International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

# Enhancing the Security System using Cryptography for IoT Based Devices

**Sheenu Sachdeva[1], Aruna [2]**

[1]Assistant Professor, Department of CSE, JCDM College of Engnierring, Sirsa, Haryana, India
[2]M.Tech. Scholar, Department of CSE, JCDM College of Engnierring, Sirsa, Haryana, India

**Article Info**
Volume 8, Issue 5
Page Number : 227-232

**Publication Issue :**
September-October-2021

**Article History**
Accepted : 01 Oct 2021
Published: 07 Oct 2021

## ABSTRACT

Internet of things (IOT) are becoming popular and taking an important place in our daily routine life. IOT based devices are making our life easy and comfortable. Although IoT explosion offers a wide range of opportunities for manufacturers and consumers, it also poses major risks in terms of security being a widespread network. A security mechanism is needed to protect the devices from cyber attacks. This can only be achieved by including security mechanism in the early stages of IoT based device's design to observe privacy and safe transmission of data over network. In existing system, standard protocols were used for data transmission and basic encryption techniques were being applied for ensuring the security of IoT based devices. But it failed in preventing against routing attacks and packet losses in transmission. To overcome these problems, a two tier security model has been proposed in present study. Therefore, this paper proposes a two tier security model for IoT based devices. In this approach the advanced encryption standard (AES) are used with multiplicative inverse encryption algorithm (MIE) to ensure the security of data. A comparative analysis between proposed model and existing model has been performed in the present study. The parameters packet size, transmission time and error rate has been determined in the comparison.

Keywords : IoT, Data Security, AES, MIE Encryption Algorithm.

## I. INTRODUCTION

Internet of things (IoT) is recognized as foremost important areas of future technology and gaining enormous attention from a wide range of industries. Internet of things (IoT) is an upheaval of the internet. It provides a platform for communication between gadgets where gadgets can manage and organize themselves. The IoT allows everyone to be connected anytime and anywhere. IoT has emerged as an area of incredible impact, with the arrival of savvy homes, savvy cities, and savvy everything. For current and future research areas it is one of the hot topics involved by both industry sector and academia. The Internet of Things (IoT) also known as a web of everything. Privacy and security are the major challenges in the Internet of Things (IoT) due to the distributed nature of IoT networks [1].

The framework of IoT consists of three layers that are Perception, Network, and Application layers. A number of security principles should be imposed on each layer to achieve a secure IoT realization.

Providing data security during data transmission is a major issue in IoT. In order to use device communication effectively, thus there is need to improve the security. Cryptography is an effective way to protect the sensitive information. This paper proposes a two tier security model for IoT based devices. This model is providing security to data at many layers. Programming of socket server and corresponding client is made to prevent unauthentic access during data transmission. More complex keys are used during encryption and decryption by integration of AES and multiplicative inverse encryption (MIE) cryptographic techniques. Encryption techniques used for Security of IoT Based devices. There are different encryption techniques which are used for the security of IoT devices. These are listed below:

### 1.1 Advanced Encryption Standard (AES)

AES is known as a cryptographic algorithm which is used in order to protect different security systems. AES stands for Advanced Encryption Standard. It is a symmetric block cipher which has been selected by government of United State in order to secure the classified data or information. In addition to this, this algorithm has been implemented within software as well as within hardware in overall the world for the encryption of sensitive information. Therefore it has become essential to secure the computer systems, to provide the cyber security. Along with this, there was the need of a secure algorithm which can secure the electronic data. This algorithms is efficient to defenses our system against different type of attacks. In AES, three block ciphers named: AES-128, AES-192 and AES-256 are comprised. In AES-128, 128-bit key length is used in order to make encryption and decryption of a block related to messages. Within, AES-192, 192-bit key length is used for this task. In AES-256, 256-bit key length is required for the encryption and decryption of content [2].

### 1.2 Multiplicative Inverse Technique

Multiplicative inverse is the reciprocal of a number in mathematics. For example the multiplicative of a, is denoted by 1/a. The multiplicative inverse of a portion x/y is y/x. if one wants to get the multiplicative inverse of a real number; divides 1 by the real number. It can be understood by another example as the reciprocal of 10 will be 1/10 whereas 2 will be the multiplicative inverse of 0.5. To get the multiplicative inverse of a number, it is required to divide 1 by the number. The function f (a) that maps a to 1/a, is simple example of a function.

The qualifier multiplicative is often neglected in the phrase multiplicative inverse and inferred understood (in contrast to the additive inverse). Multiplicative inverses can is expressed over different mathematical domains along with numbers. In such conditions, it may be occurs that $xy \neq yx$; therefore "inverse" specially involve that an element is both a left and right inverse.

### 1.3 Multilayer Encryption

Traditional data transmission modules are not efficient to secure the data during it transmission. There is need to have a secure and efficient module for data transmission securely. It is not enough to secure the data on single layer. In addition to this, it has become essential to avoid weak encryption key. Therefore there are chances of data loss. It is not sufficient to decrypt the data only one layer using single encryption technique.

Our data transmission module must consist of more than one technique. Data must be encrypted on multiple layers. Keeping in mind the issue of security, it has become vital to provide a multi techniques integrated module which can secure the data during its transmission over a network. To resolve this issue, Multiplicative and AES Encryption based module is proposed here. Such system is providing security to data at many layers.

This system is securing content using multiplicative inverse and AES approach. Session layer security would be enhanced by introducing multilayer security mechanism.

The process flow of proposed work is made here such as; Network security might be enhanced by customizing encryption techniques, Loopholes of existing security mechanisms are considered and security of network is enhanced. Programming of socket server and corresponding client is made to prevent unauthentic access during data transmission. More complex key are used during encryption and decryption by integration of AES and multiplicative inverse cryptographic techniques.

## II. REVIEW OF LITERATURE

Mahalakshmi et.al (2019) proposed the approach of combined two existing encryption algorithms and implemented their model in simulation tool named Matlab. It is very difficult to provide security to IoT based devices using traditional encryption technique. They explained that a hacker can know the cipher key. After that a plaintext image can easily get using private key. This proposed algorithm has the feature of robustness. In addition to this, it is able to offer better security than existing algorithm [3].

Marek and Ogiela (2019) proposed a new security solutions based on cognitive approaches. In this paper they considered innovative computing paradigm which is also known as cognitive cryptography. These modules have been formulated in order to semantic evaluate the encrypted data. Furthermore, they also select most appropriate and efficient mechanism or techniques for encryption process. This research work has presented a feasible application related to these mechanisms in order to resolve security tasks like authentication, secret sharing, secure data management etc [4].

Irosh and Malka (2019) considered the remote monitoring of health should be made trustworthy by incorporating WBAN, IoT, and cloud computing. These are beneficial for intelligent healthcare setting. Cloud computing also provides real-time data storage and processing for IoT devices like WBAN devices. These results can be improved and cost effective healthcare remote monitoring paradigms. The key uses of an IoT healthcare system has been enhanced the clinical care. In addition to this, the remote monitoring as well as the physiological assistance is provided to patients [5].

Yusfrizal et.al (2018) proposed a cryptographic application to secure the data during its transmission over network. Diffie-Hellman key exchange as well as AES algorithm is used in order to protect its transmission. First of all, the sender generates the key for encrypted file with the help of Diffie-Hellman key exchange. After that, this file is encrypted applying AES algorithm. On receiver hand, sender used AES and Diffie-Hellman key exchange to decrypt this content. In this way, the receiver gets the original content and can use it easily [6].

Srilakshmi and Manikandan (2018) used technologies for smart agriculture. In their research they considered the soil monitoring, water monitoring, irrigation technologies etc. They also considered a smart nitrate sensor in order to monitor amount related to nitrate. It is present in surface as well as on ground water. IoT based devices are easily monitored from a distance. Several fields are there in which the IoT based devices are used and performing very well such as Home Automation, Industry Automation. The communication between these devices could be wired and wireless. The IoT based devices use different protocols as OSI/TCP protocols because IoT devices are small and low power [7].

## III. RESEARCH METHODOLOGY

Research Methodology stands for a pattern or method which is followed in a research by the researchers. A research is the systematic approach rationalization and conceptualization of a theory. In this study Experimental research method has been used in which data processing model are executed to draw conclusion. The Experimental Research is used for testing the feasibility of a solution. In order to perform simulation the model has been developed in and run in MATLAB. In this model, user defined port number and IP address are considered in order to enhance the security of packets during data transmission over cloud. Due to two tier protection of packet during data transmission, the probability of hacking gets reduce.

## IV. OBJECTIVE

To enhance the security of IoT based devices by suitable encryption security model leading to encrypt data before sending to the receiver. Following are the major contribution of this paper.

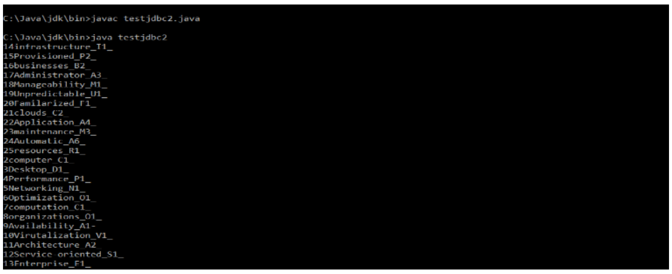
- To study the existing security mechanism.
- To propose a two tier security model using Multiplicative Inverse and AES to resolve the issues and threats related to security of IoT based devices.
- To design a simulator for comparison of securing of IoT based devices of proposed and existing system in terms of packet size, error rate and time consumption.

## V. PROPOSED APPROACH

This paper proposed a two tier security model for IoT based devices and the algorithm for integration of Multiplicative Inverse encryption (MIE) with AES are also explained .The purpose of the proposed model is to secure the data transmission between the IoT based devices. In this approach, two tier encryption (advanced encryption standard (AES) used with multiplicative inverse encryption (MIE)).

## VI. IMPLEMENTATION AND RESULTS

In two tier security model with AES and multiplicative inverse encryption (MIE) has been designed in the present paper. This model is implemented on java platform. In this research work, IP filter is considered for the rejection of unauthenticated data transmission between server and client. Port no is specified to enhance the security of data. After that, the data is encrypted with the help of Multiplicative Inverse Cryptographic technique. In next step, the packet of data is encrypted applying AES technique. In the proposed work, own socket server and client side data sender and receiver module is proposed which are coded in Net beans in order to enhance the security of data and avoid unauthentic access during data transmission. Following are the implementation result of two tier model:

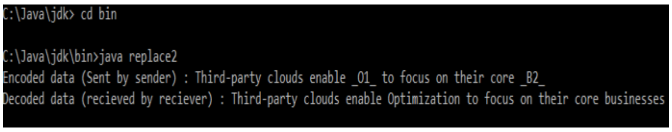


```
C:\Java\jdk\bin>javac testjdbc2.java

C:\Java\jdk\bin>java testjdbc2
14infrastructure_T1_
15Provisioned_P2_
16businesses_B2_
17Administrator_A3_
18Manageability_M1_
19Unpredictable_U1_
20Familarized_F1_
21clouds_C2_
22Application_A4_
23maintenance_M3_
24Automatic_A6_
25resources_R1_
2computer_C1_
3Desktop_D1_
4Performance_P1_
5Networking_N1_
6Optimization_O1_
7computation_C1_
8organizations_O1_
9Availability_A1-
10Virutalization_V1_
11Architecture_A2_
12Service oriented_S1_
13Enterprise_E1_
```

**Figure 5.1 Snapshot of the Input File along With defined Code Word**

Figure 5.1 shows the snapshot of input file along with their defined code word. In this figure a list of string is represented with their code word. A code word _P1_ is assigned to the performance and codeword _S1_is assigned to service-oriented.

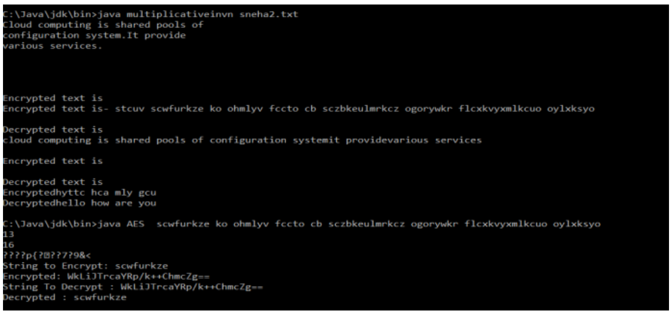


```
C:\Java\jdk> cd bin

C:\Java\jdk\bin>java replace2
Encoded data (Sent by sender) : Third-party clouds enable _O1_ to focus on their core _B2_
Decoded data (recieved by reciever) : Third-party clouds enable Optimization to focus on their core businesses
```

**Figure 5.2 Snapshot of Compressed File**

Figure 5.2 represents the output of replace2.java file. In this a compression technique is performed. In this figure selected string is replaced with their code word. During the compression optimization string is replaced with their code word _O1_ and business string is replaced with their code word_B2_.



```
C:\Java\jdk\bin>java multiplicativeinvn sneha2.txt
Cloud computing is shared pools of
configuration system.It provide
various services.




Encrypted text is
Encrypted text is- stcuv scwfurkze ko ohmlyv fccto cb sczbkeulmrkcz ogorywkr flcxkvyxmlkcuo oylxksyo

Decrypted text is
cloud computing is shared pools of configuration systemit providevarious services

Encrypted text is

Decrypted text is
Encryptedhyttc hca mly gcu
Decryptedhello how are you

C:\Java\jdk\bin>java AES  scwfurkze ko ohmlyv fccto cb sczbkeulmrkcz ogorywkr flcxkvyxmlkcuo oylxksyo
13
16
????p{?□??7?9&<
String to Encrypt: scwfurkze
Encrypted: WkLiJTrcaYRp/k++ChmcZg==
String To Decrypt : WkLiJTrcaYRp/k++ChmcZg==
Decrypted : scwfurkze
```

**Figure 5.3 Snapshot of Encryption process**

Figure 5.3 represents the snapshot of encryption process. In this Multiplicative Inverse encryption algorithm (MIE) key k is used with advanced encryption standard algorithm (AES).

## VII. CONCLUSION

In existing system, standard protocols were used for data transmission and basic encryption techniques were being applied for ensuring the security of IoT based devices. But it failed in preventing against routing attacks and packet losses in transmission. The objective of the proposed work is to improve the security of IoT based devices. This is achieved by proposes a Two Tier Security Model for IoT based devices. The data is encrypted on the sender side before sending it to the receiver. Encryption of data is performed in two stages. In first stage, advanced encryption standard (AES) is used to encrypt the data. In second stage, the encrypted data is act as an input for Multiplicative inverse encryption (MIE). Finally, obtained cipher text is sent to the receiver. This approach ensures the security of the data and also provides an efficient, secure data transmission and less time consuming module.

## VIII. REFERENCES

[1]. Vithya Vijaylakshmi, “Enhancing the security of IoT Data using Multilevel Encryption (2017)”

[2]. B.S Kumar and T.C.S.P Raju “Introduced the Intrusion Detection System- Their Types and Prevention (2013).

[3]. Trivedi,”Cryptographic Approach for Securing IoT Device” (2018)

[4]. Vinay Sagar and Kusuma S.M,”Home Automation using Internet of things” (2015)

[5]. Cryptography- Wikipedia, en.wikipdedia.org/wiki/cryptograph.

[6]. Mahalakshmi et.al,"Image Encryption Method Using Differential Expansion Technique, AES and RSA Algorithm," (2019).

[7]. Ge Wu and Willy, “Generalized public-key cryptography with tight security” (2019) Y. Yusfrizal and F. Agustin, "Key Management Using Combination of Diffie–Hellman Key Exchange with AES Encryption," 2018 6th International Conference on Cyber and IT Service Management (CITSM), Parapet, Indonesia, 2018, pp. 1-6.

[8]. Marek R.Ogiela et al.”Cognitive solutions for security and cryptography” (2019)

[9]. Xiangyu Chang and Z.Zhang, ”Cipher text-only attack on optical scanning cryptography” (2019)

[10]. IroshaJayatilleka and Malka N. Halgamuge “Internet of Things in healthcare: Smart devices, sensors, and system related to diseases and health conditions” (2019).

[11]. Z. Zhang et.al, "Summary of research on IT network and Industrial Control network Security assessment”, (2019).

[12]. S. E. Tuiri, N. Sabil, C. A. Kerrache and G. Koziel, "An EEG Based Key Generation Cryptosystem using Diffie-Hellman And AES," 2018 2nd IEEE Middle East and North Africa Communications Conference (MENACOMM), Manama, Bahrain, 2018, pp. 1-6.

[13]. Diego Mendez, IoannisPapapanagiotou, Baijian Yang “Internet of Things: Survey on Security and Privacy” (2017) IOT SECURITY.

[14]. H. Bodur and R. Kara, "Implementing Diffie-Hellman key exchange method on logical key hierarchy for secure broadcast transmission," (2017) 9th International Conference on Computational Intelligence and Communication Networks (CICN)

**Cite this article as :**

Sheenu Sachdeva, Aruna, "Enhancing the Security System using Cryptography for IoT Based Devices", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 5, pp. 227-232, September-October 2021. Journal URL : https://ijsrset.com/IJSRSET218527