ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

REVIEW PAPER

Available Online at www.ijarcs.info

Internet of Things: A Perspective from security and privacy

Deepika Khambra
M.TECH Student, Dept. of Comp.Engg.
U.I.E.T, Kurukshetra University
Kurukshetra, India

Ms. Poonam Dabas
Assistant Professor:Dept. of Comp.Engg.
U.I.E.T, Kurukshetra University
Kurukshetra, India

Abstract: Internet of Thing is a kind of network in which sensors and actuators are new to sense different type of data in the form of text and images. Security of sensors takes important role because these devices connected through internet. A malware or a misbehaving device may break down the system or forge secure or personal information from sensor node. To avoid this kind of issues cryptographic techniques is used. These techniques are AES, DES and RSA. In this paper security issue of IoT has been presented. After that a relative study of dissimilar cryptographic algorithms has been presented.

Keywords: Internet of Things (IoT), Sensor, Attack, Security, RSA, DES and AES.

I. INTRODUCTION

The Internet of Thing (IoT) is the interconnection of physical gadgets with implanted detecting and correspondence conceivable outcomes, including sensors and actuators. The Internet of Things is an extra layer of data, association, exchange and activity which is added to the Internet outfitted with information detecting, examination and correspondence capacities, utilizing Internet conventions. In the development of any IoT application security and testing structures assume a vital part. The gadgets collaborate with each other through the system and give new understanding to us. Keeping in intelligence the finish object to appreciate this new condition, security of obliged end hubs is critical [1]. Be that as it may, it be hard to actualize adequate cryptographic capacities on compelled gadgets because of the constraint of their asset. To help you make more secured and assault evidence web of things empowered gadgets and applications we display security prerequisite and some security issues that may violets security in IoT [2].

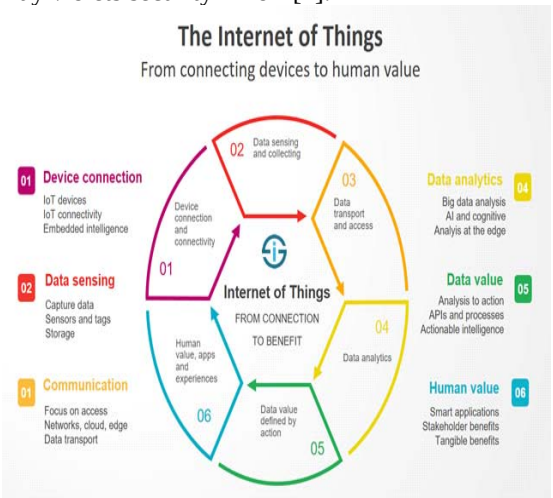

Fig1: Internet of things [2]

A. Characteristics of IoT

- Interconnectivity: as to the IoT, anything can be interconnected with the worldwide data and correspondence foundation.
- Things-related services: The IoT is fit for giving thing-related administrations inside the imperatives of things, for example, security assurance and semantic consistency between substantial equipment and their related virtual things. Keeping in intelligence the ending object to give thing-related administrations inside the limitations of things, both the advancements in physical world and data world will change.
- Heterogeneity: The gadget inside the IoT are heterogeneous as in view of various equipment stages and systems. They can associate with different gadgets or administration stages through various systems.
- Dynamic changes: The condition of gadgets change progressively, e.g., resting and awakening, associated and additionally separated and also the setting of gadgets including area and speed. Additionally, the quantity of gadgets can change powerfully.
- Enormous scale: The quantity of gadgets that should be overseen and that speak through every one extra will be no less than a request of greatness bigger than the gadgets associated with the present Internet [3].

B. Architecture of IoT

IoT considers six layers design. Coding layer is utilized to perceive the protest, recognition layer contains sensors used to detect the earth, organize layer is mindful to take computerized information from discernment layer and process it, Middle product layer is utilized for canny handling of information detected by sensor, Application

layer understands the utilizations of IoT for a large series of industry and in view of the prepared information Business layer deals with the applications and administrations of IoT [4].

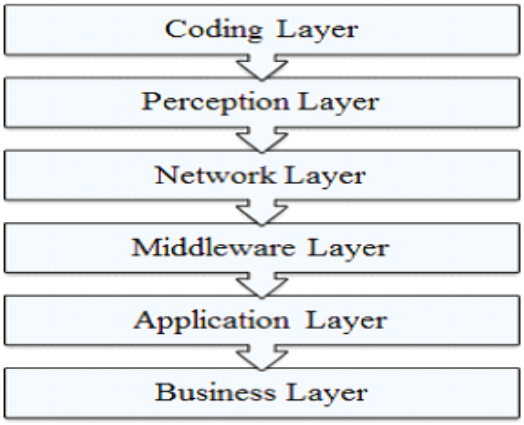

Fig 2: IoT Architecture [4]

C. IoT Security

Security in IoT is very challenging process means securing the data sense by device from any malicious node. To secure IoT fig 3 show the working architecture of a simple encryption decryption algorithm. Here in this mechanism creative memorandum be encrypted by applying encryption algorithm and the encrypted message will be transmitted towards receiver. At receiver side decryption algorithm will be applied to decrypt message and find original messages. This is the simplest mechanism for the secure transmission in IoT [5].

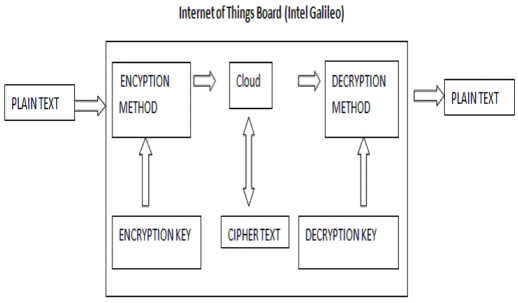

Fig 3 working diagram of IoT [5]

II. RELATED WORK

Grabovica et.al. [6] provides overview of security features for noted technologies. During accumulation to that, practical implementation and possible intrusions are introduced.

Mohsin et al. [7] proposed a formal structure near consider network configurations against diverse IoT threats. The threat specifications in conditions of adversary's capabilities and goals are fed as constraints to the model.

Kuusijarvi et al.[8] discussed the current defense challenge of loT devices and proposed a solution to secure these devices via a trusted system Edge Device.

Dalipi and Yayilgan[9] represented a comprehensive survey of the most new offerings on security and privacy aspects of IoT applications in smart grid.

Bertino[10] elaborate on privacy issues for IoT. They discussed research directions in IoT records solitude and surveyed initial work on IoT data security – an essential building block for privacy.

Raghav et al.[11] proposed a straightforward information protection model wherever information was encrypted exploitation Advanced secret writing common place (AES) before it's launched within the cloud, so making certain information confidentiality and security.

Parikh and Narkhede[12] proposed and implemented mechanism for area efficient and high performance for AES by using" Mixing of column and Inverse mixing of column operation" which was the individual of the major block of operation in AES toward execute the high performance of AES.

Sujatha and Devi [13] implement IoT authentication by experimenting with real attacks in a controlled environment.

Behrens and Ahmed [14] proposed a design model to protected message in IoT environments using existing protocols.

Husamuddin and Qayyum[15] discussed the different applications of IOT and the security threats involved. IoT has emerged as a significant technology.

III. VARIOUS ALGORITHM USED TO SECURE DATA

A. Data Encryption Standard(DES) Algorithm:

Data encryption standard is a symmetric key algorithm. DES is the block cipher- this algorithm used fixed length string of plaintext bits. The block size is 64 bits used in DES.

B. RSA algorithm:

RSA is asymmetric key algorithm. RSA is prepared by Ron Rivest, Adi Shamir, and Leonard Adlemen. RSA used two different keys in both side. RSA used public key and private key cryptographic . The public key disclose to everyone; it is used toward encrypt memorandum. And then encryption is done with public key and decryption is done with private key.

C. Advanced Encryption Standard(AES) algorithm:

Advanced encryption standard (AES) is a symmetric encryption algorithm. AES used a block length of 128, 192, 256 bits. AES is base on top of substitution-permutation network. AES used fixed block size. AES works on a 4x4 column-major order matrix of bytes.

Table 1 Comparative Analysis

Sr. No.	*Algorithm*	*Year of Development*	*Encryption/Decryption*	*Security*	*Hardware/Software implementation*	*Power consumption*
1	AES	2000	Fast	High	Fast	Low
2.	DES	1977	Medium	Medium	Sustainable for hardware not software	Medium
3.	RSA	1978	Low	Low	Not sufficient for hardware & software both	HIgh

IV. CONCLUSION

In IoT connecting devices with different architectures with secure transmission is very challenging. In this paper IoT with its layered architecture and various characteristics of IoT has been presented. After that encryption decryption mechanism has been discussed for protected information broadcast in IoT. Next we provide literature study of various related techniques of IoT security. At last we provide relative study of various security algorithms. Analysis shows AES is better among DES and RSA.

V. REFERENCES

[1]Ovidiu Vermesan SINTEF, Norway, Peter FriessEU, Belgium, "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems", Elesvier publishers' series in communications, 2013.

[2] Ovidiu Vermesan SINTEF, Norway, Peter FriessEU, Belgium, "Internet of Things–From Research and Innovation to Market Deployment", Elesvier publishers' series in communications, 2014.

[3]Karen Rose, Scott Eldridge, Lyman Chapin, "The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World", The Internet Society (ISOC), 2015.

[4]Xu Cheng, Minghui Zhang, Fuquan Sun, "Architecture of internet of things and its key technology integration based-on RFID," in 5thInternational Symposium on ComputationalIntelligence and Design, pp. 294-297, 2012.

[5] Jose L. Hernandez-Ramos, Jorge Bernal Bernabe and Antonio F. Skarmeta, "Managing Context Information for Adaptive Security in IoT environments", 29th IEEE International Conference on Advanced Information Networking and Applications Workshops, pp: 676-681.

[6] Minela Grabovica, Drazen Pezer, Srdan Popic and Vladimir Knezevic, "Provided security measures of enabling technologies in Internet of Things (IoT): A survey", IEEE Conference 2016, pp: 28-31.

[7] Mujahid Mohsin, Zahid Anwar, Ghaith Husariy, Ehab Al-Shaery and Mohammad Ashiqur Rahmanz, "IoTSAT: A Formal Framework for Security Analysis of the Internet of Things (IoT)", IEEE Conference on Communications and Network Security (CNS)2016 pp: 1-9.

[8] Jarkko Kuusijarvi, Reijo Savola, Pekka Savolainen and Antti Evesti, "Mitigating loT Security Threats with a Trusted Network Element", The 11th International Conference for Internet Technology and Secured Transactions (ICITST-2016), IEEE pp:260-265.

[9] Fisnik Dalipi and Sule Yildirim Yayilgan, "Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges", 4th International Conference on Future Internet of Things and Cloud Workshops2016, pp:63-68.

[10] Elisa Bertino, "Data Privacy for IoT Systems Concepts, Approaches, and Research Directions", IEEE International Conference on Big Data (Big Data) 2016, pp:3645-3647.

[11] Prasoon Raghav, Rahul Kumar and Rajat Parashar, "Securing Data in Cloud Using AES Algorithm", International Journal of Engineering Science and Computing,2016, ISSN 2321 3361,pp: 3672-3675.

[12] Priyesh Parikh, Satish N arkhede, "High performance implementation of Mixing of Column and inv Mixing of column for AES on FPGA", International Conference on Computation of Power, Energy Information and Communication, IEEE2016, pp: 174-179.

[13] S. Mary Sujatha and Y. Usha Devi, "Design and Implementation of IoT Testbed with Three Factor Authentication", IEEE 2015, pp: 1-5.

[14] Reinhard Behrens and Ali Ahmed "Internet of Things: An End-to-End Security Layer", IEEE 2017, pp: 146-149.

[15] Md Husamuddin and Mohammed Qayyum, "Internet of Things A Study on Security and Privacy Threats", IEEE 2017, pp: 1-5.