Internet of Things and its enhanced data security

Arpit Kumar Srivastava, Apoorv Agarwal, Abhinav Mathur

***Abstract*— The Internet of Things (IoT), an emerging global Internet-based technical architecture facilitating the exchange of information, goods and services in the internet world has an impact on the security and privacy of the involved stakeholders. Measures ensuring the architecture's resilience to attacks, data authentication, and access control and client privacy need to be established.**

This paper includes a survey of IoT and various security issues related to it. Furthermore, out of all security issues, concern over data authentication and transfer is taken into consideration. Here we will discuss the idea for two levels of security in form of two different approaches i.e. Advance Encryption Standards (AES) and the Steganography approach via an image and the simulating of these two logics in the MATLAB.

***Index Terms*— Internet of Things (IoT), RFID, Advance Encryption Standard (AES), Steganography.**

I. Introduction

Internet of Things is everything. It can be defined in many different ways, depending upon what you are dealing with, how you manage them and what are your resources. It encompasses several aspects of life-from various components (such as refrigerator, oven, and washing machine) to well-equipped semi-detached homes, from travelling tools to sophisticated devices to track down from an individual's behavior to his extent of thinking and collecting relevant data and "apply services".

IoT [1]-[2] is the next step of digital data virtualization since it can be visualized as the interaction between several packets of data from various devices and their exchange between machines and objects. Internet of Things (IoT) is something that connects 100 millions of people as an emerging global Internet-based information architecture facilitating the exchange of data and information at global level.

The term of IoT was first used by Kevin Ashton in 1999 (though the concept has been discussed since 1991) in the context of supply chain management [3]. From the technical point of view, the structure is based on data communication tools, primarily RFID-tagged items and cloud-based support services. The IoT [4]-[6] has a purpose of providing an IT-infrastructure, providing the exchange of "things" in a safe and reliable manner.

Arpit Kumar Srivastava, Department of Computer Science, Galgotias College of Engineering & Technology, Greater Noida, India, 8800157663.
Apoorv Agarwal, Department of Computer Science, Galgotias College of Engineering & Technology, Greater Noida, India, 9971049499.
Abhinav Mathur, Department of Computer Science, Galgotias College of Engineering & Technology, Greater Noida, India, 9971086947.

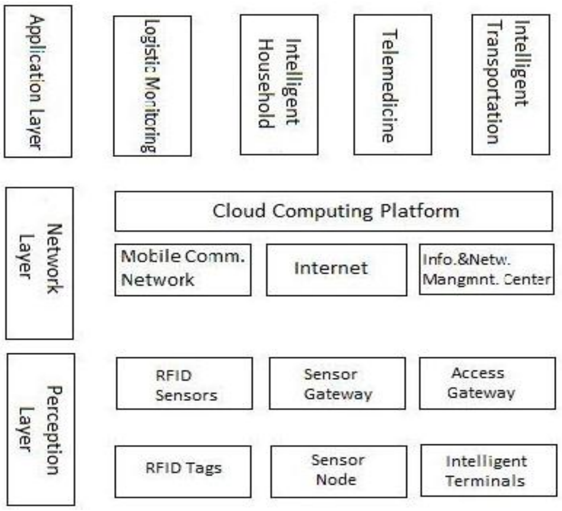

Fig. 1 Structure of IoT

Radio Frequency Identification (RFID) and sensor network technologies can be used to meet the new challenge of the next wave in the era of computing, in which information and communication system are invisibly embedded in the environment around us. This result in the generation of enormous amounts of data which need to be stored, processed efficiently and presented in a seamless and understandable form.

Security of the data, channels, medium etc. is an important aspect into which the IT organizations are most concerned about [7] Despite of the theoretical concept of the secured servers and smart devices, practical implementation of these security features are at minimal. [8]- [10]. Following security and privacy requirements can be mentioned as:

- Terminal security issue of IoT: terminal devices are easily accessible and can cause damage or data modifications. Authentication and integrity of the data is prior concern. Since passive RFID tags cannot exchange too many message with the authentication servers, main problem existed in the perception terminal includes terminal of sensitive information leakage, tampering, copying, terminal virus and other issues.
- Sensor network security problem of IoT: sensors are not only responsible for the data transmission but also data acquisition, integrity and collaboration. Therefore malicious code attacks and security risk in information transmission may occur.
- Information transmission security of IoT: security related to the security risk of IoT and the protocol vulnerabilities defects.
- Information processing safety of the IoT reflected in the middleware layer
- Data which is needed to be transferred must be encrypted before transmission. It aims to protect the confidentiality

and integrity of the information transmission and to prevent data tampering.

This research is opted because of several reasons. IoT is now becoming a world-wide technology, the potential users are exponentially increasing and the algorithm being used is cheap, easy to implement, can be easily reprogrammed and has good level of security.

This research paper is focused on the performance and the implementation of combined logic of AES and steganography. Here the data that is to be transferred between smart devices is required to undergo a set of process that includes sequential implementation of algorithms to enhance its security. Thereafter simulation of these algorithms is done on MATLAB environment.

II. RELATED WORKS

To give more description about the implementation and analysis of this 2-tier security, this section show some other work from the related field.

In [11]-[13], authors analyzed the performance of DES, AES and Blowfish encryption algorithms. Furthermore there performance is compared over varying block size, key size and number of round of the encryption input file. And thus their performance is analyzed by computing various performance parameters such as execution time and memory required. The result showed blowfish algorithm consumes less execution time, memory usage and produce more throughputs. Blowfish algorithm performed approximately 4 times faster than AES and 2 times faster than DES.

Thereafter the blowfish algorithm is studied and enhanced and its function is modified [14]. In [15] author designed an algorithm that combines the process of bits from ancient cipher and substitution boxes from modern cipher. These research present the idea that either AES, DES, 3DES or Blowfish algorithms are good enough for securing the data transmission between devices or terminals to some extent or they are even better in comparison to each other, but the level of security provided is limited to only one level.

III. DESIGN

Advance Encryption Standard: AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES uses Rijndael cipher which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits and is defined in three versions 10, 12 and 14 rounds respectively.

Fig. 2 show the functional structure of the AES. The plaintext block size of 128 bits (16 bytes) is converted into cipher text using key of length 128, 192, or 256 bits (16, 24, 32 bytes). The algorithms is referred to as AES-128, AES-192 and AES-256, depending upon the key length.

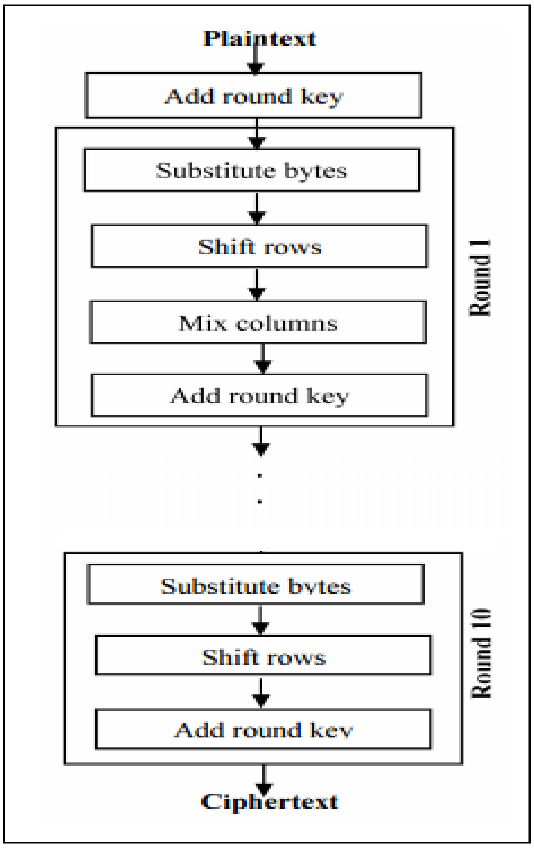

Fig. 2 Structure of AES

There are three steps performed in AES, i.e. encryption, decryption and key generation.

AES encryption
Step 1: Get the plain text and the key
Step 2: Perform the pre-round transformation using the plain text
Step 3: With ‘n’ key length, perform transformation for ‘n’ rounds
Step 4: cipher text achieved

AES decryption
Repeat the step followed in encryption in reverse order

Key Generation
Step 1: Get the key
Step 2: based upon number of round, calculate required number of words
Step 3: In an array of 4 bytes, first four words are made from the key
Step 4: Get the next word
Step 5: Repeat step 4 until required number of words are reached.

Steganography: Image steganography is the modern way of hiding the text in an image in such a way that the information hidden is secure and well away from the intruder. Apart from hiding the secret data, it is also useful in data authentication and availability of data ensuring proper usage, data monitoring, copyright protection, ownership identification, confidentiality and control of data piracy etc.

Fig.3 show flow chart of image steganography.

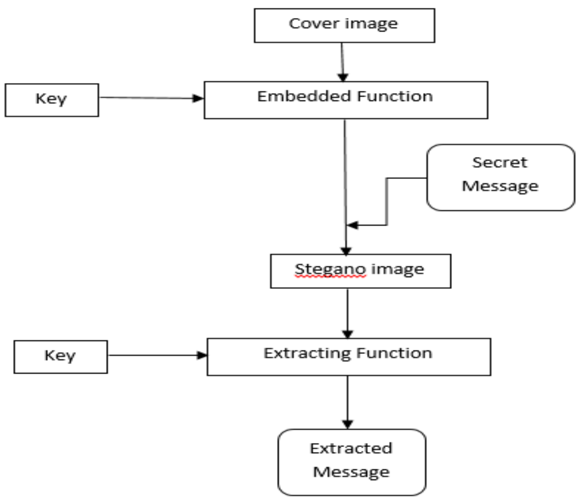

Fig. 3 Steganography workflow

IV. WORKFLOW

Securing the data and information among the devices in organization is a serious issue especially when devices are connected to the internet. Using two simple and cheap encryption algorithms but implementing efficiently could help us to achieve a bigger goal. This research uses the AES algorithm followed by image steganography. The message that is needed to be transferred from one device to another (in case of IoT, it is smart devices), is first encrypted using AES encryption and the generated cipher text is hidden in an image using steganography technique. The generated stegano image is transferred in the communication channel where it is secured from the intruder. At receiver side the mentioned steps are followed in reverse order and ultimately the plain text is achieved.

Fig. 4 show how the implementation process of the approach actually takes place.

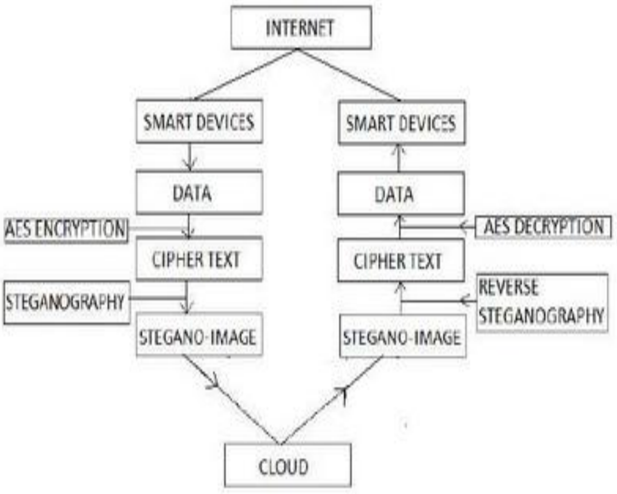

Fig. 4 Workflow

V. FUTURE WORK

This research is expected to provide us with security features and facilities that can be easily taken into consideration. The 2-tier secure channel that we are providing is not only cheap and efficient but will also enhance the integrity of the data. Smart devices now-a-days are vulnerable to many types of attacks and this approach can be helpful in distinguishing various intruders and can thus provide a broader area for analysis and data protection.

REFERENCES

[1] Rajkumar Buyya, Jayavardhana Gubbi, Slaven Marusic, Marimuthu Palaniswami -Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions, University of Melbourne, Australia.

[2] Ashton, Kevin (22 June 2009). "That 'Internet of Things' Thing, in the real world things matter more than ideas". RFID Journal.

[3] The Internet of Things. International Telecommunication Union (ITU). ITU Internet Report, 2005.

[4] Gonzalez G. Organero M, Kloos C. “Early in infrastructure of all Internet of Things in space for learning”. 8th IEEE International Conference on Advance Learning Technologies, pp-381-383, 2008.

[5] Amardeo C, Sarma J. Identities in the future Internet of Things. Wireless Pers Commun, 2009, 49:353-363

[6] Security model and key technologies for the Internet of things, The Journal of China Universities of Posts and Telecommunications, December 2011.

[7] Lan Li, Study on security architecture in the internet of things, International Conference on Measurement, information and Control (MIC), 2012.

[8] Xu Xiaohui, Study of Security problem and Key Technologies of the Internet of Things, International Conference of Computation and Information Sciences, 2013.

[9] Leusse D, Per Iorellis P, Dimitrakos P. ―Self-Managed Security Cell, a Security Model for the Internet of Things and Services Advances in Future Internet‖. 2009 First International Conference on Digital Object Identifier, pp. 47-52, 2009.

[10] Security model and key technologies for the Internet of things, The Journal of China Universities of Posts and Telecommunications, December 2011.

[11] Ramesh.A, Suruliandi.A, “Performance Analysis of Encryption for Information Security”, IEEE, 2013.

[12] G.N.Krishnamurthy, Ramaswamy.V, M.E. Ashalatha,”Performance Enhancement of Blowfish and CAST-128 Algorithms and Security of Improved Blowfish Algorithms Using Avelanche Effect”, International Journal of Computer Science and Network Security, Vol.8 No.3, 2008.

[13] Ramesh.A, Suruliandi.A, “Performance Analysis of Encryption for Information Security”, IEEE, 2013.

[14] K.Mayers Rusell, H.Desoky Ahmed,” An Implementation of the Blowfish Cryptosystem”, IEEE.2008.

[15] R.Sriram and K.Marimuthu,”Designing an Algorithm with High Avelanche Effect”, International Journal of Computer Science and Network Security, Vol 11 No.1, 2011.

Arpit Kumar Srivastava, currently perusing Bachelor in Technology from Galgotias College of Engineering and Technology, Greater Noida; completed his SSC and HSC from Metropolitan School, Gorakhpur. He also has a research paper published at IJSRP with paper title “The Rabin Cryptosystem and analysis in measure of Chinese Remainder Theorem”. He is grade A certified RIO +21 International Year of Water Cooperation India Program under UNDDD.

Apoorv Agarwal currently perusing Bachelor in Technology from Galgotias College of Engineering and Technology, Greater Noida; completed his SSC and HSC from S.S. Children Academy, Moradabad.

Abhinav Mathur currently perusing Bachelor in Technology from Galgotias College of Engineering and Technology, Greater Noida; completed his SSC from Cambridge International, Indore and HSC from St. Don Bosco, Lakhimpur. He also has a research paper published at IJSRP with paper title “The Rabin Cryptosystem and analysis in measure of Chinese Remainder Theorem”.