International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Efficient and Secure Data Transfer in IoT

Jebin Bose S, Julia Punitha Malar Dhas

Abstract*: Nowadays, the Internet of Things (IoT) has been used widely in our daily day to day life, starting from health care devices, hospital management appliances to a smart city. Most of the IoT devices have limited resources and limited storing capability. All the sensed information must have to be transmitted and to store in the cloud. To make a decision and for making analysis all the data stored in the cloud has to be retrieved. Making certain the credibility and security of the sensed information are much necessary and very important for the use of IoT devices. We tend to examine the proposed technique to be much secure than the existing one. In IoT, if the security is not ensured, then it may result in a variety of unsought issues. This survey resembles the overall safety aspects of IoT and debates the overall issues in the security of IoT.

***Keywords* : Security, Integrity, Authentication, IoT.**

I. INTRODUCTION

The IoT will hold every object, which occurs every day in our lives. In this article we, deliberate how the future technology on the internet will be designed, its aspects and its challenges [1-2]. The term Internet refers to the network connectivity and the term Things refers to the Device in which the network is to be connected and the data is to be transmitted and collected. The smart objects rule the whole world and the Internet plays a wide role in the field as a service provider [3]. The IoT came into existence only by sensors like smart objects, and the Internet. Increasing usage of sensors leads to an increase in the raw data and distributed data. The data has been collected using the Internet using Smart devices [4]. Due to the advancement in the field of wireless communication techniques, and due to the speed of the internet promoting advancement is a risky task [5]. In the IoT architecture Visualizing all the sensors as having intelligence will be the goal [6-7]. Fig.1. which describes the evolution of the IoT devices. The IoT is completely transforming very fast as every device integrated to be connected with the internet [8]. This innovation will completely change the life of humans.

The target is to check out the issues in the security of IoT and other challenges of IoT and to propose a complete overview of advanced security techniques. We encapsulate the security issues, various challenges in the data communication of IoT, that will entirely differ from the existing and traditional data collection techniques.

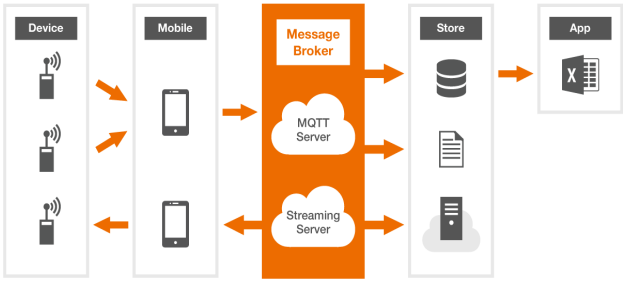

Fig. 1. Internet of Things Architecture

II. SECURITY IN IOT

A. Issues in Security

In IoT, the most important task is making certain information and providing security. The IoT enhances sensing, nanotechnology, embedded system, and RFID technology. Every risk will occur from its basic design. In IoT, one of the major identification while referring is RFID (Radio Frequency Identification). Using the electromagnetic fields, it automatically detects objects carrying tags. Major attacks from WSNs will be happening in this layer [11-17] All the security aspects has been relying upon various layer. RSN, WSNs, RFID, and RSN security has to be accessed while enhancing security. The up-gradation of RFIS and WSNs is the RSN. Securing the local network, core network, and access network security is in the transport layer. 5G, 4G, 3G, 2G, EDGE and WiFi network security is also the part of sensing, transportation, and application later. The overall security in the IoT will be provided by the Application layer.

Table- I: Architecture on issues in security

Layers in IoT	Issues in Security
Application	user authentication, information availability middleware, information privacy.
Transport	WLAN conflicts, connectivity issues, DOS attack, forgery attack, heterogeneous attacks.
Sensing	Conflict collision for RFID, fabrication, modification, Interruption.

B. IoT Security challenges

Several challenges stopped the securing of IoT devices associate with making certain end-to-end security in an IoT atmosphere.

Manuscript published on November 30, 2019.
* Correspondence Author
Jebin Bose S*, ME Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kumaracoil, India.
Julia Punitha Malar Dhas, HOD- Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kumaracoil, India.

As a result of the thought of connected devices and smart objects, security is considered to be a big issue. Also, as a result emergence of IoT in the market makes several product designers and makers square measure a lot of curious about obtaining their merchandise to plug quickly, instead of providing security or look back from the beginning of the development. One of the most important issues is the use of irrelevant passwords. Next most common issue is that several smart devices do not provide any cryptographic techniques or standards to save the relevant measures temperature or pressure.

C. Industrial security thread - Vulnerable

Hacking security will happen in any business organization. While injecting the medicine for a patient, if the values are different it may result in the loss of human life. Hacking the system and changing the values may be carried out easily. For example, in the smart refrigerator, if hacking happens and the temperature value gets changes, the medicines kept on the refrigerator may get wasted as this issue enhances the security thread to the industry that is more vulnerable than any other attacks.

III. RELATED WORKS

IoT devices have been proposed with new techniques and algorithms to provide better security. Some algorithms and techniques have been proposed for efficient and secure transfer of data that relates to security.

To ensure security during the transfer of data, Muhammad Tausif et al[19] proposed lightweight ciphers. Human life has been extremely changing from smart homes to smart objects and to smart fitness. Whatever may be, the smart devices have only less battery backup, less storage medium, and lesser RAM size. So, to provide secure connectivity, lightweight ciphers have been used. Nearly thirteen lightweight ciphers are used. To process, RAM and the code size has been used for the lightweight cipher. By using different techniques and models, the newly proposed technique has been analyzed. Association rule mining has been used to monitor the overall strategy and performance. This enhances the stability and improvement of the lightweight ciphers.

A secure IoT algorithm proposed by Muhammad Usman et al[20] provides a change in IoT security. Large sets of Big Data has been generated by the IoT. All the encryption algorithms are very difficult and are difficult to implement. The symmetric key algorithm is used to overcome this issue as it uses a 64-bit key as it encrypts 64-bit block cipher. Both the encryption and the decryption has been accessed only using 5 keys.

Manish Kumar et al[21] enhances new techniques to provide higher security. The IoT has made human life simpler than ever before but at the same time, it leads to various security-related issues with the data. In encryption, the asymmetric key has been proposed to overcome the existing technique. The proposed asymmetric key method uses a 128-bit key. It takes input data as 8 bit and produces the relevant output as the 8-bit ciphertext. This method overcomes to defend the brute force attack. In various stages, both encryption and decryption has been performed and noticed that it is somewhat better when compared to existing techniques.

The main issue with the security proposed by Ria Das et al[22] examines accessing and altering all the data and information. By using the cryptography we can prevent Integrity attacks where steganography has been used to avoid confidentiality attacks. The proposed technique by Ria Das et al differentiates two phases. Data transmission among the IoT devices and the home server has been analyzed first, here LSB and XOR combination technique has been used. Data transmission among the home server and cloud has been analyzed second. Here LSB and XOR combination along with DES or AES is used. Using Matlab it is tested. Among 01 to 100 character sets of datasets has been collected. To undergo encryption XOR simple operation has been used. Once the testing has been completed and analyzed, it results that LSB and MSB substitution technique is good.

The new hybrid method has been proposed by the Chaitanya Bapat, et al [24] as IoT runs with sensing devices. To put locks it is very difficult in our home. So IoT technique has been used in implementing the smart lock. It has been used widely around the world, here a man in the middle attack is possible with this smart lock. So the proposed work enhances the Bluetooth Low Energy. The cryptography and stenography technique has been used to overcome this attack. The client enters the encrypted key by the AES key. Now, the ciphertext will be embedded in an Image. The image will be transmitted by Bluetooth low energy. The ciphertext will be extracted from the Image, as it has been performed by the server as it is then decrypted. Then validation has been performed.

To enhance the overall security Jagdish Patil et al[26] proposed a cipher which is lightweight termed as LiCi. To a plain text, it creates 64bit ciphertext along with a 128bit key. Also 4bit input and 4bit output used for S-box. In the LiCi total of 31 rounds have been performed. This method has been tested, analyzed and noticed that it enhances much security with other existing techniques.

Next lightweight authentication using a one-time pad key has been proposed by Mrudula Sarvabhatla, et al[29] in Hadoop. The traditional databases can't handle Unstructured and high-speed data. A Hadoop Distributed File System is in need to overcome this issue. In the big data, highly confidential data like economical, financial, healthcare databases, will be stored. It needs high security. So Mrudula Sarvabhatla, et al proposed two authentication techniques. This technique represents two servers, the Registration server is the first server proposed in this technique, the backend server is the second server proposed in this technique. Once registration has been made, the details such as password, Id will be forwarded to the Registration server.

Once the details along with the request have been received, server calculation has been performed with the one time pad. With ID and password, XOR operation is performed along with the hash of the OTP key. The backend server generates a random number. For overcoming the password guessing attack, a new technique is proposed. It provides high security and is cost-effective.

Table- II: Various comparisons of Security

IoT security proposed solution	Various methods to enhance security	Requirements in security			
		I	C	Av	A
Muhammad Tausif et al[19]	Cipher for IoT that is light Weight	✓	✓	✓	✓
Muhammad Usman et al[20]	lightweight algorithm fo encryption	✓	✓	✓	✓
Manish Kumar et al[21]	dynamic key approach	✓	✓	✓	✓
Ria Das et al[22]	benefits of both cryptography and steganography by combination using hybrid approach	x	x	x	✓
Chaitanya Bapat, et al[24]	cryptography and steganography technique	✓	✓	✓	✓
Jagdish Patil et al[26]	LiCi technique that is a block cipher technique	x	x	x	x

(I represents Integrity, C represents Confidentiality, AV represents Availability, A represents Authentication)

IV. IOT SECURITY PROPOSED SOLUTIONS : A COMPARISON

A digital signature is widely used as it guarantees information security. Moreover, none of the existing techniques provides much security for IoT devices. The sign-each method has been used first causes expensive as both the signer and the verifier carries out the encryption and the decryption operation. Moreover, the Sign-each method will not observe data loss. Additionally, partial sample-rate information retrieval is not supported. Using Hash chaining the quality from O(m) to O(1) is reduced, here m represents the range of messages.

This survey presents 2 novel signature schemes, to handle the same issues to match with the present techniques and so value the performance of the system. There are two techniques namely Dynamic Tree Chaining and Geometric Star Chaining, expected to supply reliable communication.

In DTC, it enhances the partial sample-rate data. The responsibility of the application is to ensure uniformity and security. This easy technique isn't ascendable. Variety m has been forwarded as it represents one random permutation. We tend to illustrate the procedure for random permutation rule, that demonstrates Fisher-Yates shuffle.

Furthermore, resampling is permitted, which implies various sets of events from the cloud. It is very useful in various functions such as error of data [31] and learning [32]. A huge amount of references ensures the resampling usage.

Overcoming with DTC, GSC supports partial sample rate information retrieval. GSC won't allow the information client to check all the single messages as DTC did, For example, 5/8 = $(0.101)_2$. The partial information p, where $p = \sum 2^{-bi}$. The information block is termed as the sample block. For example, sampled information can be retrieved with rate 5/8, as the information will be forwarded to cloud containing approx 1/2 and 1/8 of the samples respectively.

Computing the numerical interval h(e) in this bit sequence is supported in X86 and ARM. In the case of xxHash64, 64-bit hash value will be produced so $|0\leq i\leq 64| = 65$ and $|0\leq i\leq 64| = 65$. Hence, the sensing device is constant. GSC needs a smaller buffer size on the sensing device while compared to DTC. It also enhances the uniformity and security. In GSC random permutation will not be supported.

Comparison of various signature schemes method listed in Table 3. Because of signature length in RSA1024 is 128bytes, the amortized sender or the receiver communication value will be 128+4 = 132bytes. And for other alternative Signature Schemes, cryptography time is analogous.

Table- III: Comparison on different signature methods

Signature generation method	Time for Signature generation	The cost for Sender Communication	The cost for Receiver Communication
Concatenate method	0.59 ms	4.43bytes	8.89bytes
hash changing method	0.57 ms	4.43bytes	8.86bytes
Sign each method	2.82 ms	132bytes	132bytes
DTC method	0.55 ms	4.45bytes	4.52bytes
GSC method	0.41 ms	4.43bytes	4.43bytes

V. CONCLUSION

IoT is introduced to promote advanced technologies in the field of sensing. Cloud and many others that enhance the easier pathway to human life. Various security risk that enhances the development in the IoT devices. The overall safety problems and security of IoT is focused on this survey and points out that the existing solutions cannot afford with the newer techniques. This new technique senses the data using the smart objects, pass on through the network stores it in the cloud and later can be used for verification purposes. The overall safety problems and security of IoT is focused and points out that the existing solutions cannot afford with the newer techniques. This proposed technique not only enhances security but also enhances the time and space.

REFERENCES

1. D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), "The Internet of Things," Springer, 2010. ISBN: 978-1-4419-1673-0.J.

2. L. Atzori, A. Iera and G. Morabito, “The Internet of Things: A survey,” Computer Networks (2010), doi:10.1016/ j.comnet.2010.05.010.
3. J. A. Stankovic, “Research Directions for the Internet of Things,” IEEE Internet of Things Journal, vol. 1, no. 1, pp. 3-9, 2014.
4. D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, Springer, 2010.
5. G. Tripathi, D. Singh, "EOI: Entity of Interest Based Network Fusion for Future Internet Services", ICHIT2011, September 23-25,2011, Daejeon, Korea.© Springer-Verlag Berlin Heidelberg, CCIS, vol. 206, pp. 39–45, 2011.
6. Hall, D. L., Llinas, J., “Handbook of Multisensor Data Fusion,” CRC Press, (2001).
7. J. Gubbi, R. Buyya, S. Marusi, M. Palaniswamia, Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions, Technical Report CLOUDS-TR-2012-2, The University of Melbourne, June 29, 2012.
8. J. Belissent, Getting Clever About Smart Cities: New Opportunities Require New BusinessModels, Forrester Research, 2010.
9. H. Jun-Wei, Y. Shouyi, L. Leibo, Z. Zhen, W. Shaojun, A Crop Monitoring System Based on Wireless Sensor Network, Procedia Environmental Sciences. 11 (2011) 558–565.
10. WhatisRFID? URL:http://www.centrenational-rfid.com/introduction-to-the-rfidarticle-15-gb-ruid-202.html, last accessed on: 07/01/2017.
11. S. Ozdemir, “Secure Data Aggregation in Wireless Sensor Networks via Homomorphic Encryption” Journal of The Faculty of Engineering and Architecture of Gazi University, vol.23, no. 2, pp. 365-373, June 2008.
12. A. R. Alazemi, “Defending WSNs against jamming attacks,” American Journal of Networks and Communications, vol. 2, no.2, pp. 28-39, 2013.
13. E. C. H. Ngai, “On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks,” in International Conference on Communications (ICC), 2006 Proceedings of International Conference on, 2006, pp. 1-4.
14. P. Kumar and H.J. Lee, “Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey,” Sensors 12, no. 1, pp. 55-91, 2012.
15. A. Oracevic and S. Ozdemir, “A Survey of Secure Target Tracking Algorithms for Wireless Sensor Networks,” in Computer Applications and Information Systems (WCCAIS), 2014 IEEE Conference on, January 2014, pp. 1-6.
16. A. Oracevic, S. Akbas, S. Ozdemir, and M. Kos, “Secure Target Detection and Tracking in Mission Critical Wireless Sensor Networks,” in Anti-counterfeiting, Security, and Identification (ASID), 8th International IEEE Conference on, December 2014.
17. A. D. Wood, and J. A. Stankovic, “A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks,” Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, Chapter 32, 2004.
18. F. Y. Ren, H. N. Huang, and C. Lin, “Wireless sensor networks,” Journal of Software, 2003, vol 7, pp. 1282–1290.
19. Tausif, M., Ferzund, J., Jabbar, S., & Shahzadi, R. (2017). Towards designing efficient lightweight ciphers for internet of things. KSII Transactions on Internet and Information Systems, 11(8), 4006-4024.
20. Usman, M., Ahmed, I., Aslam, M. I., Khan, S., & Shah, U. A. (2017). SIT: A Lightweight Encryption Algorithm for Secure Internet of Things, 8(1). https://doi.org/10.14569/IJACSA.2017.080151.
21. Kumar, M., Kumar, S., Budhiraja, R., Das, M. K., & Singh, S. (2017). Lightweight Data Security Model for IoT Applications: A Dynamic Key Approach. Proceedings - 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016, (3), 424-428. [22] Patil, J., Bansod, G., & Kant, K. S. "LiCi: A new ultra-lightweight block cipher," in 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI), feb 2017, pp. 40-45.
22. Das, R., & Das, I. (2017). Secure data transfer in IoT environment: Adopting both cryptography and steganography techniques. Proceedings - 2016 2nd IEEE International Conference on Research in Computational Intelligence and Communication Networks, ICRCICN 2016, 296-301.
23. Echandouri, B., Hanin, C., Omary, F., & Elbernoussi, S. (n.d.). LCAHASH-MAC : A New lightweight Message Authentication code Using Cellular Automata for RFID. nov 2017, pp. 287-298.
24. Bapat, C., Baleri, G., B, S. I., & Nimkar, A. V. (2017). Smart-Lock Security Re-engineered Using Cryptography and Steganography, Security in Computing and Communications, 325-336
25. Aljawarneh, S., Yassein, M. B., & Talafha, W. A. (2017). A resource-efficient encryption algorithm for multimedia big data. Multimedia Tools and Applications, 76(21), 22703-22724.
26. Patel, N., & Meena, S. (n.d.). LSB Based Image Steganography Using Dynamic Key Cryptography. 2016 International Conference on Emerging Trends in Communication Technologies (ETCT).
27. Sarvabhatla, M., Chandra, M. R. M., & Vorugunti, C. S. (2015). A secure and light weight authentication service in hadoop using one time pad. Procedia Computer Science, 50, 81-86.
28. R. Gennaro and P. Rohatgi, “How to sign digital streams,” Inf. Comput., vol. 165, no. 1, pp. 100–116, Feb. 2001.
29. S. Sattolo, “An algorithm to generate a random cyclic permutation,” Inf. Process. Lett., vol. 22, no. 6, pp. 315–317, May 1986.
30. J. Tukey, “Bias and confidence in not-quite large sample,” Ann. Math. Statist., vol. 29, p. 614, Mar. 1958.
31. Z.-H. Zhou, “Ensemble learning,” in Encyclopedia Biometrics. Springer, 2015, pp. 411–416
32. B. Efron, The Jackknife, the Bootstrap, and Other Resampling Plans. Philadelphia, PA, USA: SIAM, 1982, vol. 38.
33. C. K. Wong and S. S. Lam, “Digital signatures for flows and multicasts,” in Proc. 6th Int. Conf. Netw. Protocols, Oct. 1998, pp. 198–209.
34. R. C. Merkle, “A digital signature based on a conventional encryption function,” in Proc. CRYPTO, 1987, pp. 369–378.
35. D. Verbyla, “Potential prediction bias in regression and discriminant analysis,” Can. J. Forest Res., vol. 16, no. 6, pp. 1255–1257, 1986

AUTHORS PROFILE

Jebin Bose S completed his Master of Science in Software Engineering and he is presently doing Master of Engineering in Computer Science and Engineering at Noorul Islam Centre for Higher Education, Kumaracoil, Tamilnadu India. He has presented more than 10 papers in various International Conferences. He is a Professional member of Institute for Scholars (InSC). He won two Best Paper awards in the International Conferences. His areas of interests are Network Security and Internet of Things.

Dr. Julia Punitha Malar Dhas started her career in teaching since January 2000 and is currently the Head of Computer Science and Engineering Department, Noorul Islam Centre for Higher Education, India. She is a life member of Indian Society for Technical Education (ISTE). She has vast experience in teaching and has produced a number of Ph.D. candidates. She has published a number of papers in International Journals and Papers. Her main areas of interests are Computer Networks, Machine Learning, Soft and Image Processing.