e-ISSN 2320 –7876 www.ijfans.org
Vol.11, Iss.11, 2022
 **UGC CARE Listed (Group -I) Journal**

# A Review Paper on Challenges in IoT Security

DR. KULDEEP PANWAR1, MR. VINEET JOSHI2, DR. SHAMBHOO PRASAD3

1Associate Professor, Department of Mechanical Engineering, Shivalik College of Engineering, Dehradun
2Assistant Professor, College of Pharmacy, Shivalik, Dehradun
1Associate Professor Shivalik Institute of Professional Studies, Dehradun

Drkuldeep.panwar@sce.org.in

***ABSTRACT:****The Internet of Things allows wearable devices, home appliances, and software to share and send data via the Internet (IoT). Maintaining information security on shared data is a crucial issue that must not be ignored, given the huge amount of private information included within. We begin with a fundamental review of IoT information security in this essay, and then go on to the information security problems that IoT will encounter. A future in which physical things are seamlessly connected to the information network and may become active players in corporate operations. The key characteristics that distinguish IoT security problems from conventional security issues are the diverse and large-scale devices and networks. IoT security is made considerably more challenging by these two characteristics, heterogeneity and complexity. The current problems and research possibilities in IoT security were discussed in this article. Finally, we'll talk about study topics that may lead to future work on solutions to the Internet of Things' security issues.*

***KEYWORDS:****Authentication, Connect, Internet, IoT,Security.*

## 1. INTRODUCTION

When the phrase "Internet of Things" (IoT) was originally coined, one may wonder what exactly constitutes "Things." The Internet of Things has been the subject of several academic studies and attempts at definition up until recently. Haller proposed the following concept of the Internet of Things: "A world where physical products are seamlessly integrated into the information network and where physical objects may become active players in business operations." In order to expand the IoT notion, Sarma defines "Items" as physical things that represent identities with Internet connectivity.

For a long time, the cybersecurity of IoT devices has been a source of worry, with the unavoidable result of permitting both small- and large-scale assaults. The majority of these assaults are the result of minor security flaws, such as the preservation of usernames and passwords on a telnet server. The Dutch Transceiver Agency has sought assistance from our facility, Eurofins Cyber Security in the Netherlands, on how to enforce security standards on Iot nodes and their makers.Despite the fact that the IEEE IoT Initiative is working on a white paper for a formal definition of IoT, there are currently no standard definitions. We describe a "Thing" on the Internet of Things in this article as a physical or virtual item that connects to the Internet and may interact with humans or other things.

IoT security affects the procedures, tools, and precautions required to safeguard IoT networks and devices. It also includes the security of physical objects. It includes things like industrial machinery, intelligent energy grids, home automation systems, entertainment equipment, and more that often aren't built with network security in mind. Systems, networks, and data must be shielded against a variety of IoT security threats that aim to exploit four different kinds of vulnerabilities:

- Attacks on the data transmission between IoT servers and devices.
- Lifecycle attacks on IoT devices as they go from being used to being maintained.
- Software-related attacks on the device.
- Physical assaults that target the device's chip directly.

When using the security level that best suits their application demands, a strong IoT security portfolio enables developers to shield devices from all kinds of threats. While security services can defend against lifecycle assaults, cryptography technologies aid in the fight against communication threats. Software assaults may be thwarted by isolation measures, while physical attacks on the chip must be thwarted by tamper mitigation and side-channel attack mitigation methods.

The third phase of the Internet's growth is already becoming apparent: the Internet of Things. According to the data, the Internet wave of the 1990s linked 1 billion people worldwide, while the Internet wave of the 2000s connected an additional 2 billion users. The majority of Internet of Things (IoT) devices and applications were not designed to withstand security and privacy attacks, making them easy targets for hackers. This creates a number of security and privacy issues in IoT networks, including isolation, data stability, authentication, access restriction, and secrecy.

The Internet of Things (IoT) devices are always a target for hackers and invaders. According to one analysis, 70 percent of IoT devices are very simple to hack. Therefore, a strong defence system is critical to preventing hackers and attackers from accessing Internet-connected devices. Digital equipment can successfully communicate with one another using Internet Protocol (IP) addresses, and IoT smart home services are expanding daily. In a smart home setting, Internet connectivity is also present for smart home gadgets. The likelihood of malicious assaults grows along with the number of devices in the smart home ecosystem.

As we become more reliant on connection, it's critical to be vigilant. The following four items may help you safeguard your IoT network and keep yourself safe. Independently controlled smart home gadgets further reduce the likelihood of harmful assaults. Currently, it is possible to access the smart home appliances from anywhere at any time over the Internet. As a result, it makes these devices more vulnerable to malicious assaults. These days, smart gadgets are in most houses. They might be a smart speaker, camera, piece of medical gear, freezer, washing machine, etc.

With the help of the IoT, major industrial processes and applications may now be set up. For example, in an intelligent IoT transportation operation, a designated person can monitor a vehicle's current position and movement. As we become more reliant on connection, it's critical to be vigilant. The following four items may help you safeguard your IoT network and keep yourself safe. The designated individual may also forecast where traffic will be on the route in the future. The IoT was used in the previous stage to detect distinctive things. In more recent times, the academics have linked the word "IoT" to sensors, GPS techniques, mobile devices, and actuators.

The privacy of data and the security of information are crucial for the acceptance and use of emerging IoT technologies. The IoT enables several elements to be linked, monitored, and controlled, allowing for the automated collection of vital data and personal information. Comparing IoT environments to conventional networks, privacy protection is a more important

  

concern due to the high rate of IoT assaults. Every gadget provides a point of entryfor an assault. If, for example, a smart thermostat in your house is in risk, this may reveal information about all the gadgets connected to your network. IoT may be compared to a string: Its weakest link is just its weakest connection. As we become more reliant on connection, it's critical to be vigilant. The following four items may help you safeguard your IoT network and keep yourself safe.

As the Internet of Things grows, new security issues emerge and pre-existing security weaknesses worsen. The main factors are the objects' immense size and variability. The diversity of the "Things" and the "Things"' communication are further divided into two categories as part of the impact factors. Due to the fact that each category has its own unique set of security challenges, it is divided into two categories [2].

First, the "Things" have a security problem because of flaws in the software that make it possible for malware or backdoors to be installed. Such security challenges are more difficult than the ones we face right now because of the diversity and scale of the "Things" in the Internet of Things.

It is projected that the networking architecture for IoT would be varied in terms of the communication medium used by "things." Various communication mediums might run into different security problems. If these security concerns are neglected, the functionality of the "Things" will be compromised. The many data formats and communication protocols make content security more challenging. In this piece, we will briefly go through pertinent IoT research topics and the challenges that these fields of study confront.

*1.1 Difficulties in IoT Security:*

As previously stated, the heterogeneity and vast size of objects are the primary difficulties for IoT security. We'll go through these security concerns in more depth in this section.

*1.1.1 Object Recognition:*

The integrity of the data utilised in the name system must be maintained, which is the most challenging component of object identification. Despite providing name translation services to Internet users, the Domain Name System (DNS) is an insecure naming system. It is still vulnerable to several attacks, such as man-in-the-middle attacks and DNS cache poisoning.

The name architecture to addressing architecture resolution mapping is directly compromised by the poisoning attack, which injects false DNS records into the victims' cache. As a consequence, without record integrity protection, the whole naming architecture is exposed. The Domain Name Service Security Extension is used to implement DNS security extensions. A Resource Record (RRintegrity )'s and validity may be ensured using DNSSEC, and the distribution of cryptographic public keys is also permitted [3].

Although DNSSEC seems to be a solution for name services, effectively deploying DNSSEC in IoT remains a challenge. DNSSEC has a significant computational and communication cost, thus it may not be appropriate for IoT devices. It is desirable to have a new naming service.

*1.1.2 Authentication and Authorization:*

Despite the advantages of public-key cryptosystems for building authentication and authorization systems, the absence of a worldwide root certificate authority (global root CA) prevents many theoretically viable methods from being implemented. Designing an authentication solution for IoT becomes very difficult without a global root CA. Furthermore, issuing a certificate to an item in the IoT may be impossible due to the large number of objects. As a result, for IoT, the concepts of delegated authentication and delegated authorization must be considered[4].

*1.1.3 Confidentiality*

In the part before, we spoke about how important it is to ensure privacy in the IoT. We'll discuss the challenges of implementing the Internet of Things in terms of privacy protection in this section. Data collection policy and data anonymization are two categories into which the problems may be divided. The kind of data that may be gathered and the level of access control that a "Thing" has to that data are both governed by data collection policies. The data collecting policy places restrictions on the kind and volume of information that may be obtained during the data collection phase. The restricted collection and preservation of private information may safeguard privacy. The second challenge is data anonymization. Data relation concealing and cryptographic protection are both preferred to provide data anonymity. The diversity of the "Things" allows for the application of various encryption techniques. For example, systems with low resources are better suitable for lightweight cryptographic techniques [5].

The second category, data relation hiding, looks at the erasure of direct connections between data and its owner. This may also be accomplished by using data encryption, which makes jumbled data resistant to data analysis. However, with the Internet of Things, information must be exchanged across "Things," thus processing on encrypted data is another difficulty for data anonymization. Some homomorphism encryption research efforts may be useful in dealing with the issue.

*1.1.4 Safety Protocols and Lightweight Cryptosystems:*

Compared to symmetric-key cryptosystems, public key cryptosystems provide additional security features but at a larger computational cost. Nevertheless, public key cryptosystems are often favoured when data integrity and authenticity are essential. Therefore, lowering computing costs for complex security protocols and public-key cryptosystems is still a major problem for IoT security [6].

*1.1.5 Analysis of Software Vulnerabilities and Backdoors:*

Dynamic analysis is a useful tool for identifying weaknesses in a product before it is made public. Due to resource constraints, dynamic analysis may not be effectively implemented in an IoT device. Emulation, which may mimic the behaviour of devices in a server with more computing power, is necessary to enable dynamic analysis. On the other hand, there is a key issue that has to be solved about the semantic gap between the real device and the simulated system.A mismatch between the device and the simulated system is difficult to avoid. Additionally, a device's many parts, such as the GPS and gyroscope, make it much more difficult to close the semantic gap.

Taint analysis and symbolic execution, for example, are extremely reliant on the underlying system. With such a wide range of settings, an analysis system must be adaptable enough to accommodate various systems.

To decouple system dependencies, a proper interface and intermediary layer must be established. As a result, extensibility may be accomplished, allowing for the adoption of a range of systems.

The aforementioned dynamic analysis method is also a potential option for removing backdoors. It is not, however, simply a technological problem. Management and policy have a significant influence as well. To avoid the use of backdoors, multi-level inspection to minimize software vulnerabilities, reverse engineering to identify backdoors, and software audits are all helpful.

*1.1.6 Malware in the Internet of Things:*

IoT-targeted malware poses a serious threat because of the constrained resources of IoT devices. Furthermore, it may be impossible to use conventional security measures to prevent malware when switching directly from regular x86 architectural platforms to the IoT platform.

For example, antivirus software is regarded as one of the best security solutions for real-time malware detection. IoT devices' computing power, however, is much less than that of an x86-architectured PC. The real-time scanning feature of antivirus software may cost IoT devices a lot of money. Malware authors will separate their programme into a downloader and a major body if they are worried about the IoT's processing capabilities. The downloader is a pioneer in IoT device infection, and because of its short programme body, it is challenging to extract its distinctive, destructive signature [7]–[9].

Other problems, such as the divergence of hardware designs across different devices, exist in addition to the example given above. Current methods may be ad-hoc and even inapplicable without a general abstraction of IoT malware.

*1.1.7 Android Security Concerns:*

Android security issues will be brought into the Internet of Things (IoT) when heterogeneous devices connect to the Android system, forming a personal area network (PAN). The main concern is the disclosure of private data. The current permission protection only permits coarse-grain management, i.e., a binary choice, to restrict the categories of connected devices and turn off runtime control. In complicated settings and application conditions, more possible granted permissions should be taken into account. Inadvertently released in Android 4.3, Google's runtime permission management, AppOps, was swiftly removed in Android 4.4. Dynamic management is a possibility, as shown by AppOps. On the other side, Android malware poses a serious problem when IoT and Android are combined. Android is an open-source operating system, in contrast to iOS. It is thus straightforward to identify the system's shortcomings. The IoT network gets exposed when front-end devices contract malware. The computer power and data on these pervasive devices are accessible for interested attackers to use. The cost of a breach rises despite Google's release of the Bouncer for app screening, and the attack will be made worse when IoT is involved [10].

It is desirable to do a more in-depth examination of applications, such as integrating static and symbolic. Users, on the other hand, may disregard an organization's policy. Even while IoT will make things easier for the military and businesses, caution should be used. Insider threats are usually the most difficult to deal with. This problem has received little attention so far, although some research has attempted to address policy enforcement. When the Internet of Things (IoT) enters the picture, a robust auditing system is required. Developers may use audit logs to improve Android's access control system. It's a more passive method that doesn't annoy

consumers. Developers and manufacturers can enable IoT technologies and enhance our lives quickly by using Android and its expertise.

## 2. DISCUSSION

Many people weren't sure what "Things" really meant when the term "IoT" was first created. Many scholars and organisations made an effort to define the Internet of Things up until recently. Haller proposed the IoT definition as "a future where physical objects are smoothly integrated into the information network, and where physical things may become active participants in business activities." The reach of the Internet of Things notion is expanded by Sarma's definition of "things" as "physical devices that represent identities with Internet connection," and the attack will be made worse if IoT is engaged. New security problems emerge as the Internet of Things expands, while existing security vulnerabilities become more severe. The items' heterogeneity and massive size are the primary causes. "Things' diversity" and "Things' communication" are the two subgroups of effect components. It is split into two groups since each has its own set of security issues.

## 3. CONCLUSION

The author has come to a conclusion about the challenges of IoT. IoT security is an applied research dedicated to securing internet of things linked devices and networks (IoT). IoT entails connecting a system of interconnected microprocessors, physical devices machinery, items, animals, and/or people to the internet. Each "thing" is equipped with a unique identifier and the ability to transmit data instantly throughout the network. Allowing devices to connect to the network exposes them to a number of serious threats if they are not properly protected. The primary characteristics that set IoT security challenges apart from conventional ones are the numerous and expansive gadgets and networks. A number of high-profile incidents where a basic IoT device was exploited to get into and attack a large network have emphasised the need for IoT. The security of connections with IoT devices linked to them must be ensured. IoT security includes a broad variety of strategies, guidelines, techniques, and initiatives targeted at reducing the rising IoT threats facing modern enterprises. The military and corporations will find IoT to be helpful, but care should be used. The dangers from inside are often the most difficult to handle. IoT security is much more challenging as a result of these two characteristics, heterogeneity and complexity. The current issues and areas for future study in IoT security were discussed in this article. Additionally, potential remedies and new research areas are presented.

**REFERENCES**

[1] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, “IoT security: Ongoing challenges and research opportunities,” *Proc. - IEEE 7th Int. Conf. Serv. Comput. Appl. SOCA 2014*, pp. 230–234, 2014, doi: 10.1109/SOCA.2014.58.

[2] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, “IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?,” *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 41–49, 2018, doi: 10.1109/MSP.2018.2825478.

[3] Q. Gou, L. Yan, Y. Liu, and Y. Li, “Construction and strategies in IoT security system,” *Proc. - 2013 IEEE Int. Conf. Green Comput. Commun. IEEE Internet Things IEEE Cyber, Phys. Soc. Comput. GreenCom-iThings-CPSCom 2013*, pp. 1129–1132, 2013, doi: 10.1109/GreenCom-iThings-CPSCom.2013.195.

[4] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah, “A systemic approach for IoT security,” *Proc. - IEEE Int. Conf. Distrib. Comput. Sens. Syst. DCoSS 2013*, pp. 351–355, 2013, doi: 10.1109/DCOSS.2013.78.

[5] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, 2018, doi: 10.1016/j.future.2017.11.022.

[6] R. S. Sinha, Y. Wei, and S. H. Hwang, "A survey on LPWA technology: LoRa and NB-IoT," *ICT Express*. 2017, doi: 10.1016/j.icte.2017.03.004.

[7] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," *IEEE Internet Things J.*, 2018, doi: 10.1109/JIOT.2018.2812239.

[8] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and iot integration: A systematic survey," *Sensors (Switzerland)*. 2018, doi: 10.3390/s18082575.

[9] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "IoT Middleware: A Survey on Issues and Enabling Technologies," *IEEE Internet Things J.*, 2017, doi: 10.1109/JIOT.2016.2615180.

[10] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, 2018, doi: 10.1016/j.jisa.2017.11.002.

[11] Panwar, K, Murthy, D, S, "*Analysis of thermal characteristics of the ball packed thermal regenerator", Procedia Engineering*, 127, 1118-1125.

[12] Panwar, K, Murthy, D, S, "Design and evaluation of pebble bed regenerator with small particles" Materials Today, Proceeding, 3(10), 3784-3791.

[13] Bisht, N, Gope, P, C, Panwar, K, " *Influence of crack offset distance on the interaction of multiple cracks on the same side in a rectangular plate", Frattura ed IntegritàStrutturale*" 9 (32), 1-12.

[14]Panwar, K, Kesarwani, A, "Unsteady CFD Analysis of Regenerator", International Journal of Scientific & Engineering Research, 7(12), 277-280.

[15]Singh, I., Bajpai, P. K., & Panwar, K. "*Advances in Materials Engineering and Manufacturing Processes*