Engineering and Technology Journal for Research and Innovation (ETJRI)

ISSN 2581-8678, Volume II, Issue I

Security Challenges and Solutions in Industrial Internet of Things Environment

Girraj Kumar Verma

Department of Mathematics, Amity School of Engineering and Technology, Amity University Madhya Pradesh, Maharajpura Dang, Gwalior, India 47400, gkverma@gwa.amity.edu

Abstract- **The transition of industrial processes from Industry 3.0 to Industry 4.0 has inspired the technological revolution of wireless sensor networks. This revolution has created the concept of Internet of Things. The paradigm of Industry 4.0 is developed on the base of Internet of Things and jointly called Industrial Internet of Things. In this era of technology, the smart devices such as sensors, actuators, smart phones, etc. are connected through internet. These smart devices are the peer point to manage communication in Industrial Internet of Things environment. However, the wireless communication of data is highly sensitive to security threats. Therefore, this article reviews some major security related issues and discusses some efficient and strong solutions.**

Keywords- **Industry 4.0, Authentication, Internet of Things, Digital Signature.**

I. INTRODUCTION

Recently, the deployment of smart devices along with high speed networks usage has increased the popularity of internet of things (IoT). Thanks to Ashton, who coined the paradigm of IoT in 2009 [1]. It can be viewed as a network architecture comprising of sensors and actuators based embedded devices (or things) which can perform the task of sensing, data collection, and processing as per the requirements in the environment where these are deployed. These things communicate to human or machines by using public or private channels. Thus, the communication can be among things-to-things, things-to-human and human-to-thing [2]. For instance, e-health services, weather monitoring, border monitoring, sensing of farming conditions, etc. (Figure-1) are some social applications where the deployed sensors collect and transmit their data to the local or global aggregators at different time intervals [3], [4].

There are several industrial applications which are emerged from IoT and this paradigm is called as industrial internet of things (IIoT). For instance, in the manufacturing units, control units, etc., sensors can be deployed to monitor temperature, electric intensity, etc. and logistic services which also use IoT to optimize transportation complexity. In IIoT environment, advanced cyber-physical systems (CPS) are used and these systems are an integration of emerging communication technology and computation with storage units; such as cloud computing and mobile computing, machine learning, artificial intelligence based controllers, etc. This technical revolution of industrial systems using CPS is called as industry 4.0, i.e., fourth industrial revolution [5].

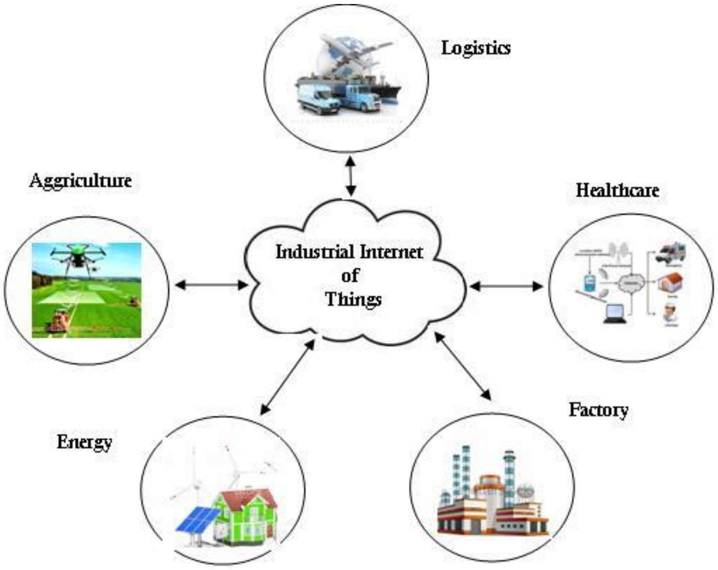

Fig 1: Applications of IIoT

In general, CPS inspires e-health monitoring, remote diagnosis, remote control of production, mitigation of complexity of supply chains, smart vehicles, smart devices (mobile phones or smart watch), smart transportation services, development of smart factories, etc. The smart products in a smart factory can be analyzed to know their history, identity, specification, documentation. These smart products can control the production process in the factory as well. These smart products are having information sensing devices with database at the backend. Thus, they collect and store data by themselves in the environment where these are deployed.

In the IIoT environment, workers use their smart devices to perform various industrial operations. In such an environment, crowd sourcing is used to retrieve the data from various sensors and actuators. The crowd-sourcing mitigate data management overhead between workers and data servers. In IIoT environment, crowd-sourced data entice the collaboration and optimizes the cost by using cloud-centric server. Thus, cloud-centric server analyzes the crowd-sourced data obtained from IIoT. In this system, several embedded or smart devices collect data from IIoT environment and send it to cloud server using the Internet. At the server end, it is needed that the data should be authentic. The authenticity and integrity of data is required for server’s security. Thus, authentication is required prior to data storage to the cloud server [2].

II. SECURITY CHALLENGES IN IIOT ENVIRONMENT

Due to the development of sensors and actuators, significant deployment of these devices in various applications has emerged. This emerging deployment in industrial applications has inspired the innovative concept of IIoT. However, the dependency on wireless networks has also a big challenge regarding security threats. To discuss these challenges, Sadeghi et al. [5] has proposed several security related issues for IIoT environment. They described that the security in IIoT environment has the same impact as traditional safety. The difference is that the security in IIoT is considered against cyber threats. In IIoT environment, the source shares the data via cloud centric network and thus, the authentication and integrity are important issues. Sadeghi et al. [5] suggested that the attestation of data can solve the issue. Thus, method of digital signing can be a good choice to execute the attestation of data.

Besides the authentication, confidentiality and data modification are other issues. To solve these issues, encryption or block chains can be used.

III. SOLUTION TO SECURITY CHALLENGES IN IIoT ENVIRONMENT

Based on the discussion, the authentication of the source and the data can be provided by method of attestation. In cryptography, method of digital signing is a good choice to achieve authentication. To provide confidentiality, encryption algorithms are good choices. The digital signature and encryption algorithms are based on public key cryptography (PKC). In PKC, each user has a (public key, secret key) pair. To execute encryption, sender uses the public key of receiver and finds the corresponding ciphertext (modified message). To execute signing, sender uses its secret key on the cipher text and obtains a signature. These two techniques can simultaneously be used to achieve authentication and confidentiality. The combination of these techniques is called sign cryption. At the receiving end, to find original message from ciphertext, receiver uses its secret key and to check the authentication, the public key of sender is used to verify corresponding signature. If the sender has used sign cryption, then receiver uses both keys (its secret key and sender’s public key) simultaneously to find and check authentication of the message.

Today, block chains are also used to provide authentication. However, the confidentiality cannot be achieved using this concept. The block chains are similar to a distributed ledger available publicly on cloud. These are designed by making a series of data blocks connected to each other. They are linked in such a manner that every last block depends on its ancestor. However, the internal structure of every block uses several networking technologies and one of these technologies is digital signature scheme.

Summarily, digital signature algorithms and encryption algorithms are the key ingredients of a security mechanism for IIoT environment.

IV. CONCLUSION

Recent deployment of smart devices to industrial processes has motivated the development of IIoT environment. However, being wireless communication the security threats against authentication, integrity, confidentiality, etc. are serious concerns. This article presented a review on such security threats and discussed the solutions as well. It is observed that cryptographic primitives such as digital signatures, encryption techniques and block chains are the most appealing technology to protect IIoT environment.

REFERENCES

[1] K. Ashton et al., “The internet of things,” RFID journal, vol. 22, no. 7, pp. 97–114, 2009.

[2] A. Karati, S. H. Islam, and M. Karuppiah, “Provably secure and lightweight certificate less signature scheme for iiot environments,” IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3701–3711, 2018.

[3] M. A. Khan and K. Salah, “Iot security: Review, blockchain solutions, and open challenges,” Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.

[4] G. K. Verma, B. B. Singh, and H. Singh, “Bandwidth efficient designated verifier proxy signature scheme for healthcare wireless sensor networks,” Ad Hoc Networks, vol. 81, pp. 100–108, 2018.

[5] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, “Security and privacy challenges in industrial internet of things,” in Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, 2015, pp. 1 6.