




## AN EMPIRICAL INVESTIGATION OF SECURING INTERNET OF THINGS DATA IN WIRELESS SENSOR NETWORK



 S.K.B. Sangeetha

Department of CSE, RMK College of Engineering and Technology, Chennai, India.

Email: [skbsangeetha@gmail.com](mailto:skbsangeetha@gmail.com)



### ABSTRACT

#### Article History

Received: 31 May 2019

Revised: 11 July 2019

Accepted: 13 August 2019

Published: 23 September 2019

#### Keywords

Internet of things  
Data security  
Wireless sensor network  
Authentication  
Smart systems  
Node security  
Crypto algorithms.

Internet of things (IoT) is an emerging technology which can interconnect low-cost and on-demand processing resources and enabling them for transmission. They are becoming viable solutions to many challenging problems such as in environmental monitoring, business, and military applications. However, deploying without security in mind has often proved to be unreasonably dangerous. This also applies to wireless sensor network (WSN) that monitor sensitive information. The development of WSN consists of sensors to monitor IoT devices. Even the IoT technology offers a variety of services, security issues concern with devices and customers is a major problem. To handle such sensitive situations and to ensure proper data security, wireless sensor network come up with the extensive use of various methods that can bring unique security concern for customers and also provide methods to prevent various possible security attacks. For this paper, huge potential efforts are made to analyze various data security methods of IoT technology in wireless sensor networks by providing as much information possible and quantifying what the tradeoffs will be.

**Contribution/ Originality:** This study contributes to the existing literature by analyzing various data security methods by providing as much information possible and quantifying what the tradeoffs will be. The available security methods have advantages and drawbacks, and many have overlapping uses. With the realistic account of all challenges and opportunities of adopting security methods in wireless sensor network from engineering perspectives, requires better analysis of categories. So better analysis of challenging directions are presented in detail.

### 1. INTRODUCTION

Today, smart systems are infrastructure based systems to connect people in a better way. The common vision of smart systems is usually associated with the internet of things (IoT) through the use of sensors to collect information through intelligent monitoring in embedded devices. In general, devices are interconnected for transmitting data in distributed sensor networks. A wireless sensor network (WSN) is formed with a large number of sensor nodes to detect activities to build information to improve the performance of infrastructure systems. WSNs become the key technology for IoT with the rapid development of technology.

In recent years, this rapid development of WSNs in the IoT makes security issues that need to be solved over time. Data brokers are doing a wide variety of businesses with the availability of information from various IoT sources that can cause the security breach of individual user's privacy. Additionally, with the development of technology, machines can make autonomous decisions that also cause an impact on the function of the environment. For example, a machine can notify the legal authorities if it was used against the law. Figure 1 depicts the integration of IoT with wireless sensor network.

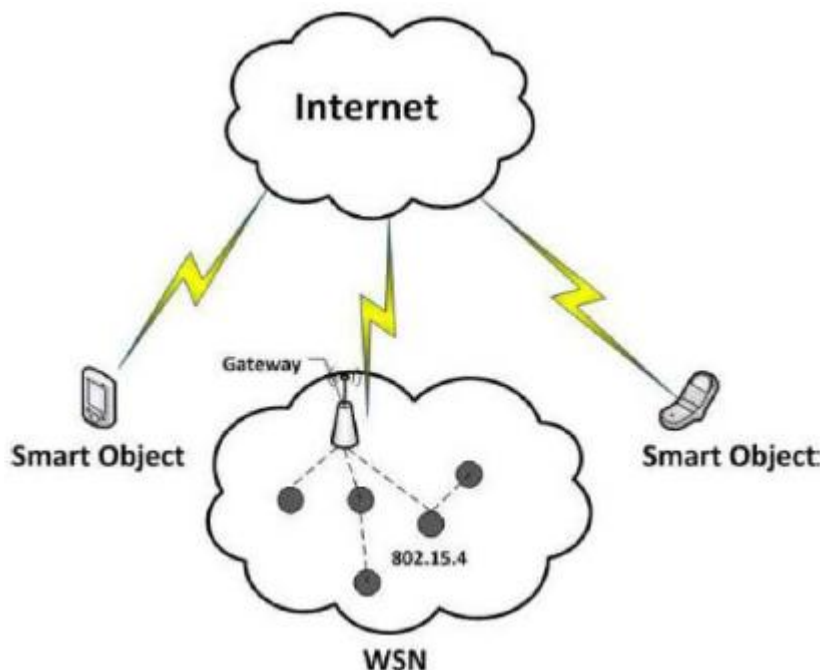


Figure-1. Integration of IoT with WSN.

When machines and technologies are becoming powerful, the individual privacy and security become more difficult to handle and makes the complex chain where the security has been created as infinite and the weakest link. Using IPv6, there are enough IP addresses used to predict the billions of data points that are secured to ensure individual privacy rights and from malicious attacks. In traditional TCP/IP networks, security used to protect data confidentiality, integrity, and availability. The available security methods make a reliable system from malicious attacks and protect from malfunctioning and information disclosure. Based on the environment of node and application, the security of WSN not only depends on traditional methods of security but also requires further methods to provide trust, security, and privacy (TSP) WSNs [1].

Further, this paper could be enhanced by broadly discussing the solutions to security issues. The security of data in WSN and the study of data in the cloud with the aspects related to it concerning security is discussed.

The main contribution of this paper is:

1. Various standard approaches of data security methods are discussed.
2. Survey related to security methods of WSN is described clearly.
3. Challenging directions of data security methods are discussed in detail.

The above-said points clearly distinguish this survey from other recent surveys. It gives the detail as broad as earlier works. The paper is organized as follows: Section II reviews data security in the WSN. Section III discusses possible future directions. Section IV summarizes the current work.

## 2. BACKGROUND AND RELATED WORK

WSNs always depends on the application scenario of IoT in which an application always requires to provide integrity, availability, confidentiality, non-repudiation, and user privacy. And also, the application has to maintain system integrity, reliability by protecting the system from malicious attacks. WSNs must provide methods to protect the nodes against tampering and also the routing in the communication channel of network layer. WSN also requires methods to detect attacks and to provide message authentication, encryption, access control, identity authentication, etc. The security methods of WSNs in IoT technology may be categorized as follows: node security, crypto algorithms, key management, secure routing, and data aggregation.

### 2.1. Node Security

A node of a WSN may be tampered with direct physical attacks or the communicated data may be relocated without authorization, or stolen in IoT devices. Node security must contain wakeup and bootstrapping in a secure manner to prevent the communication devices in IoT technology. Denial of service attacks called sleep deprivation attacks that prevent the sensor node from going to the power-saving sleep mode and reduces the lifetime of an attacked sensor node. Standard security mechanisms such as message authentication codes or frame encryption will not prevent sleep deprivation attacks because when battery power has already been spent, the attack can only be noticed. The wake-up radio used to listen on the channel when the sensor node is in sleep state and triggers the sensor wake up. To add security in IoT devices, the wake-up signal is encoded and used only once for each node [2].

### 2.2. Crypto Algorithms

Encryption is a security method to change the original information of the data sensor node and makes an unauthorized user not recognize the original information. The WSNs of public infrastructure has traditional message authentication code, symmetric encryption and public-key encryption. So an encryption system for IoT technology has to ensure the data security in wireless sensor devices. Crypto libraries are designed for different encryption mechanism at data link layer, network layer and application layer [3].

### 2.3. Key Management

In general, key management includes key generation, distribution, verification, update, storage, backup, valid and destroy. The security mechanisms, such as secure routing, secure positioning, data aggregation being used for securing IoT devices in WSNs. Typical key management schemes for providing such security in WSNs include managing global key, random key, location key, clustering key and public key. But, the join key is established during the secure bootstrapping and the choice of an appropriate bootstrapping depends on the environment of the sensor network. The appropriate bootstrapping procedure depends to a high degree on the application and several different bootstrapping procedures are available such as token based, pre configuration of the keys, physical protection of messages, in-band, and out-of-band communication [4].

### 2.4. Secure Routing

Since WSNs is self organization in networking and using multi-hop in data transfer, each node requires routing discovery, routing establishment and routing maintenance. Secure routing protocol is a prerequisite for data aggregation and redundancy elimination from a source node to a sink node. In general, secure routing networks can be divided based on network structure into three categories such as flat-based routing, hierarchical based routing, and location-based routing. Typical methods include feedback information, location information, encryption algorithm, multipath selection method and hierarchical structures. Along with, different secure routing protocols for IoT devices can solve different types of attacks such as false routing information, cesspool attack and wormhole.

Traditional secure routing protocols are suitable for static sensor networks, new secure routing protocols are needed to be developed for dynamic IoT based sensor nodes [5].

### 2.5. Secure Data Aggregation

Secure data aggregation is to provide reliable data and securely transmit them to the higher aggregation nodes to judge the credibility of data. Each aggregation node selects the reliable hop and transmits the data to the central node in which central node do the final aggregation calculation. Now secure data aggregation provides authentication and encryption to realize secure transmission schemes in IoT devices [6].

## 3. CHALLENGES OF DATA SECURITY IN IOT

IoT is characterized by a wide range of challenges in the context of the current internet but its scale is much larger and the security is even more challenge. Examples for such challenges are: range of use-case domains, difference in business models, ownership and tenancy, range of objects covered, time scales, and reliability. While the current internet depends businesses and organizations that will increase in scope due to IoT. So, new application fields such as life-stock monitoring, monitoring interest groups; traffic monitoring etc, by information and communication technologies will increase. While business IT made it possible with flows of products and RFID penetrated across organizational units, security becomes a challenge. The proliferation of IoT becomes a sizable part of the future internet. The exclusive ownership and exclusive usage of the IoT will be different and will not necessarily be owned by one group. Also, more than one organization will operate in the same system which will need remote access to the production IoT system. IoT will span from microscopic and even submicroscopic entities to macroscopic objects makes more complicated system of security.

IoT will be applied to real-time control with high reliability and might be conducted in a quasi-offline manner over time that will lead to very diverse problems IoT systems will have to solve. Specifically, security system in WSN has to address the performance of the entire IoT systems with qualitative requirements. Note that this is not an entirely novel problem in IoT due to the huge range of domains covered. Next to endangered interoperability providing security from one domain to another becomes a major challenge especially in wireless sensor network. The challenges are available not only in providing security of data but also in the policies and technologies. Uncertainty about the advantages of wireless sensor network makes various concerns about the security of IoT. Major security incidents are reduced in organizations using IoT technology and 95% of security failures occur in customer side. Since, security requirements increased physical access to data centers are strictly limited and goes through potential procedure for biometric scanning. The future of data security in IoT is promising with a major opportunity towards technical improvement for the companies and it will support faster and effective services than it is today [7].

## 4. CONCLUSION

Data security in the area of IoT is an active area of research and experimentation. To provide the level of security based on the importance of data and classification of data, the security scheme should consider the level of security includes confidentiality, encryption, integrity, and storage, etc. that are selected based on the type of data. To provide a secure environment for the execution of the IoT devices along with overall security considerations is a major challenge. A secure and trusted solution for accessing data in the wireless sensor network is the requirement that needs to be focused and addressed by the cloud computing infrastructure. This paper summarizes data security methods of IoT technologies in wireless sensor networks.

**Funding:** This study received no specific financial support.

**Competing Interests:** The author declares that there are no conflicts of interests regarding the publication of this paper.

## REFERENCES

- [1] M. Benfilali and A. Gafour, "A survey of wireless sensor network security in the context of internet of things" 2017," in *4th International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, 2017.
- [2] C. Gianfranco, M. Giovanni, P. Gaetano, R. Bruno, and S. Luigi, *IoT and sensor networks security. In security and resilience in intelligent data-centric systems and communication networks*: Academic Press, 2018.
- [3] U. Muhammad, A. Irfan, A. Imran, M. K. Shujaat, and A. S. Usman, "SIT: A lightweight encryption algorithm for secure internet of things," *International Journal of Advanced Computer Science and Applications*, vol. 8, pp. 1-10, 2017.
- [4] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the internet of things," *Computers & Electrical Engineering*, vol. 37, pp. 147-159, 2011. Available at: <https://doi.org/10.1016/j.compeleceng.2011.01.009>.
- [5] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," *Journal of Network and Computer Applications*, vol. 66, pp. 198-213, 2016.
- [6] A. Ahmed, A. Mesfar, A. Abdullah, S. A. Sultan, Al Ghamdi, and H. Rami, "Secure data aggregation scheme in wireless sensor networks for IoT," in *International Symposium on Networks, Computers and Communications (ISNCC)*, 2016.
- [7] T. Mamatha and S. Srivastava, "Issues and challenges in the integration of wireless sensor network and IOT," *International Journal of Computer Applications*, vol. 146, pp. 7-10, 2016. Available at: <https://doi.org/10.5120/ijca2016910852>.

*Views and opinions expressed in this article are the views and opinions of the author(s), Journal of Asian Scientific Research shall not be responsible or answerable for any loss, damage or liability etc. caused in relation to/arising out of the use of the content.*