WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Internet of Things: Security and Privacy Challenges

Dr. S. Manju[1], Abinaya V[2], Amudha Valli S[3]

[1]Associate Professor, Department of Computer Applications, PSG College of Arts & Science, Coimbatore.
[2,3] Student, I MCA, Department of Computer Applications, PSG College of Arts & Science, Coimbatore.

ABSTRACT:

IoT promises a great future where communication is machine-to-machine. It is a global network of physical and connected to the internet. Each one has a unique ID for identification. IoT made collaboration with anything at any time and any place. It has made advances in Information and Communication Technology (ICT). The security of IoT is the foremost priority. The primary purpose of IoT security is to protect data and ensure the security of IoT users and data. In this paper, the IoT system's security challenges and their solutions are discussed.

Keywords: IoT, Layers, Security, Challenges, Privacy, Authentication

1.Introduction:

The Internet of Things (IoT) has emerged as a revolutionary paradigm, connecting billions of devices to the Internet and enabling new applications and services across various domains. IoT provides objects with a unique identity accessible from the network [2]. It provides a sensor

network with the communication system, stores and manages the information, provides access, and handles privacy protection and data security problems [3].

In IoT every object whether virtual or physical is communicable, addressable and accessible through the Internet [4]. The great thing about IoT is that all the information based on real-time data. The IoT allows various sensors and objects to interact directly with each other without the need for human intervention [5]. There are four layers in IoT. They are

Perception layer:

The perception layer gathers useful information about the objects from the sensor devices linked with them and converts the information into digital signals which are then passed onto the network layer [1]. This layer is classified into two sections namely, the perception node and the perception network that interconnect the network layer [5].

Network layer:

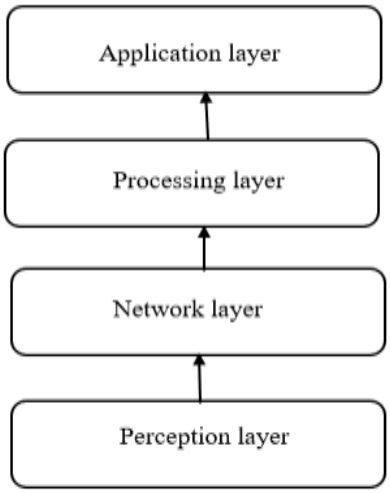
The network layer is used to receive useful information in the form of digital signals from the perception Layer and transmit it to the processing systems in the Middleware Layer [1]. It is also known as the transport layer [4].

Processing layer:

The processing layer works to combine the network layer and the application layer [3]. In the Processing layer, all the data transmitted from the transport layer is further stored, processed, and analysed [4].

Application layer:

The application layer provides services as per user demand [3]. Application Layer's tasks are very much dependent on the data from the processed layer. The goal of the application layer is to create distinct IoT applications [4].



IoT layers

2.Literature review:

"A Review on Internet of Things" by M.U. Farooq, Anjum Khairi (2015). In this paper, overview of the Internet of Things scenario, six-layered design and highlights of the major issues that are associated with it. It also discussed about technologies that helps in development of IoT and some application of IoT like smart home, smart environment, smart traffic system [1]. "A Review of Security Concerns in Internet of Things" by Engin Leloglu (2017). This paper extensively reviewed the security concepts of IoT, challenges of security measures. The paper concluded by presenting recent solutions for these threats and introducing research directions, such as cryptographic mechanisms and firewalls, to address security concerns [2]. This paper [3] discussed about four layered architectures of IoT and their security. This discussed various security aspects like cryptography, communication security, sensor data and their countermeasures on each layer. This paper [4] discussed about major security issue like identification, authentication, data management and heterogeneity and also provide solution to this security issues. "Internet of Things security: A survey" by Fadele Ayotunde Alaba, Mazliza Othman (2017). This paper discussed about security scenario and provides analysis of the possible attacks [5]. Security is defined as a process to protect a resource against physical damage, unauthorized access, theft. IoT enables the improvement in various application like smart cities, smart homes, healthcare etc. This paper [6] discussed about security challenges and future research area in IoT. "Introduction to IoT" by Pradyumna Gokhale, Omkar Bhat, Sagar Bhat (2018). This paper discussed about the basic concepts of IoT and architecture of IoT [7]. The heterogeneity and complexity make IoT security more difficult. This paper [8] discussed about research opportunities in IoT and ongoing challenges in IoT. "The current research of IoT security" by Jian Zhang, Huaijian Chen, Liangyi Gong (2019). This paper discussed the security threats of IoT in three aspects and explains about some IoT security model [9]. This paper [10] discussed IoT layered models and some solution to IoT problems.

3.Discussion about challenges:

The discussion on IoT security challenges is crucial due to the increasing integration of IoT devices in various aspects of daily life. Some key challenges include:

Threads	**Description**
Identification	The identification is one of the most crucial challenges in IoT security services. It is required to know whether it is an original or malicious node.
Authentication	Authentication is verifying the identity of a user to grant access to a device, network, or system. Insufficient authentication results in the exploitation of sensitive data stored in these devices and confidential organizational information being at risk due to data breaches.
Encryption	Encryption is a security measure that transforms data into an unreadable format when transmitted between IoT devices and networks. The exposure of sensitive data, unauthorized access to sensitive data, and manipulation of the transmitted data are encryption problems.

Heterogeneity	The biggest security and privacy issue so far is the issue of device heterogeneity. Each device communicates and works differently as compared to another device. Device heterogeneity can affect many other aspects of difficulty in integration, privacy, identification, etc.
Software Vulnerabilities	Software is associated with more advanced applications and programs that run on it. Software vulnerabilities include unauthorized access by hackers to IoT devices, intrusion into other devices connected to the same network, and data breaches.
Privacy	IoT devices can collect, store, and use your data for convenience. It becomes scary when IoT devices use your information without your awareness or consent. IoT security challenges include privacy concerns arise as data is shared with third parties, eroding users' trust in the device.
Physical security risk	IoT devices are tangible, which makes them vulnerable to physical threats. Insecure physical installations and limited monitoring can compromise your IoT devices. Some risks are theft or loss of IoT devices and unauthorized access.
Limited resources	The rapid growth and complexity make it difficult for organizations or individuals to allocate resources for security measures.

Suggestions:

Authentication: For the authentication problem, the suggestion is to use a strong password, two-factor authentication, and biometric authentication.

Encryption: For encryption problems, the suggestion is to use the best encryption algorithms like AES, End-to-end encryption (E2EE), and secure encryption protocols like SSH and TLS.

Heterogeneity: To eliminate the problem of heterogeneity, the IDRA architecture**,** which is specially designed for all devices**,** must be used**.** IDRA can connect objects directly without a gateway.

Software vulnerabilities: For the software vulnerabilities problem, the suggestion is to use secure coding practices and regularly update software.

Privacy: For the privacy issues, the suggestion is to use privacy-enhanced technology, strong data security, and transparent privacy policies.

Physical security risk: To overcome this, we suggested keeping tracking on devices and secure installation.

Limited resources: To overcome this, we suggested keeping tracking on devices and secure installation.

4. Conclusion:

Securing Internet of Things (IoT) devices is paramount to ensure the privacy, integrity, and availability of personal and critical data. They have made contributions to making technology adapted to our daily lives. It also faces many challenges, including security and privacy threats. In this paper, we discussed four-layer architecture (perception layer, network layer, application layer, and processing layer) and various attacks on them. Finally, we discussed the security challenges like authentication, heterogeneity, software vulnerabilities, encryption, privacy, and physical security risks and stated some suggestions for those problems.

5.REFERENCES:

[1] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi, Talha Kamal, “A Review on Internet of Things (IoT)”.

[2] Engin Leloglu, “A Review of Security Concerns in Internet of Things”.

[3] Mian Muhammad Ahemd, Munam Ali Shah, Abdul Wahid," IoT Security: A Layered Approach for Attacks & Defenses”.

[4] Aqeel-ur-Rehman, Sadiq Ur Rehman, Iqbal Uddin Khan, Muzaffar Moiz, Sarmad Hasan, “Security and Privacy Issues in IoT”.

[5] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, Faiz Alotaibi, “Internet of Things security: A survey”.

[6] Anca D. Jurcut , Pasika Ranaweera, and Lina Xu, “Introduction to IoT Security”.

[7] Pradyumna Gokhale, Omkar Bhat, Sagar Bhat, “Introduction to IoT”.

[8] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shiuhpyng Shieh, “IoT Security: Ongoing Challenges and Research Opportunities”.

[9] Jian Zhang, Huaijian Chen, Liangyi Gong, Jing Cao, Zhaojun Gu, “The current research of IoT security”.

[10] Lo’ai Tawalbeh, Fadi Muheidat , Mais Tawalbeh and Muhannad Quwaider ,"IoT Privacy and Security: Challenges and Solutions".