International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-9 Issue-1, May 2020

An Effective Method of Hybrid Encryption on IoT

Lalit Kumar, Neelendra Badal

Abstract*: In the real world scenario, people are using various electronics devices according to their use. These devices are connected to each other in direct and indirect manner. This connection provides communication and sharing of information and data to one and another. This overall communication system uses various technologies i.e. Internet of Things, Cloud Computing, Fog Computing and other. The communication in IoT is based on Layered Structure. This layered structure helps to transfer data in safe and secure manner. For safe and secure transmission of data over IoT, user uses encryption method, but on encryption algorithm can be easily recognized by attacker so here user uses a hybrid approach. This hybrid approach is based on AES and Transpositional Reverse Algorithm. Here Transpositional Reverse Algorithm helps the users to secure the AES encryption scheme and helps to create an efficient Hybrid scheme.

Keywords: Internet of Things (IoT), Cloud Computing, Data and Information Security, Encryption Algorithms, Hybrid Encryption Method, AES, Transpositional Encryption Algorithm (TEA).

I. INTRODUCTION

Internet of things plays a vital role to create a huge interconnected device network. The network of IoT is based on collecting and gathering information, preprocessing of these data, share the data over the network, create abstraction for hiding hardware details and show the useful extracted information on application. On the Basis of this, we can create a layered structure for Internet of Things. On the basis of working of IoT we can divide the whole processing into five parts. So the layered structure of the IoT containing all five process is drafted below, where you can easily understand the whole working phenomenon of Internet of Things [4] [5].s

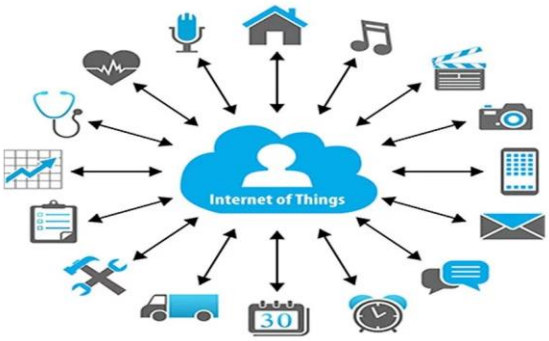

Fig. 1: Structure of IoT

The layered Structure of Internet of Things is drawn below:

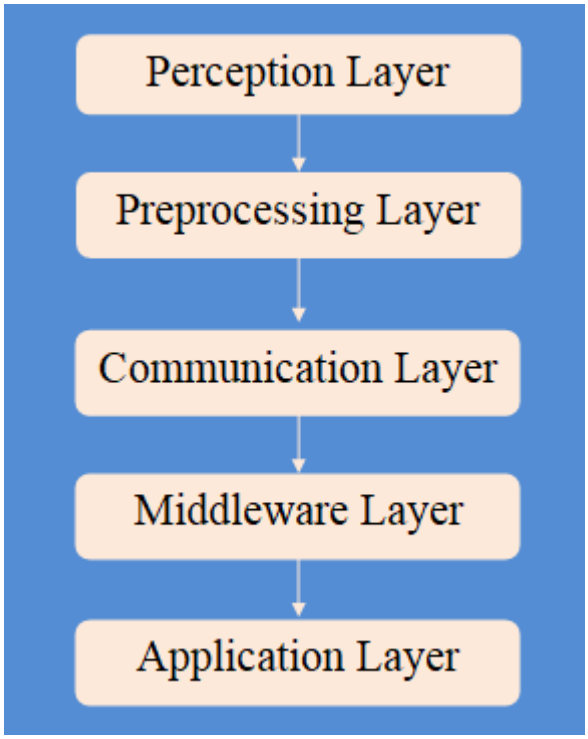

Fig. 2: Layered Structure of Internet of Things

A. Perception Layer: - In the Perception Layer of the Internet of Things, Here the huge amount of data is collected from various sensors. Theses based on various field such as Environment, Medical, Natural, Chemical Biosensor, Infrared Sensor and Mobile.

Here Sensor is a device, module, machine, or subsystem whose aims to detect executed events or various changes in its system and send the collected information to other electronics devices.

Manuscript received on May 07, 2020.
Revised Manuscript received on May 29, 2020.
Manuscript published on May 30, 2020.

* Correspondence Author

Lalit Kumar*, Department of Computer Science and Engineering, Seth Vishambhar Nath Institute of Engineering and Technology, Barabanki, India. Email: lalitkmr170@gmail.com.

Neelendra Badal, Department of Computer Science and Engineering, Kamla Nehru Institue of Technology, Sultanpur, India. Email: n_badal@hotmail.com.

B. Pre-processing Layer: - After collecting all data at the perception layer, a set of data is prepared. But this data is not in ready format so it needs preprocessing of data. By using the preprocessing of the data, we filter, extract and summarize data before sending it on the communication layer. So this layer is mainly helps to extract the useful information from a large amount of data that are observed by sensors in perception layer.

C. Communication Layer: - After extracting the useful data by filtering and summarizing the data at the preprocessing layer. The data is transmitted over a network for different-2 entities using various protocols and standard. This communication layer is working same as network and transport layer of Computer Network.

D. Middleware Layer: - Here at this layer, it creates an abstraction such as hiding hardware details and other information from the end user. Middleware is basically helps to separate the all things from the end users. It only shows the required information which is gathered by the sensors at the perception layer. The main applications of this layer is:

- Interoperability and Programming Abstraction
- Device Discovery and Management
- Scalability
- Big Data Analytics
- Security and Privacy
- Cloud Service
- Context Detection

E. Application Layer: - In this layer, Here various application uses that improves user experience and increase efficiency of data. This is the last layer of this architecture, this layer contains a knowledge full data by the decision making takes place in various situation. This decision is based on the gathered data by sensors. This Layer is works as Front End for User. The use of this layer is done in

- Energy Conversation
- Smart Transport
- Social Life and Entertainment
- Supply Chain Logistics
- Health and Fitness
- Smart Environment
- Home Automation
- Smart Agriculture

So after discussing all this information about Internet of Things, Here an issue originated i.e. data security over the transmission of data. The data transmission of the sensors is transmitted over the cloud using Internet. This data is very useful for the receiving device so user used various encryption techniques here to encode the information during the transmission of data on cloud using internet. But here an issue arises that is stealing of data over the internet or on cloud, so user need to keep the data in encrypted form (data abstraction) in middleware. But in Today world scenario a single encryption techniques cannot protect your data so here we need to Hybrid encryption. Hybrid Encryption is defined as the using of two or more encryption technique to encrypt the data. Hybrid encryption is very helpful for securing data because here the attacker cannot easily recognized the encryption technique so it cannot be easily decrypted by the attacker. Before applying the hybrid encryption of the data on the cloud for Internet of Things, user should clear that the used algorithm is efficient and takes less time for execution. In present world scenario, user uses many encryption techniques i.e. AES, DES, Blowfish, 3DES, TwoFish Encryption Algorithm, IDEA Encryption Algorithm, MD5 Encryption Algorithm, RSA Security and other encryption methods has been used to encrypted data.

II. LITERATURE SURVEY

Now we discussed about all the paper by this we tried to find the problem and try to remove that.

Lalit Kumar and Neelendra Badal [1], introduced an encryption model where the author uses the hybrid approach for providing security to data and passwords in the system. Here author also tried to make an efficient hybrid encryption system in sense of execution time by adding a transpositional encryption algorithm with the hash encryption system instead of using another hash function.

L. Kumar et al. [2] explored and reviewed on cloud computing for the hybrid encryption scheme. In this paper author presents some preceding information about the variety of works and the author's main emphasis is on AES and FHE's hybrid approach. This hybrid approach helps the author to keep extra redundant and convenient records in comparisons with several specific ones. With this approach, users can guard the attackers ' confidentiality of information, privacy and honesty. talk about its operation in this technique section of this paper consumer by using go with the flow chart and algorithm to understand this approach well. Diego Mendez Mena, Ioannis Papapanagiotou & Baijian Yang [3], here the user's intention to provide a revolutionary survey of IoT protection and privacy challenging circumstances from the technical and systemic perspective used. This paper focuses on intrinsic IoT vulnerabilities and their consequences in the confidentiality, honesty and availability of security threats to the critical documents. This survey's methodology is to summarize and synthesize published paintings in IoT; link them to the sphere's protection conjuncture; and task forward directions for future studies.

Atzori, Luigi & Lera, Antonio & Morabito, Giacomo [4], this survey paper targets those who wish to pursue and contribute to the growth of this dynamic discipline. Various visions of this model of the Internet of Things are recorded and the technologies are checked. What emerges is that the research community is still facing big issues. Y. Chandu et al. [6], through this paper we will be explaining the various algorithms and benefits and drawbacks, and how the advanced standard algorithm is implemented we have a great influence on cryptography and the various processes in the process of encryption and decryption.

III. ENCRYPTION ALGORITHM

Here in this paper we basically discussed on two encryption scheme i.e. AES (Advance Encryption Standard) and Transpositional Encryption Algorithm.

A. AES (Advanced Encryption Standard)

The Advanced Encryption Standard (AES) is the most popular and commonly accepted algorithm for symmetric encryption which is likely to be found today. It finds itself six times faster than triple DES [1] [2], at least.

As its key size was too small it took a replacement for DES. It was deemed vulnerable to exhaustive key search attacks with increased computing capability. To overcome this constraint, Triple DES was designed but found to be sluggish.

Working of AES:

AES is an iterative cipher, rather than a Feistel. This is based on the' substitution' network-permutation. It consists of a sequence of connected operations, some involving replacement of inputs with different outputs (substitutions) and some involving shuffling bits (permutations) around them.

AES performs all its computations on bytes rather than bits. Consequently AES treats the 128 bits of a plaintext row as 16 bytes. These 16 bytes are broken down into four columns and four matrix-processing lines [7].

Unlike DES, the number of rounds in AES is variable, and depends on the length of the key. In 10 rounds AES uses 128-bit keys, in 12 rounds 192-bit keys and in 14 rounds 256-bit keys. Growing round uses another round key of 128 bits, determined from the original AES key [6].

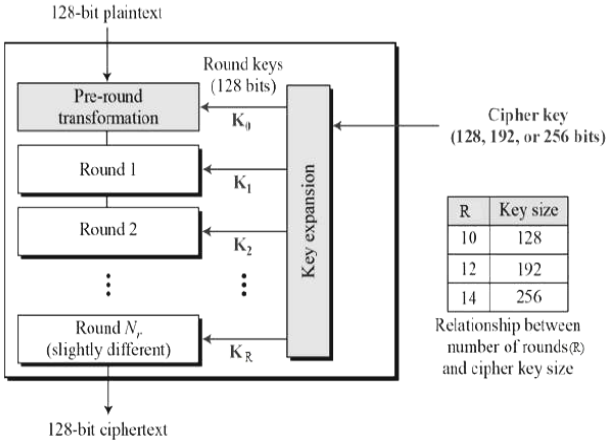

Figure 3: Working Process of AES Encryption Scheme

B. Transpositional Encryption Algorithm (TEA)

Transposition cipher is a simple scheme to encrypt data. In Cipher transposition, the plaintext characters are moved to form cipher text in some regular sequence. User can use different techniques in the Transposition Encryption Process. Here consumer uses the easy to implement reverse string transposition algorithm [1].

Transposition Cipher includes all of the plain text Alphabet but in a way that is not understandable without Key. Key is used here to assign or position an alphabet at a specific spot. Here user changes only the position of the plain text character.

For example, if a Text is “encryption” then after relating Transposition method. It will be “noitpyrcne”.

The Basic Algorithm of this method is

1.) If there is a word which is consist of ‘n’ alphabets
i.e. p(1), p(2), p(3), p(4) ---------- p(n)

2.) Then after Converting it into the cipher text it will be
p(n), p(n-1), p(n-2)----------p(3), p(2), p(1).

Proposed Method

This Proposed work is based on advancement of AES Encryption scheme because attacker can easily recognized the used encryption algorithm in the encryption process. So here user tried to achieve more security using TEA on AES encryption Scheme.

Here in this method, when we give any input string then the respective cipher text generated using AES Encryption Scheme. This Cipher text is again passed through TEA. After that a desired output is generated that contains the property of both encryption algorithms i.e. AES and Transpositional Encryption Algorithm. The working Process is

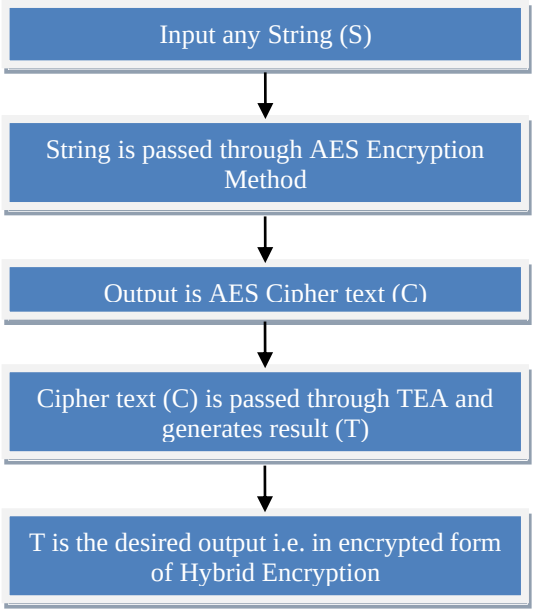

Figure 4: Hybrid Encryption Process of Proposed Work

IV. Result and Analysis

In this section we tried to show the execution time in reference of various length strings. Here we take various length strings and apply hybrid encryption on that strings and analyze the working time of AES and Hybrid Encryption.

There are designed two tables, where each table contains set of strings and their respective execution time (in millisecond). Both tables contain variable length string to analyze the execution time.

Table 1: Execution Time of AES Encryption Algorithm respected to some strings

S. No.	Strings	Execution Time for AES (millisecond)
1	Aaaaaaaaaa	35
2	AA@123$22	35
3	Avbjhdhj$12	35
4	A@9876543	36
5	Homogeneous	36
6	Heterogeneous	36
7	Popoualrity@3423	37
8	123#Colleges	37
9	Lion@Wisdom	37

10	Guru@432132	38

Here the (Table 1) designed to show execution time of AES Encryption schemes to the respect of some strings.

Table 2: Execution Time of Hybrid Encryption Algorithm (AES+ Transpositional Reverse Algorithm) respected to some strings

S. No.	Strings	Execution Time for AES+ Transpositional Reverse Algorithm (millisecond)
1	Aaaaaaaaaa	36
2	AA@123$22	36
3	Avbjhdhj$12	37
4	A@9876543	37
5	Homogeneous	38
6	Heterogeneous	38
7	Popoualrity@3423	38
8	123#Colleges	39
9	Lion@Wisdom	39
10	Guru@432132	39

Here the (Table 2) designed to show execution time of Hybrid Encryption schemes to the respect of some strings. Here we create an approach that contains the property of both encryptions Algorithm. Firstly we apply AES encryption scheme on set of string then apply transpositional Reverse Algorithm.

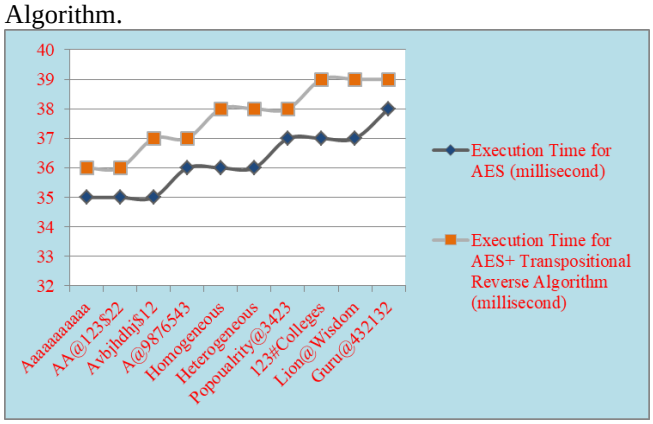

Figure 5: Comparison Chart of AES and Hybrid Encryption Execution Time in respect of various strings

V. CONCLUSION

The overall motive of this paper is based on information and data security. In this paper, we tried to create an approach which helps to make efficient AES encryption scheme. This approach helps to hide the identity of itself from the attackers. By this user can keep our data in secure and effective manner.

Another conclusion of this approach is to create a safe and secure hybrid encryption scheme by adding a hash algorithm with a transposition Algorithm. This Hybrid encryption system is also efficient in terms of execution time because it takes a little bit more execution times in comparison of AES Encryption Algorithm.

REFERENCES

1. L. Kumar and N. Badal. Minimizing the Effect of Brute Force Attack using Hybridization of Encryption Algorithms. International Journal of Computer Applications 178(33):26-31, July 2019
2. L. Kumar and N. Badal, "A Review on Hybrid Encryption in Cloud Computing," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-6.
3. D. M. Mena, I. P. & B. Yang (2018): Internet of things: Survey on security, Information Security Journal: A Global Perspective, DOI: 10.1080/19393555.2018.1458258
4. A., L. & Lera, A. & Morabito, Giacomo. (2018). THE INTERNET OF THINGS: A SURVEY. DOI: 10.25073/0866-773X/64.
5. Said, O. & M., Mehedi. (2013). Towards Internet of Things: Survey and Future Vision. International Journal of Computer Networks. 5. 1-17.
6. Y. Chandu, K. S. R. Kumar, N. V. Prabhukhanolkar, A. N. Anish and S. Rawal, "Design and implementation of hybrid encryption for security of IOT data," 2017 International Conference On Smart Technologies For Smart Nation (Smart Tech Con), Bangalore, 2017, pp. 1228-1231.
7. A. M. Deshpande, M. S. Deshpande and D. N. Kayatanavar, "FPGA implementation of AES encryption and decryption," ICCACEC, Perundurai, Tamilnadu, 2009, pp. 1-6.

AUTHORS PROFILE

Lalit Kumar, who is working as Assistant Professor at Seth Vishambhar Nath Institute of Engineering and Technology. He completed his master's (M.Tech. in CSE) from Kamla Nehru Institute of Technology Sultanpur. His Dissertation is based on Data and Information Security under the supervision of Dr. Neelendra Badal. He also completed his B.Tech. From Sagar Institute of Technology and Management (Affiliated with AKTU).

Dr. Neelendra Badal is a Professor in the Department of CSE at Kamla Nehru Institute of Technology at Sultanpur , U.P., INDIA of Dr. A.P.J. Abdul Kalam Technical University, UP Lucknow INDIA (Formerly Uttar Pradesh Technical University, (UPTU), Lucknow). He received B.E. (1997) from Bundelkhand Institute of Technology, Jhansi (U.P.), INDIA, in CSE, M.E. (2001) in Communication, Control and Networking from Madhav Institute of Technology and Science, Gwalior (M.P.), INDIA and PhD (2009) in CSE from Moti lal Nehru National Institute of Technology, Allahabad (U.P.).