A Mobile Cloud Security on Electronic Healthcare Monitoring System through Virtual Private Network using Blowfish Algorithm

R. Parameswari, N. Prabakaran

Abstract*— An *Electronic Healthcare Monitoring System (EHMS) provides a mechanism to transfer patient's healthcare records and images to healthcare professionals in an encrypted format by using blowfish algorithm for securing sensitive and confidential information as it is stored in cloud server through virtual private network (VPN). The mobile cloud server respects the privacy of a patient and keeps it secured by protecting the medical images and healthcare record like Electronic Health Record (EHR), Electronic Medical Record (EMR) and Personal Health Record (PHR) of the patients. EHMS is conserving the privacy of the healthcare information ensuring that this information cannot misuse. The Digital Imaging and Communications in Medicine (DICOM) medical images are considered with an aim to secure them during its storage and transmission. This is achieved using Blowfish Algorithm, a type of symmetric key cryptography. The two processes, encryption and decryption together form the cryptographic process. For ensuring security, the patients' healthcare record and images are encrypted by the patient before transmitting them and are decrypted by the doctors' after receiving them so that only the sender and the intended person can see the content in the healthcare record as well as images. Blowfish algorithm which uses a key of variable size up to 448 bits simply iterates the function 16 times (Feistel network). In this system DICOM image processing is done using* **MATLAB** *and the Blowfish encryption-decryption is performed using the VHSIC HDL (Very High Speed Integrated Circuit Hardware Description Language) platform. All the encrypted images and healthcare records will be stored it in a cloud server through virtual private network in a secured manner.

***Index Terms* — Cloud Computing, Virtual Private Network, Blowfish algorithm, DICOM Images.**

I. INTRODUCTION

A framework for secure Electronic Healthcare Monitoring System (EHMS), which helps to provide a high level data accuracy, interoperability and sharing of healthcare data among healthcare providers, patients' and healthcare professionals. Mobile cloud computing offers significant benefits to the healthcare sector; Doctor's clinic, hospitals, and health clinics and these require quick access to computing and large storage facilities which are not provided in the traditional settings, moreover healthcare data needs to be shared across various settings and geographies which further burdens the healthcare providers and the patients causing significant delay in treatment and waste of time. Cloud caters to all these requirements thus providing the healthcare organizations an incredible opportunity to improve services to their customers, the patients, to share information more easily than ever before, and improve operational efficiency at the same time.

Healthcare industries are interested in Virtual Private Network (VPN) technology because it promises low-cost, secure data transmission via the internet and can be used to replace long- distance telephone charges and dedicated lines. VPN supports secure solution for mobile users. VPN is based on Internet Protocol Security (IP Sec) which provides added security features. IP Sec includes such security measures as authentication, encryption and key management. VPN setup needs two configuration files. The first one is the security – level definition and the second one is secure network map files. The security level definition contains parameters like the types of authentication, encryption scheme and so on. The secure network map file specifies which gateway is responsible for which remote VPN node. VPN offers a number of authentication schemes such as Handshake Message Authentication code, RSA Data Security public-Key cryptosystem, Message Digest 5, Secure Hash Algorithm and shared secret. Encryption technologies supports Blowfish algorithm, Data Encryption Standard (DES), Triple DES, International Data Encryption Algorithm, RSA, and RC5. VPN security related to Electronic Healthcare Monitoring System (EHMS) includes healthcare records like EHR, EMR, PHR sharing and integration in healthcare clouds and analyzing the arising security and privacy issues in access and management of healthcare data. VPN Security encompasses the collective measures that ensure healthcare data and transmission security within a VPN connection over a public network. It includes security methodologies and tools that ensure communication confidentiality, user authentication and message integrity in a VPN.

II. REVIEW OF TERMINOLOGIES

Electronic Healthcare Record (EHR) is an official health record for an individual that is shared among multiple facilities and agencies. Digitized health information systems are expected to improve efficiency and quality of care and, ultimately, reduce costs.

An EHR typically includes: Contact information, Information about visits to health care professionals, Allergies,

Manuscript Received on May13, 2015.

Ms. R. Parameswari, Research Scholar, St. Peter's University, Avadi, Chennai, India.

Dr. N. Prabakaran, Senior Vice Principal, St. Joseph College of Information Technology, Ruhuwuko, Songea, Tanzania.

Insurance information, Family history, Immunization status, Information about any conditions or diseases, a list of medications, Records of hospitalization, Information about any surgeries or procedures performed.

Personal Healthcare Record (PHR) is a collection of health-related information that is documented and maintained by the individual it pertains to. The data maintained in a PHR varies from one person to another and from one system to another but information in a typical record might include: Information about visits to health care professionals, Allergies, Family history, Immunizations, Information about any conditions or diseases, A list of medications taken, Records of hospitalization, Information about any surgeries or procedures performed.

Electronic Medical Record (EMR) is a digital version of the traditional paper-based medical record for an individual. The EMR represents a medical record within a single facility, such as a doctor's office or a clinic.

Healthcare Professional: person who delivers health care services, e.g. physician, dentist, pharmactics etc.

Healthcare Provider: organization that provides services of health professionals, e.g. doctor's practice or hospital.

Digital Imaging and Communications in Medicine (DICOM) is basically medical imaging standard for storing, transmitting, printing, and handling information. DICOM is implemented in almost every medical imaging device like radiotherapy device, cardiology imaging and radiology (ultrasound, X-ray, MRI, CT etc.). DICOM files are generally having varying data densities. Density of data represents the amount of different information present in the data file. A file is said to be dense, if file size is less and the content is more.

III. STUDY OF CRYPTOGRAPHY

Cryptography is a method of storing and transmitting data in an encrypted form so that only those for whom it is intended can read and process. It is a science of protecting information by encoding it into an unreadable format. It is an effective way of protecting sensitive information as it is stored on media like cloud storage and transmitted through network communication paths. The best possible solution to deal with Security issues is Data Encryption. Various algorithms exist to encrypt the data in Cloud Computing such as blowfish, DES, 3DES, AES, RC2, RC5 etc.

Symmetric key cryptography: Symmetric key cryptography is sometimes referred to as conventional cryptography or secret key cryptography. Here, the sender and the receiver will both have a common secret key.

The two different types of secret key cryptography are discussed below:

A. *Block Cipher*: Block ciphers take a number of bits and encrypt them as a single unit, padding the plaintext, so that it is a multiple of the block size. Blocks of 64 bits have been commonly used.

B. Stream Cipher (State Cipher): Stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudo random cipher digit stream (key stream).

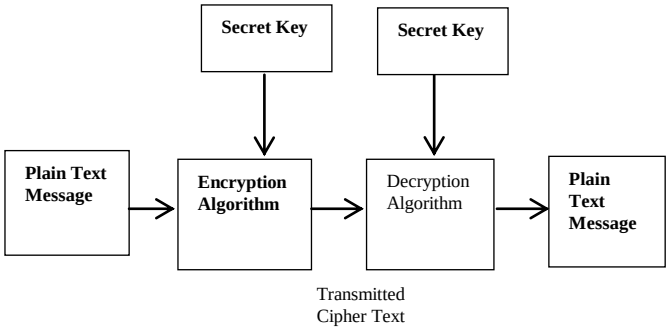

Figure1. Symmetric Key Cryptography

IV. BLOWFISH ALGORITHM

Blowfish Algorithm is a symmetric block cipher, designed in 1993 by Bruce Schneier as a fast, alternative to existing algorithms such AES, DES and 3 DES etc. It takes a variable-length key from 32 bits to 448 bits making it ideal for securing data. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits and the key can be of any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors. Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time. It follows the Feistel network and this algorithm is divided into two parts namely Key Expansion part and Data Encryption part [1], [6].

(i) Key Expansion

It converts a variable-length key of at most 56 bytes (448 bits) to several sub key arrays totaling 4186 bytes. Keys are generated before the image encryption and decryption process. There is a P array and four 32-bit S boxes. The P array contains 18 32-bit sub keys and out of four S boxes, each S box contains 256 entries. The generation of Key can be mathematically represented as,

$$F = ((S1[a] + S2[b] \bmod 2^{32}) \text{ XOR } S3[c]) + S[d] \bmod 2^{32}$$

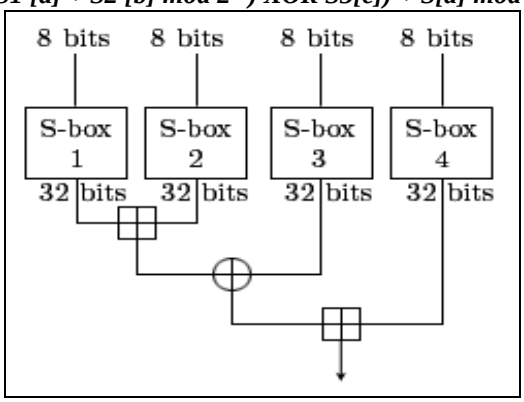

Figure 2: Schematic Representation of Key Generation

(ii) Data Encryption

After the string initialization, the first 32 bits of the key are XORed with P1 (the first 32-bit box in the P-array). The second 32 bits of the key are XORed with P2, and so on, until all 448, or fewer, key bits have been XORed. Starting from the first bit of the key bits, all key bits are XORed with the P-array to get cipher text using blowfish encryption algorithm.

Data Encryption is as follows:

Blowfish has 16 rounds.

The input is a 64-bit data element, x.

Divide x into two 32-bit halves: xL, xR.

Then, for i = 1 to 16:

xL = xL XOR Pi

xR = F(xL) XOR xR

Swap xL and xR

After the sixteenth round, swap xL and xR again to undo the last swap.

Then, xR = xR XOR P17 and xL = xL XOR P18.

Finally, recombine xL and xR to get the cipher text.

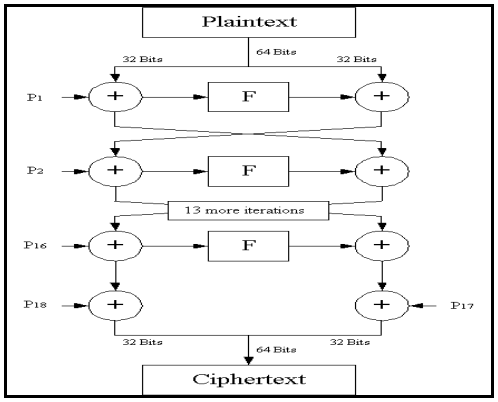

Figure 3: Blowfish Encryption

The process of decryption is the reverse process of encryption. Because Blowfish is a symmetric algorithm, the same procedure is used for decryption as well as encryption. The only difference is that the input to the encryption is plaintext and output is cipher text, but for decryption, the input is cipher text and output must be the plaintext. During Decryption, the cipher text block of 64 bits is divided into two halves of 32 bit each. The sub keys are all used in the reverse order as in the encryption process. That is, the process starts with the last elements of P array (p17 and p18) and ends with its first element (p1).

Sample Output:

$ ./Blowfish 37 D0 6B B5 16 CB 75 46 16 4D 5E 40 4F 27 52 32

Key: 37 d0 6b b5 16 cb 75 46
Plaintext: 16 4d 5e 40 4f 27 52 32
Cipher text: 5f 99 d0 4f 5b 16 39 69

V. MOBILE CLOUD HEALTHCARE

Mobile cloud computing technology will contribute to healthcare sectors in the following ways:

- Integrating healthcare data dispersed among different healthcare organizations and social media.
- Providing a shared pool of computing resources that is capable of storing and analyzing healthcare big data efficiently to take smarter decisions at the right time.
- Providing dynamic provision of reconfigurable computing resources which can be scaled up and down upon user demand. This will help reduce the cost of cloud-based healthcare systems.
- Improving user and device scalability and data availability and accessibility in healthcare systems.

Mobile cloud computing combines the power of mobile devices with the cloud computing concepts thus providing the users with unlimited pool of resource from cloud without hampering mobility of user. A healthcare user can store healthcare data and medical images (DICOM) on cloud and other authenticated users can read and see the images but there is the possibility to manipulate the data and images by the hackers, thus affecting the user privacy and integrity. So data and medical images stored on the cloud should be encrypted, disallowing unauthorized users to access stored data and medical images. The existing algorithms used for encrypting healthcare data and medical images on cloud are not efficient for handling security issues. In this work, the healthcare data are encrypted using blowfish algorithm and medical images are encrypted using MATLAB with VHSIC HDL (Very High Speed Integrated Circuit Hardware Description Language) platform using blowfish algorithm. Any algorithm or technique used for securing mobile users data should take into account above constraints for effective uses of cloud for mobile users.

VI. RELATED WORK

In past, health care providers have stored medical records of their patients on paper locally. This allowed a controlled environment with easy management of data privacy and security: keeping the paper records in a locked cabin at the doctor's practice. Even the increasing use of personal computers and modern information technology in medical institutions allowed for a moderate effort to manage privacy and confidentiality of individual medical records. This was due to the decentralized and locally managed infrastructure of each institution. But nowadays outsourcing of IT infrastructure (e.g. cloud computing) and other services (e.g. billing processing, accounting for medical practice) leads to a complex system where privacy-sensitive data are stored and processed at many different places. Hence, it becomes attractive to store and process healthcare data "in the cloud". While healthcare monitoring system's promise a more cost – efficient service and improved service quality, the complexity to manage data security and privacy increases. Himani Agrawal, implements some of the commonly used,

Symmetric encryption techniques in MATLAB software using Blowfish.

His work compares avalanche effect due to one bit discrepancy in key keeping the plaintext constant, bit discrepancy in plaintext keeping the key constant, memory required for implementation, key length, input block size, output buffer size, simulation time required for messages of different length and number of rounds needed for complete processing[9]. The commercial system like Google Health, Microsoft HealthVault and ICW Life Sensor are providing a way to store people health related data. In this model, patients need to manage complex access rights and need to understand their implications and also they need to rely on the robustness and correctness of the security mechanisms implemented at the PHR server provider. In general, it may be possible for the server provider to gain access to the data stored in PHRs [11].

VII. PROPOSED WORK

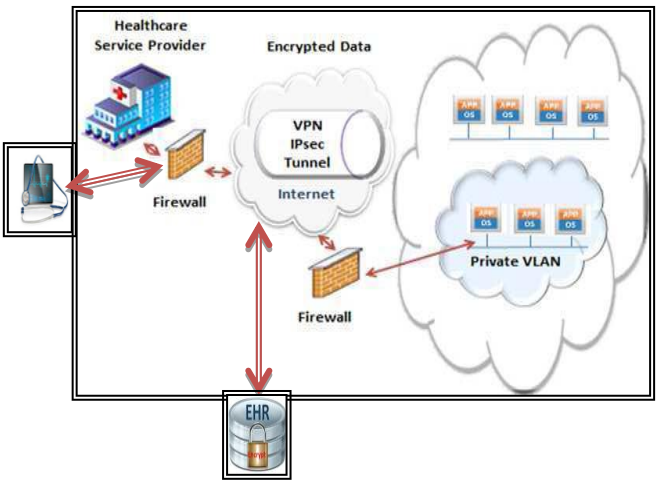

Figure 4: Secure Healthcare data via Virtual Private Network (VPN)

This system provides a mechanism to transfer patient's healthcare records and images to healthcare professionals in an encrypted format by using blowfish algorithm for securing sensitive and confidential information as it is stored in cloud server through virtual private network (VPN). The two processes, encryption and decryption together form the cryptography process. For ensuring security, the patients' healthcare records and images are encrypted by the patient before transmitting them and are decrypted by the doctors after receiving them so that only the sender and the intended person can see the content in the healthcare record as well as images. Blowfish algorithm uses a key of variable size up to 448 bits and simply iterates the function 16 times (Feistel network). In this proposed system, DICOM image processing is done using MATLAB and the Blowfish encryption-decryption is performed using the VHSIC HDL (Very High Speed Integrated Circuit Hardware Description Language) platform. All the encrypted images and healthcare records are stored in a cloud server through VPN in a secured manner. In patients and out patients are able to access their records and authorize doctors to access it. The security of this approach relies on modern cryptography schemes and their incorporation into an EHR infrastructure [5].

Algorithm

Step 1: Initializing variables for encryption.
The input is a 64-bit data element.
Crypto(byte in [16], byte out [16],
key_arrayround_key [Nr+1])
byte state [16];
state = in;
Get (i1, i2, i3…n)

Step 2: Converting healthcare data into cipher text as per the 16 rounds perform using Feistel network.
Encrypt (plaintext[n])
BlowfishKey (state, round_key [0]);
For i = 1 to Nr-1 step size 1 do

Step 3: Encrypted healthcare data will be stored into cloud via virtual private network.
Store (Crypto [])
Maintain ()

Step 4: Converting encrypted data into decrypted in secure manner.
Decrypt (Crypto(byte in[16]))
Plain (byte [16]);
End

VIII. ANALYSIS OF BLOWFISH ALGORITHM

The Blowfish algorithm has a better performance and has more efficiency than other common encryption algorithms. Blowfish is not having any known security weak points so far, so it is an excellent candidate to be considered as a standard encryption algorithm. When compare to other block cipher algorithms, blowfish for encryption and decryption will provide more security and confidential data.

The following graph shows the performance of blowfish algorithm compare to other standard encryption and decryption algorithm.

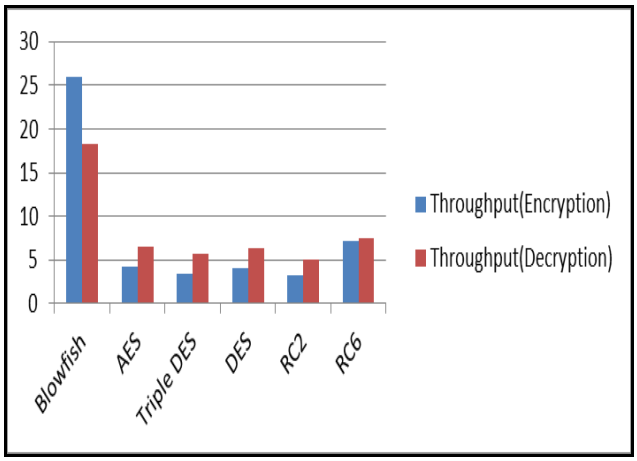

Figure 5: Performance of blowfish algorithm

IX. EVALUATION AND RESULT

The blowfish algorithm provides an integral protection mechanism for healthcare data. It performs and analyses the healthcare data and DICOM images. The two ways of analysis are,

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

(i) Healthcare data Protection (Like EHR, EMR, PHR etc.)

(ii) DICOM Images encryption and decryption

(i)

(ii) Healthcare data Protection:

Patient healthcare data is encrypted and decrypted using blowfish algorithm. The data stored on cloud is only on encrypted format with high level security. When the doctors tries to view the patients records in mobile devices it is decrypted based on the authentication. The implementation of this algorithm with sample data is shown below:

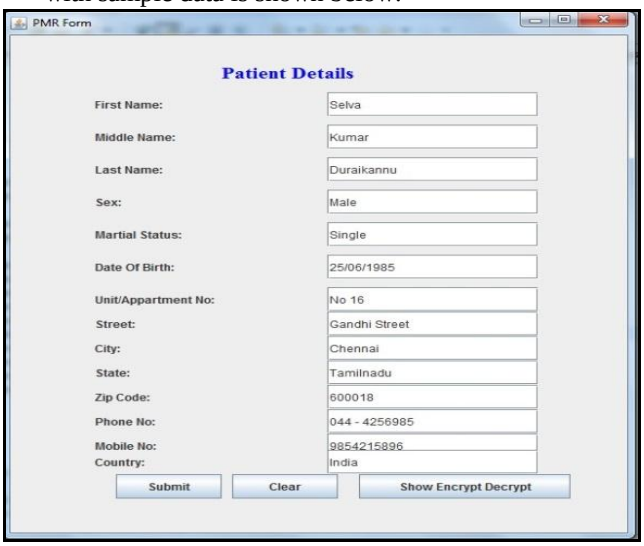

Figure 6: Patient Medical Record Form

Sample Output:

String To Encrypt: Selva
key Value: com.sun.crypto.provider.BlowfishKey@18e8e
Encrypted Value :DdeP7ZIFzd8=
Decrypted Value :Selva
String To Encrypt: Kumar
key Value: com.sun.crypto.provider.BlowfishKey@18e8e
Encrypted Value :9QJuTBmakYg=
Decrypted Value :Kumar
String To Encrypt: Duraikannu key Value:
com.sun.crypto.provider.BlowfishKey@18e8e
Encrypted Value :vMO/0oLJZAEu/S5CqCTwig==
Decrypted Value :Duraikannu

(iii) DICOM Image encryption and decryption:

The Medical Image Processing part is done using MATLAB software of version 7.5 (R2008b). It includes the visualization of medical images before and after encryption and decryption. The encryption and decryption part is done using VHSIC HDL (Very High Speed Integrated Circuit Hardware Description Language) platform, Xilinx ISE 10.1[1].

The sequence of steps is as follows:

i. View the input image taken to encrypt.
ii. Collect the pixel values of the viewed image.
iii. Provide the pixel values to VHDL encryption and decryption coding.
iv. Collect the encrypted and decrypted pixel values.
v. Provide these pixel values to visualize the encrypted and decrypted images.
vi. Verify that the decrypted image is an exact replica of the input image.

In blowfish algorithm, the input is processed as a group of bytes that are fixed in size (like 64, 128 or 256) long for encryption and decryption. Here the input is 64 bits long. In this work, the pixel values are encrypted one by one. Each pixel is 1 byte (8 bits); hence in order to make it 64bits, add 56 zeros to it before passing it to the Feistel network. The pixel values are temporarily read into a variable till 64 bits are read and each byte or each pixel is encrypted. Since the taken image is a 64×64 sized image, this process is continued till 4096 pixel values are read. The encryption and decryption code is written in VHDL. The implementation of this algorithm with sample image is shown below:

Figure 7: Input DICOM Image

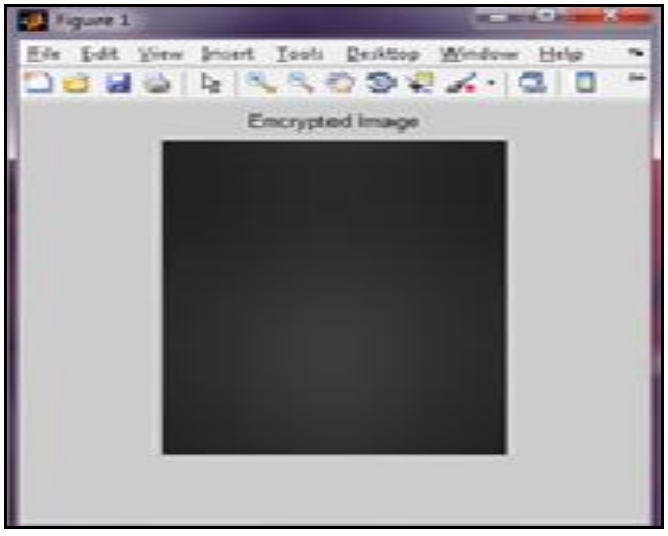

Figure 8: Encrypted Image

The decrypted pixel values of DICOM image is collected and fed into the MATLAB coding so as to view the decrypted image. Since there were a total of 4096 pixel values (from the input image) to be decrypted, the output will also have a total of 4096 pixel values.

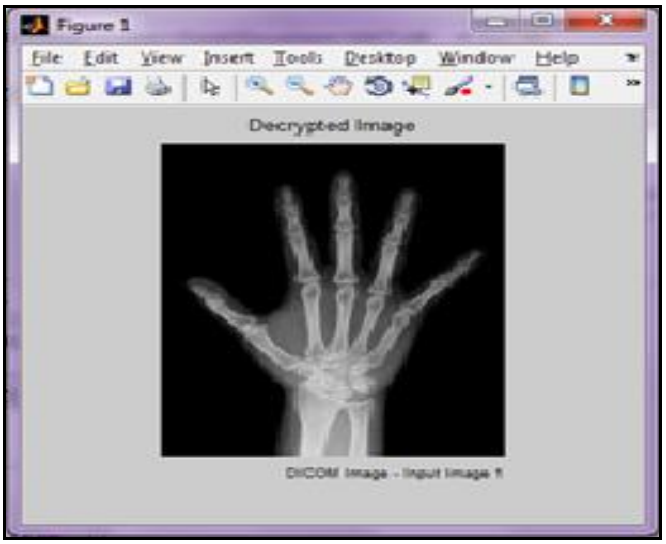

Figure 9: Decrypted Image

X. CONCLUSION

The mobile cloud security in healthcare sector is a growing research area in the information security field. Because low cost mobile devices, easy access of internet, availability software encourages the people to store their healthcare records in remote servers mostly on cloud storage. The main issue here is protecting their data from hackers. It is a challenging task. Compare to other fields security in healthcare data is a major concern because manipulation of health records directly affects the human life. The existing algorithms are not providing that much of security for protecting the healthcare data in cloud storage. This work increases the level of security in mobile cloud healthcare and the results are compared with existing algorithms.

In future, the huge size of healthcare data and DICOM images will increase in the speed, in which this data is generated in the big data analytics to find useful insights that help healthcare professionals take critical decisions in the right time.

REFERENCES

1. Dr. J. Abdul Jaleel, Jisha Mary Thomas, "Guarding Images using a symmetric Cryptographic Technique: Blowfish Algorithm" International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 2, August 2013
2. Irfan Landge, Burhanuddin Contractor, Aamna Patel and Rozina Choudhary "Image encryption and decryption using Blowfish algorithm" Proceedings of the 2012 National Conference of Emerging Trends in Information Technology, Shirpur, Maharashtra, April 21 , 2012.
3. Deepak Kumar Dakate and Pawan Dubey, "Blowfish Encryption: A Comparative Analysis using VHDL", IJAET, vol. 1, pp. 2249-8958, 2012.
4. Dr. V Ramaswamy and Krishnamurthy G N, "Performance Analysis of Blowfish and its Modified Version using Encryption quality, Key sensitivity", International Journal of Recent Trends in Engineering, vol. 1, pp, 1-4, May 2009.
5. P. Umamaheswari, K. Ashok Kumar," An Encryption Technique to Maintain the E-Health Information Using Blowfish Algorithm, Transactions on Engineering and Sciences ISSN: 2347-1964 (Online) 2347-1875 (Print) Vol.3, Issue 3, March 2015
6. Bruce Schneier. The Blowfish Encryption Algorithm Retrieved October 25, 2008, http://www.schneier.com/blowfish.html
7. Shasi Mehlrotra seth, Rajan Mishra — Comparative Analysis of Encryption Algorithms For Data Communicationl, IJCST Vol. 2, Issue 2, June 2011
8. A.A. Tamimi, "Performance Analysis of Data Encryption Algorithms. Retrieved October 1, 2008 from http://www.cs.wustl.edu/~jain/cse567-06/ftp/encryption_perf/index.html
9. Himani Agrawal, "MATLAB Implementation, Analysis and Comparisonof AES and BLOWFISH", International J. of Multidispl.Research & Advcs. in Engg. (IJMRAE), ISSN 0975-7074, Vol. 2, No. II, July 2010. pp. 283-290.
10. Vaishnavi B, Yogeshwari R, "A Secured Patient Healthcare Monitoring in Cloud Infrastructure" International Journal of Scientific Engineering and Research (IJSER), Volume 2 Issue 1, January 2014
11. H. Lo¨hr, A.-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud,"Proc. First ACM Int'l Health Informatics Symp. (IHI '10), pp. 220- 229, 2010.