An Implementation Of Twofish Algorithm In Healthcare System To Enhance Data Security

Veena Miranda[1] , Dr.R.Karthikeyan[2]

[1]Student ,Department of MCA,veenamiranda03@gmail.com,BIHER,Chennai

[2]HOD of Department of MCA,rkarthikeyan16798@gmail.com,IHER,Chennai

ABSTRACT

There is a vast increase in growing population which leads to an increasing demand for hospitals in healthcare sector. Due to which hospitals need to be provided with an efficient management system with data security and integrity . In this research paper we have discuss about the advance security features used to secure the data in database of the healthcare management system . As we know that even small scale hospitals require large database to store the the information of patients , doctors and nurses , etc , Which needs to be more secure and efficient. The proposed model stored the data of the healthcare system to the cloud database by implementing twofish algorithm , a block cipher for storing data by encryption and retriving the same by decryption . The implementation of an twofish algorithm in healthcare system provides high security to our data , which can be accessed only by an authenticate user . Using this algorithm we will encrypt the 128 bit block cipher using variable length key 128, 192 or 256 bits just as the AES algorithm.

KEYWORDS :*Twofish, AES, Block Cipher,Authentication,Steganography,health care system.*

1. INTRODUCTION :

The increasing demand for hospital systems is to provide an efficient reports along with efficient management of the patient data , doctors data ,etc is a formidable part of healthcare system. This has led the healthcare system to devise a faster and efficient method which compiles with the logistical and technical methods to operate faster and with much more accuracy and security providing immunity against cryptic attack .As we know that even small scale hospitals require large database to store the the information of patients , doctors and nurses , etc , Which needs to be more secure and efficient. The proposed model stored the data of the healthcare system to the cloud database by implementing twofish algorithm , a block cipher for storing data by encryption and retriving the same by decryption .

An healthcare management system was developed to assist the patient at the front desk of a hospital. The patient will be able to learn about the doctors, appointment times, relevant departments,patient details and the specific information about his/her meditation . System will provide an intelligent front desk information service for the patients at the hospital entrance. It will also provide software assistance for the doctors to diagnose easily and rapidly by using the program's decision mechanism .Developed system is a comprehensive, integrated information system designed to manage the organizational, financial and clinical aspects of a hospital. As an area of medical healthcare , the aim of the system is to achieve the best possible support of patient care and administration by electronic data processing.

For a medical treatment with smart-based facilities, physicians always have to pay much more attentions to the raw medical records of target patients instead of directly making medical advice, conclusions or diagnosis from their experiences. Because the medical records in smart-based Healthcare Management System (HMS) are dispersedly obtained from distributed devices such as tablet computer, personal digital assistant, automated analyzer and other medical devices, they are raw, simple, weak-content and massive. Such medical records cannot be used for further analyzing and decision supporting due to that they are collected in a weak-semantic manner. In this paper, we propose a healthcare system where we is significantly enriched and useful for healthcare analysis and decision making, and further demonstrate the feasibility and effecttiveness of our approach for database accessing.

Cloud computing is a technology that provides access to information and computing resources from anywhere that a network is available. Hence, there is a need to secure the patients data stored on the cloud. The proposed paper uses two fish encryption algorithm to protect integrity of the patients’ reports against unauthorized attacks. However, for all cloud computing applications, performance and cost of implementation are also major concerns. And two fish algorithm provides the required security and performance so the encryption algorithm is balanced.

2. TWOFISH ALGORITHM :

2.1 Encryption: Two fish:

The Two fish was first published in 1998 by the American cryptographer Bruce Schneier. The two fish algorithm is a type of block cipher that makes use of a key size of 128, 192 or 256 bits and a plaintext of 128 bits. Compared to Rijndael, Two fish is quite complex, but makes use of many similar functions. The basic process of Two fish is given as follows (depicted in figure 1).

i) The plaintext is broken up into four 32 bit words and each is XORd with a 32 bit expanded key(The first word is XORd with KK0the second word with KK1 and so on).

ii) The first word is broken up into 4 bytes, each of which is applied to a substitution box (or S-box, like the lookup table mentioned in AES). The second word is first rotated left by

8 bits and then is also applied to the same set of S-boxes.

iii)From here both the first and second words are applied to an MDS matrix (Maximum Distance Separable) which serves to diffuse the newly substituted data of the 32 bit word amongst its 4bytes.

iv)After the MDS matrix multiplication the first word is applied to a pseudo-Hadamard Transform:

aa'=aa + bbmmmmmm 232

where a is the first word, b is the second word and a' is the new first word.

Using the 'new' first word as input the second word is applied to the same transform. which can equivalently be represented as :

bb' = aa + 2bbmmmmmm 232

This operation serves to diffuse the two words amongst each other.

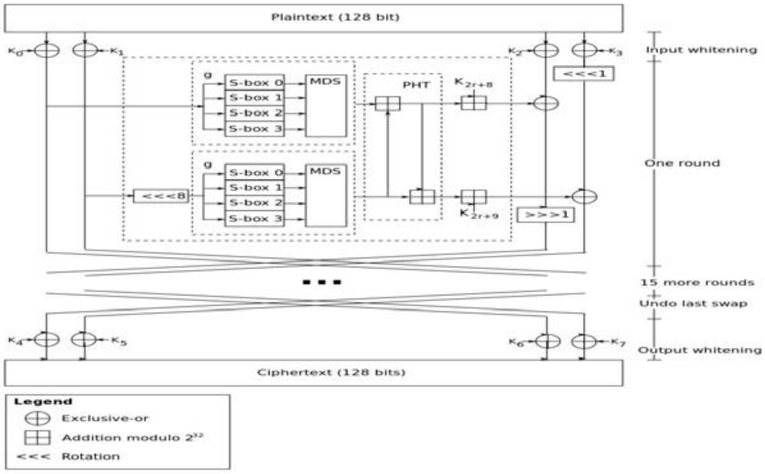

Fig.1. Two fish algorithm implementation

v)At this point the first two words are XORd with a round key each.

vi)Following this step the third word is XORd with the output of the first word (the new first word or WW0') and then rotated right by pne bit producing what will be the new third word(WW2'). At the same time the fourth word is rotated left by one bit and then XORd with the output of the operations on the second word(WW1')producing what will be treated as the new fourth word(WWW3').

vi)The next round begins (starting at step 2) with the first and second words (WW0 and WW1) at the beginning of the previous round becoming this rounds third and fourth words while the new first and second words are the output from the previous round (WW2' and WW3' respectively).

vii)Step 2 through 7 are repeated for a total (including the first)of the 16 rounds.

viii)The first and second words are swapped with the third and fourth words, effectively undoing the iproducing the cipher text.

An important note to make about Two fish however is that the S boxes used in the rounds (while the same 4 S- boxes for each round) are key dependant (dependant on the original source key, not the round keys). This adds an extra layer of security in that the S-boxes are now an unknown quantity to a would be attacker, making it much more difficult to crack a single round without knowledge of the key, since for two unique keys the primary substitution scheme will be different.

2.2 Cloud Storage :

Security is a major concern in cloud computing as our data is stored in a cloud and it becomes very difficult to perform operations on the encrypted data, hence we can use symmetric two fish encryption to secure our data and also perform operations on it. With symmetric two fish encryption, a laboratory can encrypt its entire database of reports and upload it to a cloud. Then it could use the cloud- stored data as desired—for example, to search the database to understand how its workers collaborate. The results would be downloaded and decrypted without ever exposing the details of a single patient report.

The encrypted file is stored in cloud database and secure from external unintended modifications to the file. The encrypted file can later be retrieved as and when required maintaining the integrity of the data by a user with proper login credentials.

2.3 Data Retrival :

The users can access data based on the permissions set by the administrator using the aunthenticate user id and password accesssed to the system. The encrypted data is then decrypted which can be accessed by the logged in user . This helps the system to increase the data security featues and accessibility .

3. IMPLEMENTATION :

The proposed paper is healthcare management software for storing patients data in Mysql database which is stored in a cloud. The person authorized to view and edit data permissions are set by the administrator. The administrator sets the respective read write permissions for accessing database securely thus preventing unnecessary threat to the patient database. The large dataset of the patient requires cloud storage whose services can be availed based on the hospital requirement whether small, medium or large scale laboratory instead of investing in data storage equipments which would further require manpower for maintenance and updation.

The software has been developed in PHP. The database stored is encrypted using two fish algorithm and retrieved using decryption two fish algorithm which uses same key known for both sender and receiver. The encryption of the file is done as shown in fig 2 using 128 bit encryption. The encrypted file is stored in cloud database and secure from external unintended modifications to the file. The encrypted file can later be retrieved as and when required maintaining the integrity of the data by a user with proper login credentials. The decrypted file from cloud can be then used by researchers for study and analysis of blood count data in predictive analysis for various health sector research studies. This contributes to tremendous help by researchers to the community resulted by the data analytics.

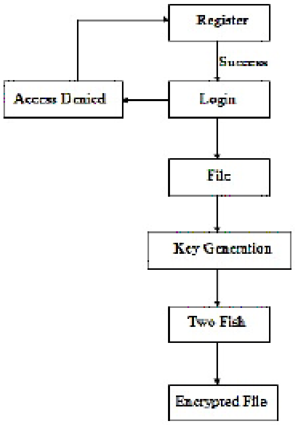

Fig. 2. Two fish algorithm implementation to the patients' database

The generalized implementation is as shown in fig 3 with cloud storage making the system more secure as it reduces the frequent crashes of the local database and can be retrieved at any point of time.

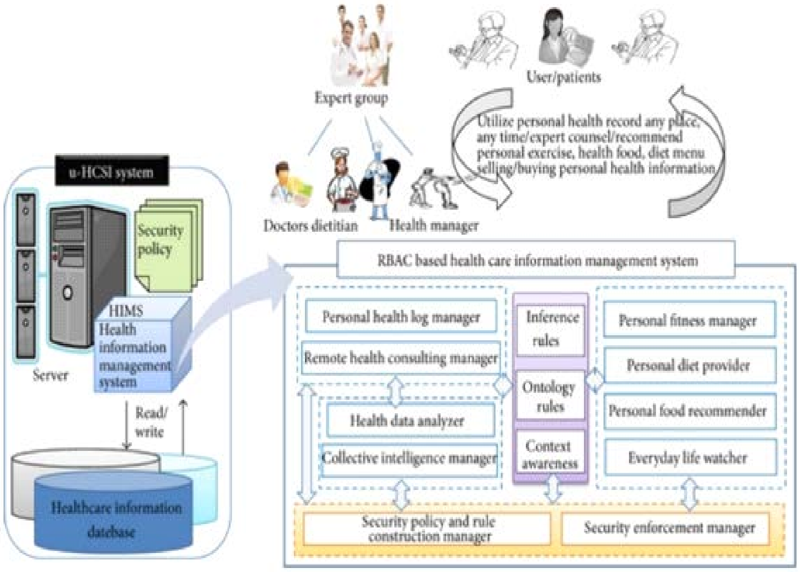
Expert group
User/patients
Utilize personal health record any place, any time/expert counsel/recommend personal exercise, health food, diet menu selling/buying personal health information
Doctors dietitian
Health manager
u-HCSI system
Security policy
Server
HIMS
Health information management system
Read/ write
Healthcare information datebase
RBAC based health care information management system
Personal health log manager
Remote health consulting manager
Health data analyzer
Collective intelligence manager
Inference rules
Ontology rules
Context awareness
Personal fitness manager
Personal diet provider
Personal food recommender
Everyday life watcher
Security policy and rule construction manager
Security enforcement manager

Fig.3. Healthcare Management System Implementation

The proposed system is very easy to operate. Speed and accuracy are the main advantages of proposed system. There is no redundancy of data. The data are stored in the cloud server hence it can be easily receive and used at any time. The proposed system will easily handle all the dataand the work done by the systems with tight security to data.

4. CONCLUSION:

Data Security is the major concern in hospital software of any healthcare institution. To achieve security, various cryptographic algorithms are used to encrypt and decrypt the data. The chosen algorithm should provide best performance in securing database which the two fish algorithm implementation provides for patient database in the proposed paper. As analyzed, Two fish will give better performance than blowfish. Because as compared to Blowfish, Two fish is a 128-bit block cipher and uses at most 128-bit key. This work can also be extended to determine the performance of cloud in terms of throughput, power consumption and memory consumption. This work can also be extended to the future work in encryption and decryption of large size of text files, images, audio files and video files.

REFERENCES :

[1] R.anderson and E. Bihan, "Two practical and provably secure block cipher BEAR and LION", fast software encryption, third international workshop proceedings, springer – verlag, 1996, pp. 113-120

[2]K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring", IEEE Internet Computing, Vol. 14, No. 5, pp. 14-22, 2010.

[3]C. Wang, B. Zhang, K. Ren, J. M. Roveda, C. W. Chen, and Z. Xu, ''A privacy-aware cloud-assisted healthcare monitoring system via compressive sensing,'' in Proc. INFOCOM, Toronto, ON, Canada, Apr. 2014.

[4]J. Sun, X. Zhu, C. Zhang, and Y. Fang, ''HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare,'' in Proc. ICDCS, Minneapolis, MN, USA, Jun. 2011, pp. 373–382.

[5]M. Li, S. Yu, N. Cao, and W. Lou, ''Authorized private keyword search over encrypted data in cloud computing,'' in Proc. ICDCS, Minneapolis, MN, USA, Jun. 2011, pp. 383–392.

[6]] D. Boneh, G. Crescenzo, R. Ostrovsky, and G. Persiano, ''Public key encryption with keyword search,'' in Proc. EUROCRYP, Interlaken, Switzerland, 2004, pp. 506–522

[7] K. Jashanpreet Pal, K. Rajbhupinder, "Security Issues and Use of Cryptography in Cloud Computing ", International Journal of Advanced Research in Computer Science and Software Engineering ISSN: 2277 128X vol. 4, issue 7, (2014) July.

[8]S. Joachim, “Cloud Services”, 4th IEEE International Conference on DEST, Germany, (2010).

[9] D. Akansha, K. Janda Harneet, B. Sayalee, “Security on Cloud Using Cryptography” International

Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, issue 3, (2015) March ISSN: 2277 128X.

[10] U. Blumenthal and S. Bellovin, “A Better Key Schedule for DES like ciphers” pragocrypt “96proceedings, 1996, pp.42-54.

[11]J. Jara, M.A. Zamora-Izquierdo, A. F. Skarmeta, “Interconnection framework for mHealth and remote monitoring based on the Internet of Things,” IEEE J. Sel. Areas Commun. 31(9) (2013) 47-65.