IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Lightweight Security Solution to Secure the Data in IoT System

Prabha Singh
M.Tech Student, Buddha Institute of Technology, Gorakhpur, Uttar Pradesh
Sudhir Agarwal
Professor, Buddha Institute of Technology, Gorakhpur, Uttar Pradesh

**Abstract- The Internet of Things (IoT) is an interactive environment, which interconnects material things to the internet and provides advance and intelligent services to a wide range of applications. This kind of complex and dynamic system is often susceptible to attack during data transmission and processing. Therefore, it is essential to know the origin of data and to assure that the source is reliable and the integrity of data is maintained during transmission. However, the limitation on the resources and heterogeneous environment brings several challenges for securing the data in the IoT system. Traditional security solution becomes infeasible because of low energy devices in the IoT system. The purpose of this paper is to present a lightweight security solution for the IoT system by using the Received signal strength indicator. RSSI values would be used to generate the link fingerprint. By comparing the link fingerprints values of various nodes on the server, the presence of adversarial nodes in the system can be detected. This method required very less energy in comparison to the other conventional method.**

**Index Terms: Internet of Things, Security, RSSI, Link Fingerprint.**

## 1. INTRODUCTION

The recent advancement in IoT has rapidly enhanced its utilization in various industries. The main factor for the spread of the IoT worldview is that numerous industry-driving producers, specialist organizations, and programming and system designers are making interests in the IoT future world vision. Cisco predicts that the worldwide IoT market will be $14.4 trillion by 2022 [4]. The idea of IoT is multi-dimensional since it grasps a wide range of innovations, technologies, and communication architecture. The IoT revolution is appropriately transforming ordinary devices into intelligent devices. Every device can obtain the information from the surroundings of the environment in which they are set as well as to provide various data to other devices. Such conduct creates a distributed network, in which heterogeneous devices can communicate with each other and can retrieve the information from their surroundings and users. Because the IoT devices generate and process huge amounts of critical data, therefore it is essential to create a secure environment for data transmission and processing. However, ensuring security and privacy in the IoT system is not straightforward. To mitigate the security issues in the IoT system, a strong security mechanism must have implemented. A security mechanism is required to ensure the credibility and trustworthiness of the data. However, applying a security solution to IoT can be troublesome. This is because of the large amount of data and the involvement of devices having constrained computation power. An elevated level of heterogeneity, alongside the wide extension of IoT applications, amplifies the security issues of the current Internet. In more detail, conventional security countermeasures can't be straightforwardly applied to IoT because of their restricted resources; additionally, the high number of interconnected devices raises adaptability issues [6]. Simultaneously, to gain more

acceptances from user, it is obligatory to characterize legitimate security, protection, and trust models appropriate for the IoT application. This paper presents a lightweight security solution for the IoT system. The content of the paper is organized as follows: Section 2 gives a review of the idea of IoT, its latent capacity, and difficulties. Section 3 features the issues of security and protection in IoT. Section 4 talks about the implementation of a lightweight security solution to mitigate security and protection issues. Section 5 looks after the present methodologies fathoming IoT challenges. Finally, the paper concludes, and future work is presented in secti

## 2. IoT OVERVIEW

Internet of Things is getting generally utilized for comprehensively characterizing a future wherein objects outfitted with sensing and actuation capacities get associated with a worldwide organized network, ready to connect the hole between the physical and advanced domains. An IoT system is comprised of smart entities that can communicate with each other to satisfy a shared objective and access the data from and following upon the environment in which they are. The entities can be substantial or immaterial items with constrained resources, for example, energy, transfer speed, and computational power. They are fit for producing huge amounts of information. To examine the enormous data delivered by these devices, the information is typically moved into large centralized data-centers, the cloud. IoT can be considered as the intersection of the Internet with data and things. In a more precise manner it is allowing the things to be connected on internet for exchanging the data by using industry standards that provides interoperability. Various applications require regulating the system remotely using the Internet: monitoring and managing things by specialists (e.g., a patient's medical condition while he/she is at the solace of their home); control different things in smart cities; and, at long last, giving progressively moderate amusement what's more, games for kids and grown-ups. These are instances of gigantic business and administration chances to support the financial effect for buyers, organizations, governments, hospitals, and numerous different elements. There are four stages of the IoT network system. The first stage comprises networked things, normally wireless sensors and actuators. The second stage incorporates sensor data aggregation systems and analog-to-digital data conversion. A third stage controls IT systems to perform preprocessing of the data before it moves on to the data center or cloud. At fourth stage, after analysis of data it is stored on a data center system. While IoT has the capability of improving numerous aspects of human lives, various difficulties may impede its utilization like equipment and architectural challenges, interoperability, lack of standard, and business issues.

## 3. SECURITY ISSUES IN IoT AND THREAT MODEL

For secure application data anonymity, integration and confidentiality must be ensured. A proper authentication mechanism should be implemented that guaranteed the prevention from unauthorized access to the data from the system. Since the system may oversee the personal and sensitive data hence data privacy and confidentiality should be ensured. At long last, trust is a key issue since the IoT environment is described by various devices that need to process and handle the information in consistence with user needs [13]. An IoT-based system may endure of various types of attacks, which can be recognized into three gatherings: (I) attacks against the IoT devices (including physical attacks); (ii) attacks against the data transmission (including accessing and altering the data/ routing attacks); (iii) attacks against the network (including DoS attack). Legitimate countermeasures must be set up to address every one of them. There are some challenges to implementing a secure IoT application. This is expected due to the entangled attributes of IoT that include: unspecified parameters, its exceptionally dynamic nature, heterogeneity of devices, worldwide availability, and wide openness. In IoT frameworks devices have restricted processing capacities. Due to this reason, it is tough to implement safety measures on them. Various security threats can influence IoT objects.

These threats incorporate attacks focusing on different correspondence channels, Denial of service, eavesdropping, physical attacks, and numerous others [20]. The intrinsic unpredictability of the IoT, where numerous heterogeneous devices situated in various locations, can exchange data with one another. This can additionally increase the complexity and security threats. The conventional cryptographic method is not suitable for resource constraint devices. Another reason that may ruin the adoption and advancement of IoT is the concern of privacy. Since the information that is communicated between devices is very sensitive, hence users should be provided with the tools to protecting their privacy. The threat model of an IoT network can be considered as: when data is transmitted from one node to another, an adversary node can affect the data transmission in an adverse manner [10]. It can capture the information that is being transmitted. Other possibilities are as follows.

1. Nodes on the transmission path can be compromised to extract the information.
2. Any intruder node can be deployed in between the source and destination node.
3. Privacy of data can be break by accessing the RFID tags.
4. Alter some portion of the provenance chain.
5. Provenance data can be forging by using fake keys.

An appropriate strategy to address significant portion of the previously addressed security and privacy issues is through the utilization of information provenance. In the following segment, information provenance is featured with a conversation of its latent capacity.

## 4. LIGHTWEIGHT SECURITY SOLUTION

It has been found that there exists a linear relationship between the RSSI values of two adjacent nodes in the system. This phenomenon can be used for the detection of any adversarial node in the system. A link fingerprint value is generated for the nodes in the system. These link fingerprint values are eight bits of binary stream conversion of the RSSI values recorded for the communicating nodes. The link fingerprint for a particular node is encoded by the eight-bit key of that node. At the server, this value is decoded by the key of that particular node. By the observation, it has been found that the value of the correlation coefficient for two adjacent nodes that are communicating in the system will be very high if there is no adversarial node between them. Let us assume a system as defined by figure 1.

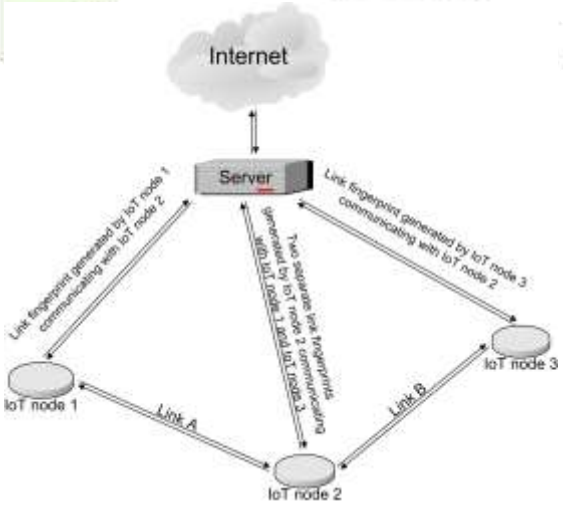


**Figure 1 System Model.**

The RSSI values for the system can be recorded by using MICA nodes in the real time. The recorded value of RSSI for a node is quantized by using word length of 8 bits. This 8- bit value will represent the LF (Link Fingerprint). The value of LF for a node 1 will encrypted by $K_1$ key, node 2 by $K_2$ and $K_3$ for node3.

$$LF_{encrp}(1 \rightarrow n) = (LF_{1 \rightarrow n}, K) \text{----------1)}$$

Server will decode all the XoR received values of LF for different nodes by their corresponding keys.

$$LF_{1 \rightarrow n} = XoR\ (LF_{encrp}(1 \rightarrow n), K) \text{----------2)}$$

The decoded values will be converted into the decimal values. A correlation value will be calculated for communicating nodes. The larger value of correlation coefficient indicates that there are no adversarial node is present between two communicating node. If there will be any adversarial node between node 1 and node 2 there will be a nonlinear relationship between the variation of RSSI values of node1 and node2. Similarly for node 2 and node 3, if there will be no adversarial node between them then a large value for correlation coefficient will exist.

## 6. LITERATURE SURVEY

Since there are huge quantities of heterogeneous devices are associated in the IoT consequently it is difficult to ensure these system. There are different researches has been done to bring a protected answer for the IoT framework. Albeit some security arrangements like encryption and hashing have suggested, there is a solid security arrangement is expected to protect the system from different vulnerabilities and threats [3], [4]. IoT is dynamically impacting our life in a more extensive number of ways than beforehand. In this manner researchers must deal with and resolve the security issues of the IoT system. Furthermore, the IoT based undertakings like transportation, clean water, brilliant home, remote wellbeing observing and sewerage control frameworks present raised security risks [11], [12]. Security dangers are a reality for the different IoT system and around 60,000 vulnerabilities were found by two Russian security experts that can bargain the total framework [13].There are few works have been done to illuminate the previously mentioned problems. There is a requirement for progressively rich methodologies for a complete solution. Aziz and Singh [18] have proposed the method of compressive sensing for providing lightweight security for the IoT system. They used compressive sensing for encrypting the data during the transmission. Medded and Glisaa [19] have highlighted the drawbacks of DTLS and IP6 with 6LoWPAN. Kong et al. [16] suggested the use of random for the encryption process. Proposed method uses probabilistic encryption procedure. Wang, K.-H [23] have focused on the vulnerabilities of the existing lightweight protocol. Domb et al. [24] have offered the three ways solution to mitigate the problems with RSA encryption. They had used Machine learning and parallel processing approaches for the detection of anomaly and implementation of RSA on the sensor. By using the concept of one way function and exclusive XOR operation a light weight protocol (LAAP) is proposed by Gope., Shahid Raja and Runar [25] have presented TinyIKE which is light version of Internet Key Exchange Protocol.

## 7. CONCLUSION

The objective of this paper is to use provenance practices into the IoT system, to moderate their safety and confidentiality issues. This study suggests that IoT is still at the initial stage of advancement in which various issues and difficulties have not been completely addressed. It has been observed that conventional data securing techniques are hard to utilize in the IoT system. A threat model has offered potential risks to the data in the IoT system. Energy required for the proposed solution is very less in comparison to the other proposed solution as well as the time complexity is O (1). On the basis of analysis, some open issues like enormous data managing, flexibility support, decentralization, and privacy preservation have been finding as big challenges that can be subject to forthcoming research.

**REFERENCES**


1. J. Granjal, E. Monteiro and J. Sa Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," IEEE Communications Surveys & Tutorials, vol. 17, pp. 1294-1312, 2015.
2. M. Ambrosin et al., "On the Feasibility of Attribute-Based Encryptionon Internet of Things Devices," in IEEE Micro, vol. 36, no. 6, pp. 25-35, Nov.-Dec. 2016. doi: 10.1109/MM.2016.101
3. T. Hahn, S. Matthews, L. Wood, J. Cohn, S. Regev, J. Fletcher,E. Libow, C. Poulin, and K. Ohnishi, "Ibm point of view: Internet of things security," White paper, April, 2015.
4. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the internet of things," Digital Communications and Networks, vol. 4, no. 2, pp. 118–137, 2018.
5. D. Storm, "Hackers exploit scada holes to take full control of critical infrastructure," Computerworld, vol. 15, 2014.
6. Ge, M., Hong, J. B., Alzaid, H., & Kim, D. S. (2017) Security modeling and analysis of cross-protocol IoT devices. IEEE Trustcom/BigDataSE/ICESS (pp. 1043–1048).
7. Kamal, R. (2017). Internet of Things: Architecture and Design Principles, (p. 403), TMH, India, ISBN-13: 978-93-5260-522-4.
8. Biswas, K., Muthukkumarasamy, V., Wu, X. W., & Singh, K. (2016). Performance evaluation of block ciphers for wireless sensor networks. In R. Choudhary, J. Mandal, N. Auluck, & H. Nagarajaram (Eds.), Advanced Computing and Communication Technologies. Advances in Intelligent Systems and Computing, Vol. 452. Springer, Singapore.
9. Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security in the integration of low-power wire- less sensor networks with the internet: A survey. Ad Hoc Networks, 24, 264–287.
10. Zhao, K., & Ge, L. (2013). A survey on the internet of things security. In: 2013 9th International Conference on Computational Intelligence and Security (CIS), IEEE (pp. 663–667).
11. Badel, S., Dağtekin, N., Nakahara, J. J., Ouafi, K., Reffé, N., Sepehrdad, P., & Vaudenay, S. (2010).
12. ARMADILLO: A multi-purpose cryptographic primitive dedicated to hardware. In: Proceeding of International Workshop on Cryptographic Hardware and Embedded Systems (pp. 398–412). Berlin: Springer.
13. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, 8–27.
14. Hatzivallis, G., Fysarakis, K., Papaefstathiou, I., & Manifavas, C. (2018). A review of lightweight block ciphers. Journal of Cryptographic Engineering, 8, 141–184.
15. Schinianakis, D. (2017). Alternative security options in the 5G and IoT Era. IEEE Circuits and Systems Magzine, Fourth Quarter (pp. 6–28).
16. Kong, J. H., Ang, L.-M., & Hatzivallis, K. (2015). A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments. Journal of Network and Computer Applications, 49, 15–50.
17. Mohd, B.J., Hayajneh, T., & Vasilakos, A. V. (2015). A survey on lightweight block ciphers for lower source devices: Comparative study and open issues. Journal of Network and Computer Applications, 58, 73–93.
18. Aziz, A., & Singh, K. (2018). Lightweight security scheme for Internet of Things. Wireless Personal Communication Issue: 104, 2/2019, Springer online available: 26 Oct 2018. https ://doi.org/10.1007/s1127 7-018-6035-4.
19. Meddeb, A., & Glissa, G. (2019). 6LoWPSec: An end-to-end security protocol for 6LoWPAN. AdHoc Networks, *82*, 100–112. https ://doi.org/10.1016/j.adhoc .2018.01.013.
20. Wu, X.-W., Yang, E.-H., & Wang, J. (2017). Lightweight security protocols for Internet of Things. IEEE Conference.
21. Schinianakis, D. (2019) Lightweight security for the Internet of Things: A soft introduction to physical unclonable functions. IEEE Potentials, March/April 2019 (pp. 21–28). Doi: https://doi. org/10.1109/MPOT.2018.28498 50. Date of publication: 6 March 2019.
22. Aghili, S. F., Mala, H., Kaliyar, P., & Conti, M. (2019). SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT. Future Generation Computer Systems, *101*, 621–634. Doi: https ://doi.org/10.1016/j.futur e.2019.07.004.
23. Wang, K.-H., Chen, C.-M., Fang, W., & Tsu-Yang, W. (2018). On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags. *Journal of Supercomputing*, *74*, 65–70. https ://doi.org/10.1007/s1122 7-017-2105-8.
24. Domb, M. (2017). An adaptive lightweight security framework suited for IoT. In J. Sen (Ed.), Internet of Things: Technology, Applications and Standardization, IntechOpen. http://dx.doi.org/10.5772/intec hopen .73712 .
25. Gope, P. (2019). LAAP: Lightweight anonymous authentication protocol for D2D-Aided fog computing paradigm. Computers & Security, 86, 223–237. https ://doi.org/10.1016/j.cose.2019.06.003.
26. Liu, Z., & Seo, H. (2019). IoT NUMS: Evaluating NUMS elliptic curve cryptography for IoT platforms. IEEE Transactions on Information Forensics and Security,14, 3.
27. Raza, S., & Magnusson, R. M. (2019). TinyIKE: Lightweight IKEv2 for Internet of Things. IEEE Internet of Things Journal, 6(1), 856–866.
28. Pahuja, S., & Jindal, P. (2019). Cooperative communication in physical layer security: Technologies and challenges, wireless personal communication. Berlin: Springer Nature.

**Prabha Singh is** currently pursuing M.Tech in Computer Science and Engineering from Dr. A.P.J. Abdul Kalam Technical University, Lucknow. Her area of interest includes Internet of Things, software Engineering and mobile computing. She has completed her Master in Computer Application from the same University. She has published five more papers on different areas.

**Dr. Shudir Agarwal** is currently working as a professor in Computer Science and Engineering department, BIT, Gida, Gorakhpur. He has 12 publication to his credit and attended many conferences and seminars.