are still a lot of questions and problems that need to think and answer. IoT has a large field of area of it connected devices via the Internet; therefore it has a large field to do further more research.

VI. REFERENCES

1. J. P. Nzabahimana, "Analysis of security and privacy challenges in Internet of Things," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kiev, 2018, pp. 175-178. doi: 10.1109/DESSERT.2018.8409122
2. S. Koley and P. Ghosal, "Addressing Hardware Security Challenges in Internet of Things: Recent Trends and Possible Solutions," 2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), Beijing, 2015, pp. 517-520. doi: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP.2015.105
3. A. K. Singh, A. Tripathi, P. Choudhary and P. C. Vashist, "Research and Challenges of Security & Privacy in Internet of Things (IoT)," 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 2020, pp. 487-492.doi: 10.1109/ICCAKM46823.2020.9051526
4. A. F. Skarmeta, J. L. Hernández-Ramos and M. V. Moreno, "A decentralized approach for security and privacy challenges in the Internet of Things," 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, 2014, pp. 67-72. doi: 10.1109/WF-IoT.2014.6803122
5. Harbola J, Vaisla KS, Harbola A. An Examination of Network Intrusion Detection System Tools and Algorithms: A Review. International Journal of Computer Applications. 2014 Jan 1; 95(6).
6. S. Rachid, Y. Challal and B. Nadjia, "Internet of things context-aware privacy architecture," 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), Marrakech, 2015, pp. 1-2.
7. C. Li and B. Palanisamy, "Privacy in Internet of Things: From Principles to Technologies," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 488-505, Feb. 2019. doi: 10.1109/JIOT.2018.2864168
8. I. K. Poyner and R. S. Sherratt, "Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 2018, pp. 1-5.
9. A. Terkawi, N. Innab, S. al-Amri and A. Al-Amri, "Internet of Things (IoT) Increasing the Necessity to Adopt Specific Type of Access Control Technique," 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, 2018, pp. 1-5.
10. B. V. S. Krishna and T. Gnanasekaran, "A systematic study of security issues in Internet-of-Things (IoT)," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 107- 111.
11. N. Rastogi, S. K. Singh and P. K. Singh, "Privacy and Security issues in Big Data: Through Indian Prospective," 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, 2018, pp. 1- 11.
12. P. Ramanathan, "Tutorial T2D: Privacy Assurances in the Internet of Things (IoT) World," 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID), Pune, 2018, pp. xlii-xlii.
13. E. Shaikh, I. Mohiuddin and A. Manzoor, "Internet of Things (IoT): Security and Privacy Threats," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019, pp. 1-6.
14. S. Sezer, "T1C: IoT Security: - Threats, Security Challenges and IoT Security Research and Technology Trends," 2018 31st IEEE International System-on-Chip Conference (SOCC), Arlington, VA, 2018, pp. 1-2.
15. N. Fabiano, "The Internet of Things ecosystem: The blockchain and privacy issues. The challenge for a global privacy standard," 2017 International Conference on Internet of Things for the Global Community (IoTGC), Funchal, 2017, pp. 1-7. doi: 10.1109/IoTGC.2017.8008970
16. T. Choudhury, A. Gupta, S. Pradhan, P. Kumar and Y. S. Rathore, "Privacy and Security of Cloud-Based Internet of Things (IoT)," 2017 3rd International Conference on Computational Intelligence and Networks (CINE), Odisha, 2017, pp. 40-45.
17. S. Deshmukh and S. S. Sonavane, "Security protocols for Internet of Things: A survey," 2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2), Chennai, 2017, pp. 71-74.
18. S. Ray, S. Bhunia, Y. Jin and M. Tehranipoor, "Security validation in IoT space," 2016 IEEE 34th VLSI Test Symposium (VTS), Las Vegas, NV, 2016, pp. 1-1. doi: 10.1109/VTS.2016.7477288
19. K. K. Singh, P. Dimri and J. N. Singh, "Green data base management system for the intermediaries of Indian stock market," 2014 Conference on IT in Business, Industry and Government (CSIBIG), Indore, 2014, pp. 1-5, doi: 10.1109/CSIBIG.2014.7056996.
20. A. H. Imam and M. A. Azer, "Internet of Things security framework," 2017 13th International Computer Engineering Conference (ICENCO), Cairo, 2017, pp. 378-382. doi: 10.1109/ICENCO.2017.8289818
21. E. Anthi, L. Williams and P. Burnap, "Pulse: An adaptive intrusion detection for the Internet of Things," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 2018, pp. 1-4. doi: 10.1049/cp.2018.003
22. G. A. Fink, D. V. Zarzhitsky, T. E. Carroll and E. D. Farquhar, "Security and privacy grand challenges for the Internet of Things," 2015 International Conference on Collaboration Technologies and Systems (CTS), Atlanta, GA, 2015, pp. 27-34.
23. R. S. Apare and S. N. Gujar, "Research Issues in Privacy Preservation in IoT," 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, 2018, pp. 87-90. doi: 10.1109/GCWCN.2018.8668616
24. 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," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1606-1616, April 2019. doi: 10.1109/JIOT.2018.2847733
25. Aditya Harbola, Priti Dimri, Dipti Negi and Y.S. Chauhan, "Green Computing Research Challenges: A Review", IJARCSSE V3110-0408 1075- 1077, Oct 2013.
26. Z. Ren, X. Liu, R. Ye and T. Zhang, "Security and privacy on internet of things," 2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC), Macau, 2017, pp. 140-144. doi: 10.1109/ICEIEC.2017.8076530
27. N. Shahata, "The Challenges, the Threats and Policy Implications to a Compromised Privacy and Security," 2018 International Conference on Networking and Network Applications (NaNA), Xi'an, China, 2018, pp. 314-317. doi: 10.1109/NANA.2018.8648733
28. M. Frustaci, P. Pace, G. Aloi and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," in IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483-2495, Aug. 2018. doi: 10.1109/JIOT.2017.2767291
29. A. Harbola, J. Harbola and K. S. Vaisla, "Improved Intrusion Detection in DDoS Applying Feature Selection Using Rank & Score of Attributes in KDD-99 Data Set," 2014 International Conference on Computational Intelligence and Communication Networks, Bhopal, 2014, pp. 840-845, doi: 10.1109/CICN.2014.179.