(7)

2019-20
National Conference.
UGC listed. Group II.

National Conference

on

RECENT ADVANCES IN PHYSICAL AND MATHEMATICAL SCIENCES

(NCRAPMS-2020)

18th January 2020.

ORGANIZER

Shri Shivaji College Of Arts, Commerce & Science, Akola

Study On Current Security Issues in Internet Of Things

Ms. U. R. Patil & Dr. V.M. Patil
(Research Scholar) 1
Head, Dept. of Computer Science & IT, Shri Shivaji College, Akola 2

Abstract

Internet of Things (IoT) is an innovative and new age technology, which supports global infrastructure for exchange and sharing of data by interconnecting the uniquely identifiable physical and virtual devices without any interference of humans. Security is one of the important aspect related to the IoT technologies, applications, and platforms. The main objectiveof IoT security is to preservation of privacy, confidentiality and to make sure the security of the users, infrastructures, data, and devices of the IoTandgive the assurancefor availability of the services offered by an IoT ecosystem. This paper represent the study about the related security issues during data transmission and the some cryptographic algorithms used along with IoT.

Keywords: Internet of Things, Security algorithm, Encryption.

I. Introduction

Internet of Things is the new age technology concerned with devices and networks through Internet. The Internet of Things (IoT) is composed of physical objects embedded with electronics, software, and sensors, which allows objects to be sensed and controlled remotely across the existing network infrastructure, facilitates direct integration between the physical world and computer communication networks, and significantly contributes to enhanced efficiency, accuracy, and economic benefits [1]. Therefore, IoT has been mostlyused in various applications such as environment monitoring, energy management, medical healthcare systems, building automation, and transportation. Unfortunately, due to the resources of IoT devices, they always highly complex to give assurance.

II. Introduction To Iot Security

Due to the variation of the devices and number of communication protocols in an IoT security relief based on the traditional IT network solutions. In fact, the current security measures which are applied in a conventional network may not be sufficient. Attack vectors as listed by Open Web Application Security Project (OWASP) concern the three layers of an IoT system, which are hardware, communication link and interfaces/services. Hence, the implementation of IoT security mitigation should encompass the security architecture at all IoT layers, as presented in Figure 1. Radio Frequency Identification (RFID) and Wireless Sensor Network (WSN) are considered as part of an IoT network.

In the present internet scenario, enormous number of protocols and technologies are available to address most of the security issues for wireless networks, but still the existing tools have a constraint in applying them in the domain of internet of things (IoT) because of limitations in IoT hardware nodes and WSNs. Another reason is conventional security protocols devour large amounts of memory and computing resources. Also IoT devices usually have to work in harsh, erratic and even intimidating surrounding environments, where they are prone to various security breaches. By 2020, more than 25 billion IoT devices uses the various categories of industries that will be using IoT. Unauthorized access, theft or damage of confidential information, replication of SIM information, imitation of air interface information are the major security issues related to the terminals of sensors in internet of things (IoT). Any security mechanism should be designed to provide confidentiality, Integrity, authentication and non-repudiation. Both IEEE (Institute of Electrical and Electronics Engineers) and IETF(Internet Engineering Task Force) is mainly working towards the design of communication and security issues for communication between IoT and the internet.

III. Secured Iot Architecture

IoT has to ensure the security of all layers. In addition, IoT security should also include the security of entire system crossing the perception layer, network layer, middleware layer and application layer.

Three IOT Layers, Its Operations and Security problems.

There are three layers in the IOT Architecture. That are Perception Layer, Network Layer and Application Layer

MS. U.R. Patil

PRINCIPAL
SNBP College of Arts, Comm., Sci. & Management Studies
Sant Dnyaneshwar Nagar, Morwadi, Pimpri, Pune-18

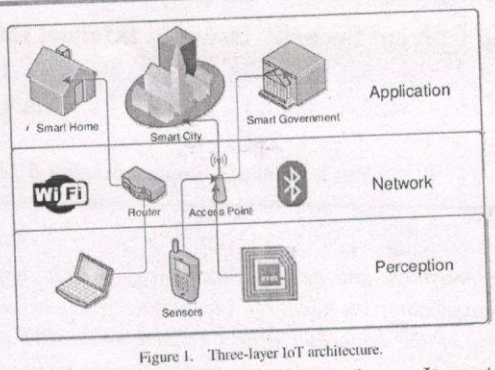

Figure 1. Three-layer IoT architecture.

1. Perception Layer: The perception layer is kwon to be object layer. It contains the sensors and actuators for identifying any particular operations. The main responsibility of perception layer is to digitizing and transferring data to the object abstraction layer through secure channels. The main responsibility of Object layer is to collects the required information from the physical objects and converts that to digital signal and pass it to network layer. The collection of sensors and actuators is the object layer that forms WSN (Wireless Sensor Network).

At physical level the security problem includes the physical security and it supports the sensing devices and security for the collection of information. Due to plain and uncertain protective capability of sensing nodes the security of WSN, RFID and M2M terminal [4] are affected.

WSN:

Security is a challenging thing for WSN as it is not simple task for always watching the sensor nodes but in order to prevent the transmission of data from attackers it must be secured. The WSN security necessities are availability, confidentiality, integrity and authentication and other requirements such as localization, self-organization and data freshness.

In sensor node, the data move from several medium stages so the loss of the data will be more. In such stage the data confidentiality supports encrypted data so that only the receiver can decrypts it to get back the original data. The data received by the receiver should not be get changed by the intruder that is data integrity. The data authentication checked that the data is received from the authenticated node [5]. The data availability to make sure that the data is available even after the attack. At the time of transmitting data using location details of the sinking nodes, the location must be secured otherwise the malicious nodes may control the non-secured data by sending incorrect signal strengths or replaying signals. This is source localization one of the fantastic thing with the security in WSN is self-particular infrastructure for the nodes to be organized and have self-healing property. Data freshness make sure that only the new and fresh data is transmitted and no old data is being transmitted or replayed. The glow can be verifies by including some time related counter.

RFID (radio frequency identification):

It is an automatic technology for identification of objects and human beings. This technology mainly uses RFID tags for exchanging data without manual support. The different attacks and security issues of the tags are:unauthorized tag disabling,unauthorized tag cloning,unauthorized tag tracking and Replay.

2. Network Layer: IoTobserve a number of risks and crises in network layer such as virus attack, destruction, confidentiality, integrity, man-in-the-middle attack. The mostlyregular attack is Dos attack which is affected by enormous requirement of nodes for data transfer. And also sending huge amount of data affected congestion. Some of the security concern at the network layer is detect the authentication, Anti-ddos, Encryption mechanism, communication security. Earlier by-hop encryption mechanism was taken; using this in the transmission strategy the information is encrypted [6]. In occurrence of communication security TLS/SSL or IPsec are used to encrypt the bridge in the transport layer and protect security of network later. Protecting sensors are used to assure the privacy of the humans and objects from the physical world.

3. Application Layer The security needed for several of application environment are different, and one of the characteristics are data sharing [7]. The authority of traffic management is carried by this layer. At this level only the path-based DOS attack was sponsored. Only at this level the service desire by the customer will be supported. For a large scale development of IOT application this layer was very important. It is the top most

layers that found formulas, business logic and UI to user end. The security necessities [2][3] in this layer is authentication and key agreement, privacy protection, security education and management. few of the application layer protocols are CoAP which has a transport UDP and security DTLS, MQTT which has a transport TCP and security TLS/SSL, XMPP which has a transport TCP and security TLS/SSL, RESTFUL which has a transport HTTP and security[9] HTTPS, AMQP which has a transport TCP and security TLS/SSL, Web socket which has a transport TCP and security TLS/SSL, DDS which has a transport TCP/UDP and security TLS/SSL, SMQTT which has a transport TCP and has own security[8]. As technology gets updated every day, android/mobile applications [7] can be linked with IoTs with incorporated and inbuilt security handling techniques in the future.

IV. Encryption Algorithms

The requirement for the lightweight cryptography have been discussed [2], [3], also the lack of the IoT in terms of constrained devices are highlighted. There in reality exist few lightweight cryptography algorithms that does not always effort security-efficiency trade-offs. over the block cipher, stream cipher and hash functions, the block ciphers have shown approximately better performances.

1. ECC (Elliptical Curve cryptography) ECC is a public key cryptography, in this type one key is given for encryption while the other is given for decryption, This algorithm is placed on elliptic curve theory [3]. ECC has a 164-bit key which can fulfil a level of security while the others need 1024 bit key [4] Even with low computing power and battery usage we accept the same level of security and this is frequently used for mobile applications. The main advantage of the ECC algorithm is the key size is very small and storage.

2. mCryptonmCrypton algorithm is developed for small type of devices like RFID tags and sensors. mCrption has 3 key types 64 bits, 96 bits and 128 bits. This serve us in enabling much compress implementation of hardware and software. This is frequentlypredefined as a security block for applications like smart cards, security tokens. In devices with minimum cost RFID tags and sensors it is not possible to execute primitive due to cost constraints. This is developed with extreme efficiency in management of the resource and consumption of power. This algorithm is placed on the architecture of crypton[5]. This has very good flexibility due to variant key sizes [6].

3. AES (Advanced encryption standard) The AES algorithm is predefined for electronic encryption of data. It gives either public or private key. It has variable key length like 128/192/256 bits [6]. Each and every key could encrypt or decrypt a 128 bit data. AES is confirm to be a reliable algorithm. AES given a high security.

V.Conclusion

The invention of the IoT paradigm in the last decade has led to number of threats and attacks against security or privacy of Internet of Things (IoT). In this paper gives a brief idea that as more and more IoT applications are developed, it results in the development of the possibility of surface area for external attacks. There will be security attacks based on the 3 layers of the IoT architecture and discussed them with possible solutions. Also here summarized some encryption methods providing security and their limitations in various layers. In order to hold the IoT technologies and applications, these privacy and security issues and limitations need to be solved and implemented, so that power of IoT technology can be used for constructive applications.

VI. References

1. Mardianabinti Mohamad Noor , Wan Haslina Hassan, "Current research on Internet of Things (IoT) security: A survey", Computer Networks, 27 November 2018 PII: S1389-1286(18)30703-5.
2. R.Nandhini1, Aparna R, P.Srilakshmi," Study on Security issues in Internet of Things", International Conference on IoT 24th August 2018,,pg-no.130-134.
3. TamannaSiddiqui,SaifSaffahBadrAlazzawi," Security of Internet of Things", International Journal of Applied Science-Research and Review ISSN 2394-998, Vol. no.5 pg No.2:8 ,May 31, 2018.
4. "Security in Internet of Things: Issues, Challenges and Solutions",© Springer Nature Switzerland AG 2019 F. Saeed et al. (Eds.): IRICT 2018, AISC 843, pp. 396–405, 2019.
5. Mohammed El-hajj, Ahmad Fadlallah , MarounChamoun and Ahmed Serhrouchni," A Survey of Internet of Things (IoT) Authentication Schemes", 14 April 2019, IEEE 15thStudent Conference on Research and Development (SCOReD), Putrajaya, Malaysia, 13–14 December 2017; pp. 67–71.

6. P.shrilaxmi and R. Aparna, "Cryptography in Network Security, A much Needed",Journal Of Advance Research In Computer Science, volume 9, Special issue no 1, February 2018.
7. Noshina Tariq , Muhammad Asim , Feras Al-Obeidat , Muhammad ZubairFarooqi,Thar Baker, Mohammad Hammoudeh and Ibrahim Ghafir,"The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey", Published: 14 April 2019.
8. Jun Zhou, Zhenfu Cao, Xiaolei Dong, and Athanasios V. Vasilakos,"Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions". IEEE Communications Magazine • January 2017,pg no.26-32 © 2017 IEEE.
9. Rwan Mahmoud, TasneemYousuf, FadiAloul, Imran Zualkernan ,"Internet of things (IoT) security: Current status, challenges and prospective measures",**10th International Conference for Internet Technology and Secured Transactions (ICITST),@2016 IEEE.**