Suresh Gyan Vihar University Journal of Engineering & Technology
(An International Bi-Annual Journal)
Vol . 7, Issue 2, 2021, pp 41-46
ISSN: 2395-0196

Security and Privacy Challenges in Internet of Everything (IoE) with Security Requirements.

Amit Jaykumar Chinchawade[1] **, Onkar Sing Lamba**[2]

[1]Research Scholar, Dept. Electronics & Communication Engineering, Suresh Gyan Vihar University, Mahal Road, Jagatpura, Jaipur, Rajasthan, India

[2]Professor & HOD, Dept. Electronics & Communication Engineering, Suresh Gyan Vihar University, Mahal Road, Jagatpura, Jaipur, Rajasthan, India

[1]amitchinchawade@yahoo.co.in, [2]onkar.lamba@mygyanvihar.com

Abstract

Internet of Everything (IoE) is a new concept of information exchange in Internet networks. IOE contains the main fields in Smart Home, Smart Agriculture, Smart City, Smart Healthcare, Smart Industry and in Human data exchange networking. It is not only data exchange between any probes and big data centre. It is very important to have sufficient type approval and cyber security mechanism for this new concept. The main aim of this paper to identify the various issues in IoE security and Privacy challenges, IoE security requirement and Application areas of IoE.

Keywords:- IoE (Internet Of Everything), IoT (Internet Of Thing), M2M (Machine –to-Machine), Wireless Sensors Nerwork.

1.Introduction

Internet of Everything (IoE) is replaces the Internet of Thing (IoT). The IoE has foul Pillars, these are People, Process, Data and Thing. Now a day's Millions are peoples are connected and communicate to each other in day to day life. Process is the delivering the right information to right person or the Thing. Data is the more useful for decision making in any application. Thing is nothing but the IoT, number of Devices are connected and communicated to each other by using the Internet.

Suresh Gyan Vihar University Journal of Engineering & Technology
(An International Bi-Annual Journal)
Vol . 7, Issue 2, 2021, pp 41-46
ISSN: 2395-0196

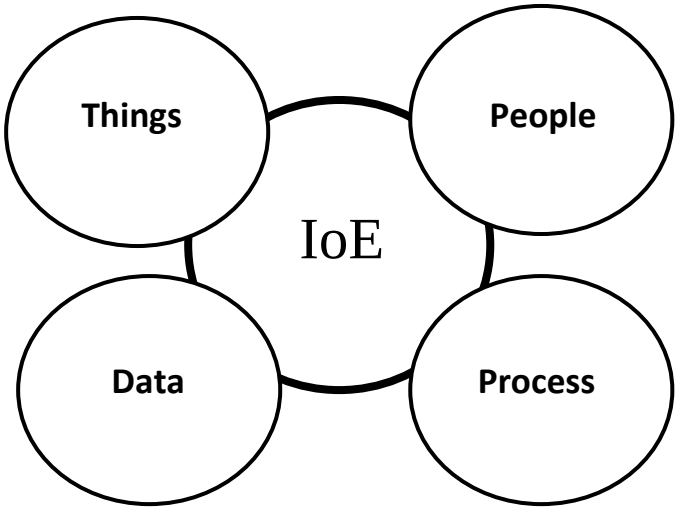

Fig. 1. Pillars of Internet of Everything (IoE)

2. Security And Privacy Challenges In The IoE

The Internet of Everything is a multi-domain environment. IOE consist of a large number of devices and services connected together to exchange information. Each every domain apply its own security, privacy, and trust requirements. Now, some challenges in IOE securities are:

2.1 User privacy and data protection in IoE:

In IoE Privacy is an important issue. User privacy is an very sensitive subject in many research works. In IOE People, Process, Data and Things are connected, and data is communicated and exchanged over the internet. Privacy in data collection, data sharing, data management, and data security is needed in IOE network.[1]

2.2 Authentication and identity management:

In IoE Authentication and identity are a combination of processes and technologies. The aim f this is to managing and securing access to information and resources. Identity identifies objects, and authentication between two communicating parties.[2]

2.3 Trust management and policy integration:

In IoE scenario number of things communicate, trust plays an important role in establishing secure communication between things. To gain user trust, there should be an effective mechanism in IoE environment. [3]

Suresh Gyan Vihar University Journal of Engineering & Technology
(An International Bi-Annual Journal)
Vol . 7, Issue 2, 2021, pp 41-46
ISSN: 2395-0196

2.4 Authorization and access control:

Authorization enables determining if the person or object, once identified, is permitted to have the resource. By wide range of criteria condolingly access to resources are granted or denied. Using the of access controls, authorization is implemented. [4]

2.5 End-to-End security:

Security at the endpoints between IoE devices and Internet hosts is likewise important. For complete end-to-end security, session keys and algorithms must be securely implemented. [5]

2.6 Attack resistant security solution:

There are various types of devices are connected to the internet of Everything. Since these devices may suffer by different attacks, there, such as denial-of-service, flood attacks, etc.[6]

3. Machine To Machine (M2m) Communication In IoE Systems:-

Machine to Machine (M2M) is the technology that allows wireless and wired systems that can communicate with other devices. M2M communications are common in industrial automation for machine instrumentation and monitoring. The “Internet of Everything” (IoE) is a combination people, process, data, and things to make networked connections more relevant and valuable. IoE encompasses both M2M and IoT technologies, and it is the pervasiveness of IoE than can be leveraged to achieve many things for many people, including first responders.

4. IoE Security Requirements

The main IoE security requirements are:

Sr. No	Security Requirements	Descriptions
1)	Confidentiality	The data is secure and only available to authorized users by protecting information against unauthorized access
2)	Integrity	Unintended interference can be imposed by maintaining end-to-end security in IoE communication, and by using digital signatures to ensure the integrity of data.
3)	Availability	Data, devices and services must be available and reachable whenever users need it in.

Suresh Gyan Vihar University Journal of Engineering & Technology
(An International Bi-Annual Journal)
Vol . 7, Issue 2, 2021, pp 41-46
ISSN: 2395-0196

4)	Authentication	Every object in the IoE must be able to identify and authenticate other objects. In IoE; many entities line devices, people, services, service providers and processing units are in interaction in this process
5)	Non repudiation	No repudiation is considered as a cyber security requirement that provides proof of entities behaviors in IoE networks.

Table .1 IOE security requirements

5.Application Areas Of IoE

5.1 Smart Home

The smart home, ranking the highest IoE application on all channels. Smart home is the residential extension of building automation and involves the control and automation . It defines a residence that has appliances, lighting, heating, air conditioning, TVs, computers, entertainment systems, big home appliances such as washers/dryers and refrigerators/freezers, security and camera systems capable of communicating with each other and being controlled remotely by a time schedule, phone, mobile or internet.

5.2 Smart City

Smart cities uses IOE devices such as connected sensors, lights, and meters to collect and analyze data. The cities then use this data to improve infrastructure, public utilities and services, and more. IoE solutions offered in the smart city sector solve various city-related problems, comprising of traffic, reducing air and noise pollution, and helping to make cities safer.

5.3 Smart Grids

The Smart Grid is part of an IoE framework, which can be used to remotely monitor and manage everything from lighting, traffic signs, traffic congestion, parking spaces, road warnings, and early detection of things like power influxes as the result of earthquakes and extreme weather. The Smart Grid does this through a network of transmission lines, smart meters, distribution automation, substations, transformers, sensors, software and more that are distributed to businesses and homes across the city.

5.4 Connected Health (Digital Health/Telehealth/Telemedicine)

Suresh Gyan Vihar University Journal of Engineering & Technology
(An International Bi-Annual Journal)
Vol . 7, Issue 2, 2021, pp 41-46
ISSN: 2395-0196

In Healthcare system latest trends of IoE is used. IoE software helps patients to reduce health-related threats and hospital expenses by gathering patient information and processing data using cloud services to exchange data sources.

5.5 Smart Retail

The IoE is enabling retail stores to evolve into smart stores, which obtain data about customers' tastes, needs, and habits in real time. This enables retailers to predict customers' behavior and provide them with the products or services they want and need.

5.6 Smart Supply Chain

Supply chains have already been getting smarter for a couple of years. Offering solutions to problems like tracking of goods while they are on the road or in transit or helping suppliers exchange inventory information are some of the popular offerings. With an IoE enabled system, factory equipment that contains embedded sensors communicate data about different parameters, such as pressure, temperature, and utilization of the machine. The IoE system can also process workflow and change equipment settings to optimize performance.

5.7 Smart Farming

The number of farming operations is usually remote and the large number of livestock that farmers work on, all of this can be monitored by the Internet of Everything and can revolutionize the way farmers operate day to day.

Conclusion

Internet of Everything (IoE) replaces the IoT. Security in IoE network is essential now a days. These security and Privacy issues are the major challenges in IoE. The various IoE security requirements are helpful in various sectors like Home automation, Smart City, Smart Agriculture etc. to make the systems automated.

References

[1] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Perception, vol.111, 2015.

[2] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," Computer, vol. 44, 51-58, 2011.

[3] R.Mahmoud, T. Yousuf, F.Aloul, I.Zualkernan, Internet of things (IoT) security: Current status, challenges and prospective measures.10th International Conference for Internet Technology and Secured Transactions, ICITST 2015, pp. 336341, 2016.

[4] M.A.Khan, K.Salah,IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, pp. 395411, 2017

[5] .Yaqoob, E.Ahmed, M.H.Rehman, A.I.A.Ahmed, M.A.A.-garadi, The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks, 129, pp. 444458, 2017.

[6] S.Moganedi., & J.Mtsweni,Beyond the convenience of the internet of things: Security and privacy concerns. 2017 IST-Africa Week Conference (IST-Africa), pp. 110, 2017.

[7] M.U. Farooq, M.Waseem, A.Khairi, S.Mazhar, A Critical Analysis on the Security Concerns of Internet of Things (IoT). International Journal of Computer Applications, 111(7), pp. 16, 2015.