Data Security in Cloud for Medical Sciences using AES 512-bit Algorithm

R. Sai Sindhu Theja
Assistant Professor
Department of CSE
Sreenidhi Inst of Science & Tech.
R.R District, T.S, India
thejasindhu@gmail.com

G. Kalyani
Assistant Professor
Department of CSE
Sreenidhi Inst of Science & Tech
R.R District, T.S, India
kalyani_ghanta@yahoo.co.in

K Krishna Jyothi
Assistant Professor
Department of CSE
Sreenidhi Inst of Science & Tech.
R.R District, T.S, India
kogantikrishnajyothi@gmail.com

Abstract - Cloud computing is typically defined as a type of evaluation that relies on sharing computing resources to handle applications. There is a requirement to redesign the medical system to meet their better needs among the growing technologies .With the initiation of cloud computing the doctors can keep their information about the latest diseases, emergency cases and complex problems. However the privacy and security of data is extremely exigent. To guarantee privacy and security of data in cloud computing, we have proposed an effective approach for data security by the process of encrypting and decrypting the data through the concept of cryptography. In this paper the proposal is to prevent data access from cloud data storage centers by unauthorized access using AES-512 bit algorithm with key size and input block size of 512-bits that makes it more defiant to cryptanalysis.

Keywords: *Cloud, AES, Cryptanalysis.*

*****

I. INTRODUCTION

Cloud describes the use of group of services, applications, data, and infrastructure comprised of pools of networks, data and storage assets. These components can be rapidly implemented, decommissioned, and measured on demand utility similar to replica of allocations and consumption. NIST defines cloud by the following characteristics and models.

Characteristics

- On-demand service: Can calculate capabilities as desired without human intervention
- Broad Network Access: Services accessible over the net by means of desktop, laptop, PDA, mobile phone
- Resource pooling: supplier assets pooled to server several clients
- Rapid Elasticity: capability to speedily scale in/out service
- Measured service: organize, optimize services based on metrics

Service models

- SaaS (Sofware as Service)
  * It uses the purveyor applications
  * It doesn't supervise or have power over the network, servers, OS, storage or applications
- PaaS (Platform as Service)
  * It deploys the applications in the cloud
  * Reins their applications
  * Client doesn't administer servers, storage and IS
- IaaS (Infrastructure as Service)
  * Customers get access to the cloud to deploy their stuff
  * Do administer or control the system components

Deployment Models

- Public Model: Cloud infrastructure is available to the general public, owned by organization advertising cloud services
- Private Model: Cloud infrastructure for single organization may be checked by the organization or a third party, on or off hypothesis
- Community Model: Cloud infrastructure shared by several organizations that have shared concerns, managed by organization or a third party
- Hybrid Model: combination of more than two clouds bound by normal technology

II. CLOUD IN MEDICAL SCIENCES

Cloud computing is defined as a model for enabling ever-present, expedient, inexpensive, on-demand network access to a shared group of configurable computing resources that can be quickly provisioned and released with negligible management effort. Computers play an tremendous role in the education sector, business and IT sectors. They also play major role in medical sector also. With accessibility of high information rarely match with doctor, require a distinctive solution. Here an innovative cloud computing validation for hospitals to better access patient's medical information is expected. The core aim of cloud based clarification is to cut the cost (construction and maintenance), to reduce data loss risk, to assemble all the hospitals on one platform to better access patients' medical information.

In medical field a doctor can keep information on cloud to distribute over the globe. A doctor can get the obscurity of illness attacked to the patient; he will analyze, get the details and the solution of that illness. At this instant the doctor can set all the data of that case in a cloud. If the same case happens to another patient that doctor can get the information from cloud.

In cloud computing data storage is a significant issue because the entire data reside over a set of interconnected resource pools that enables the data to be accessed through virtual equipment. It sends the application software's and databases to the large data centers where the management of data is truly complete. The resource pools are positioned over various corners of the world, the organization of data and services could not be totally steadfast. So, there are a set of issues that have to be addressed with respect to all the security concerns of data.

Here we propose an effective and flexible scheme for providing security to data when it is residing at cloud. The proposal of cryptography is explained by 512bit AES algorithm; as the encrypted information is placed on cloud and only the authenticated doctors can decrypt the information from cloud[4].

Due to the increasing desires for safe interactions, highly securable cryptographic algorithms have to be planned and implemented. The new algorithm (AES-512) uses input block size and key size of 512-bits which makes it more resistant to cryptanalysis. AES-512 bit would be suitable for applications with eminent security and effective necessities[3]. The bigger key size makes the algorithm further secure.

III. AES ENCRYPTION METHOD

The below stature represents the general structure of AES encryption procedure. The cipher text takes a plain text block size of 512 bits, or 64 bytes. The input to the encryption and decryption algorithms is a single 512-bit block. The block is depicted as an 8x8 matrix of bytes which is copied into state array, which is modified at each stage of encryption or decryption. State is copied to an output matrix after the final stage. Similarly the key is depicted as a square matrix of bytes.

The cipher contains N rounds, which depends on the key length[2]. The number of rounds Nr can be calculated as Nr= (K/32) +6, where K is the number of bits of plaintext.

Number of Rounds Nr= (512/32) +6=22 rounds

This key is expanded into an array of schedule words. The formula for finding the number of words N_w is N_b * (Nr+1) words[3]. Here N_b is number of bytes of each word and Nr is number of rounds.

Number of words N_w= 8*(22+1) =184 words

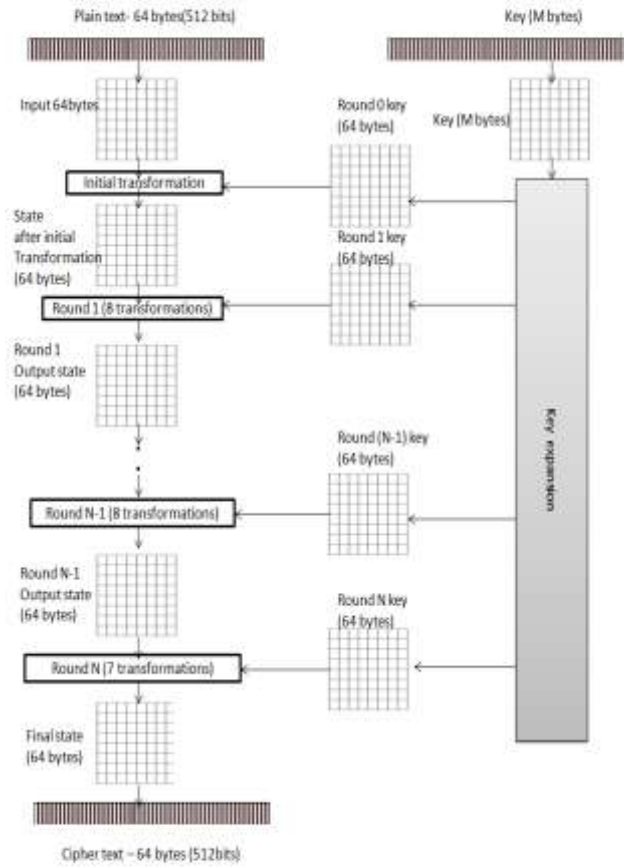

Plain text- 64 bytes(512 bits)
Key (M bytes)
Input 64bytes
Round 0 key (64 bytes)
Key (M bytes)
Initial transformation
State after initial Transformation (64 bytes)
Round 1 key (64 bytes)
Round 1 (8 transformations)
Round 1 Output state (64 bytes)
Round (N-1) key (64 bytes)
Round N-1 (8 transformations)
Round N-1 Output state (64 bytes)
Round N key (64 bytes)
Round N (7 transformations)
Final state (64 bytes)
Cipher text – 64 bytes (512bits)
Key expansion

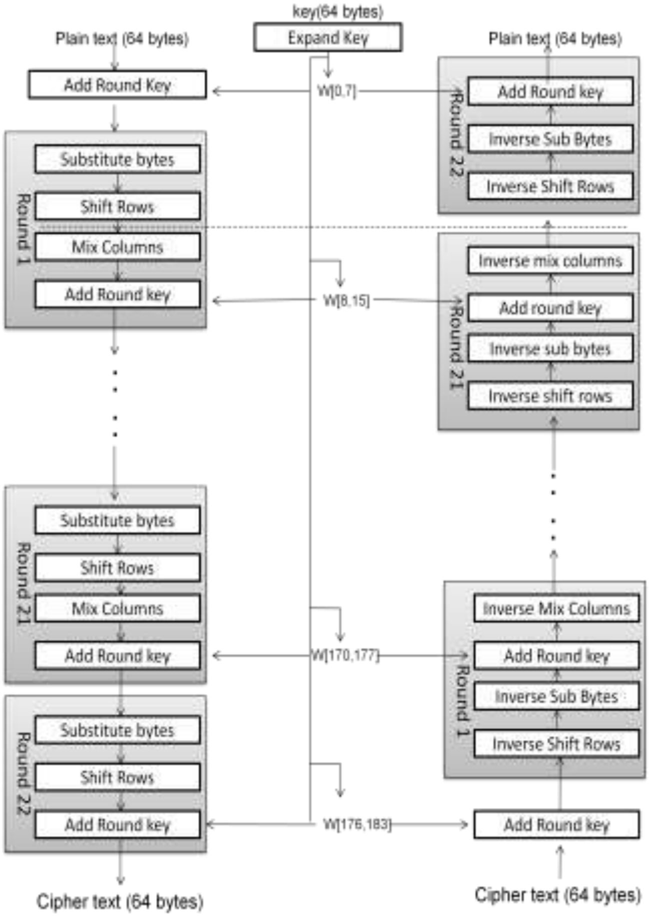
Figure 1: AES Encryption

Each word is eight bytes, and the total key schedule is 184 words for the 512-bit plaintext input to the encryption cipher which occupy the first column of the matrix; the second eight bytes occupy the second column, and so on.

The first N-1 rounds consist of four distinct transformation functions: Sub Bytes, Shift Rows, Mix columns and Add Round Key which are described consequently. The final round contains only three transformations, and an initial single transformation (Add Round key) before the first round, which is considered Round 0. Every transformation takes one or more 8x8 matrices as input and generates an 8x8 matrix as output. The above figure shows that the output of each round is an 8x8 matrix, with the output of final round being the cipher text. Also, the expansion function generates N+ 1 round key, each of which is a distinct 8x8 matrix. Each Round key serves as one of the inputs to the Add Round Key transformation in each round.

IV. AES ENCRYPTION AND DECRYPTION

The stature below shows the AES cipher in more detail, representing the sequence of transformations in each round and showing the equivalent decryption function. Encryption is shown as top to down process and decryption is just the turn around of it[2].



(a) Encryption (b) Decryption

Figure 2: Encryption and Decryption Process

Four stages are performed, one is permutation and three are substitutions.

- Substitute bytes: A Byte by byte substitution of the block is performed
- Shift Rows: A simple permutation performing row by row
- Mix Columns: A substitution that uses arithmetic over GF (2^8)
- Add Round key: Performing a bitwise XOR of the current block with a part of the expanded key

The cipher begins with Add Round Key stage, followed by 21 rounds that each includes all the four stages, followed by a 22nd round of three stages which is shown in the below figure. Only the Add Round key stage uses key. The cipher begins and ends with Add Round Key stage for this reason. The other three they would not provide any security because they do not use the key. We can view the cipher with alternating operations of XOR encryption of the block, followed by the other three stages, followed by encryption, and so on.

Each stage is easily reversible. For the three stages an inverse function is used in the decryption algorithm. Inverse is applied for the Add Round key by XORing the same round key to the block. The decryption process uses the expanded key in reverse order. Once it is established that the four stages are reversible, it is easy to verify that decryption do recover the plain text.

Hence, AES 512bit is extremely safe and sound as we are using 22 rounds of encryption and decryption which provides excellent security for the data.

V. PROPOSED SYSTEM

In the proposed system we introduce the cloud concept in medical sciences. For example if we consider the disease "Ebola" since 2014 January, thousands of people were affected to the Ebola virus, and almost 6,000 people have died in Guinea, Sierra Leone, and Liberia to date. Liberia has affirmed a national emergency. Eight other countries remain on high alert. The Ebola spreads directly with bodily fluids from infected people or animals, and there is no cure. Now the country West Africa is suffering a lot with Ebola. It has not spread to other countries also. If the result for Ebola is invented then it should be maintained behind closed doors. If an unauthorized user desires to cause harm to the neighboring countries by changing the solution of the Ebola may create a new problem that affects people.

In order to provide security for such type of medical data, we introduce the concept of data storage on cloud and apply AES 512bit algorithm [1]. The data which is encrypted 22 rounds is very hard to detect the original data of Ebola solution and thus we can maintain high security for the valuable data.

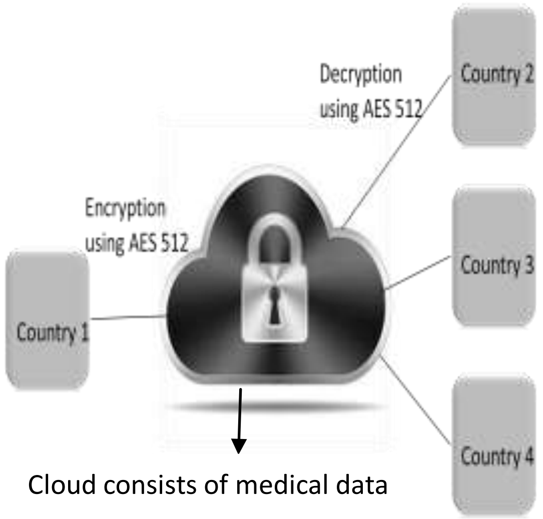


Figure 3: Data storage in a cloud

In the above diagram if the cloud consists of 2048 bits, then the data is divided into four 512 bits and the 512bit AES algorithm is applied. The solution found by one country can be shared by many countries without any risk. The authorized doctor only knows about the key and decrypts the data.

VI. CONCLUSION & FUTURE WORK

In this paper 512bit AES algorithm is used to provide security on medical data present in cloud. So that only the authorized persons can decrypt the data. It is highly securable and very efficient. The only disadvantage of AES-512 is the need for more design area. In the future work the 512bit AES algorithm which consists of 22 rounds may be minimized to 18 rounds which reduces time consuming and cost.

REFERENCES

[1] Avula Tejaswi, Nela Manoj Kumar, Gudapati Radhika, Sreenivas Velagapudi, "Efficient Use of Cloud Computing in Medical Science" in American Journal of Computational Mathematics, 2012

[2] Abidalrahman Moh'd, Yaser Jarerweh, LO'ai Tawalbeh," AES-512: 512-Bit Advanced Encryption Standard Algorithm Design and Evaluation" in 2011 7th International Conference on Information Assurance and Security (IAS).

[3] Rishabh Jain , Rahul Jejurkar , Shrikrishna Chopade , Someshwar Vaidya , Mahesh Sanap

[4] "AES Algorithm Using 512 Bit Key Implementation for Secure Communication" in International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 3, March 2014.

[5] M. Anand Kumar and Dr.S.Karthikeyan, "A New 512 Bit Cipher for Secure Communication" in I. J. Computer Network and Information Security, 2012

[6] "Ebola virus" https://www.planusa.org

Assistant Professor R. Sai Sindhu Theja, received B.Tech in Computer science and Engineering from JNTU, Hyderabad, India, holds a M.Tech in Computer Science from KL UNiversity, Vijayawada, A.P., India. She has 4 years of experience in Computer Science and Engineering areas pertaining to academics. She is presently working as Assistant Professor, Department of Computer Science and Engineering, Sreenidhi Institute of Science and Technology , Ghatkesar , R.R.Dist.,T.S, INDIA. She is currently working in the areas of advanced Programming languages, Database paradigms and Network Security. She can be reached at thejasindhu@gmail.com.

Assistant Professor G.Kalyani, received B.Tech in Computer science and Engineering from JNTU, Hyderabad, India, holds a M.Tech in Computer Science from IETE, Hyderabad, A.P., India. She has 9 years of experience in Computer Science and Engineering areas pertaining to academics. She is presently working as Assistant Professor, Department of Computer Science and Engineering, Sreenidhi Institute of Science and Technology , Ghatkesar , R.R.Dist.,T.S, INDIA. . She is currently working in the areas of advanced Programming languages , Compiler Design , Network Security and Discrete structures. She can be reached at kalyani_ghanta@yahoo.co.in.

Assistant Professor K.Krishna Jyothi, received B.Tech in Computer science and Engineering from JNTU, Hyderabad, India, holds a M.Tech in Computer Science from JNTU, Hyderabad, A.P., India. She has 5 years of experience in Computer Science and Engineering areas pertaining to academics. She is presently working as Assistant Professor, Department of Computer Science and Engineering, Sreenidhi Institute of Science and Technology , Ghatkesar , R.R.Dist.,T.S, INDIA. She is currently working in the areas of advanced Programming languages, Database paradigms and Network Security. She can be reached at kogantikrishnajyothi@gmail.com.