© 2018 IJSRSET | Volume 4 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
National Conference on Advanced Research Trends in Information and
g Technologies (NCARTICT-2018), Department of IT, L. D. College of Engineering,
Ahmedabad, Gujarat, India. In association with
International Journal of Scientific Research in Science, Engineering and Technology

RFID based Security in Internet of Things: A Study

Thomson Christain*[1], Lalit Sengunthar[2], Oneel Christian[3], Urja Mankad[4]
*[1]PG Scholar, L. J. Institute of Computer Applications, Ahmedabad, Gujarat, India
[2]PG Scholar, L. J. Institute of Computer Applications, Ahmedabad, Gujarat, India
[3]PG Scholar, L. J. Institute of Computer Applications, Ahmedabad, Gujarat, India
[4]Assistant Professor, L. J. Institute of Computer Applications, Ahmedabad, Gujarat, India

ABSTRACT

The Internet of Things (IoT) provides connectivity for everything and everyone. The IoT can be considered as the future evaluation of the Internet that realizes machine to machine (M2M) learning. Security and privacy are the main issues for IoT applications and facing some enormous challenges. This paper analyses the security architecture and security requirements of IoT as a whole and privacy protection, trust management is being discussed with the help of RFID which is explained in detail with all its consequences and also shown its application in different areas.

Keywords: Internet of Things (IoT), Security, Radio Frequency Identification (RFID), machine to machine (M2M).

I. INTRODUCTION

Internet of Things (IoT) is an ecosystem of connected physical device that are accessible through the internet, i.e. objects that have been assigned an IP address and have the ability to collect and transfer data over a network with automatic assistance or intervention. Nowadays, IoT is widely applied to social life applications such as smart grid, intelligent transportation, smart security, and smart home [1]. The IoT is considered as the future evaluation of the Internet that realizes machine-to-machine (M2M) learning [2]. The basic idea of IoT is to allow autonomous and secure connection and exchange of data between real world devices and applications [3]. The IoT links real life and physical activities with the virtual world [4]. The numbers of Internet connected devices are increasing at the rapid rate. These devices include personal computers, laptops, tablets, smart phones, PDAs and other hand-held embedded devices. Most of the mobile devices embed different sensors and actuators that can sense, perform computation, take intelligent decisions and transmit useful collected information over the Internet [5]. Using a network of such devices with different sensors can give birth to enormous amazing applications and services that can bring significant personal, professional and economic benefits [6]. The IoT consists of objects, sensor devices, communication infrastructure, computational and processing unit that may be placed on cloud, decision making and action invoking system [7]. The objects have certain unique features and are uniquely identifiable and accessible to the Internet. These physical objects are equipped with Radio-Frequency Identification (RFID) tags or other identification bar-codes that can be sensed by the smart sensor devices [6]. The IoT is a hot research topic that is getting increasing popularity for academia, industry as well as government. Many European and American organizations and multinational companies are involved in the design and development of IoT to achieve different type of useful and powerful automated services [1].

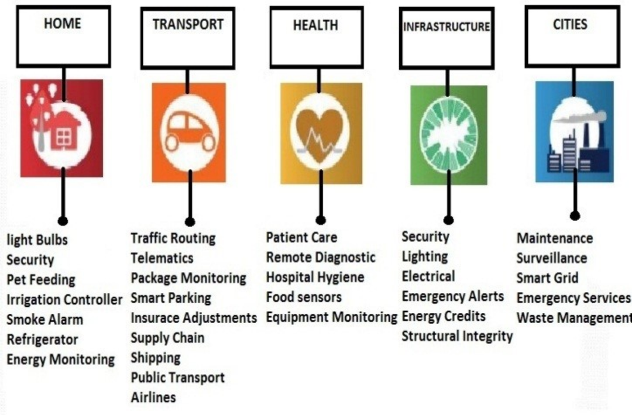

Figure 1. Applications of IoT [27]

Smart city, smart energy, smart transportation, smart health, smart agriculture, and many more areas of IoT are generating curiosity among world's population as shown in the figure 1. Smart surveillance, automated driving, smarter electricity management systems, urban security and environmental monitoring all are examples of internet of things applications for smart cities [28].

RFID

Radio frequency identification system (RFID) is an automatic technology and aids machines or computers to identity objects, record metadata or control individual target through radio waves. The RFID technology was first appeared in 1945, as an espionage tool for the Soviet Union. Main advantage of the RFID is the automated identification and data capture that promises wholesale changes across a broad spectrum of business activities and aims to reduce the cost of the already used systems such as bar codes [10].

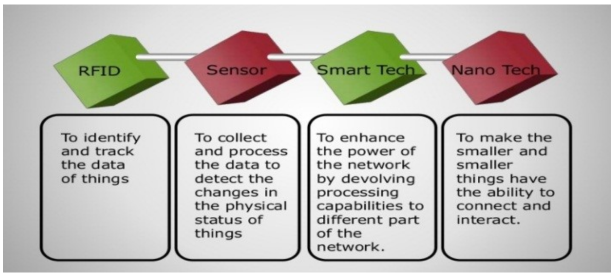
RFID
Sensor
Smart Tech
Nano Tech
To identify and track the data of things
To collect and process the data to detect the changes in the physical status of things
To enhance the power of the network by devolving processing capabilities to different part of the network.
To make the smaller and smaller things have the ability to connect and interact.

Figure 2. Perceptual Layer Devices [15]

The IoT can be viewed as a huge network consisting of networks of devices as shown in the figure 2 and computers connected through a series of intermediate technologies where numerous technology like RFID's, wireless connections may act as enablers of this connectivity [8].

1) Tagging Things: RFID trace and addresses the real-time item.
2) Feeling Things: Sensors collects data from the environment
3) Shrinking Things: Miniaturization and Nanotechnology has provoked the ability of smaller things to interact and connect within the smart devices or "things".
4) Thinking Things: Embedded intelligence in devices thorough sensors has formed the network connection to the Internet.

This paper will cover the security architecture of IoT (section II), security requirements in IoT in context of RFID (section III) and conclusion (section IV).

II. SECURITY ARCHITECTURE OF IoT

In general, the IoT can be divided into four key levels [9]. Figure 3 shows that the level architecture of the IoT [34].

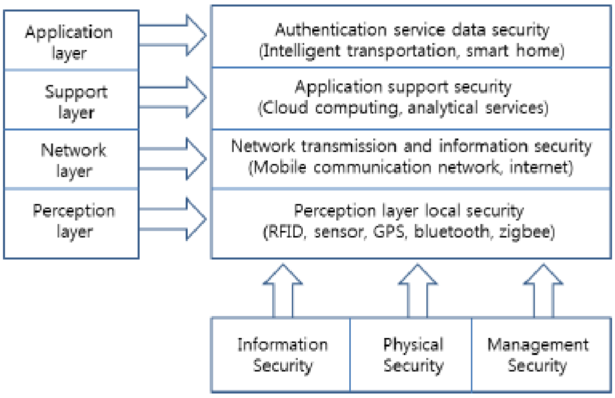
Application layer
Support layer
Network layer
Perception layer
Authentication service data security
(Intelligent transportation, smart home)
Application support security
(Cloud computing, analytical services)
Network transmission and information security
(Mobile communication network, internet)
Perception layer local security
(RFID, sensor, GPS, bluetooth, zigbee)
Information Security
Physical Security
Management Security

Figure 3. Layered Architecture of IoT

A. Perceptual Layer: The most fundamental level is the perceptual layer (otherwise called recognition layer), which gathers a wide range of data through physical gear and distinguishes the physical world, the data incorporates object properties, environmental condition and so on; and physical equipment incorporate RFID per user, a wide range of sensors, GPS and different types of equipment. The key segment in this layer is sensors for catching and representing the physical world in the digital world.

B. Network Layer: The second level is network layer. Network layer is responsible for the transmission of information from perceptual layer, classification, initial processing of information and polymerization. In this layer the information transmission is depend on several basic networks, which are the International Conference on Computer Science and Electronics Engineering. Internet, satellite nets, wireless network, mobile communication network, network infrastructure and communication protocols are also essential to the information exchange between devices.

C. Support Layer: The third level is support layer. Support layer will set up a reliable platform for the application layer, on this platform all kind of intelligent computing powers will be organized through cloud computing and network grid. It plays the role of combining application layer upward and network layer downward.

D. Application Layer: The application layer is the topmost and terminal level. Application layer provides the personalized services according to the user's requirements. Users can access to the internet of thing through the application layer interface using of personal computer, television, or mobile equipment and so on. Management and network security play an important role in above each level.

III. SECURITY REQUIREMENTS

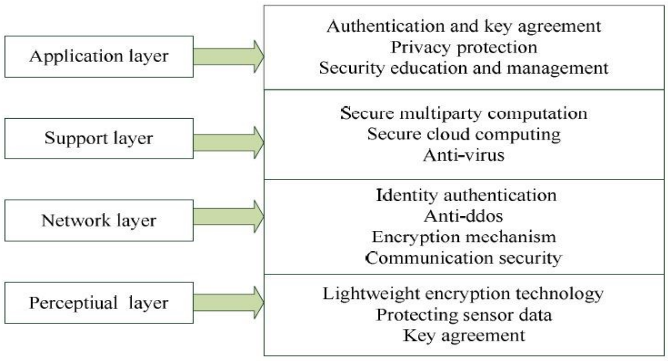

Figure 4. Security requirements in each level [34]

We can summarize the security requirements for each level in the following layers, as shown in Figure 4.

A. Perceptual Layer: At first node authentication is necessary to prevent illegal node access, secondly to protect the confidentiality of information transmission between the nodes, before the data encryption key agreement is an important process in advance and data encryption is absolute necessity. The stronger are the safety measures the more is consumption of resources to solve this problem lightweight encryption technology becomes important, which includes Lightweight cryptographic algorithm and lightweight cryptographic protocol. At the same time the authenticity and integrity of sensor data is becoming research focus.

B. Network Layer: In this layer existing communication security mechanisms are difficult to be applied. Identity authentication is a kind of mechanism to prevent the illegal nodes, confidentiality and internality are of equal importance, and thus we also need to establish internality mechanism and data confidentiality. Besides distributed denial of service (DDoS) in the network and is particularly severe in the internet of thing, it is necessary to prevent the DDoS attack for the vulnerable node is another problem to be solved in this layer [14].

C. Support Layer: Support layer needs a lot of the application security architecture such as secure multiparty computation and cloud computing, almost all of the strong encryption algorithm and stronger system security technology, anti-virus and encryption protocol.

D. Application Layer: To solve the security problem of application layer, we need two aspects. One is the authentication and key agreement across the heterogeneous network, the other is user's privacy protection. In addition, education and management are very important to information security, especially password management [25].

A. RFID Components For IoT

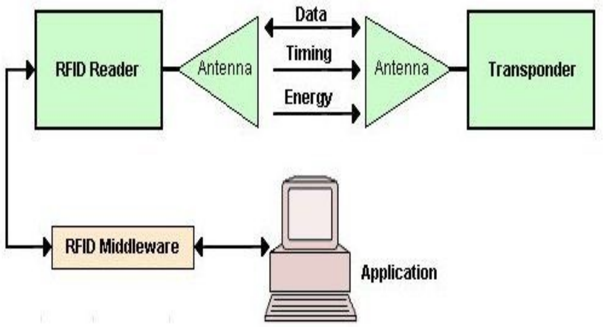

Figure 5. Components of IoT system [26]

RFID consist of different components like tags, readers and application, as shown in Fig. 5.

1. Transponder/Tags (transmitters/responders): The tag is a microchip connected with an antenna, which can be attached to an object as the identifier of the object.
2. Readers (transmitters/receivers): The RFID reader communicates with the RFID tag using radio waves.
3. Application system

B. SECURITY ISSUES OF RFID TECHNOLOGY AND SOLUTIONS

RFID (Radio Frequency Identification) is a non-contact automatic identification technology, which can automatically identify the target tag signal to obtain relevant data, identifying the process does not require manual intervention, and can work in harsh environments [11][38]. While RFID is widely used, it exposes a lot of problems as follows [36]

a. Uniform coding currently there is no uniform International encoding standard for RFID tag. The EPC (Electronic Product Code) standard supported by European and The most influential standards are the UID (Universal Identification) standards supported by Japan. It may cause problems that errors may occur in the reading process or the reader cannot obtain access to the tag information.

b. Conflict collision as multiple RFID tags may also transmit data information to the reader at the same time, which may cause the reader not able to get data correctly [12]. Using the anti-collision technique can prevent multiple tags from transmitting information to the reader simultaneously. RFID conflict collision can be divided into two categories: tags' collision and readers' collision [15]. When a large number of labels are in the reader's working scope, and the reader cannot access to data correctly, this is called tags' collision. IoT requires wide range of RFID sensor coverage, and multiple readers' cooperative work is particularly important, but the working scope of reader overlaps. So information may become redundant which increases the burden on the transmission of network. This is called readers' collision. Different collisions have different solutions. Currently, tag anti-collision algorithm has been studied adequately, but research for reader anti-collision algorithm is not enough. Reader anti-collision algorithm is mainly divided into solutions based on the scope-based and time-base solutions [16, 17]. The main idea of the scope-based anti-collision algorithm is to try to avoid overlapping of reader work scope to achieve the purpose of reducing the conflict zone, but this solution requires an additional central control area to calculate the working scope between the readers, which increases the complexity and cost [18].

C. RFID PRIVACY PROTECTION

Low cost tags led to RFID's limited resources, such as weak computational capabilities and low storage capacity, thus it requires lightweight solutions for privacy protection, which includes location privacy and data privacy.

a. Data Privacy: RFID security and privacy technologies can be divided into two categories: physical-based schemes and password-based schemes, the former sends deactivation kill command, block tags, signal interference etc. The later includes schemes such as hash locks [19], random hash lock [20], anonymous ID [21], re-encryption [22]. Different organization styles for IoT require different ways of privacy protection agreement. A compromise solution for data privacy issues is to store less important information in RFID tag, and store important information in the up level service.

b. Location privacy: Although RFID tags do not store important information, but hackers can still get the tag ID information for the purpose of tracking the position of the tag [23]. For example, when a reader equipped with vehicle GNSS information reads a tag's information, it can easily obtain the approximate location information of the tag according to its effective operational range.

D. TRUST MANAGEMENT

Trust management in IoT, we must take node privacy more seriously. So we need to introduce trust management into IoT RFID system. Trust management exists not only just between the RFID tags and readers, but also between the base stations and the readers. In trust management field digital signature technology is of great usage. It has been used for device authentication, data authentication and data exchange between different applications for a long time. Protocols and cryptographic algorithms play important roles for digital signature technology. While standard cryptographic algorithms and protocols require storage space and computing resources more than the available resources of RFID tags, so RFID authentication algorithm must not only take into account security and privacy issues, but also consider the tag storage and computing power. Limited resources of RFID tags would be the focus of ongoing research and complexity of security. Above all, uniform encoding, conflict collision, privacy protection and trust management are four typical technologies for the security issues of RFID. With uniform encoding standard, we encode tag information uniformly, which can maximize information exchange. With a good conflict collision resolution technology, minimize potential data interference and we can make RFID readers read information correctly. With a good lightweight data privacy protection, we have helped protect data privacy and location privacy. Finally, with appropriate trust management algorithms, we can enable trust management for reader's/ RFID tags, base stations and readers [14].

.

IV.CONCLUSION

We have focused on the security architecture and security requirements of IoT, We concisely reviewed security in the IoT and requirements from four layers' perceptual layer, network layer, support layer and application layer. For perceptual layer RFID technology is of great importance, we analyzed the security issues of RFID technologies and their corresponding solutions including: Uniform Coding, Conflict Collision, RFID Privacy Protection, and Trust Management. This paper will help to analyse the IoT major security issues for research and development.

V. REFERENCES

[1] Sundmaeker, H., Guillemin, P., Friess, P., &Woelffle´, S. (2010). Vision and challenges for realising the internet of things.Cluster of European Research Projects on the Internet of Things—CERP IoT.

[2] Y. Huang and G. Li, “Descriptive Models for Internet of Things,” in IEEE International Conference on Intelligent Control and Information Processing (ICICIP), August 2010.

[3] T. Fan and Y. Chen, “A Scheme of Data Management in the Internet of Things,” in 2nd IEEE International Conference on Network Infrastructure and Digital Content, Sept. 2010.

[4] Y. Huang and G. Li, “A Semantic Analysis for Internet of Things,” in International Conference on Intelligent Computation Technology and Automation (ICICTA), May 2010.

[5] Q. Zhou and J. Zhang, “Research Prospect of Internet of Things Geography,” in 19th International Conference on Geoinformatics, June 2011.

[6] J. Li, Z. Huang, and X. Wang, “Countermeasure Research about Developing Internet of Things Economy,” in International Conference on E - Business and E -Government (ICEE), May 2011.

[7] Y. Yu, J. Wang, and G. Zhou, “The Exploration in the Education of Professionals in Applied Internet of Things Engineering,” in 4th International Conference on Distance Learning and Education (ICDLE), October 2010.

[8] https://www.slideshare.net/MohanKumarG/internetofthings-iot-aseminar-ppt-by-mohankumarg

[9] G. Yang, J. Xu, W. Chen, Z. H. Qi, and H. Y. Wang, “Security characteristic and technology in the internet of things,” Journal of Nanjing University of Posts and Telecommunications (Natural Science), vol. 30, no. 4, Aug 2010.

[10] https://www.slideshare.net/swethak36/iot-rfid-finalppt

[11] Hu, F., & Wang, F. (2010). Study of recent development about privacy and security of the internet of things. In Proceedings of the international conference on web information systems and mining (pp. 91–95).

[12] Lv, B. Y., Pan, J. X., Ma, Q., & Xiao, Z. H. (2008). Research progress and application of RFID anti-collision algorithm. In Proceedings of the international conference on telecommunication engineering (vo1. 48, no. 7, pp. 124–128).

[13] http://assets.devx.com/articlefigs/15504.jpg

[14] https://www.researchgate.net/profile/Jiafu_Wan2/publication/254029342_Security_in_the_Internet_of_Things_A_Review/links/550b9adf0cf290bdc111f796/Security-in-the-Internet-of-Things-A-Review.pdf

[15] Finkenzeller, K. (2003). RFID handbook fundamentals and applications in contactless smart cards and identification (2ndEd.). West Sussex: Wiley.

[16] Wang, D., Wang, J. W., & Zhao, Y. P. (2006). A novel solution to the reader collision problem in RFID system. In Proceedingof the IEEE wireless communications, networking and mobile computing (WiCOM 06) (pp. 1–4).

[17] Song, I. C., Hong, S. H., & Chang, K. H. (2009). An improved reader anti-collision algorithm based on pulse protocol with lotoccupied probability in dense reader mode. In Proceeding of the IEEE 69th vehicular technology conference (pp. 1–5).

[18] Kim, J., Lee, W., Yu, J., Myung, J., Kim, E., & Lee, C. (2005). Effect of localized optimal clustering for reader anti-collision inRFID networks: Fairness aspects to the readers. In Proceeding of the IEEE international conference on computer communications and networks (pp. 497–502).

[19] Juels, A., Rivest, R. L., &Szydlo, M. (2003). The blocker tag: Selective blocking of RFID tags for consumer privacy. In Proceedings of the 10th ACM conference on computer and communications security (CCS 2003), (pp. 103–111).

[20] Ohkubo, M., Suzuki, K., & Kinoshita, S. (2003). Cryptographic approach to privacy- friendly tags. RFID privacy workshop (p.82). Cambridge, MA: MIT.

[21] Duels, A., Pappu, R., & Euros, S. (2003). Privacy protection RFID-enabled banknotes. In Proceedings of seventh internationalfinancial cryptography conference (pp. 103–121).

[22] T2TIT Research Group. (2006). The T2TIT—Thing to thing in the internet of things-project. ANR.

[23] Lakafosis, V., Traille, A., & Lee, H. (2011). RFID-CoA: The RFID tags as certificates of authenticity. In Proceedings of theIEEE international conference on RFID (pp. 207–214).

[24] https://www.slideshare.net/indravi/will-internet-of-things-iot-be-secure-enough

[25] Hachem, S., Teixeira, T., &Issarny, V. (2011). Ontologies for the internet of things (pp. 1–6). New York: ACM.

[26] https://image.slidesharecdn.com/internet-of-things-iota-seminar-ppt-by-mohan-kumar-g-160122172302/95/internetofthings-iot-aseminar-ppt-by-mohankumarg-7-638.jpg?cb=1453483528/

[27] https://www.slideshare.net/MohanKumarG/internetofthings-iot-aseminar-ppt-by-mohankumarg

[28] https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/

[29] https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical/

[30] https://www.forbes.com/sites/gilpress/2017/03/20/6-hot-internet-of-things-iot-security-technologies/#6ab252291b49

[31] https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html

[32] https://www.ericsson.com/en/.../ericsson.../end-to-end-security-management-for-the-iot...

[33] www.collaberatact.com/IoT/Security

[34] Suo, Hui, et al. "Security in the internet of things: a review." Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on. Vol. 3. IEEE, 2012.

[35] Tamboli, Jinita, et al. "Security in the Internet of Things." Communication, Cloud and Big Data: Proceedings of CCB 2014 (2014).

[36] Kamath, Srikanth H., Suyashi Pandey, and Kar Tanisha. "Security Issues in Internet of Things." International Journal of Emerging Research in Management &Technology 6.5 (2017): 260-264.

[37] Dezhgir, Hamid, And Haniyeh Hooshmand. "Security On The Internet Of Things." (2017).

[38] Sayana, Laxman Singh, And Bineet Kumar Joshi. "Security Issues In Internet Of Things."