Data Security on Patient Monitoring for Future Healthcare Application

B. Vinoth Kumar
Research Scholar,
Dept. of Computer Applications
Madurai Kamaraj Univerisity,
Madurai, India

M. Ramaswami
Associate Professor,
Dept. of Computer
Applications, Madurai Kamaraj
Univerisity, Madurai, India

P. Swathika
Assistant Professor,
Department of CSE,
Kamaraj College of Engg. and
Tech., Virudhunagar, India

ABSTRACT
Many researches in the past ignore the need to encrypt the data for security perspective. However in recent years, researchers have given top priority for data security for smooth transmission of data over network by incorporating many encryption strategies along with actual data. In this paper, we consciously discuss the need to secure the data for patient monitoring using various algorithms and plug out the one which is best suit for inbound data security for future healthcare application. As the fields of IoT and Cloud are distinct by their intrinsic technologies, there is a need for integration of Cloud with IoT is obligatory to facilitate and resolve issues involved in data storage as well as data security. In the field of modern healthcare environment, automation has emerged to be more necessary to route and stock the facts about employers (doctors), employees (staffs) and customer (patients). Hence doctors in need of such a stored voluminous information's about a particular person, whom which the condition has to be diagnosed. The clinical and other facts about a person is indeed to be private (trust worthy) and should not be revealed by any other private identity. While establishing bi-directional connections to the internet, communication is a threat and has to be secured without involving any security threads. The offered work makes use of blow fish data encryption and IPv6 based addressing scheme for high data security and increased probability of number of nodes to reduce network congestion.

Keywords
Encryption, inbound data security, automation, network congestion, addressing scheme

1. INTRODUCTION
The internet technology serves the entire globe by offering its diversity as per the application. In particular, the IoT is slowly allowing for the health care industry to reduce its dependency on humans and steadily improving health care and providing early diagnosis and treatment of serious issues. Advances in IoT technology are making the creation of new data much easier by tracking the customer's health on 24 x 7 time scale. To be useful, all those data need to be communicated, stored, aggregated, and analyzed in ways that enable new and more effective problem solving. There are hundreds to thousands of useful—even life-saving—IoT medical applications that are changing the environment of health care industry today. On the other hand, cloud plays the vibrant part of internet, through which the storage platforms have reached a different facet [1].

The cloud storage has provisions like secure data storage and efficient retrieval of data. Many applications like customer services, education and research etc use cloud as a platform for storing and retrieving huge data. The user establishing connection can partially share their data over cloud using aggregate key generated by aggregate cryptosystem [2]. This technique is proven to be unique to generate a cryptographic key that not only used to secure data but in turn bind the processes of generating cryptographic key aggregate cryptosystem [3]. But the foremost problem here is how a common people believe that it is safe. There are provisions for cyber hackers to unzip our personal information. Such issue can be overcome by encrypting the data using specific algorithms. The usage of algorithms make use of a secret key to bound the data, which is not readable to foreign users [4]. On the other side, the little knowledge on encryption algorithms makes us to study and compare the behavior of algorithms available in literature. In this regard algorithm one like Blowfish achieves higher security and rapid execution when compared to algorithms like AES (Advanced Encryption standard) and DES (Data Encryption Standard) [2-4]. Another important nature of blowfish algorithm is that this algorithm is publically available and unpatented; therefore no license is required to be implemented it in various areas application domain.

2. PROBLEM ANALYSIS
In today's world, many people who survive past 65 years and above have chronic or life-limiting medical conditions that require a high level of healthcare. In most cases aged parents are living alone and their offspring keep away parents due to their social working conditions. Moreover they are not well aware of their medications that are available today. Besides their health condition, they always to like to stay in home than care centre. The patients who stay away from medical centre need ceaseless observation and advice from the health care takers (doctors and medical practitioners). To cater a service with hassle free environment, IoT and cloud provide a framework for healthcare that integrates medical centre and patient space [3]. In such circumstances, to keep patients records and medications prescribed by the doctor's reserve from unauthorized accessing agents in open cloud environment. Thus the concrete solution is required to secure the patient data in the integrated platform of IoT and Cloud. Moreover the data to be monitored for second by second is under risk and requires a solution using encryption algorithm.

3. NEW PATIENT CONTROLLED ENCRYPTION (PCE)
Moving to electronic health records is a significant enhancement in healthcare monitoring system and motivates the study of patient controlled encryption (PCE) system to secure the digital information over cloud. The key aggregation method is essential to preserve patient's privacy in electronic health record systems and it facilitates the patients can share

their data over cloud and can also decide with which user he/she needs to be shared and what data to be shared. In PCE, the health record is divided into a hierarchical representation based on use of different ontologies, and patients are the parties who generate and store secret keys. When there is a need for a healthcare system to access part of the record, a patient will release the secret key for the concerned part of the record. Any patient can draw his own hierarchy or follow the set suggested by electronic medical record system. When the patient wishes to give access rights to his doctor, he can choose any subset of these categories and issue a single key, from which keys for all these classes can be computed.

As shown in Fig. 1, the first step is to integrate IoT and Cloud environment is to develop a general architecture for future patient monitoring system [14] and subsequently propose a scheme to secure the healthcare data as shown in Fig. 2. In this architecture, first user divides his data into classes in his database over cloud and keys are generated for data. Using these keys, classes of data are encrypted and stored over cloud. Now user extracts an aggregate key for a single class of data which he needs to share with another. Now customer decrypt only allowed class of data with the aggregate key and data is received. Thus using key aggregate cryptography (KAC) the purpose of partial data sharing over cloud is fulfilled.

4. DATA ENCRYPTION ALGORITHMS FOR PCE

The algorithms used for encryption is generally categorized into two types; 1) using symmetric key 2) using public key. The strength of mentioned algorithms is primarily based on key length and there are two classes. The first class makes use

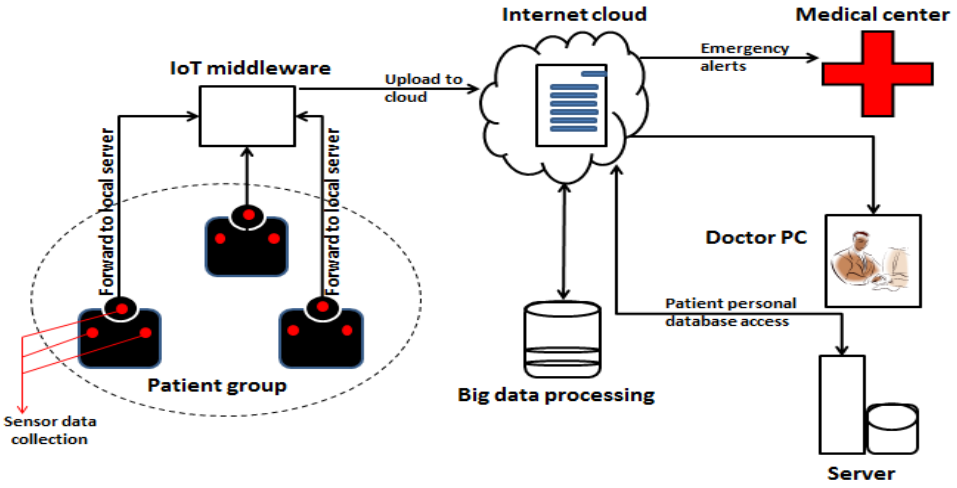

Fig 1: IoT and cloud based patient monitoring scheme

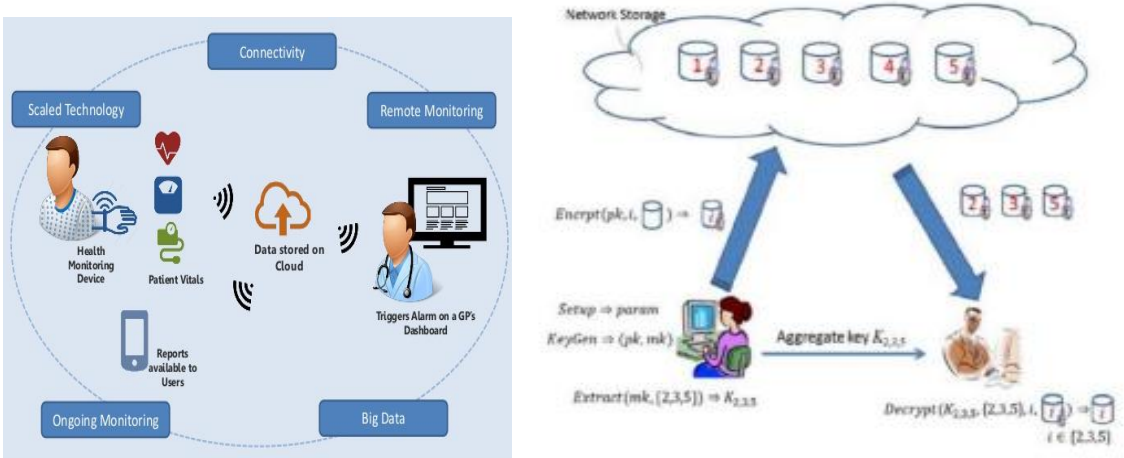

Fig 2: Security based IoT and cloud architecture for patient monitoring scheme

of symmetric algorithm with identical at both ends of encryption and decryption. Second key makes use of public key with non-identical keys at ends of encryption and decryption [5]. On the other hand, when comparing the mathematical operation in encryption and decryption, symmetric key is faster than public key. Since, public key uses basic mathematical logic operators, whereas public key uses two separate tedious mathematical functions at encryption and decryption [6]. Therefore the speed of execution is good and fast in symmetric key when compared to public key mode. Hence, based on uniqueness in using symmetric key, various symmetric key algorithms such as Blowfish, data encryption standard (DES), advanced encryption standard (AES) and Rivest Cipher 4 (RC4) [7] were proposed. The algorithms can be characterized using block cipher and stream cipher. Blowfish is among symmetric block cipher algorithm that uses a variable key length between 32 and 488 bits and has a 64-bit of block size. DES is a symmetric block cipher algorithm [8] and AES has a fixed 128-bit block size and its key sizes are 128, 192 and 256 bits. In RC4, 256-bit array S is filled from 0 to 255 and swap values of S with the key [9]. Upon comparison of various

security encryption algorithms, the performance of Blowfish on real world entities proves to be fast and secure. It was also observed that for all the four simulations Blowfish algorithm took relatively less time than other symmetric key cryptographic algorithms for encryption.

It was also concluded that performance of AES is better than DES. In paper [6], the author has simulated different symmetric key cryptographic algorithms like AES, DES and Blowfish. The simulation was done on 0.5 to 20MB data blocks. The simulation results shows that the Blowfish yields better results than other symmetric key cryptographic algorithms when it comes to processing power. AES yield poor results as it requires high processing power. In paper [7], the author compared AES and DES algorithms on image file format. The performance metric chosen by the author was encryption time. Performance metric like throughput to determine the speed of encryption, CPU process time to calculate the amount of time taken by CPU to process the file, memory utilization to keep the check on usage of memory. From the experiment it was concluded that AES is not energy efficient for performing encryption and decryption on a file as RC4. In paper [11], the author compared the three symmetric key cryptographic algorithms Blowfish and DES. In paper [9], the author has compared the three symmetric key cryptographic algorithms Blowfish, DES and AES for different block cipher modes, like ECB, OFB and CBC. It was found that for all the three phases Blowfish algorithm was giving best execution time for encrypting a file among all the algorithms and Blowfish algorithm model from literature is presented in Fig.3.

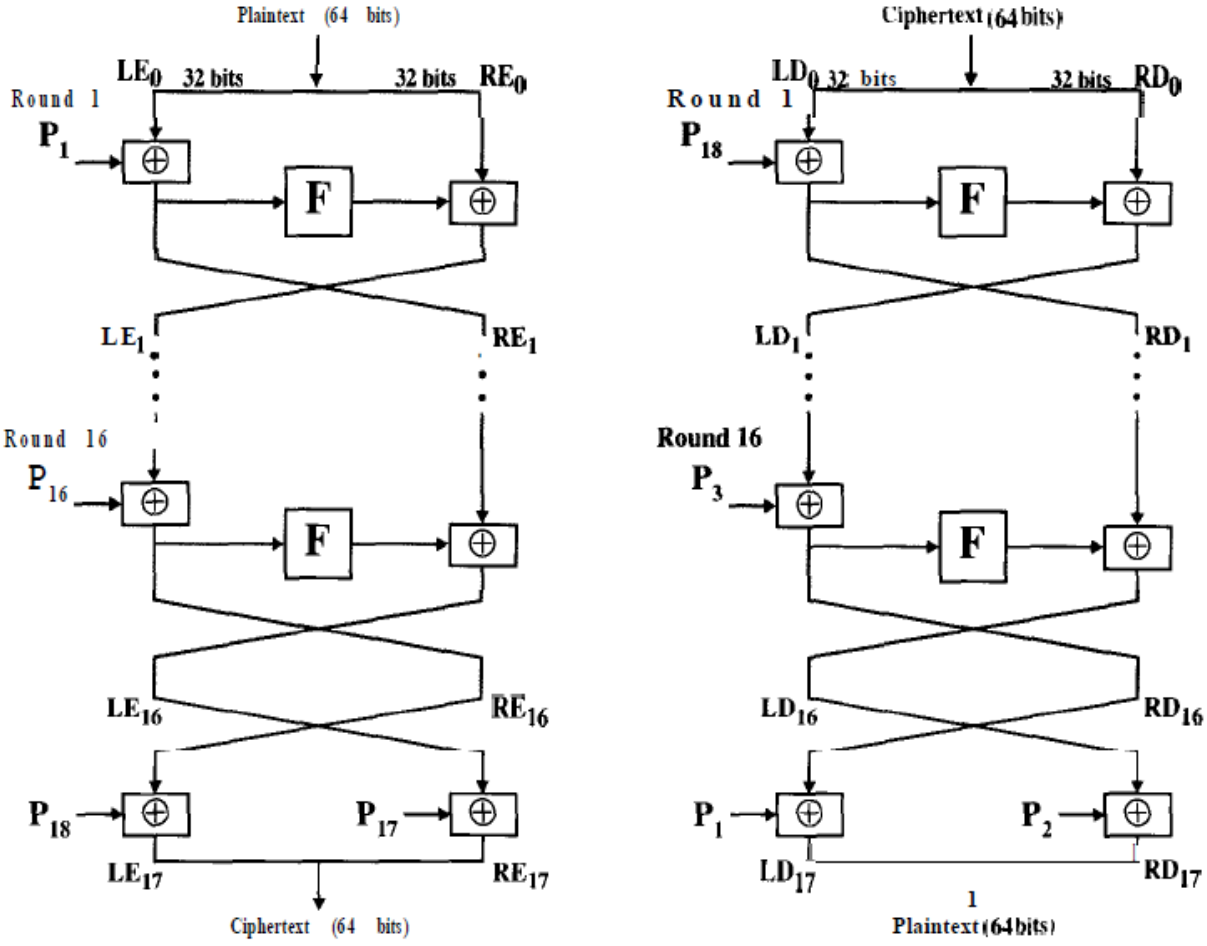

Fig 3: Blowfish model

The proposed PCE system incorporates the Blowfish algorithm which was designed in 1993 by a great scientist Bruce Scheier [13] as a swift, substitute to accessible encryption algorithms like AES, 3DES and DES etc. Blowfish algorithm is a symmetric block encryption scheme which provides:

- Fast: Data encryption takes place at a rate of 26 clock cycles per byte on 32-bit microprocessor.
- Compact: 5K of memory is more and enough to execute efficiently.
- Simple: It makes use of XOR, addition, lookup table with 32-bit operands.
- Secure: The key length is variable, it can be in the range of 32~448 bits: default 128bits key length.
- It is appropriate for applications where the key does not alter often, like communication link or an automatic key encryptor and it was royalty-free.

4.1 Description of Algorithm

Blowfish algorithm encrypts block data of 64-bits at a time. This algorithm is mainly divided into two parts. 1. Key-expansion 2. Data Encryption.

4.1.1 Key expansion

The key expansion process converts a key of 448 bits into numerous subkey arrays making it to a size of 4168 bytes.

Blowfish makes use of a large number of subkeys. These keys will be generated earlier to any data encryption or decryption. The p-array consists of 18, 32-bit subkeys: P1,P2,……,P18 Four 32-bit S-Boxes consists of 256 entries each: S1,0, S1,1,……..S1,255 S2,0, S2,1,……..S2,255 S3,0, S3,1,……..S3,255 S4,0, S4,1,.....S4,255

4.1.2 Data encryption

Data encryption is having a function to iterate the function 16 times of network. Each separate round consists of a key-dependent transformation and a key and data-dependent changeover. All operations performed are XORs and the additions on the 32-bit words. The only supplementary operations to the above functions are four indexed array data lookup tables for each round. Divide x into two 32-bit halves: xL, xR For i = 1to 16: xL = XL XOR Pi xR = F(XL) XOR xR Swap XL and xR Swap XL and xR (Undo the last swap.) xR = xR XOR P17 xL = xL XOR P18 Recombine xL and xR Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order. Implementations of Blowfish require the fastest speed should unroll the loop and ensure that all subkeys are stored in cache.

5. CONCLUSION

We studied the security algorithms that remained necessary to secure transmission data in a biomedical telemetry of u-Health monitoring system. We also investigated the security algorithms that could work properly in an embedded system with limited computation capabilities and small memory unit. Compared to all other algorithms the blowfish algorithm has made its mark in the cryptographic field. Similarly blowfish has a long key length and ensures safety and maintains lower memory usage than other algorithms. Thus the supreme strength of the encryption algorithm is mainly rest on the key length and moreover Key Aggregation helps the user to share their data over cloud storage partially. Using this technique we have developed Patient Controlled Encryption framework which helps user to store their medical records over cloud and partially share their data with preferred user. Thus, we concluded that blowfish was the most appropriate algorithm for the proposed healthcare system.

6. REFERENCES

[1] S. Pallavi and G. Navish, "Secure and optimized data storage for IoT through cloud framework", International Conference on Computing, Communication and Automation, Vol. 7, No. 15, pp. 720-723, 2015.

[2] B. Elisa, "Data Secusity and Privacy – Concepts, Approaches and Research Directions", IEEE Annual Computer Software and Applications Conference, pp. 400-405, 2016.

[3] K. Heshan, K. Ibrahaim, A. Abdulatif, T. Zahir and Y. Xun, "Secure Data Analytics for Cloud-Integrated Internet of Things Applications", IEEE Cloud Computing, Vol. 16, pp. 46-55, 2016.

[4] X. Chen, W. Lifeng, J. Zhu and C. Tiemeng, "A Multi-level Intelligent Selective Encryption Control Model for Multimedia Big Data Security in Sensing System with Resource Constraints", Vol. 6, No. 16, pp. 148-153, 2016.

[5] Jiho. P, Yong-Gyu. L and Gilwon. Y, "Implementation of Security Algorithms for u-Health Monitoring System", International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:6, No:5, 2012.

[6] AL.Jeeva1, Dr.V.Palanisamy and K.Kanag aram, "Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May -Jun 2012, pp.3033-3037.

[7] S. Soni, H. Agrawal, M. Sharma, "Analysis and comparison between AES and DES Cryptographic Algorithm", International Journal of Engineering and Innovative Technology, Vol 2, Issue 6, December 2012, pp.362-365.

[8] S. Nidhi and J.P.S.Raina, "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology, Vol 2, Issue 6, July-Aug 2011, pp.177-181]. DES has a block size of 64 bits and uses a 56-bit key. AES is also a symmetric cipher algorithm

[9] T. Jawahar and K. Nagesh, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, Vol 1, Issue 2, pp.6-12, December 2011.

[10] S. Preet Singh and R. Maini, "Comparison of Data Encryption Algorithms", International Journal of Computer Science and Communication(IJCSC), Vol. 2, Issue 1, , pp. 125-127, January-June 2011.

[11] N.A. Kofahi, T. Al-Somani, K. Al-Zamil, "Performance evaluation of three Encryption/Decryption Algorithms", IEEE 46th Midwest Symp osium on Circuits and Systems, 30-30, pp. 790-793, Dec. 2003.

[12] Jiho. P, Yong-Gyu. L and Gilwon. Y, "Implementation of Security Algorithms for u-Health Monitoring System", International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:6, No:5, 2012.

[13] Rashmi. K, Roshani. A, ""Development of improved Aggregated Key Cryptosystem for scalable data sharing", International Journal of Computer Science and Information Technologies, Vol. 6, No. 2 , pp. 1792-1794, 2015.

[14] B. Vinoth Kumar, M. Ramaswami, P. Swathika and P. Abinaya, "IPv6 based patient monitoring architecture for future healthcare application", International Journal of Computer Science and Information Security, Vol.14,No. 10, pp. 278-284, October 2016.