International Journal of Engineering and Management Research e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-1 (February 2020)
www.ijemr.net https://doi.org/10.31033/ijemr.10.1.5

Security and Privacy Issues in IoT Environment

Navod Neranjan Thilakarathne
Lecturer, Department of ICT, Faculty of Technology, University Of Colombo, SRILANKA

Corresponding Author: navod.neranjan@ict.cmb.ac.lk

ABSTRACT

Internet of Things (IoT) is becoming an emerging trend superseding other technologies and researchers considered it as the future of internet. As now the connectivity to the World Wide Web is becoming highly available cost is drastically decreasing so everyone can afford the technology. As Internet of Things provides a great opportunity to develop an important industrial systems and applications with the help of various kind of sensors that can sense out the environment using number of devices that is connected to the internet, usage of IoT is drastically increasing and becoming a common thing. With this sky-rocketed usage and the demand, Communication and storing of the information faces serious security issues as the security of IoT devices become just an afterthought when manufacturing most of the devices. This study tries to summarize this IoT security issues in terms of primary information security concepts confidentiality, integrity and availability with regards to its architecture.

Keywords-- Internet of Things, IoT, Security, Privacy, IoT Security, IoT Environment

I. INTRODUCION

Internet, basically started as small interconnected network of less number of computers and now it is become a large network which contains billions of interconnected computers that shares and stores information. The term IoT stands for Internet of Things and we can describe an IoT system as one that comprise of interconnected smart devices that embedded with electronics ,software ,sensors and actuators and network connectivity which enable these objects to collect and exchange data.**[1]**

Following are the basic components of typical IoT environment. **[1]**

Sensors: Those are electrical components that are able to detect events or changes in the environment, such as temperature, humidity.

Actuators: Any component of a machine responsible for moving or controlling a mechanism or system.

Software: This can be described as compiled computer instructions that control the sensors and actuators, thus determining the final goals or outcomes of the system. Some software could reside on the sensor or actuator devices in a really less space.

Network: The channel through which the interconnected devices are communicated.

IoT systems can also be described using a basic three layer architecture.

Perception layer – The Perception layer is the typical external physical layer, which includes sensors for sensing and gathering information about the surrounding environment such as temperature, humidity, pressure and so on.

Gateway layer – The Gateway layer is responsible for connecting to network devices, interconnected smart devices and servers. Its features are also used for transmitting and processing sensor data.

Cloud layer - The IoT Cloud Layer represents the back-end services required to set up, manage, operate, and extract business value from an IoT system. It will deliver the application specific services to the user so they can operate and monitor the devices.

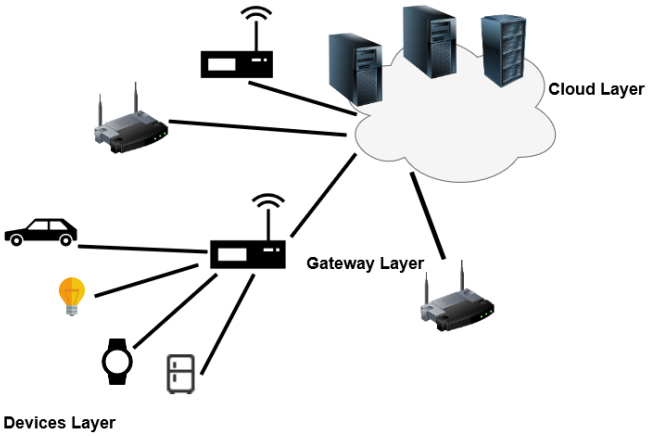

Figure 1: Typical IoT Architecture

This IoT promises to advance our day to day life and it provides contributions towards major important industries such as agriculture, supply chain management, location tracking, remote monitoring, and real time analysis and so on**. [2]** As this is becoming a hot topic this has received much attraction from researchers and industrialists all around the word. Even though this promises many benefits this also has many potential issues and challenges. This paper deals with one of the prominent issues that is security in IoT. Security remains one of the supreme issue that stump the development and applications of IoT**.**

The main objective of this study is to highlight security and privacy issues surrounding IoT ecosystem. In IoT, the things will communicate with each other as everything is interconnected, so privacy can be hindered So, we can say that lots of security and privacy issues will

arise and more attention is required from researchers in IoT especially with regard to issues like authenticity, confidentiality and integrity and availability of data and services in IoT

This paper is divided in to serveral sections, which section two describes about IoT attack vectors in terms of its layers, section three and section four describes privacy issues in IoT with example use case of IoT attack. In the final two sections we are discussing about countermeasures and the conclusion.

II. IOT ATTACK VECTORS IN TERMS OF ITS LAYERS [6-14]

A. Perception Layer

This layer is the lowest layer in the IoT architecture and also called as the Devices layer. Main objective of this layer is to collection of all sorts of information from sensing devices and sending them to the gateway layer. Physical devices like RFID, actuators, sensors exists in this layer.

Following table will depict the different security threats that is arising against Perception Layer.

Table 1 Perception Layer Attack Vectors

Name of the Threat	**Description**
Denial of Service Attack	IoT sensing nodes have limited capacity and capabilities thus attackers can use Denial of Service attack to stop the service. Eventually servers and the devices will be unable provide its service for users.
Hardware Jamming	Attacker can damage the node by replacing the parts of the node hardware.
Insertion of Forged nodes	Attacker can insert a falsified or malicious node between the actual nodes of the network to get access and get control over the IoT network.
Brute Force Attack	As the sensing nodes contains weaker computational power brute force attack can easily compromise the access control of the devices.

B. Gateway Layer

The second or the middle layer of the architecture is known as Gateway Layer and main purpose of this layer is to providing reliable communication between Perception Layer and the Cloud Layer. This acts as an intermediate bridge between Gateway Layer and the Cloud Layer.

Following table will depict the different security threats that is arising against Gateway Layer.

Table 2 Gateway Layer Attack Vectors

Name of the Threat	**Description**
Denial of Service Attack	As this layer provide network connectivity by following a DOS attack, servers or devices are unable to provide the services to the user.
Session Hijacking attacks	Attackers can hijack the session and obtain the access to the network through this kind of attack.
Man in the middle attacks	Attacker can intersect the communication channel between two sensing nodes and easily obtain classified information if there is no proper encryption mechanism in place.

C. Cloud Layer

This is the topmost layer in the IoT architecture which is responsible for providing the end user service. Basically this provides an interface which users can operate and monitor their devices.

Following table will depict the different security threats that is arising against Cloud Layer.

Table 3 Cloud Layer Attack Vectors

Name of the Threat	**Description**
Data security in cloud computing	All the Data that is collected will be processed and stored on the cloud, Cloud service provider will be hold the responsibility of protecting this data.**[5]**
Application layer attacks	Most applications are hosted on the cloud as a Software as a Service and delivered through web services, so the attacker can easily manipulate the application layer protocols and get access to the IoT network.
An attack on Virtual Machines	Security of cloud virtual machines is very important and any security breach can cause the failure of entire IoT environment.

III. PRIVACY ISSUES IN IOT

As internet is becoming a part of our daily lives everything is being shared over the internet like photos, videos, various kind of records and many more, hence privacy becomes a big concern when it comes to information security**.** It is the right of an entity (person), to determine the amount of information it is willing to share with others. **[4]**

As in the IoT everything is connected with the internet, privacy will become a serious issue. A lot of earmarked information of a person can be composed without the awareness of the person. Control on the diffusion of all such information is impossible in current scenario. So, the users of the IoT system need to deal their own data. The owners should know who are using their data and when it is used. **[2]**

IV. EXAMPLE USE CASE MIRAI

On October 21, 2016 many of the major platforms and services in North America and Europe were inaccessible due to a Distributed Denial of Service attack (DDOS). Those affected services and platforms were spanned across multinational industries, social media platforms and many government services. This outage affected by the DDOS attack which targeted domain name service (DNS) provider that resolves domain names for a considerable portion of the internet.**[1]**

Investigated followed by the incident discovered that this malicious DDOS traffic originated from IoT devices around the world which had been compromised by the malware known as Mirai. Those malware infected devices include cameras, printers, residential gateways and baby monitors. It was investigated that owners of these malware infected IoT devices didn't know a least thing that their devices were already compromised. This provides us a great example why you need to be cautious about the security of the internet facing IoT devices.

V. COUNTER MEASURES

The Open Web Application Security Project, or OWASP, has released latest vulnerabilities that will target IoT devices. Following are the current ranked list of the top issues and things to avoid**. [3]**

1. Weak, guessable, or hardcoded passwords
2. Insecure network services
3. Insecure ecosystem interfaces
4. Lack of secure update mechanism
5. Use of insecure or outdated components
6. Insufficient privacy protection
7. Insecure data transfer and storage
8. Lack of device management
9. Insecure default settings
10. Lack of physical hardening

Basic IoT system requires following to be fulfilled in order to become a secure system.

1. Authentication
2. Authorization
3. Confidentiality
4. Integrity
5. Non Repudiation

Authentication verifies the identity of the users or a devices in an IoT system. Authorization checks for what are the privileges possess by the authorized entity to execute on the system. In terms of confidentiality and the data integrity it will make sure that the data is encrypted so no one can tamper even in the storage or during the transmission. Non repudiation assures that authenticity of the origin source of data and integrity of data. Exploiting an IoT system deals with compromising any of the aforementioned security attributes which we need to take actions before compromising.

Following table will depict what we can do to improve the security in terms of aforementioned security attributes.

Table 4 Countermeasures to Improve the Security

Security attribute	**Action**	**Description**
Authentication	Use security credentials Use identity and access management methods	Identification of users and devices need to be done and need to configure strong security credentials for the devices by removing the default credentials.
Authorization		
Confidentiality	Use appropriate encryption mechanism as devices may contain less computational power	Data must be encrypted so only authorized users can access the data.
Data integrity	Use Hashing techniques	Non tampering of data can be assured by various hashing techniques
Non repudiation	Using Digital signatures	Origin source of the data can be assured by using digital signatures.

As IoT systems are consists of heterogonous devices with heterogonous technologies determining security requirement and taking pre caution is a huge challenges as of the complexity.

VI. CONCLUSION

Internet of Things is vast field and evolving day by day making the life better of mankind. As this is a highly evolving technology number of researchers are working towards betterment and the safeguard of the technology. As everything is connected with the World Wide Web security plays a major important role in the IoT arena. Even though there are number of researchers working towards the security issues of IoT there are still lot of fields that is under development as still there are lots of key issues which has no solution yet.

This paper outlines the issues and challenges related to security in IoT in terms of its architecture. A brief insight is being provided about security of IoT environment along with various security threats prevalent at various layers of architecture and some security initiatives which are currently required is also highlighted in this paper.

REFERENCES

[1] Fagbemi, D., Wheeler, D. M., & Wheeler, J. (2020). *The IoT architect's guide to attainable security and privacy*. New York: Auerbach Publications.
DOI: https://doi.org/10.1201/9780367440930

[2] Joshitta, R. Shantha. (2016). Security in IoT environment: A survey. *International Journal of Information Technology & Mechanical Engineering, 2*, 1-8.

[3] TechWell. (2019). *OWASP Releases Latest Top 10 IoT Vulnerabilities*. Available at: https://www.techwell.com/techwell-insights/2019/01/owasp-releases-latest-top-10-iot-vulnerabilities [Accessed 16 Dec. 2019].

[4] Vikas, B. O. (2015). Internet of Things (IoT): A survey on privacy issues and security. *International Journal of Scientific Research in Science, Engineering and Technology, 1*(3), 168-173.

[5] Thilakarathne, N. N. & Wickramaaarachchi, D. (2018). Improved hierarchical role based access control model for cloud computing. *International Research Conference on Smart Computing and Systems Engineering-SCSE 2018*. Available at: http://repository.kln.ac.lk/handle/123456789/18990

[6] Patel, Ashish. (2017). Comprehensive Survey on Security Problems and Key Technologies of the Internet of Things (IoT). *International Conference on Engineering and Technology*. Available at: https://www.researchgate.net/publication/321161091_Comprehensive_Survey_on_Security_Problems_and_Key_Technologies_of_the_Internet_of_Things_IoT.

[7] Pasha,M., Myhammad,S., & Pasha,U. (2016). Security framework for IoT Systems. *International Journal of Computer Science and Information Security, 14*(11), 99-104.

[8] Flauzac, Olivier, Carlos Javier Gonzalez, & Nolot, Florent. (2015). New security architecture for IoT network. *Procedia Computer Science. 52*, 1028-1033.

[9] Efe, Ahmet, Aksöz, Esra, Hanecioğlu, Neslihan, & Yalman, Şeyma. (2018). Smart security of IOT against ddos attacks. *International Journal of Innovative Engineering Applications, 2*(2), 35-43.

[10] Zhang, Guoping & Gong, Wentao. (2011). The research of access control based on UCON in the internet of things. *Journal of Software, 6*(4), 724-731.

[11] Iqbal, A., Suryani, M. A., Saleem, R., & Suryani, M. A. (2016). Internet of things (IoT): On-going security challenges and risks. *International Journal of Computer Science and Information Security, 14*(11), 671.

[12] Ouaddah, A., Bouij-Pasquier, I., Elkalam, A. A., & Ouahman, A. A. (2015, Mar). Security analysis and proposal of new access control model in the Internet of Thing. *In: 2015 International Conference on Electrical and Information Technologies (ICEIT)*, pp. 30-35.

[13] Rao, T. A. & Ehsan-ul-Haq. (2018). Security challenges facing IoT layers and its protective measures. *International Journal of Computer Applications, 179*(27), 31-35.

[14] Ali, I., Sabir, S., & Ullah, Z. (2019). *Internet of things security, device authentication and access control: A review*. Available at: https://arxiv.org/abs/1901.07309.