Influence of IOT with Cryptography in Healthcare Applications : A Review

[1]Jayachandran Balakannan, [2]Subhashree Pattanayak, [3]Laxmiparbati Das

[1]Professor in Dept. of Computer Science, GIET Gangapatna, Bhubaneswar
[2]Assistant Professor in Dept. of Computer Science, GIET Gangapatna, Bhubaneswar
[3]Assistant Professor in Dept. of Computer Science, GIET Gangapatna, Bhubaneswar

Abstract: One of the catchwords in the field of Information Technology is the Internet of Things (IoT). The Internet of Things is poised to transform real-world objects into intelligent virtual objects in the near future. It aims to integrate everything in our world under a common infrastructure, providing us with control over our surroundings and keeping us informed about the state of things. This review article explores IoT concepts through a systematic review of scholarly papers, corporate white papers, expert discussions, and online databases. It covers definitions, origins, basic requirements, characteristics, and aliases of the Internet of Things, as well as architectures, vital technologies, and their everyday applications. This document is intended to provide a comprehensive understanding for new researchers interested in exploring the field of Internet of Things and facilitate efficient knowledge collection.7978208082

Introduction

The Internet of things (IoT) outlines the network of physical objects which are embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the Internet. The definition of the Internet of things has developed gradually due to the functioning of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems. Traditional fields of embedded systems, wireless sensor networks, control systems, automation such as home and building automation, and others all contribute to enabling the Internet of things. In the consumer market, IoT technology is most closely associated with products about the concept of the "smart home", including devices and appliances (such as lighting fixtures, thermostats, home security systems and cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as smartphones and smart speakers. It is also "the interconnection and exchange of data among devices or sensors".

Executing and Controlling a high dynamic ad hoc IoT things or devices network is a difficult chore with the traditional networks architecture, Software Defined Networking (SDN) provides the quickly moving dynamic solution that can deal with the specific requirements of the diversity of innovative IoT applications [1]. Privacy concerns have led many to consider the possibility that big data infrastructures such as the Internet of things and data mining are inherently incompatible with privacy [2]. There are numerous serious issues about risks in the growth of IoT, especially in the areas of privacy and security, and as a result industry and governmental moves to address these concerns have begun including the development of international standards. There is a transformation in human's daily life as well as in working conditions in organizations after the advent of IT and ITeS technologies. This is becoming a familiar concept across many horizontal and vertical markets including a common man's everyday life in society, as it has several applications. The development of the Internet of Things [IoT] has been primarily driven by the needs of large corporations that stand to benefit greatly from the foresight and predictability afforded by the ability to follow all objects through the commodity chains in which they are embedded. The ability to code and track objects has allowed companies to become more efficient, speed up processes, reduce error, prevent theft, and incorporate complex and flexible organizational systems through IoT. The IoT is a technological revolution that represents the future of computing and communication, and its development depends on dynAmic technical innovation in several important fields, from wireless sensors to nanotechnology. They are going to tag each object for identifying, automating, monitoring, and controlling.

Vision

A networking era has been discussed by the International Telecommunication Union in which networks are linked and everything from tires to attires will be part of this huge network. Suppose you are performing an internet

search for your watch which has been lost somewhere in your own house. So, this is the main image of the Internet of Things. It creates an environment where things can do communication and their data can be processed to perform desirable tasks with the help of machine power hardware working together with real-time web software to make this imagination a reality. Moreover, different-different people and corporations have different imaginations for the Internet of Things. In-Network World, a document was published which shows Internet of Things strategies of top IT Vendors. If we see from HP's vision, it creates a world where people are always in link with their content. Cisco holds an opinion in the industrial automation and convergence of operation. Intel is also interested to empower billions of existing devices with intelligence. Microsoft does not look attentively at the Internet of Things as any futuristic technology; they consider that it already exists in powerful devices and that the devices just need to be connected for a large amount of information which could be helpful. IBM has a different image of a Smarter Planet by controlling the devices remotely with the help of secure servers. Although they all have different visions they all agree about a network of interconnected devices. Hence, within the coming decades, more developments can be seen which will include a new transformed information society.

Cryptography

Cryptography is derived from two Greek words: "Kryptos" which means hidden and "graphein" which means to write [3]. Cryptography is also known as cryptology. It is a method for secure communication that prevents third parties from reading private messages[4]. Cryptology is about creating protocols that protect the data and prevent it from access by third parties[5]. There are four important aspects of Information Security:

(i) Confidentiality

(ii) Data integrity

(iii) Authentication

(iv) Non-repudiation[6].

Earlier ciphers were often used for encryption or decryption without making use of authentication and integrity checks. There are two types of cryptosystems namely symmetric and asymmetric cryptosystems. In Symmetric systems, the secret key (same key) is used to encrypt and decrypt a message whereas, in Asymmetric systems, a public key is used to encrypt a message and a private key is used to decrypt a message. In symmetric systems, data manipulation is faster as compared to asymmetric systems as they make use of shorter key lengths. Asymmetric systems enhance more secure communication. Symmetric systems use AES (Advanced Encryption Standard) which is the replacement of DES (Data Encryption Standard) [7].

Applications of Cryptography can be seen in the field of Mathematics, Computer Science, Electrical Engineering, Communication Science, Electronic commerce, Chip-based payment cards, Digital currencies, Computer passwords, and Military communications.

Internet of Things

"Internet of Things" is also known as IoT. It is a combination of two words i.e. the first word is "Internet" and the second word is "Things". To serve billions of users all over the world, TCP/IP Internet protocols are used by the Internet to connect computer networks.

It consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by optical, electronic, and wireless networking technologies as shown in figure 1. Nowadays more than a hundred countries are linked with each other to exchange their data, news, and opinions through the Internet.

Things are the real objects in this physical or material world. Secure and privacy- preserving transmission with reduced energy and reduced communication bandwidth of keyframes to medical specialists can be provided by the Internet of Things.

Fig. 1 Internet of Things Radio Frequency Identification (RFID)

Radio Frequency Identification is a technology that helps in making objects identifiable uniquely. It also minimizes the size to make it integrable into any object. It reduces the cost also. It is a transceiver microchip that is almost similar to an adhesive sticker which could be both active and passive, depending on the type of its usage. Active tags are always active as they have a battery connected to them. They consistently emit the data signals. Passive tags get activated when they are triggered. Active tags are more expansive than Passive tags. Also, active tags have a very large range of useful applications. Radio Frequency Identification system is made up of readers and it is combined with RFID tags which when got triggered by the generation of any appropriate signal, sends the identification, location, or any other specifics about the object. The emitted object-related data signals are passed on to the Readers with the help of radio frequencies which are further transmitted

to the processors for analyzing the data. A book named Spychips describes how Organizations and Government bodies plan to track our every move. This book gives the courage to think about a world where there is no privacy where every purchase is recorded in a database server and everything is counted, where anyone from a foreign nation has a record of everything you have ever bought, what more than that they can track from a remote location? Where your every purchase is monitored and recorded in a database and your every belonging is numbered. Where someone many states away or perhaps in another country has a record of everything you have ever bought. What's more, they can be tracked and monitored remotely"[8].

Depending on its type of use, RFID frequencies are divided into four different types of frequencies which are as shown below:

(1) Low frequency

(2) High frequency

(3) Ultra-High Frequency

(4) Microwave Frequency

In the healthcare system, there is a need for increased visibility, efficiency, and gathering of data around relevant interactions. RFID tracking solutions can help in managing healthcare facilities, mobile medical equipment, improve patient workflow, monitor environmental conditions, and protect patients, staff, and visitors from infection or other hazards. In the medical industry, to opt for RFID is very effective. A combination of active and passive RFID can be seen in Hospitals. It has been noticed in many successful industries that active technology tracks high-value whereas passive technology tracks smaller and lower cost items that only need room-level identification. Bar Code has almost the same functioning as that of an RFID, but the difference is that RFID is more effective than a Bar Code due to its numerous benefits. Being a radio technology, RFID does not require the reader to be physically in its vision while Bar Code is an optional technology that does not work until its reader is placed in front of it. To trigger different types of events, RFID can work as an actuator. If compared to the Bar codes, they also have modification abilities. In healthcare systems, there is a need for enhanced efficiency, visibility, and collection of data around relevant interactions. To manage mobile medic RFID tracking solutions can help healthcare facilities in managing mobile medical types of equipment, improve workflows of patients, supervise environmental conditions, and helps in protecting patients, staff, and visitors from infection or other hazards.

Wireless Sensor Networks (WSN)

As Wireless communications, digital electronics, and microelectromechanical technologies have transformed with the advancements, it has led to the development of miniature devices. These miniature devices are known as nodes which are interconnected to create a wireless sensor network. It can be shown with the help of figure 2 shown ahead. These miniature devices can sense, communicate wirelessly over short distances, and perform any computation. It can search for applications in infrastructure monitoring, environmental monitoring, and traffic monitoring, etc. Wireless Sensor Network is made up of the following components.

1. Wireless Sensor Network hardware: It consists of sensor interfaces, processing units, transceiver units, and power supply.
2. Wireless Sensor Network communication stack: Nodes in Wireless Sensor Network need to communicate with themselves to send data in single or multi-hop to a base station. The sink node collects the communication. The sink node must be able to interact with the world via the internet to act as a gateway to the subnet of Wireless Sensor Network and Internet.
3. Wireless Sensor Network Middleware: It is a process to combine cyberinfrastructure with Service Oriented Architecture(SOA) and sensor networks to provide them access to heterogeneous sensor resources. This Wireless Sensor Network middleware is based on isolating resources that can be used by several applications.
4. Secure Data Aggregation: A secure data aggregation is required to append the lifetime of networks as well as the trustworthy data collected from sensors. To assure security is a very critical task because the system is linked with the actuators and it protects the system from unauthorized access which is very much important.

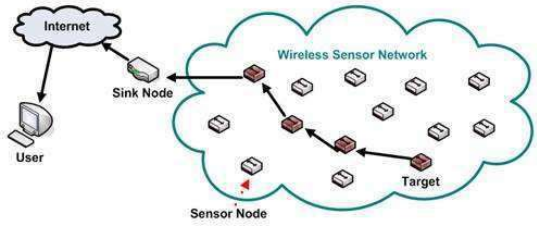

Fig. 2 Wireless Sensor Network

Some algorithms reduce node's redundant sensor information to decrease communication costs. These algorithms also help to avoid forwarding data which is of no use. This mechanism has been used for distributed anomaly detection[9].

Applications of IOT in Healthcare System

Medical and Health data should be kept confidential to take care of patient's privacy

Healthcare data consists of images, graphs, and other medical information about the patients in which confidentiality is a must. There are some drawbacks in

digital data properties and traditional encryption schemes over one-dimensional data, therefore it can not be applied directly to electronic health data. When a patient's data is sent over the open channels, the patient may lose his privacy of the data. To ensure on-time, correct, and privacy of electronic health services, a very secure lightweight keyframe extraction method is required. Besides this, to achieve a satisfactory level of security is very difficult to achieve considering the cost-effective way in real-time electronic health care applications. Internet of Things with cryptology can provide a secure healthcare system by maintaining the patient's privacy.

Smart devices, mobile internet, and cloud services give their contribution to the continuous and systematic innovation of healthcare systems and it also enables cost-effective, efficient, on-time, and very high quality medical services. The services provided include chronic disease management, elderly care, wellness and fitness programs, etc. Microchip– induced tumors have been noted during animal trials.[10] Internet of Things in Healthcare contributes to maintaining Electronic Health Record. Electronic Health Record is a repository of electronically maintained information about an individual's lifetime health status and health care which needs to be maintained private. It deals with the following points:

1. Integrated access to patient's data anywhere
2. Flexibility and Adaptability
3. Single copy in a single format
4. Supports images, videos, and graphs
5. Legible and coherent information
6. Initial investment
7. Time to learn how to deal with the system
8. Security issues
9. Contingency plans in case of failure

Because of the increase in population and lifestyle we follow nowadays, we will be facing a lot of health problems by 2020 as described by the WHO (World Health Organization).

As health issues are rising, medical professionals are not enough in the world to fight these health problems. Health problems are one of the major concerns of the government and organizations in developing countries. One of the major problems is in house treatment which has been faced by many medical professionals. It has gained a lot of attention from researchers on the Internet of Things, and it is the most promising solution because with the Internet of Things patients can maintain their health problems and emergencies [11].

Several advanced IoT applications have been developed to support medical officers and patient report management, emergency medical conditions, medical treatment, and other facilities. It helps to enhance the quality of healthcare applications.

Hospitals use the Internet of Things to check patients continuously and provide real- time health care facilities. Internet of things has the stamina to track people, services, and objects accurately. So, analyzing that data gives accurate results. In the medical and healthcare field, accurate and precise information lead to the best-resulted treatments. With the Internet of Things, doctors can compute vital signs and other biometric information of patients with the help of attached sensors to patients. So, diseases and problems could be diagnosed very quickly. With the help of the Internet of Things, hospitals and ambulance services can quickly receive a notification when the patient requires their services. Also, with IoT roads and traffic lights can be controlled to support ambulances to reach the hospital very quickly [12]. Internet of Things has the stamina to keep people healthy. It reminds people to take mandatory actions to remain healthy. Wearable medical devices are very much popular among people. The impact on the fitness and health domain. With the help of wearable devices, Patients can check their heart rate, blood sugar level, ECG, and spO2[13]. The sudden increase in the population has brought many challenges in health services which led to the scarcity of medical resources. These challenges need to be addressed and its solution must be provided considering the limited resources. The IoT mobile and network connectivity provide the best solution due to their lower cost and easy-to-use features [14]. The Internet of Things' main attention is to provide a rich user experience at a low cost. It also focuses on improving the quality of life [15]. The main function of the Internet of Things is to provide a connection to the available medical resources at the moment. It should be an effective, trustworthy, and smart healthcare system.

It is very beneficial for aged patients who suffer from chronic diseases. A smart healthcare system in the medical field is introduced by IoT which consists of sensors with a very well functioning, remote server, and network. This system gives attention to providing monitoring with multi-dimensional features and basic treatment suggestions [16].

Conclusion

As IoT technologies continue to grow, they are poised to become unstoppable, developing on a large scale. This evolving networking pattern will soon impact every aspect of our daily lives, ranging from automated homes to intelligent health and environmental monitoring by embedding intelligence into the objects around us. In this review paper, we discussed the vision of IoT and cryptography, which helped us outline a precise architecture for its deployment. We then highlighted various enabling technologies and some related security threats. Finally, we explored numerous IoT applications that will enhance our daily lives. While research is already underway for its widespread adoption, addressing the challenges in its development is crucial to ensuring data confidentiality, privacy, and security for

users. The deployment of IoT requires considerable efforts to combat and address its security and privacy-related threats.

References :

[1] Sadek, R. (2018). An Agile Internet of Things (IoT) based Software Defined Network (SDN) Architecture. Egyptian Computer Science Journal, 42(9), 13-29.

[2] McEwan, Adrian (2014). "Designing the Internet of Things" (PDF). Retrieved 1 June 2016.

[3] Bellare, M., & Rogaway, P. (2005). Introduction to modern cryptography. Ucsd Cse, 207, 207.

[4] Menezes, A.J., & Van Oorschot, P.C. (1997). Scott a. Vanstone. Handbook of Applied Cryptography. Vol. 106.

[5] Liddell, H. G., & Scott, R. (1897). A greek-english lexicon. New York: American Book Company.

[6] Wirsing, M. (1990). Handbook of theoretical computer science. Formal Model and Semantics Chapter 13.

[7] Sharbaf, M. S. (2011, November). Quantum cryptography: An emerging technology in network security. In 2011 IEEE International Conference on Technologies for Homeland Security (HST) (pp. 13-19). IEEE.

[8] Albrecht, K., & McIntyre, L. (2005). Spychips: How major corporations and government plan to track your every move with RFID. Thomas Nelson.

[9] Bosman, H. H., Liotta, A., Iacca, G., & Wörtche, H. J. (2013, October). Anomaly detection in sensor systems using lightweight machine learning. In 2013 IEEE International Conference on Systems, Man, and Cybernetics (pp. 7-13). IEEE.

[10] Albrecht, K. (2010, June). Microchip-induced tumors in laboratory rodents and dogs: A review of the literature 1990–2006. In 2010 IEEE International Symposium on Technology and Society (pp. 337-349). IEEE.

[11] Abo-Zahhad, M., Ahmed, S. M., & Elnahas, O. (2014). A wireless emergency telemedicine system for patients monitoring and diagnosis. International journal of telemedicine and applications, 2014.

[12] Gotadki, S., Mohan, R., Attarwala, M., & Gajare, M. P. (2014). Intelligent ambulance. Int. J. Eng. Tech. Res. (IJETR), 2(4), 2321-0869.

[13] Li, C., Hu, X., & Zhang, L. (2017). The IoT-based heart disease monitoring system for pervasive healthcare service. Procedia computer science, 112, 2328-2334.

[14] Tyagi, S., Agarwal, A., & Maheshwari, P. (2016, January). A conceptual framework for IoT-based healthcare system using cloud computing. In 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence) (pp. 503-507). IEEE.

[15] Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: a comprehensive survey. IEEE access, 3, 678-708.

[16] Yuehong, Y. I. N., Zeng, Y., Chen, X., & Fan, Y. (2016). The internet of things in healthcare: An overview. Journal of Industrial Information Integration, 1, 3-13.