International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-4, February 2019

Hybrid Approach for Securing the IoT Devices

M Sai Prasanthi,Venkata Bharath Katragadda, Hrushik Perumalla, Bandla Sowmya

Abstract: ***Today the Internet has turned out to be omnipresent, has touched every edge of the globe, and is influencing human life in incredible ways. We are presently entering a period, where different kind's appliances are associated with the web. We are entering a time of the IoT. Internet of Things enables the appliances to communicate and perform their activities based on network activity. Today, a PC is substantially less helpful without an association of internet; tomorrow, that will be the situation with apparatuses like a fridge. To put it plainly, these apparatuses should convey to one another. Sensors in the perception layer gather the information from the sources. This information will be transmitted through the system layers over the web to the cloud. Today IoT deals with huge amount of data. This information may be exceptionally touchy and their protection and security must not be endangered. Here comes the requirement for security algorithms to protect the information. In this paper, we provide a hybrid approach of security algorithms (AES along with RSA) to secure the data in network layer***.

Index Terms: Cryptography, Symmetricencryption, Asymmetric encryption, AES,RSA,Image slicer.

I. INTRODUCTION

IoT is perhaps the subsequent stage in the enhancement of the web. IoT alludes to many physical gadgets that are connected with trade information with one another over the internet [1]. It decreases human mediation in ordinary activities. It very well may be any gadget extending from PCs, telephones, and IoT associated vehicle. It is assessed that there will be 100 billion gadgets in the span of next 5 years [2].Such gadgets, when associated with a system, perform capacities that make life simpler all in all. It includes objects with the capability to sense and communicate using Internet [3]. Our Bluetooth gadgets, surveillance cameras, printers, fridges, and smart homes and other associated gadgets are on the whole essential models of IoT Devices. These makes the gadgets/things to be digitalized.

Today situation in the digital transmission whatever in-formation you transfer should be encrypted to improve the security [4], which may be retrieved by the user in an easy manner. Cryptanalysts are thinking far behind our brain which leads them to steal our data within a fraction of seconds and keep our data in their fingertips. Imagine you stored all the private data in our gadgets and you think that you secured your data [5] but hackers can breach your data at any moment. IOT is a quickly developing innovation by making every gadget as smart. Regardless of hardware utilities, toys and dresses would now be able to be made wise by joining sensor innovation with machine learning. Be that as it may, the nearness of such information serious innovation around us has made us helpless against security and protection dangers [6]. Wherever there is voluminous information there is an extent of abuse.

Every gadget that we use are associated with the web and associated with huge measure of information. This information need to be secured [7]. The main principal smart gadget is gather the information and send it over the web for applications to analyze it. Computerization IoT applications have exceptional constant requirements; they are excepted to have a high level of reliability and regularly work in security basic condition. These necessities legitimize extraordinary security and well-being measures. The quick improvement of Internet-of-Thing (IoT) gadgets empowers the huge reconciliation of advances from detecting technology, correspondence innovation, information processing, to distributed computing. In this situation, sensors in the perception layer gather information from the surroundings and do quick preparing. At that point, this information is transmitted through the system layers over the web through the cloud. These layers are also termed as channel. This channel should be secured In the cloud, information is additionally handled by various applications.

II. DIFFERENT APPROACHES FOR CRYPTOGRAPHY

There two different approaches of cryptography are symmetric key cryptography and asymmetric key cryptography.

Symmetric Key Cryptography

Symmetric encryption is a two-way algorithm as for both encryption and decryption a common shared key will be used. This shared key is essential so as to acquire the original message from the cipher content. Symmetric encryption is also called as secure-key encryption.

The main advantage of symmetric encryption is that it provides authentication until the key is kept confidential. Here data encryption is faster compared with asymmetric approach.

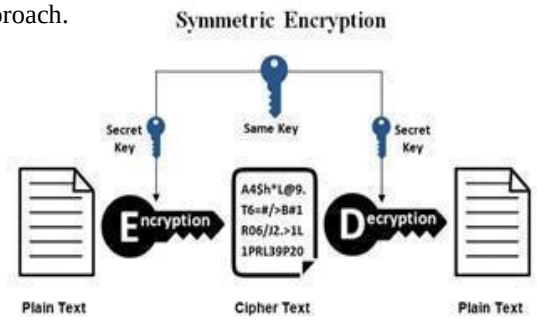


Fig 1: Symmetric encryption

Manuscript published on 28 February 2019.
*Correspondence Author(s)
M sai Prasanthi, CSE, Koneru Lakshmaiah Education Foundation, Guntur, India.
Venkata Bharath Katragadda, CSE, Koneru Lakshmaiah Education Foundation , Guntur,India.
Hrushik perumalla, CSE, Koneru Lakshmaiah Education Foundation , Guntur,India.
Bandla Sowmya, CSE, Koneru Lakshmaiah Education Foundation , Guntur,India.

Asymmetric Key Cryptography

Asymmetric encryption is quite opposite to symmetric encryption as it doesn't deal with a shared key it utilizes a pair of keys, public key and a private key. Here public key will be used to encrypt the information whereas the private key will be used to decrypt the encrypted data.In asymmetric key cryptography, the security depends upon the keys. No security is required for public key as it is publicly available and it can be passed over internet for information exchange. The only security measure to be taken is to secure the private key as it is the requirement for decryption.The process of asymmetric encryption goes as follows:

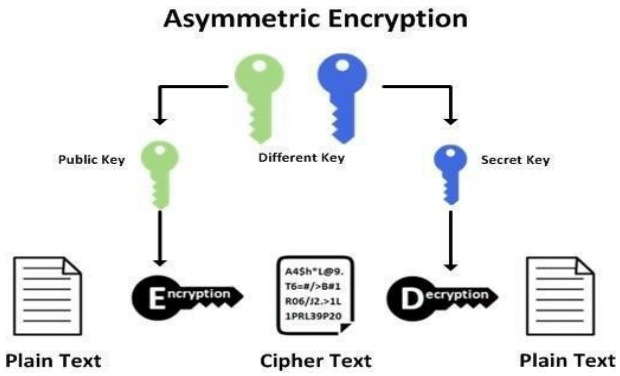


Fig 2: Asymmetric Encryption

III. AES

The Advanced Encryption Standard, AES, is a symmetric encryption calculation and a standout amongst the most secure. This technique utilizes a block cipher, which encrypts information one block size at once at once, in contrast to different sorts of encryption, for example, stream ciphers, which encode information bit by bit.AES is of types AES-128, AES-192 and AES-256. The key bit you choose encrypts and decrypts blocks in 128 bits, 192 bits and so on. There are distinctive rounds for each key. A round is the way toward transforming plaintext into cipher text. For 128-bit, there are 10 rounds; 192-bit has 12 rounds; and 256-bit has 14 rounds. Since AES is a symmetric key encryption, you should share the key to people for them to get to know the encrypted information. Besides, in the event that you don't have a safe method to share that key and unapproved people access it, they can decode everything encoded with that particular key.

A. AES Encryption

In Advanced Encryption Standard(AES) encryption of plain text will be done in four steps

1. Key addition
2. Substitution
3. Shift Row
4. Mix Column

1) **Key Addition:** This is also called Add Round key .From the matrix the 16 bytes are considered as 128 bits. The XOR operation will be carried out between the 128 bits and the 128 bits of the round key. The result will be cipher text if this is the final round. If this is not the last round then we need to interpret the resulting 128 bits as 16 bytes, and then we need to start with another similar round.

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Fig 3: each state is entitled as above figure

Internally, the AES calculation's activities are worked on a two-dimensional cluster of bytes known as State. It comprises 4 rows, each consists of Nb bytes, Nb sections, constituted with 32-bit words. Sr,c indicates the byte in line r and section c. The variety of bytes in information is duplicated in the State framework. Toward the end, the State framework is replicated in the yield grid

Include round key (state, key):

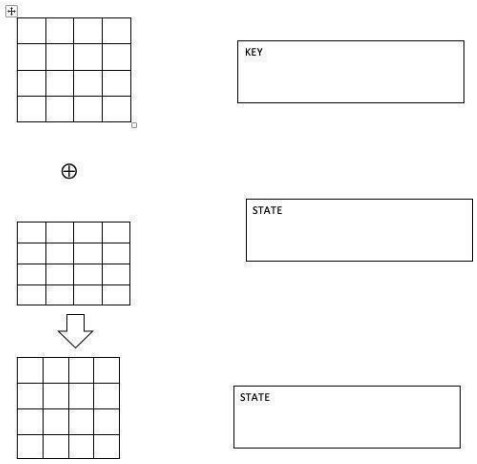


Fig 4: Add Round key

2) **Byte Substitution:** By looking at the s-box the input 16 bytes are substituted. The output is in form of a matrix(4X4) containing four rows and four columns.

3) **Shift Rows**: From the matrix obtained each of the four rows is shifted to the left. Any section that tumble off will be reinserted on the right side of row. The Shift will be completed as follows-

First row will not be shifted. Second row will be shifted one position(one byte) towards the left. Third row will be shifted two positions towards the left. Fourth row will be shifted three positions towards the left. The output obtained will be a new matrix(4X4) of the same 16 bytes. But in the new matrix all the 16 bytes will be shifted with respect to each other [12].

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

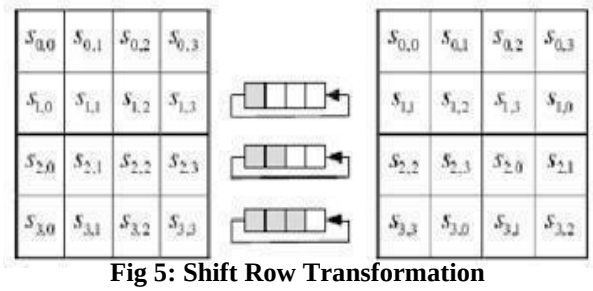


Fig 5: Shift Row Transformation

4) Mix Columns: Using a special mathematical function, in the matrix each column consisting of four bytes is transformed. The four bytes of one column will be the input for the function. The function outputs completely four new bytes, that will replace the actual existing column. The result obtained will be a matrix(4X4) of 16 new bytes. The main point to be noted is that in the last round this step shouldn't be performed. Bytes in columns are mixed linearly. Explain every column as a vector of length 4 [12]. Every column of State is restore by another column acquired by multiplying that column with a matrix in a specific field (Galois Field) [12].

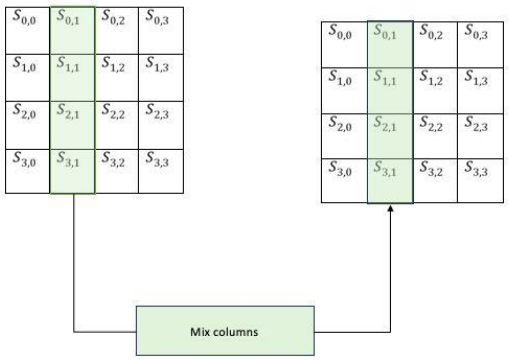


Fig 6: Mix Column Transformation

B. AES Decryption

The strategy of decryption of AES ciphertext is like encryp-tion technique in the switch arrange [13]. every round comprises of the four procedures directed in the reverse order [13].

1.Add a round key

2.Mix columns

3.Shift rows

4.Byte Substitution

Since sub-forms in each round are in opposite manner, not like as a Feistel Cipher [13], the encrypted and the decrypted algorithms needs to be individually developed, while they are firmly associated.

C. AES Analysis

As per todays cryptography, AES is generally accepted and support in both equipment and also in programming. Up to now, no handy cryptanalytic strike against AES has been found [13].Furthermore, AES has worked in flexibility of key size, which allows a level of 'future-sealing' in opposite to the developments in the ability to perform complete key ventures [13].Despite, similarly regarding to DES, the AES security is undertaken just on the off chance that it is accurately actualized and great key supervision is used .

IV. RSA

RSA is an algorithm and utilizing in the advanced system condition to scramble and decode the information. Asymmetric cryptosystem implies two distinctive keys are utilizing in the encryption and unscrambling. In the two keys, one key is utilizing for encryption and the second key is utilizing for decoding. This RSA algorithm is named as public key cryptography. Since one of the private keys can be given to everybody which implies open. The other key must be kept private.

The RSA algorithm comprises three house ventures in encryption and unscrambling. The means are following as,

A) Key Generation

B) Encryption

C) Decryption

A. Key Generation

The key generation is the initial step of RSA calculation. The RSA includes an open key and a private key. On those keys, people in general key can know everybody and it is used for encoding messages. These algorithm is based on generating the two prime numbers [15]. Messages encrypts with the public key can decrypts using the private key. The keys for the RSA algorithm is produced by the accompanying advances,

1) d First, pick the two particular prime numbers p and q.
2) For security issues, the whole number p and q have to be selected, and it have to be the comparative piece length. Prime whole numbers can be productively found by a esentially testing.
3) Then figure then esteem, n = p*q.
4) n is used as the modulus for both people in general and private keys [16]. Its length, typically communicated in bits, is the key length.
5) Compute '(n) = '(p)'(q) = (p 1) *(q 1) = n - (p+q - 1), where ' is Euler's totient work. This esteem is kept private
6) Choose a whole number e with the end goal that 1 < e <'(n) and gcd (e, '(n)) = 1 [16]; i.e., e and '(n) are co-prime. e is discharged as people in general key. e has a short piece length and little Hamming weight results in more productive encryption. In any case, considerably littler estimations of e have been appeared to be less secure in a few settings.
7) Determine d as d e 1 (mod '(n)); i.e., d is the particular multiplicative backward of e (modulo '(n)). This is expressed as tackle the d given d*e 1 (mod '(n)).This is registered using broadened Euclidean calculation. It is using the pseudo code in the Secluded numbers area, inputs an and n compare to e and '(n), separately

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

8) d esteem is kept as the private key.General society key consists the modulus n and the open key e [16]. The private key has the modulus n and the private key d, and it keeps in mystery. p, q, and ’(n) values are kept in secret since they can be utilized to figure 6.

B. Encryption

A transmits her public key (n, e) to B and keeps the private key d secret. Then B sends the message M to A.Along these lines, first changes M into a whole number m, to such an extent that 0 m < n and gcd(m, n) = 1. At that point, it processes the figure content c.This can be done proficiently, even the numbers are 600-bit numbers, it is utilizing the Modular Exponentiation. B transmits c to A . Refer to “(1)”.

C = pow (M, e) (mod n) which is a chiper text. (1)

C. Decoding

A can regain m from c by using her private key that is d by means of figuring. Given m, she can recoup the unique message M by exchanging the padding plan. Refer to “(2)”.

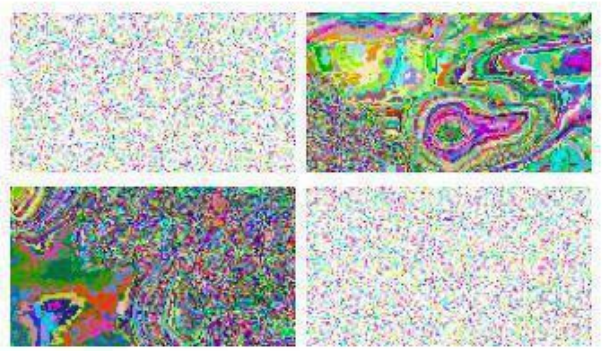
M = pow (C, d) (mod n) this is an original message. (2)

V. IMPLEMENTATION AND RESULTS

Fig 7: Original Image Without Encryption

Making the original into an 2*2 pieces

After making the image into n*n pieces now we have select the n pieces and it should be encrypted with AES and remaining n pieces should be encrypted with RSA. In this example first and fourth pieces are encrypted by AES, whereas remaining pieces are encrypted by the RSA.

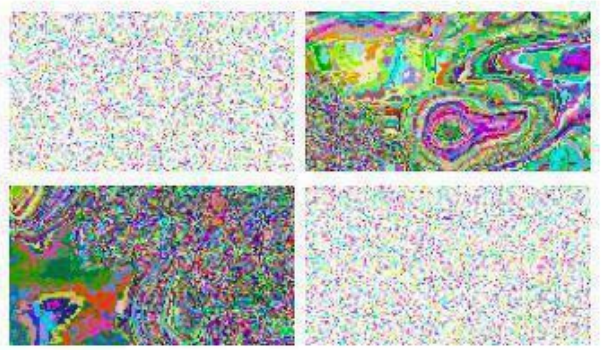


Now we have to combine individual encrypted piece of image should be merged into a single image which is an encrypted image.

Fig 8: An Encrypted Image

Now this combined image can be transferred through the network. As this image is unpredictable it has more security than the single encryption of AES or RSA

When the point of decryption comes into a picture, the image needed to be sliced and decrypt the individual pieces. The sender will inform the receiver which pieces of image is encrypted by the AES and which pieces of image is encrypted by the RSA.



After slicing the combined image into individual pieces, since the receiver has the information about the individual pieces of images he can decrypt the individual piece of an image.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

After decrypting with the correct key

Fig 9: A decrypted individual images

Now the task of a receiver is to combine the individual piece of image in to a single image

VI. CONCLUSION

IoT deals with huge amount of the data, this data can be any form such as images. In Digital world, the securing the images has become very important task. In this paper, we proposed an idea of encrypting the image with high security for security purpose, we used the both AES and RSA algorithms to encrypt an image. This encryption model provides very high security with low computation time. By following the similar we can even secure the data/text and other files. These implementation leads to an increase of security in the IoT devices.

REFERENCES

1. Abdelali El Bouchti, Samir Bahsani, Trik Nahhal “Encryption As A Service For Data Healthcare Cloudsecurity. “
2. C. Perera, A. Zaslavsky, P. Christen, D. Georakopoulos,“Context Aware Computing For The Internet Of Things.”
3. J. Gubbi, R. Buyya, S. Marusic, And M. Palaniswami, “Internet Of Things (Iot): A Vision, Architectural Elements, And Future Directions.”
4. Ch. Qiang, G.Quan, B.Yu, L.Yang, “Research On Security Issues Of The Internet Of Things.”
5. M. Friedemann, And C. Floerkemeier. "From The Internet Of Computers To The Internet Of Things."
6. Y.Challal, E. Natalizio, S.Sen, And A.Maria Vegni “Internet Of Things Security And Privacy: Design Methods And Optimization”, Add Hoc Network
7. L. Tawalbeh, M. Mowafi And W. Aljoby, "Use Of Elliptic Curve Cryptography For Multimedia Encryption," In Iet Information Security.
8. L. A. Tawalbeh, Y. Jararweh And A. Moh’md. “An Integrated Radix-4 Modular Divider/Multiplier Hardware Architecture For Cryptographic Applications”.
9. Iot Ecosystem Components: The Complete Connectivity Layer
10. konink Lijke Phulips: Meethu Personal Wireless Light-ing,(2013).
11. "Cellular Automata For Dynamic S-Boxes In Cryptog-raphy."
12. Implementation Of Multi Mode Aes Algorithm Using Verilog"
13. A Novel Approach To Secure Data Sharing Scheme For Dynamic Members Through Different Secure Methods.
14. A Survey On Applications And Security Issues Of Internet Of Things
15. R. L. Rivest, A. Shamir And L. Adleman, "A Method For Obtaining Digital Signatures And Public-Key Cryptosys-tem”.
16. An Hybrid Of Rsa Token And Iterated Hash Algorithm For Secured Data Transfer

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)