Security and Privacy of E-Health Data using Two Fish Encryption Algorithm

Varsha Vatsala, T. Poongodi

Abstract: ***The rapid growth development of the Internet of Things (IoT) has supported communication between various smart devices and it helps to exchange data between them. IoT is very highly demand topics between the researchers. The main goal of IoT in health care is to provide real time monitoring of the patient. But these new challenges also introduced the privacy and security to the health care data. Security is a major concern of the data. A system requires with authentic protocol for maintaining privacy of health care data. After going through all methodologies of the protocol encryption will be carried out of data of the health care with "two fish" encryption technique. At server side, it will automatically get decrypted after applying key. Two fish encryption algorithm is a block cipher algorithm of 128 bit. The key length vary until 256 bit. Key is divided in two parts as the first half of the key will encrypt the plain text and second half of the key will modify the encryption algorithm.***

Keywords – IoT, Cryptography, AES, DES, Two Fish, Plaintext, Cipher text, Block Cipher

I. INTRODUCTION

The billions of individual devices are connected with one-other and sharing their data and information. Due to increased work of (WSN) wireless sensor network and (RFID) Radio Frequency Identification leads to development of new technology named as Internet of Things (IoT). Thanks to this development, which help technology to expand in various area and let the world to get smart environments. The main target of IoT is to build smart cities, smart hospital, smart transport, smart offices and various things.

IoT has lot of application in various fields. In 2020, there will be approx. 200 billion devices connected with each other. In upcoming years there is exponentially increase of IoT devices. Many markets are running behind IoT and many are ready to adapt this emerging technology. However, with rapid increases of use of this technology the basic concern is "SECURITY OF DATA". Every user wants that his data must be secured. Many researchers had research various technique to secured the data. For protection of data, we must know the characteristics of security:

1. Confidentiality- The data is secure between sender and receiver.
2. Authentication- It will check the authenticated user to update or read the information.
3. Integrity- It will check the sender and recipient data is same.
4. Encryption- It will encrypt the data using public key before sending it to the receiver.

Security of data leads to the idea of cryptography to secured the data.

Revised Manuscript Received on May 15, 2020.

Dr. T. Poongodi, Professor, Galgotia University, Greater Noida, India.
Varsha Vatsala, M. Tech, Galgotia University, Greater Noida, India.

The data is encrypted with the succour of public key and decrypted with the private key in the cryptographic process. There are two types of encryption algorithm.

1. Symmetric Algorithm- In this encryption algorithm the data is encrypted with the aid of key and decrypted with the aid of same key.
2. Asymmetric Algorithm- In this encryption algorithm the data is encrypted with the aid of public key and decrypted with the aid of private key.

- Public key – We use this for encryption.
- Private key- We use this for decryption.

In this survey paper, we will discuss concerning the recent work of the protection of data with the assistance of cryptography. The recent work of two fish algorithm carried a lot of information regarding encryption algorithm.

II. LITERATURE REVIEW

Cryptography- As there are many security threats which leads to the leak of privacy of data so we are using the basic way to secured the data. There are three main basic components of the cryptography.

- Plain text
- Key
- Cipher text

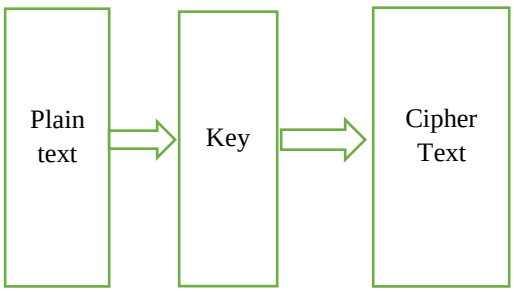

Figure 1

In this paper [1], present the meaning of security and it also present the type of attack with the aid of which the attacker will leak the data and update the data. It forecast the necessary information regarding the security challenges concerned within IoT. This paper also present the information regarding Internet of Things that what actually the IoT is and what is its architecture. IoT help helps individual to connect devices at anytime, anywhere with any device.

Challenges like reassuring ability, attaining a business model during which many immeasurable objects can be connected to a network and security and privacy of challenges, like authentication and authorization of system area unit introduced within the next few years, addressing these challenges.

In this paper [2], present an overview current factor of IoT security. At the same phase, this paper tell the attack and vendor of the IoT security. Simulation tools used to simulate and finally validate the result. IoT simulation tools and modelers helps the fast growth of the IoT in various field. The various number of protocol used in IoT to secured the data. In cyber security the authentication, encryption, availability, integrity and firewall all are used to secured the data. Encryption is a best credible way to secured the data. It just translate the data into cipher text with the aid of key. And on the network layer we will secure the data with the assist of the end-to-end encryption technique. Low cost cryptography is used at physical layer.

In this paper [3] , it present the request of IoT and privacy importance in IoT network. IoT not only useful for us to connected with the various device but it also help to innovate various smart devices. As it helps us to design smart house, smart appliances, smart industry and various things .The market of IoT is booming now a days. In paper [4], it present the architecture, types of attacks and challenges in the IoT. As every researchers give their own perspective regarding the architecture of the paper for example Debasis and Jaydip [5] showed the data layer at bottom and application layer at top. This architecture is made due to meet the requirement of the various school, industries, governments and many more. Internet layer is used to communicate with the gateway of the network. There are various types of attack, which is done to leek the data as they are Man in the Middle attack, Physical attack , Denial of Service attack , Eaves drooping and too many. In man in the middle, attack the intruder attack on the data as the third person interpretation to leak the data. It take data before reaching to the receiver. In physical attack, attack is done with the use of hardware components. In DOS attack, the attacker try to find to make a machine unavailable for specified user. Eaves dropping this attack is too much easiest attack if the cryptographic algorithm does not protect the data. In this paper [6], it present the protection of data using the specific model in which it include the four node i.e. person, technology, process and intelligent object. These nodes interact through the security, privacy, authenticated use. But this model will basically not that much secure to protect the IoT data. As they, there no specific algorithm used to prevent the data from attacker. In this paper [7], it present the sketch of the various cryptography algorithm. In this survey paper, they present the efficiency of encryption algorithm and there speed of execution as how much time taken to complete the execution. For example in lightweight cryptography algorithm, the size of hardware is minimum. Implementation cost is less and it is secure too. In this paper [8], it compare the cryptographic technique as it has taken AES as main algorithm to secured the data and compare AES with various algorithm as with the complexity , execution time, memory size and various parameters. In this paper [9], it present the AES and reviewed on that. In this paper they overviewed about cryptographic as what basically cryptography is how it is used. AES is very lightweight cryptography it has too much factor also but it has some pitfall like it uses very simple algebraic structure, which is very easy to crack. Block encryption is done in same way. It is tough to implement with the software. In this paper [9], the DES algorithm is presented in very effective way. In DES the data will be of 64 bit and key will be of that 56 bit. DES is also block cipher encryption algorithm. But it also has some pitfall i.e. keys which is used are very weak and it can be decrypted using Brute Force Attack. In this paper[10], they present regarding two fish encryption algorithm. In this paper we are going to encrypt the data using “TWOFISH” encryption algorithm. We will describe how the two fish encryption algorithm work and how it will encrypt the data. There many types of attacks which are done on the data. In this paper we are taking the “MAN IN THE MIDDLE ATTACK”. In which the attacker relays the message and alter the message. So we are going to encrypt the message. Two fish encryption algorithm is type of symmetric algorithm in which the encryption and decryption is done with same key.

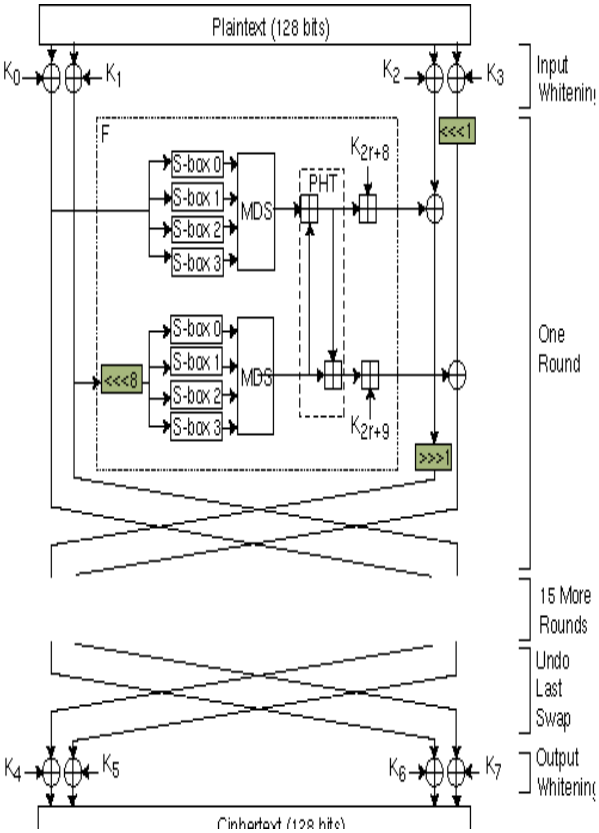

Figure 2

Two fish is a Feistel network. This means that in each circular round, first half of the text block is sent through an F function, and then XORed with the other second half of the text block. DES is one of the Feistel network. Blowfish (another Schneier algorithm) is a Feistel network. The 5 submitted AES network are feistel network. Feistel networks have been studied in cryptography for a long time, and that we knowledge they work. In every spherical round of Twofish, two 32-bit word (the 2 vertical lines on the left side of Figure 1) function input in the F operate. Every word is jerky in four bytes.

These four bytes sent through four very different key-dependent S-boxes. The four output byte (the S-boxes have 8-bit inputs and outputs) combined employing a Most Distance Separable (MDS) matrix and combined with the 32-bit word. Then the 2 32-bit words get combined employing a Pseudo-Hadamard Transform (PHT), extra to 2 spherical sub keys, then XORed with the next right half of the text.

There also are 2 1-bit rotations occurring, one before and one after the XOR. Two fish additionally has one thing known as "prewhitening" and "postwhitening;" extra sub keys are XORed into the text block each before the primary spherical and after the last spherical.

The algorithm may look haphazard, however we tend to did everything for a reason. Nothing is in Two fish unintentionally. Something within the algorithm that we tend to could not justify, we removed. The result is lean, mean algorithm that is robust and conceptually straightforward. Every step of the spherical function is bijective. That is, every output is feasible. We have seen too several attacks against data that do not have this property to not embrace it. The spherical perform blend up operations from totally non-identical algebraic groups: S-box inclusion, associates MDS matrix in GF(2^8), addition in GF(2^{32}), associates in GF(2) (also known as XOR), and 1-bit rotations. That makes the algorithm tough to attack mathematically. The key-dependent S-boxes are designed to be unaffected by the 2 massive attacks of the first 1990s—differential cryptanalytics and linear cryptanalysis—and resistant against no matter unknown attacks return next. Too several algorithm designers enhance their styles against specific attacks, stupidly regarding resistance against the unknown. Our design philosophy was a touch different: adequate against glorious attacks, and enough nastiness to (hopefully) resist unknown attacks. Key-dependent S-boxes were one way we did that. Key-dependent S-boxes were not handpicked indiscriminately, as they were in Blowfish. Rather, we tend to rigorously designed S-box construction rules, and tested them with all potential 128-bit keys (and a set of potential longer keys) to create certain that each one all the S-boxes were so sturdy. This approach allowed us to mix the strength of fastened fixed, strong S-boxes with the strength of secret S-boxes. And Two fish has not a single weak keys, as Blowfish will be in reduced-circular variants. The MDS matrix is rigorously chosen to produce smart diffusion, to maintain its MDS property even after the 1-bit rotation, and to make it quick in each hardware and software package. This suggest that we tend to had to go looking through all viable matrices and realize the one that has best met our criteria. The PHT and key addition give diffusion between the sub blocks and therefore the key. And victimization the LEA directive on the Pentium, we will do all 4 additions in just 2 operations. The circular sub keys square measure rigorously attentive calculated, utilize a mechanism indistinguishable to the S-box construction rules, to forestall interconnected-key attacks and to produce smart key mixing. One among the things we tend to learned throughout during this process is that a decent key schedule is not grafted onto a cipher, however designed in tandem bicycle with the cipher. We tend to spend lot of time on the Two fish key schedule, and pleased with the results. Rotation of 1-bit is style to jerk with the byte structure; expect it, all the things operates on bytes. This operation have existence to frustrate cryptanalytics; it surely frustrated our strive at cryptanalyzing Two fish. Prewhitening and post whitening appear to add minimum single round to the struggling of any attack. Since eight XORs are low-priced than a round, it makes sight to leave them in.

Component of two fish encryption algorithm:

1. Plaintext:
   The user data before encryption is known as plain text. As we have to encrypt the plain text using key to secure the user data.
2. Key:
   Key is used to encrypt the data. Data, which is encrypted using key, is said to be as plain key.
3. Cipher Text:
   Encrypted data is said to be as cipher text.

In encryption algorithm, the plain text is converted into cipher text using key value. In two key encryption algorithm the circular round function is applied on the plain text in two half.

Table 1: Two fish algorithm Property

TWOFISH ALGORITHM	
Key Size	128,192,256
Block Size	128
Rounds	16
Structure	Feistel Network
Derived From	Blowfish, Safer, Square

Two fish have following properties:

1. It is of 128-bit symmetric block cipher.
2. Key length 128, 192, 256 bits.
3. Weak keys are not there.
4. Can be easily used on hardware and software.
5. Design is flexible.
6. Design is simple and easy to understand.
7. Key can be accepted upto 256-bit.
8. The data which get encrypted must be less than 500 clock cycle.
9. It will not contain any information that make it not efficient on 32 bit microprocessor.
10. Variety of performance of system according to the potential of the key.

Two Fish Goals of Cryptography:

1. 16 round two fish in which plain text should not be chosen.
2. 12 round two fish in which no related key attack

Two Fish Basic Building:

III. FIESTEL NETWORK

A Feistel Network is a usual method of changing any method into permutation. It was originated through various people as some help in design and some in algorithm. Invented by “Horst Feistel” and designed by “Lucifer”. The basic building block of Feistel network is the method “F” which is key dependent to map input to get output string. The method “F” is non-linear.

F:{0,1}^n\2* {0,1}^N →{0,1}^n/2 (1)

where n is that the block size of the Feistel Network, and F could be perform on n/2bits of the block and N bits of a key as input, associated manufacturing an output of length n/2 bits. In every spherical round, the "source block" is that the input to F, and therefore the output of F is Xored with the "target block," when that these 2 blocks swap places for ensuring the next round. The idea here is to associate an F function, which can be a weak encryption algorithm when associated by itself, and repeatedly repeat it to build a strong encryption algorithm. Two spherical rounds of a Feistel network is named as a "cycle". In one cycle, as every bit of the text block has been changed once. Twofish is a 16-circular round Feistel network with bijective F function.

IV. S-BOXES

An S-box could be a table-driven non-linear replacement operation utilized in most of the block ciphers. S-boxes chnages in each input size and as well as in output size, and might be created either every way or algorithmically. S-boxes was 1st used in Lucifer, then DES, and subsequently in maximum encryption algorithms. Twofish uses totally four different, bijective, key-dependent, 8-by-8-bit S-boxes. These S-boxes are engineered victimization 2 fastened 8-by-8-bit permutations and key material.

V. MDS MATRICES

A maximum distance separable (MDS) code on top of a field could be a linear mapping in distinction to a field components to b field components, manufacturing a compound vector of a+b components, with the attributes that the minimum variety of non-zero components in any non-zero vector that is minimum of b+ one [MS77] place otherwise, the "distance" (i.e., the amount of components that differ) between any 2 distinct vectors made by the MDS mapping is a minimum of b + one. It will simply be shown that no mapping will have a bigger minimum distance between 2 distinct vectors, thus the term most distance divisible. MDS mappings will be pictured by associate degree MDS matrix consisting of a × b component. Reed-Solomon error correcting codes area unit well known to be MDS. A necessary associate degreed sufficient condition for an a × b matrix to be MDS is that everyone attainable sq. sub matrices, obtained by discarding rows or columns, area unit non-singular. Cloth Vaudenay 1st projected MDS matrices as a cipher style component. Shark and sq. use MDS matrices; though we tend to 1st saw the development utilized in the unpublished cipher Manta3. Twofish uses one 4-by-4 MDS matrix over GF(28).

VI. PSEUDO-HADAMARD TRANSFORM:

A pseudo-Hadamard transform (PHT) could be a easy commixture operation that runs faster in package. Given 2 inputs, a and b, the 32-bit PHT is outlined as:

a' = a + b mod 232 (2)

b'= a + 2b mod 232 (3)

SAFER uses 8-bit PHTs extensively for diffusion. The 32-bit PHT is used by Two fish which combine the output with its 2 parallel 32-bit g function. This PHT are often executed in 2 opcodes on most modern microprocessors, as well as the Pentium family.

VII. WHITENING

Whitening, the technique of xoring key material before the primary spherical and once the last spherical, was utilized by Merkle in Khufu/Khafre, and severally fictional by Rivest for DES-X [KR96]. In [KR96], it was absolutely shown that whitening substantially escalate the difficulty of key search attacks against the rest of the cipher. Due to attacks on the reduced-round Twofish variants, we tend to discovered that whitening considerably increased the struggling of attacking the cipher text, by hiding from an wrongdoer the precise inputs to the first and last rounds' F functions. Twofish xors 128 bits of sub key prior to the primary Feistel round, and another half of 128 bits once the final Feistel round get completed. These sub keys units are calculated in the same manner as the round sub keys, but are not used anyplace else within in the cipher.

VIII. KEY SCHEDULE

The key schedule is that the means by that the key bits area units become into spherical keys that the cipher will use. Two fish desires a lot of key material, and features a difficult key schedule. To facilitate analysis, the key schedule uses similar primitives as the round function operate.

IX. FUNCTION

The function F could be a key-dependent permutation on 64-bit values. It lay hold of 3 arguments, 2 input words R0 and R1, and therefore the round range r accustomed choose the suitable sub keys. R0 is passed via the g function, that relent T0. R1 is revolved left by 8 bits and then passed via the g function to relent T1. The results T0 and T1 are combined in a exceedingly manner PHT and 2 words of the swollen key are expanded where (F0, F1) is the results of F. We incline to conjointly the function F0 to be used in our analysis. F0 is identical to the F function, except that it doesn't add any key blocks to the output

X. ATTACKS ON TWOFISH:

Basically there are various types of attack like DDOS Attack, Eavesdroping, SQL injection, Phishing and so many. But in this system we are taking only one attack i.e. MAN IN THE MIDDLE ATTACK. In this attack the third person interrupt in between the two people. The third person can outpour all data of the specified person and can update or change the data. This may cause the disaster in the data. It may leads to the wrong information. But in the twofish algorithm the key are too much strong and the cipher text are encoded in too much round function so that it is just impossible to encode those cipher text.

XI. RESULT

In this proposed system we are securing our data using twofish encryption algorithm as the mathematical expression is very strong to decrypt it.

It will secure the data of patient when it will send from one system to another system.

XII. CONCLUSION

Security is the main area to focus in the era of information security and IoT. Data is the most important thing in this world. Basically it is difficult to find the clear approach to secured the IoT device. Some devices afford very high security application to secure the data. Some device work on the very low security application. But the security application which are used to secure the data must be less complex and versatile. We should use very high security and trusted algorithm. The algorithm, which is used, is must be non-breakable. The main aim is to find the best solution to secure the data. Twofish algorithm is one of the best algorithm to secured data. As it is most difficult algorithm to break. After a lot of research, we are able to find that symmetric key cryptography is best. In this paper, we find out the drawback of the AES and DES algorithm and finally proved that two fish algorithm is good way to secured data. It is good to find the algorithm that is best executable on the hardware and the software. In this survey paper we discussed properly that twofish algorithm is the best way to encrypt the data. We also read various survey paper to find out the drawback of the existing system. The round function just help the algorithm to encrypt the data. The final algebraic structure is too secure that it can't be decrypted using any attack. Twofish symmetric algorithm is the most secured and trusted algorithm. Researchers are still working on it to make it suitable for IoT. In our future work, we will work on the architecture of the algorithm and how it works.

REFERENCES

1. Security and privacy challenges in Internet of Things, Molugu Surya Virat, Bindu S M, Aishwarya B, Dhanush B N, Manjunath R Kounte, School of Electronics and Communication, REVA University, Bengaluru, India, second international conference on Trends in Electronics and information (ICOEI 2018).
2. Current research Internet of Things (IoT) security: A survey, Mardiana Mohamad Noor, Wan H Hassan, Universiti Tecknologi Malaysia, December 2018.
3. Data security and privacy in the Internet of Things (IoT) Environment, Vijayaraghavan Varadharajan, Shruti Bansal, July 2016.
4. Security and privacy in IoT current status and open Issues, Mohamed Abomhara , Geir M.Koien Department of information and communication technology , University of Agder , Grimstad , Norway , May 2014.
5. Internet of Things: Application and challenges in technology and standardization, D. Bandyopadhyay and J. Sen, vol. 58, 2011.
6. A systemic approach for IoT security, Arbia Riahi, Yacine Challal, Enrico Natalizio, Zied Chtourou and Abdelmadjid Bouabdallah, 2013.
7. A survey of cryptographic algorithm for IoT device, Susha Surendram , Amira Naseef, Babak D. Beheshti, May 2018
8. Light weight cryptography for Internet of Insecure Things: A Survey, Indira Kalyan Dutta, Bhaskar Ghosh, Dr. Magdy Bayoumi, Center of Advanced Computer Studies University of Louisiana at Lafayette, IEEE 2019
9. A survey on cryptography algorithm, Omar G. Abood, Shawkat Guirguis, July 2018
10. Twofish: A 128-Bit block cipher, Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson, June-15-1998.