Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 8, August 2018, pg.196 – 202

Energy Efficient Technique for IoT: A Review & Survey

Ashish Verma, Amandeep Kaur, G.N. Verma

Department of Computer Science & Engineering, Sri Sukhmani Institute of Engineering & Technology,
I.K.Gujral Punjab Technical University, Jalandhar, India
E-mail: ashishverma6990@gmail.com

Abstract— Internet of Things is the technology in which the sensed information is passed to the base station which is uploaded on the internet. Due to the decentralized nature of the network security, energy consumption is the major issue of the network. In the base paper technique security to the network is provided in which unidirectional and bi-directional communication is possible. The security to the network takes place in which security keys are generated using the clocks of the sensor nodes. In the paper, it has been discussed that clocks of the sensor nodes are weekly synchronized. Due to weak clock synchronization of the sensor nodes, security of the network gets compromised. In this work, improvement in the existing technique will be proposed by providing strong clock synchronization. The RSA algorithm is been used which will establish secure channel from source to destination. The time-lay technique will be implemented which provide strong clock synchronization between the sensor nodes. The encryption keys are generated for the data encryption is depends upon the clocks of the sensor nodes and strong clock synchronization improved the network security. This improvement will lead to reduce energy consumption of the network and increase network throughput.

Keywords— IoT (Internet of things), RSA (Rivest-Shamir-Adleman), DES (Data Encryption Standard), 3DES (Triple Data Encryption Standard) , AES (Advanced Encryption Standard).

I. INTRODUCTION

The internet of things is the technology that allows users to achieve deep analysis, integration and automation within the system. In this technology sensor nodes pass information to base station. That gathered information than uploaded to the main server. When sensors change their positions handoff mechanism is installed. With the help of this accuracy and reach to the area of the system can be improved. In order to sense the network and robotics various technologies are emerged. It also exhibits the modern advance in the software technology as well as in hardware. The new advancements in the delivery of products, goods, and services; and the social, economic [1].

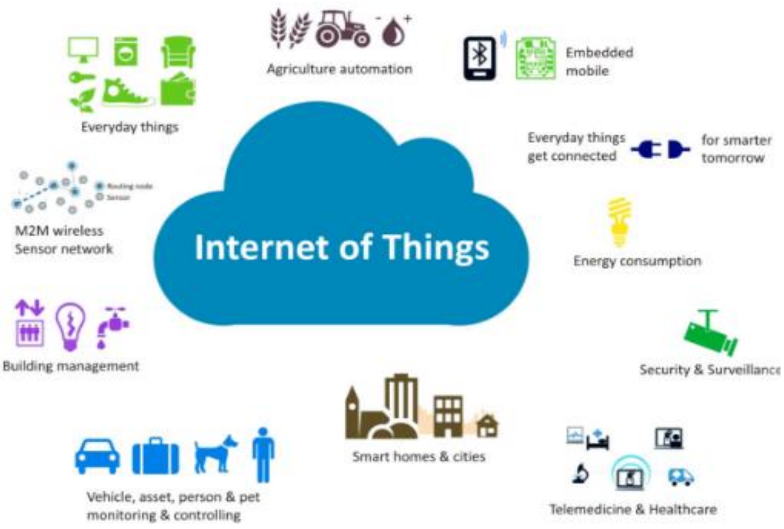


Figure 1. Example of a Internet of Things.

II. CHALLENGES OF IOT

The development potential of IoT is slowdown by the various challenges. When the IoT technology is deployed in the systems, there are various challenges that arise amongst which some are explained below:

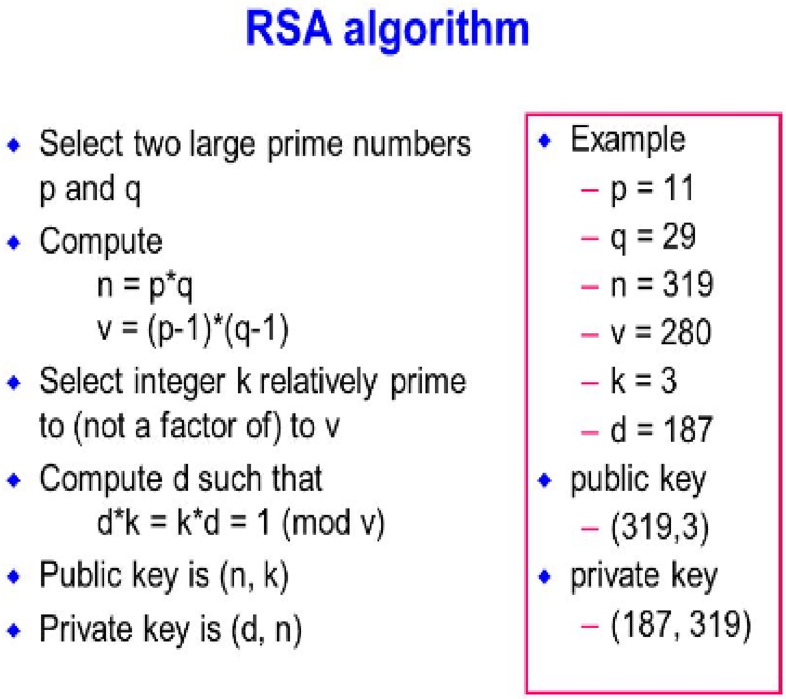
- Deployment of IPv6: previously world working on the IPv4, that slows down the potential of IoT's progress due to requirement of unique IP address to the each sensor. The management of network becomes easier with the help of IPv6 as it provides the auto configuration capabilities and offers improved security features [2].
- Security: Security within these systems is always a major concern as there are numerous systems involved during the communication being held. Thus, the data involved within these systems is to be made secure. Various data isolation techniques are provided here which can help in providing encryption measures within the systems. With the application of these systems it can be made sure that the data being transmitted to the destination reaches there without any modifications or stealing of important information by the unauthorized access.
- Privacy: One of other major concerns within these systems is the violation of privacy of data present in them. In order to ensure that only the authorized users are given access to the private information, various algorithms are proposed here which can ensure that no unauthorized users have access to this information [3].
- Cost versus Usability: The physical objects can be connected to the internet using IoT technology. The cost of components must be inexpensive in near future that are needed to support capabilities such as sensing, tracking and control mechanisms in order to grow the adaptability of IoT.
- Interoperability: The basic requirement of the interconnectivity is to connect with systems that operate on the same protocols and encodings. To support different application various standards has been utilized by huge number of industries. these diverse entities becomes important due to the use of standard interfaces where large amount of data and
- Heterogeneous devices are embedded. This application mainly utilized for the applications that supports cross organizational and various system boundaries. Therefore, high degree of interoperability needs to be handling in the IoT system.
- Data Management: It is very difficult to manage such large amount of data hence it is considered as the critical aspect in the Internet of Things. When daily exchange of data is numerous and the objects are connected from worldwide than it becomes difficult challenge for internet of things to provide optimal results. The involved process becomes critical for those data [4].
- Scalability: As the things are in cooperated within the open environment the Internet of things becomes the major concept as compare to the conventional Internet of computers. Therefore, it is required to function equally in the basic functionality such as communication and service discovery. To gain the efficient operation for scalability, IoT requires new methods and functionalities.

III. SECURITY ISSUES OF IOT

- Unpredictable Behaviour – The behaviour of the internet of things are unpredictable due to the sheer volume of deployed devices and their long list of enabling technologies. There is no prediction about how systems works when it interact with others hence is required a specific system that is well designed and within the control of administration [5].
- Device Similarity –They are uniform in their nature. Internet of things utilized the same components and connection technology. All the present nodes in the network have the same specification for the transfer of data from source to destination. If one system or device suffers from the same issue other devices also show vulnerability and did not perform well.
- Problematic Deployment – The main goal of the IoT is to place advanced networks and analytics at the place where it is not possible to go physically. [6].
- No Upgrade Support –Many up gradation are offered that are ignored by the user or not recognized. Hence, up gradation of a system from time to time is very essential in IoT [7].
- Web interface vulnerability: In order to circumvent access controls by hackers this is security vulnerability in web applications. Some security issues are vulnerable weak sessions, poor credentials management and cross-site scripting. This becomes major issue as most of these devices pride access through the cloud.
- Poor or No Transparency – According to their functionality many IoT devices fail to provide transparency. The user not aware of the internal processing of the system hence fails to access and observer the functionality of devices. [8].

IV. SECURITY ALGORITHM

RSA algorithm (Rivest-Shamir-Adleman) -RSA is a public-key encryption, and used for securing sensitive data, over an insecure network. In RSA cryptography, both the public and the private keys use to encrypt; the opposite key is used to decrypt it. RSA provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.[9]



RSA algorithm

- Select two large prime numbers p and q
- Compute
  n = p*q
  v = (p-1)*(q-1)
- Select integer k relatively prime to (not a factor of) to v
- Compute d such that
  d*k = k*d = 1 (mod v)
- Public key is (n, k)
- Private key is (d, n)

- Example
  - p = 11
  - q = 29
  - n = 319
  - v = 280
  - k = 3
  - d = 187
- public key
  - (319,3)
- private key
  - (187, 319)

Data Encryption Standard (DES) - DES works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key. Once the go-to, symmetric-key algorithm for the encryption of electronic data.[10]

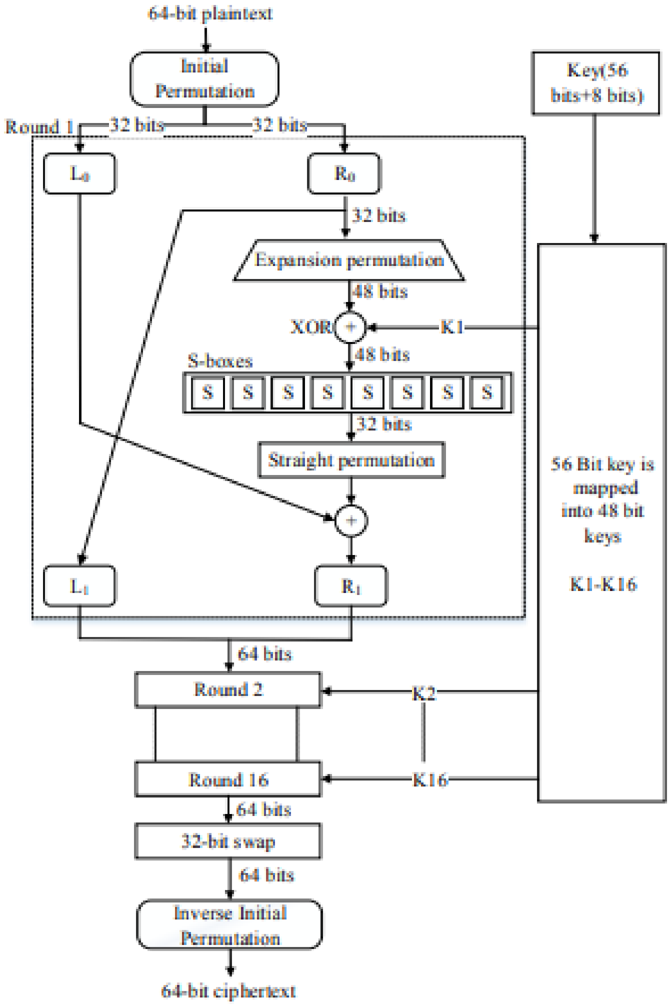
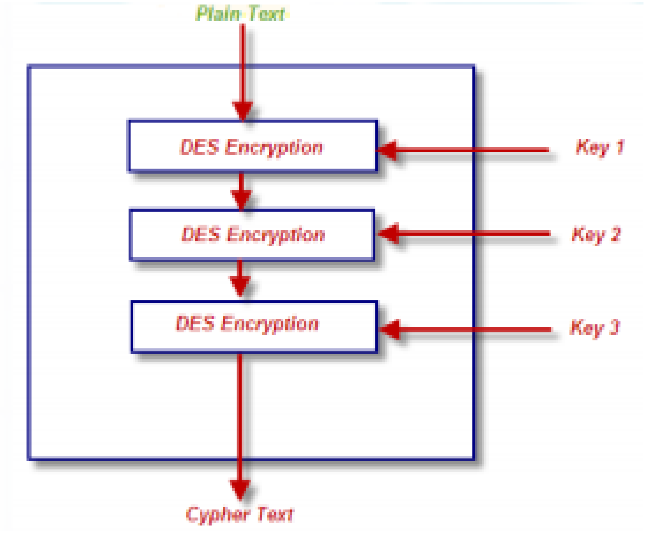


Figure 2. General Depiction of DES.

Triple DES (3DES) -Triple Data Encryption Standard (DES) is a computerized cryptography where block cipher algorithms are applied 3 times to each data block. The key size is increased to ensure additional security. Each block contains 64 bits of data[11]. Three keys are referred to as bundle keys with 56 bits per key.



Triple DES.

Advanced Encryption Standard (AES) - Advanced Encryption Standard is the new encryption standard to replace DES. The AES has three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits. Key size is unlimited, whereas the block size maximum is 256 bits. [12].

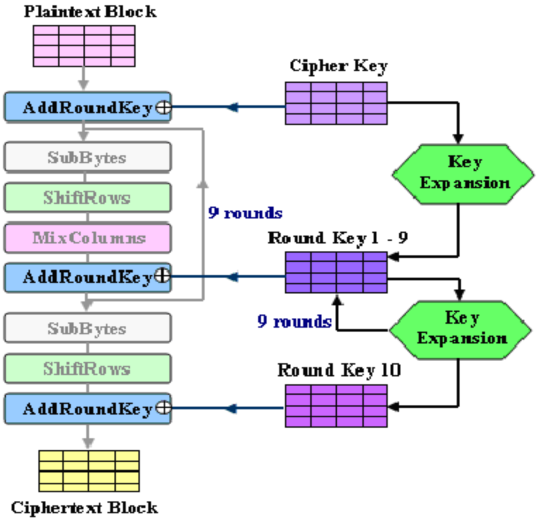


Figure 4. AES Sub Keys Generation.

V. LITERATURE REVIEW

Daemin Shin, et.al (2016) presented in this paper [13] that there are various services Smart Home Internet of Things (SH-IoT) within which the mobile nodes communication. However, the PMIPv6 security protocols do not support the secure route optimization involved when the mobile nodes communicate with external IoT devices in these services. In order to ensure the security and performance across the path of MNs and the IoT devices, the trust amongst the PMIPv6 domain and smart home is utilized in the newly proposed protocol. The steps for secure Route Optimization (RO) and handover management are involved within the proposed protocol. On the basis of analysis performed using BAN-logic and AVISPA, the correctness of proposed algorithm is calculated. The efficiency of proposed is calculated in the basis of network simulations performed. It is seen through the Bluetooth, Wireless network and ZigBee. The cryptography and security measures are provided on MAC layer by the ZigBee. On the basis of 128 bit PMIPv6 is resolved and the handover latency is minimized due to which the transmissions provided by proposed algorithm are highly secure to existing protocols.

Shuai Zhang, et.al (2017) presented in this paper [14] that within the Internet of Things (IoT), delay and security are the two important factors to be considered. A secure analytical framework is proposed in this paper through which the delay and secrecy of the network are to be characterized. The location of IoT devices and the temporal arrival of packets are modelled with the help of adopting stochastic geometry and queuing mechanisms initially. To enhance the performance of the network, a secure on-off mechanism is proposed. Further, in terms of packet delay and packet secrecy outage probability, the delay and secrecy performance evaluations are made. There is observed to be a trade-off amongst the delay and secrecy within the IoT systems. The delay and secrecy performances can be enhanced here with the help of secure on-off mechanism. The delay-security trade-off is reflected with the help of using secrecy transmission rate. On the basis of simulation results, the effects caused by the secure on-off scheme are seen in terms of the performance results on delay and secrecy of the IoT systems.

Dr.ReshmaBanu, et.al (2016) presented in this paper [15] that the traditional security mechanisms cannot handle the newly derived IoT systems which include advanced properties, techniques and issues within them. The new actors and their communications need to be studied along with the various security issues being faced which need to be resolved with the help of new secure IoT mechanism. These networks have been proposed with the involvement of biologically inspired models which help in security the IoT paradigms in much better way. There is a need of strong and decentralized security method in order to handle the features of these systems. The bio inspired techniques are gaining popularity due to their interesting methods generated due to the similarities amongst the biological methods and the operations of the networks. For different robust and computationally efficient security methods present in IoT, the research gaps are proposed in this paper along with the numerous biologically inspired algorithms that have used to improve the security of these techniques.

MinelaGrabovica, et.al (2016) presented in this paper [16], a study related to the Internet of Things (IoT) which includes within them various electronics, software and network connectivity based deviceswhich are of everyday use. In order to extract the important information, the users communicate with the devices through this manner. The major issue within the IoT is the data security. There are various communication technologies used within IoT that utilize the security protocols which are studied in this paper.

The most commonly used protocols are RFID, keys and AES encryption, ZigBee provides access control, encryption, integrity of frame as well as the sequential freshness. There are two different security modes which are with and without authentication that are provided in by Bluetooth. Once the link is established, there is security procedures initiated in case there is no authentication present. The numerous techniques are compared and an analysis of these techniques amongst each other is presented in this paper.

ZimuGuo, et.al (2016) presented in this paper [17] that the endpoint devices and the physical objects are connected to the Internet within the Internet of Things (IoT). Although there are many advantages of the IoT systems in our daily lives, however, there are various security issues as well which have been faced by the users. There is a need to ensure the security related measures in proper manner within the IoT systems. Also the security mechanism should begin from bottom up approach. The devices as well as humans need to interact with each other through the IoT devices. The convenience as well as security of IoT applications needs to be enhanced which is provided by the biometrics. The advantages as well as disadvantages related to the biometrics present within IoT are to be considered in this paper. The novel biometrics is combined with the system-level obfuscation techniques so that the unauthorized users cannot access the IoT devices. With the help of this technique the security of IoT devices is improved.

José L. Hernández-Ramos, et.al (2015) presented in this paper [18] that with the rise of Internet of Things (IoT), there is now being introduced the real time pervasive computing. The information that is being received from the surroundings needs to be identified and communicated with the help of smart objects that are equipped in our daily use through this system. On the basis of changes and dynamic conditions, the entities are deployed within the environments. This can help in modifying the operation or behaviour of systems. The mechanism through which the information is utilized by the smart objects in order to make various security decisions is presented in this paper. The so-called context-aware security present on the IoT systems is computed by taking this gathered information as a first-class component. Amongst the various components related to security of framework, the interactions are provided by this method. This helps in generating awareness amongst the systems by providing envisioned security methods. As per these methods, the security decisions are adapted by this system.

VI. TABLE OF COMPARISON

Author	Description	Problem /Issues	ProposedMethod
Daemin Shin, et.al (2016)	Various services Smart Home Internet of Things(SH-IoT).	PMIOv6 security protocol do not support the secure route optimization (in communicate with external Iot Device).	Secure Route Optimization (RO) and handover management are involved within proposed protocol.
Shuai Zhang, et.al (2017)	A secure analytical framework is proposed in this paper through which the delay and secrecy of the network are to be characterized.	location of IoT devices and the temporal arrival of packets are modeled with the help of adopting stochastic geometry and queuing mechanisms initially.	A low-complexity secure on-off mechanism is proposed.
Dr. Reshma Banu, et.al (2016)	traditional security mechanisms cannot handle the newly derived IoT systems.	The new actors and their communications need to be studied along with the various security issues being faced which need to be resolved with the help of new secure IoT mechanism.	biologically inspired algorithms that have used to improve the security of these techniques.
Minela Grabovica, et.al (2016)	This paper explores security protocols provided by communication technologies used in IoT such as: RFID, Bluetooth, Wireless network and ZigBee	The major issue within the IoT is the data security.	The cryptography and security measures are provided on MAC layer by the ZigBee. 128 bit keys and AES encryption, ZigBee provides access control, encryption, integrity of frame as well as the sequential freshness.
Zimu Guo, et.al (2016)	The endpoint devices and the physical objects are connected to the Internet within the Internet of Things (IoT).	There are various security issues as well which have been faced by the users. There is a need to ensure the security related measures in proper manner within the IoT systems.	The security mechanism should begin from bottom up approach. Security of IoT applications needs to be enhanced which is provided by the biometrics.
José L. Hernández-Ramos, et.al (2015)	Introduced the real time pervasive computing. The information that is being received from the surroundings needs to be identified and communicated with the help of smart objects.	The mechanism through which the information is utilized by the smart objects in order to make various security decisions.	context-aware security present on the IoT systems.

REFERENCES

[1] Keyur K Patel, Sunil M Patel, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges", IJESC, 2016..

[2] S. Sicari, A. Rizzardi , L.A. Grieco , A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead", Computer Networks, vol. 56, pp. 133-151, 2015.

[3] Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal, Zied Chtourou, "A Roadmap for Security Challenges in Internet of Things", vol. 12, pp. 15-21, 2017.

[4] Kim Thuat Nguyen, Maryline Laurent, Nouha Oualha, "Survey on secure communication protocols for the Internet of Things", Ad Hoc Network, vol. 7, pp. 5-15, 2015.

[5] David Linthicum, "Responsive Data Architecture for the Internet of Things", IEEE Computer, Vol 49, Issue 10, pp. 72-75, October 2016.

[6] Dongsik Jo and Gerard Jounghyun Kim, "ARIoT: Scalable Augmented Reality Framework for Interacting with Internet of Things Appliances Everywhere", IEEE Transactions on Consumer Electronics, Vol. 62, Issue. 3, pp. 334-340, August 2016.

[7] Xinlie Wang, Jianqing Zhang, Eve. M. Schooler, "Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT", Communications (ICC), 2014 IEEE International Conferenc , 2014.

[8] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," Elsevier Future Generation Computer System, Vol. 29, 2013.

[9] Ajay Kakkar, M. L. Singh and P.K. Bansal, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network", International Journal of Engineering and Technology, Volume 2 No. 1, pp. 87-92, January 2012.

[10] "DES", http://www.tropsoft.com/strongenc/des.htm.

[11] "3DES", http://en.wikipedia.org/wiki/Triple_DES.

[12] "AES",https://www.techopedia.com/definition/1763/advanced-encryption-standard-aes.

[13] Daemin Shin, Vishal Sharma, Jiyoon Kim, Soonhyun Kwon, and Ilsun You, "Secure and Efficient Protocol for Route Optimization in PMIPv6-based Smart Home IoT Networks", 2016, IEEE.

[14] Shuai Zhang, Jianhua Peng, Kaizhi Huang, Xiaoming Xu and Zhou Zhong, "Physical Layer Security in IoT: A Spatial-Temporal Perspective", 2017, IEEE.

[15] Dr. Reshma Banu, Dr. G. F. Ali Ahammed, Nasreen Fathima, "A Review on Biologically Inspired Approaches to Security for Internet of Things (IoT)", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016.

[16] Minela Grabovica, Dražen Pezer, Srdan Popic, Vladimir Kneževic, "Provided security measures of enabling technologies in Internet of Things (IoT): A survey", 2016, IEEE.

[17] Zimu Guo, Nima Karimian, Mark M. Tehranipoor and Domenic Forte, "Hardware Security Meets Biometrics for the Age of IoT", 2016, IEEE.

[18] José L. Hernández-Ramos, Jorge Bernal Bernabe, Antonio F. Skarmeta, "Managing Context Information for Adaptive Security in IoT environments", 2015 29th International Conference on Advanced Information Networking and Applications Workshops.