IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 7, Issue 2, February 2020

A Study on Internet of Things: Security Issues and Solution Approaches

Roshansanju.R[1], Varshini.A[2], Janaranjani.C[3]

Students, Dept of Computer Technology, Sri Krishna Adhithya College of Arts and Science,

Coimbatore-042, Tamilnadu, India[1,2,3]

Abstract: From the isolated systems the world faces a dramatic rapid shift on Internet-based executable 'things' are capable of communicating with each other and creating data that can be analyzed to get valuable information. This highly integrated global network structure of IoT is the life of the well-known people, improving business efficiency, improving government efficiency and the list continues. Wireless communication networks are highly vulnerable to security threats. However, this new reality (IoT) is based on the Internet, has a new kind of challenge from security and privacy perspectives. The earlier techniques are not directly applicable to the concept of IoT. Mainly security affects the major features of IoT. It is better to understand the real reasons for the new threats in the IoT projects.

Keywords: Internet of Things (IoT), Wireless Technologies, Micro-Electronic Systems (MEMS) and Digital Electronics, Distributed Denial of Service (DDoS)

I. INTRODUCTION

IoT helps to send and receive data by connecting to the computing devices embedded in daily materials on the Internet. This concept has been extended due to new IoT network applications such as e- healthcare, agriculture and transportation applications over the last decade [1]. IoT's main targets of smart environment and self-independent independent devices such as smart home, smart living, smart health, smart objects, smart cities. The development of the wireless technologies, the development of Micro-Electronic Systems (MEMS) and digital electronics, the IoT's evolution has its origin. In the era of the IoT relationship between humans and machines is still tender and begins to handle human services and people are trying to trust the machine [3].

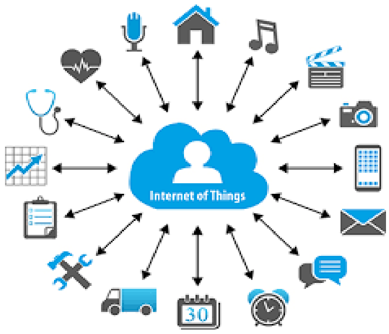

Figure: 1 Overview of IoT

The number of devices connected to the world has increased to 75.44 in 2017 at 20.35 billion in 2025[2].
Along with the growth of integrated application with internet cyber attacks will also be increased. IoT devices are widely used in industrial, military and other key areas, hackers can easily break public and national security systems [4]. Unfortunately, most of these devices and applications are not designed to handle security and privacy attacks, which increases security and privacy issues in IoT networks such as Confidence Detective, Authentication, Data Integrity, Access Control, Secret, etc. IoT Monitoring represents the dark world of privacy and security violations, and consumer locking. Surveillance concerns arising from internet-connected vehicles, voice-aware features on "smart" televisions, and backward privacy fears from the misuse of IoT data have attracted public attention [5].

II. SECURITY THREATS

Smart House services may be subject to cyber attack because the service provider does not consider safety parameters in the initial stages. The security threats in a smart home are eavesdropping, Distributed Denial of Service (DDoS) attacks and leakage of information, etc. Smart home networks are threatened with unauthorized access.

DOI 10.17148/IARJSET.2020.7203

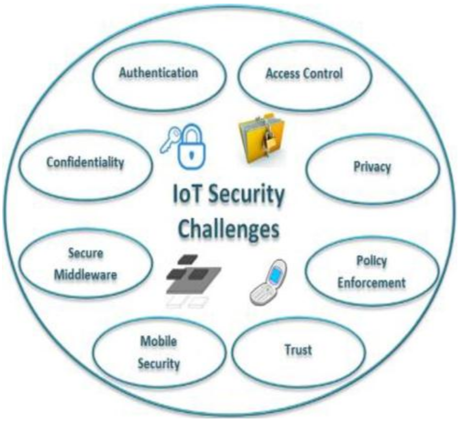

Figure2: Security challenges on IoT

1) Trespass: Smart door lock is activated by malicious codes or if it is accessed by an unauthorized party, the attacker cannot cross the smart home by hitting the door. The result of this effect can be in the form of loss of life or property. Authentication mechanism & access control should be applied to the system at this situation it is difficult to break the security system [7]

2) Monitoring and personal information leakage: Security is one of the main objectives of Smart Home. Therefore, there are many sensors such as elastic surveillance, child monitoring and house breaking. If these sensors are hacked by intruder he can track the house and access the personal information. To avoid this attack, data encryption will be used between the gateway and sensors or user authentication for the discovery of unrecognized parties [7].

3) Denial of Services: Attackers can send the entire message for smart devices such as Clear To Send (CTS) / Request To Send (RTS) to a smart home network. Malicious code targets the device to perform Denial of Service attack which is connected with smart home system. To avoid these kinds of attacks, authentication mechanism will restrict the unauthorized accessibility [5].

4) Falsification: When smart home devices have a connection to the application server, the attack packets can be collected by changing the routing table through the gateway. Although the SSL (Secure Sockets Layer) technique is used, the attacker can pass a forged certificate [4]. In this way, attack data can be misunderstood or leaks to the confidential data. To protect the smart home network from this attack, the SSL technique should be used with proper authentication. This is important to prevent unauthorized devices accessing smart home network.

III. SECURITY CHALLENGES IN IoT

Safety concern is IoT's biggest challenge in the wireless technology. The application data from the industry or from the individual should be preserved. It should also be a secret against stealing and fraud. For example, IoT apps can store results in a healthcare for patients or shopping details for consumer [1].

1. Data Privacy: Data privacy covers secret data transmissions, which do not reveal the unwanted attributes, e.g. a person's identity. This requirement is considered a great challenge when each device that meets personal needs is collected, such as the highest level of data such as the personal identifiable information enough to identify a person [6].

2. Data protection: Data protection is a big challenge. When sending the file, it is important to hide Surveillance devices on the Internet. Network security requirements are divided into confidentiality, authenticity, integrity, and availability. Factors like heterogeneity and constrained resources must be considered while applying these to IoT architectures. Interconnecting the devices require to have better confidentiality so technologies such as IPSec and Transport Layer Security (TLS) are employed to meet this requirement [3].

3. Lack of common standards: Since there are many standards for devices and IOT manufacturing plants. Therefore, it is a big challenge for the difference between the allowed and unwanted devices attached to the Internet. Proper protocol has to apply to the system for securing data transferred from one end to other end [1].

4. Technical concerns: Due to increased use of IoT devices, even the traffic produced by these devices will increase. So you have to increase the network efficiency, and also make all integrated devices more effective usage. So, it's a challenge to store large amounts data for analysis and final storage [7].

DOI 10.17148/IARJSET.2020.7203

Security attacks and computer vulnerabilities:

There is a loT of work in the IoT security scenario now. The related task can be split into computer security, application security, and network security.

a) System Security: System security mainly focuses on overall IoT system to identify different security challenges, to design different security frameworks and to provide proper security guidelines in order to maintain the security of a network.
b) Application security: Application Security works for IoT application to handle security issues according to scenario requirements.
c) Network security: Network security deals with securing the IoT communication network for communication of different IoT devices.

IV. APPROACHES AND SOLUTIONS

Different approaches are being employed for secure End-to-End communication in WSNs and IOT they can be classified into major research directions as follows

- Centralized Approaches
- Protocol-based Extensions and Optimizations
- Alternative Delegation Architectures
- Solutions that Require Special Purpose Hardware Modules

a) Centralized Approaches: The centralized security solution approaches is considered to be appropriate for sensor networks that control resources, but the general problem is the measurement of key management. The terminal must be built in advance with the shared keys of all elements before the terminal [5].

Some of the common centralized based approaches are SPINS that is a centralized architecture for securing unicast and multicast communication in constrained networks, composed of two security protocols SNEP and µTESLA and the Polynomial-based scheme has key agreement between distributed network.

b) Protocol-based Extensions and Optimizations: Approaches such as compression aimed at improving the protocol by breaking security attributes. There are many compression programs such as IPv6 header, extension captions and standard UDP (User Datagram Protocol). These approaches include some compact DTLs handshake (short handshake allows resume session to review state information from the previous session). TLS session No need to restart the server without a server-side state again, the server encrypted status is off-screen for the client and the handwriting handset, the TLS cache information extension is certified chains from this big signature.TLS Cached Information extension allows for omitting cached information, such as these large certificate chains from the handshake. Compression of header information is an approach to reduce the transmission overhead of packets in constrained environments, it defines already header compression mechanism for IP packets.

c) Delegation-based Architectures: In this Representative-based structures Public-key activities engaged in session companies, representing computationally active tasks such as more powerful devices Some important approaches are Server-based Certificate Validation Protocol (SCVP), Certificate valid for a trusted server provides a customer with a complex task of managing validation or certification path. The SCVP server must be trusted. It delegates the public-key-based operations to a more powerful device, such as the Gateway (GW). They describe the procedure for IKE session establishment, where the GW intercepts session establishment and pretends to be the end-point. After calculation of the session key, this key is handed over the constrained device and both peers can directly protect their communication with the session key. But in the vision of IoT, not always a trusted GW is present e.g. in the home automation scenario, constrained devices of different manufacturers might be present in the constrained network [4].

d) Hardware-based Approaches: Security solutions are a class of additional hardware security modules, such as TPMs. Trusted Platform module (TPM) is a tampered proof hardware that supports cryptographic predictions especially for public-key-based cryptographic primitives. TPMs can have keys in the protected memory area, such as RSA individual keys In addition; the TPM's cryptographic acceleration is capable of calculating encryption computations with higher performance. In contrast, ECC provides the same level of security with considerably smaller key sizes [3]. Therefore, ECC is preferred and recommend for constrained environments.

DOI 10.17148/IARJSET.2020.7203

V. CONCLUSION

This paper aims to provides the reader a basic overview about Internet of Things, the major security and privacy challenges because of its exponential growth and what kind of security primitives and solution approaches are being taken to make communication secure and to protect the user's data. Conventional security primitives cannot be applied due to the heterogeneous nature of sensors, low resources and the system architecture in IoT applications. To prevent unauthorized use of user's data, protect their privacy and to mitigate security and privacy threats, strong network security infrastructures are required. Any unauthorized use of data may restrict users to utilize IoT based applications. This review paper provides the security solution approaches been proposed recently identifying both the challenges related to security and privacy and the attack techniques used to compromise/fail the sensor nodes in Internet of Things as well. Current approaches are focused on pre-deployed, pre-shared keys on both ends whereas certificate-based authentication is generally considered infeasible for constrained resource sensors [2].

REFERENCES

[1]. J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," International Journal of Computer Applications, vol. 90, no. 11, 2014.

[2]. M. Abomhara and G. M. Køien, "Security and privacy in the internet of things: Current status and open issues," in Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE, 2014, pp. 1–8.

[3]. S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of iot: Applications, challenges, and opportunities with china perspective," IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359, 2014.

[4]. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct 2010.

[5]. M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015, pp. 21–28.

[6]. L.Da Xu, W.He, & S.Li, "Internet of things in industries: A survey," IEEE Transactions on industrial informatics, vol.10, no.4, pp.2233– 2243, 2014.

DOI 10.17148/IARJSET.2020.7203