Advances and Applications in Mathematical Sciences
Volume 18, Issue 8, June 2019, Pages 627-636

CRITICAL REVIEW OF SECURITY ISSUES OF INTERNET OF THINGS UNDER CLOUD COMPUTING ENVIRONMENT

MANDEEP KAUR[1], SANCHI KAKKAR[1] and V. P. SINGH[2]

[1]Panipat Institute of Engineering Technology
Samalkha, Panipat, Haryana
E-mail: mandeep.kaur79@gmail.com

[2]CSED, Thapar University
Patiala, Punjab, India

Abstract

Internet of Things (IoT) is developing at an exceptionally quick pace in almost every field of life; industry, home, resistance and medical science, e-commerce, agriculture, defense and space research. The working and technology of different devices used in these domains have exceptionally changed due to communication speed, data generation, selection, storage and processing. Utilization of Artificial Intelligence (AI) and Big Data has further enhanced the potential, efficiency and accuracy of such devices. Role of Cloud Computing as storage, networking, processing and security application in the overall working of IoT devices cannot be ignored as these devices are generally too small to do all these operations on its own. The paper discusses the current scenario of IoT devices, future scope, security issues and its solutions in light of the supporting Cloud Computing environment.

1. Introduction

Internet of Things (IoT) is quickly entering into our life and created a "Third wave" after the first "web wave" and the second "mobile wave" in the field of communication technologies. It utilizes the artificial intelligent gadgets containing sensors that record useful information related to touch, recording of voice, movement, light, speech, gestures, biometrics and other technologies to take actions on the basis of decision making algorithms. These IoT gadgets can work on tremendous pace to generate, record, filter,

2010 Mathematics Subject Classification: 91Cxx.

Keywords: Security and privacy, IOT, Cloud Computing, Behavioral science, Cloud Databases, Security Attacks.

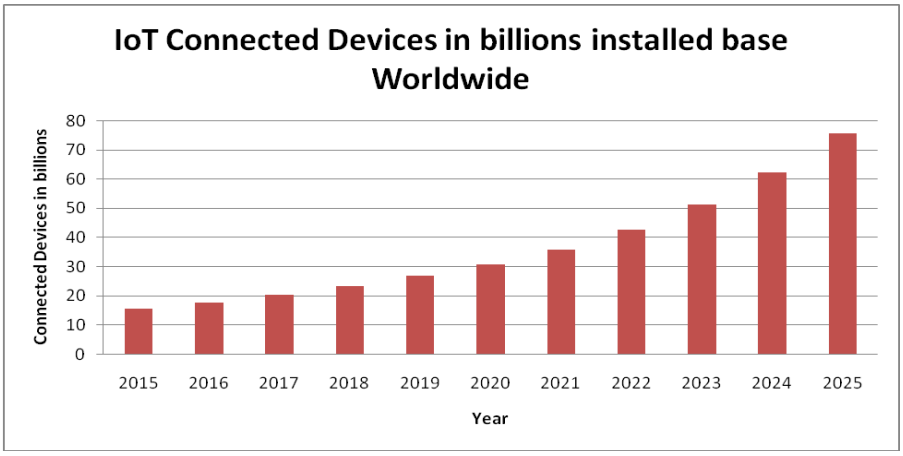
Received February 20, 2019; Accepted March 15, 2019

process and store the sensed information. Cloud computing servers can be used by these IoT devices for easy storage, processing, network devices and security services. Inspite of various advantages of IoT gadgets, there are also some critical issues that need to be answered soon. Moreover, the non-standardization of IoT technology has further worsened the situation as even formulation of certain regulations cannot control the methodologies used in such devices. Also the inherent issues related to security and privacy of information placed on cloud servers pose further security threats and misuse of the IoT devices. Researchers throughout the world are trying to formulate newer approaches to beat the challenges of security and data protection in the newer world of IoT devices. Such endeavors are required in the parent technology along with the supporting technologies of sensors, ad-hoc networks, cloud storage, security and privacy. This paper presents a review of the present situation of security, privacy and protection of data in the emerging world of IoT gadgets. It also shall peek into the future of IoT devices, threats and possible solutions that shall eventually be of use for further advancement of this domain.

2. Internet of Things

Internet of Things (IoT) is an arrangement of interconnected smart gadgets that sense the environmental factors to create some useful information used for decision making and take further action. Such devices can exchange information/data/advise with different gadgets over the communication channel without the human-to-human or human-to-PC intervention. Presently, such devices include home appliances, mobiles, electronic gazettes, healthcare devices, weather sensing devices etc. (see Figure 1) that contain programming, sensors, actuators that utilize sensed data for decision making and control of other devices available over the same network.

Figure 1. Present Day IoT Devices in Real life.



Source: IHS Statista 2018

Figure 2. Expected number of IoT devices worldwide upto 2025.

3. Growth of IoT Devices Worldwide

The IHS Statista 2018 survey shows the prediction that, the expected number of IoT enabled devices will continue to grow at the rate of 10% each year and reach 75.44 billion IoT devices upto year 2025 (refer Figure 2). These devices will be related to manufacturing technologies, healthcare,

agriculture, animal care, security, home appliances and industrial control systems. If IoT devices enter into other related domains also, the expected number can increase to twice the present expected value. The global worth of the IoT industry is expected to reach 6.2 trillion dollars by the year 2025. Further boost shall be provided by upcoming 5G technology in communication, higher generation of data using the smart devices with sensors, use of Cloud servers for storage and processing of huge amount of data using Data analytics for final action.

4. Objectives

Cloud technology is a boon for IoT devices that need storage for large chunk of data produced by smart sensors that constantly generate data. This data is of the form of big data and needs high storage, processing, security and applications for derivation of useful information which is cheaply possible by use of cloud services in such domains. The pay-per-use model of the cloud servers prove cheaper as compared to the proprietary solutions purchased by the users, organizations and companies that use the power of smart devices in automating some part of the system(s). Automatic process of data generation, communication, storage, analysis, extraction and performing action can be supported by "as-a-service" model of the cloud computing technologies. Cloud architecture also has its own issues related to data sharing, storage safety, privacy and protection apart from job scheduling and resource sharing algorithms.

5. Security and Privacy

Privacy and security of information has always been important since many years. Historically also we see many methods used by people in different civilizations that tend to refrain information read by people who are involved in communication. The need of security and privacy of information has grown manifolds in the present world of IoT. Security means a state when someone feels free from any kind of risk or danger. In the same way state of privacy means one is not watched by others directly or indirectly. Security and privacy are the expressions that term anyone to be free from dangers and undesirable outer impacts. In the current scenario, when the speed of communication is very high, storage devices have become much

cheaper, processing power doubles every year, the requirement of securing data from external influences is almost impossible [1]. Even countries have modified their laws to suit the era of Information Technology. In India also, the impact of smart devices can be seen in the industry, homes, health affairs, medical science, engineering, defense, space science, weather forecasting, agriculture, control units, financial markets etc (see Figure 1). Researchers all over the world are working on use of IoT devices in various other domains also. However, these automated solutions that generally involve artificial intelligence also should be tested on the grounds of security and privacy [2]. Security and protection concerns have already surfaced in countries like USA where it was alleged that use of big data analytics was done to influence Presidential elections, Russia and China trying to take control of many public networks, electric grids and defense servers, allegations of tampering of EVMs in India by many political parties, utilizing web-data on social networking sites for predicting biases and influence voters, recent leaks of data from Sony, Google accounts, Facebook etc also point to misuse of customer information for commercial or non-commercial matters [3]. The world is still left in dark in case of IoT technologies too. The non-standardization of the upcoming technology and different vendors that are producing their own protocols and rules used in smart devices have made it difficult to have an easy control on the data generated, processed and analyzed by such devices.

6. Current Status

Presently, the smart machines not only include mobile phones but televisions, refrigerators, cars, smart watches, websites, ATMs, cameras etc. These generate data using sensors that sense environment using receptors, sort useful data, communicate it to other devices using the network. Smart phones monitor each and every action user to make certain decisions, hear voice commands using its mic and respond to it, capture photographs to identify persons using the camera, record other behavioral statistics from the touch screen etc. and report to the publishers of the applications and operating system to control the action performed on such devices through internet connectivity. Usually such permissions are taken from the users during installation of application on the devices.

Smart Televisions are also using mic and internet connectivity to report sounds heard. Smart watches report data related to human activities, sleeping patterns that may prove a severe breach of privacy as many things can be predicted about our activities when vital statistics of heartbeat, temperature, sweat level and other things can be recorded. It can also use the camera or mic to record videos and sounds at desired times by the service providers that cannot be even traced as it can go on as a background event.

7. Reasons

There can be many reasons for the difficulty faced by different organizations in keeping the IoT devices foolproof. Some of the points that lead to difficulties in securing and protection of data of these devices are as follows:

7.1. More devices, more issues

As the number of devices that are coming in the domain of being a smart device, there are more and more devices that are automatically communicating with each other. This leads to a situation when we need to protect data for more and more devices. This means earlier we were only concerned with securing the data on the desktops and laptops. But now we are to worry about securing smartphones, homes, vehicles, appliances, wearable computers and many more such intelligent devices.

7.2. Non-Standardization and no Updates

Another reason why the IoT devices are posing greater threat to our security and privacy is that there is no particular standardization of protocols have been followed by these devices. Even if some new device is good at the time of launch, it becomes vulnerable to attacks as the organizations do not provide technological updates from time to time to keep it safe.

7.3. Data storage on Cloud

Even if data on the devices are safe, we cannot confirm about the safety of data placed on the remote cloud servers being used to store the huge information being produced by such smart devices. Cheaper data storage clouds may also lead to breach of security as hackers may attempt to access information related to many customers by attacking the cloud storage servers

of the smart devices used by service organizations rather than attacking single smart device.

7.4. Laziness of Customers

Most of the devices come with an option of automatic updates, which generally all customers do not choose due to issues related to smaller internet data plans or low bandwidth they subscribe to. They are also reluctant to check for any updates that are available for devices to continue keep them secure and free from bugs and vulnerabilities that may be used to compromise the data.

These factors play an important role in deciding the overall security and privacy that is possible for such IoT devices and may lead to serious breaches that can cost economic or psychological losses to the customers. Moreover, it is hard to formulate single protocol for security and data protection that may bind these heterogeneous devices.

8. Recent Attacks on IoT

In the recent past, a number of researchers have successfully hacked the IoT devices. Instances of successfully hacking the car to disable brakes, turning off lights to control the car, GPS signal hacking to affect its navigation, home control device hubs hacking, hacking of smart TVs, hacking bulbs using worms attack, DDoS attack on networks thereby posing serious threat to other devices connected to the compromised network appears [3,4]. It is clear that traditional security approach is not successful in such a scenario. As the futuristic smart machines will have greater autonomy to take their own decisions in the domain of defense, education, gaming, home security, banking, business and marketing [6] due to high speed computing power and communication efficiency, it is the need of the hour to use a combination of more than one method of security and privacy for IoT. Some of the methods have been discussed in the next section of the paper.

9. Solutions

There may be different methods of safeguarding the information generated at the IoT device and at the cloud server level.

9.1. IoT device based solutions

Switching the sensing power on/off

The user must choose some IoT device that has some method that can make it switch on/off. That is when the user does not want the sensors to sense the environment, one can instruct the device not to use the sensors for recording of data. This is important to stop the smart devices to hear, see, sense the environment when not required.

9.2. IoT sub-network

It is suggested that the smart devices must be connected to create a smaller network. This ensures that minimum number of security issues are faced in case of a hacking attack or DDoS attack.

9.3. No Single Solution

It is also good to choose different service providers with different platforms, architectures, protocols and service methods so that a single breach may not lead to greater loss of privacy and data. Difference in the methodologies shall pose some restriction over the single gate entry to the entire security system in the other case, which may lead to greater losses to the organization.

9.4. Cloud based security solutions

The cloud based methods deal with securing the data that needs to be placed over cloud services of any kind by the IoT device. It is still the responsibility of the IoT service provider to choose at least one of the suggested solution discussed as follows:

9.4.1. Using encrypted Clouds

IoT devices use some servers to store the information. Mostly, it is some kind of a cloud service. To ensure the overall security and privacy, data security at cloud server is also important. One should prefer to use the encrypted cloud services.

9.4.2. Encrypt data

Another solution may be that the data can be encrypted using some encryption method before being placed it over the cloud server. This ensures that no one other than the actual user can decrypt it and therefore remains secure.

9.4.3. Data Storage norms

When the data is placed using the cloud storage service, one should avoid sensitive information placed over the cloud. The Service Level Agreement (SLA) of cloud services must be read properly to know how actually the data will be stored on the cloud server, whether replica will be made to maintain availability of data at all times. Does the cloud server maintain a local copy of the data on the client side? If yes, how safe it is? It is also important to note any provision if someone other than the actual user including the service provider can directly access the data or not?

9.4.4. Private or Public cloud

There is also a choice between a private cloud service and a public cloud service. If money is not an issue then private cloud service should be used to place important data on the cloud server. However, if the services should also be cheaper, then a reliable public server has to be used to store data. Clients must therefore check the health of data placed over such cloud service from time to time to ensure data is not compromised.

10. Conclusion

The war between the attackers and the security professionals is always on. Security professionals will try their best to secure the systems and the attackers shall always strive hard to find some vulnerability, some loophole to break into the so called secure systems. Therefore, the threats of security and privacy breach shall continue to exist in the world of IoT. One has an option to use security mechanisms like using switching on/off the intelligence mode of devices, using non-standard private key based encryption of data when moved to external devices like the cloud servers, creating separate layer of IoT network devices for minimal damage in case of a network hack, removal of vulnerabilities in devices by updating the firmware of such devices.

11. Future Scope

Standardization of IoT devices, non-usage of unreliable communication channels, security of data when moved to cloud are still open problems to be solved for fool proof security of IoT devices. Efforts must also be made to develop innovative security techniques for data to be shared between

different devices, newer and stronger encryption methods of information security before sharing with cloud servers etc. for better security and privacy of IoT.

References

[1] Lopez Amanda, Protecting Your Privacy in an IoT-Connected World, accessed from https://www.iotforall.com/protecting-privacy-in-iot/ on March 3, 2019.

[2] A. Cavoukian and J. Jonas, Privacy by Design in the Age of Big Data, Information and Privacy Commissioner of Ontario, Canada, pp. 1-17, 2012.

[3] M. Richardson, et al., Privacy and The Internet of Things, Lexis Nexis: Watching Me, Watching You: Surveillance, Privacy and The Media, vol. 21(3) (2016), 336-351.

[4] R.H. Weber, Internet of Things-New Security and privacy challenges, Computer Law & Security Review, vol. 26 (2010), 23-30.

[5] Article Internet of Things accessed from https://datafloq.com/read/internet-of-things-iot-security-privacy-safety/948

[6] Article titled "4 critical security challenges facing IoT" available at https://www.networkworld.com/article/3166106/4-critical-security-challenges-facing-iot.html