International Journal of Trend in Scientific Research and Development (IJTSRD)

International Open Access Journal

ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Securing Mechanism of Healthcare Data on Cloud

Sripriya A N, Rahisha Pokharl, Manjunath C R

Department of Computer Science and Engineering,
School of Engineering and Technology, Jain University, Bengaluru, Karnataka, India

ABSTRACT

Healthcare data are very sensitive records which hold patient's information. In order to make this information secured it should not be made available to unauthorized people. Information technology is increasingly used in healthcare with the goal to improve and enhance medical services and reduce cost. Hospitals across the globe are in the process of moving away from paper-based manual information processing to Electronic Health Records (EHR) and Hospital Information System (HIS) in order to provide effective and efficient healthcare services. Cloud computing model is becoming popular in healthcare IT infrastructure for providing EHR sharing and EHR integration. However, they also come along with new risk and raise challenges with respect to security and privacy aspect. There are different techniques used to protect the data which includes Data Encryption, Data Masking, and Access Control. Encryption is a process of changing the actual text in order to secure the original data. Ensuring security and privacy is a major factor in the cloud computing environment. Hence, securing healthcare data stored in the cloud is an important measure for healthcare IT system.

I. INTRODUCTION

Medical data refers to health related information that is associated with regular patient care or as a part of clinical trial program which are the most sensitive data. Privacy of the data is the main concern when it comes to access and sharing of health and medical data. In this modern era of healthcare, there is a requirement for an infrastructure that reduces the efforts, time consumption and operation cost to obtain medical records on the patient. To increase the quality of service there is a demand for Electronic Medical Record (EMR) and Hospital Information System (HIS) by the healthcare industry. Cloud services improves patients care by providing secure, better, faster service at a lower cost which meets the requirements. Cloud storage also refers to services and applications that run on a distributed network using virtualized resources and can be accessed by networking standards and common Internet protocols. Here the resources are unlimited, virtual and as well as the details of the physical systems on which software runs are abstracted from the user.

II. Impact of cloud storage in healthcare

Around one tenth of revenue is been invested by healthcare providers into field of Information technology as compared to any other industries that regularly invest almost quarter of their revenue. Health care organizations are trying to implement the best features of cloud computing, which can be helpful to provide quality service to their patients. The decision makers of healthcare are rapidly considering alternate measures to implement innovative solutions and to reduce the cost.

There are numerous advantages and benefits on implementing cloud computing in healthcare industry. Some of them are:

- **Mobile component:** Cloud computing provides more mobility to its users. It allowing professionals and authorized people to store and access data remotely on a Smartphone, tablet and other mobile gadgets.

- **Security and privacy:** Patient's record contains data that are confidential which needs to be protected at all time. With the recent HIPAA update, cloud healthcare service providers are now responsible for HIPAA compliance as healthcare entities they serve.

- **Cost reduction**: by adapting cloud technique in healthcare industry, patients, doctors, and other medical organization cost of experience would highly reduce. Since the service provider would take care of the infrastructure and maintenance.

- **Authorized access:** Access to hospital system is prohibited until the permission is granted to the authorized user by the hospital data in charge. The authorized people are provided with login ID and password credentials to access the medical records stored on cloud.

- **Risk for data loss:** Cloud application for healthcare would have constant updates for which there would be security bar. Cloud technology performs update without affecting the actual data and prevents data loss in real time.

A. Service Models

There are three different service models described below in this literature. Service models are categorized as:

- **Software as a Service:** In SaaS the applications are hosted on the cloud as a service where the customers can access it via internet. When making use of SaaS under the healthcare organization standard software framework is utilized. Various organizations utilize different cloud software frameworks for their, recruitment, virtualization, resources planning, database management, human resource management and content management. With the help of SaaS service for healthcare organization, the organizations will be provided with all the services like platform, infrastructure and information management.

- **Platform as a Service:** **Another** application delivery model among the cloud services is Platform as a Service (PaaS). All the resources required to build application is provided by PaaS from internet connectivity to the software which need not be downloaded or installed. Healthcare providers can develop their application with the help of libraries that are provided by the cloud service provider. Various features are provided by the PaaS service provider which will take the burden off from the healthcare organizations like security, disaster management, etc. With the help of Paas services for healthcare organization, clinical information of the healthcare data can be developed.

- **Infrastructure as a Service:** Infrastructure as a Service (IaaS), also called as Hardware as a Service (HaaS) is the next form of service available in cloud computing. It simply offers the hardware so that your organization can put whatever they want onto it. IaaS provides infrastructure, storage, virtual machines, and other hardware resources. In typical hospital scenario, the IaaS provider can also act as the back- up repository server, where data storage is facilitated by the IaaS provider which can also be stored in public server in turn.

III. Need for security of healthcare data on the cloud

Many healthcare organizations are employing cloud computing in order to improve data analytics efficiency and to reduce administrative costs. The cloud allows the healthcare professionals to access patient information from any Wi-Fi-enabled device at any location. Cloud security is important to protect patient privacy, abide by health care laws, and to ensure that only authorized health care professionals are capable of accessing the correct data. Due to the complexity of structuring cloud computing to comply with the Health Insurance Portability and Accountability Act (HIPAA), which regulates how health organizations protect private healthcare information, some health organizations are reluctant to adopt cloud computing.

A. Challenges of Cloud Security

Effective cloud security must address key challenges in the following areas:

- **Unauthorized access:** when someone gains access to a website, service, or other system using someone else's account or identity it is referred to as unauthorized access. Stopping unauthorized access to information is what makes privacy protection possible. When a unauthorized person gets to access the medical reports of the patients there is a high chances that the records will be manipulated which would read to wrong analysis of the report which might even cost patient's life.

- **Safety access from mobile devices:** Health professionals and patients should be able to access data securely from mobile devices like cell phones, tablets, or laptops. If network security isn't optimal, vulnerable data could be lost or stolen when accessed through an unsecured mobile device.

- **Protecting databases:** Data stored in database is vulnerable at many points in any storage space, and many security techniques and types of functionality can be employed to protect it. Confidentiality, integrity, and availability are the hallmark of database security. Privilege to modify the data stored on the database should not be given to anybody.

IV. Encryption Algorithms

Encryption is a process of translating plain text data into something that appears to be random and meaningless. Decryption is a process of converting cipher text back to plain text. To encrypt more than a small amount of data, symmetric encryption algorithms are used.

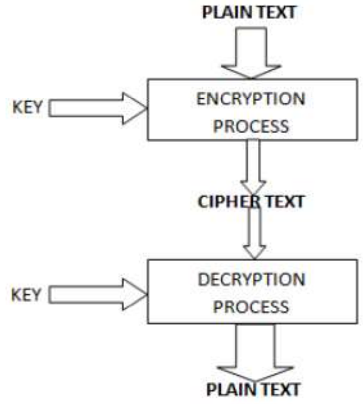

Fig. 4.1 Encryption process

Here is an overview of various symmetric and asymmetric encryption algorithms. Encryption is done at different levels. Some algorithms are used to encrypt data before uploading onto the cloud and some are used after uploading the actual data onto the cloud.

Some of the algorithms used to encrypt data before moving it onto the cloud are:

1. 3DES (Triple Data Encryption Standard):

Triple Data Encryption Standard (3DES) basically applies the Data Encryption Standard (DES) encryption algorithm three times to each data block. Triple-DES was proposed by IBM in 1978 as a replacement to DES. Three DES is also called as T-DES. It uses the simple DES encryption algorithm three times which in turn enhances the security of encrypted text. Using 3DES, the encryption becomes even stronger and more difficult to break. Triple DES is basically a Block cipher that uses 48 rounds (Three times the DES) in its computation, and has a key length of 168 bits. 3-DES also uses the Block size of 64 bits for encryption. In this type of encryption, some data are encrypted two more times using DES. Hence, the encryption becomes stronger and more difficult to break.

2. RSA Algorithm:

RSA is a cryptosystem, which is known as one of the first feasible public-key cryptosystems. It is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, i.e. on the factoring problem.

The keys for the RSA algorithm are generated in the following way

- Choose two distinct prime numbers p and q.
- Compute n = p*q.
- Select the public key (i.e. the encryption key) e such that it is not factor of (p-1) and (q-1)
- Select the public key (i.e. the decryption key) d such that the following equation is true: (d * e) mod (p-1)*(q-1)=1.
- For encryption calculate the cipher text CT from the plane text PT as follows CT=PT e mod n
- Send CT as the cipher text to the receiver
- For decryption, calculate the plane text PT from the cipher text CT as follows. CT d mod n

3. Blowfish:

Blowfish is basically a symmetric block cipher having variable length key from 32 bits to 448 bits. It operates on block size 64 bits. It is a 16-round feistel cipher and uses large key dependent S-Boxes. Each S-box contains 32 bits of data. Blowfish is a variable key length algorithm and it is having 64-bit block cipher. The algorithm consist of two sub parts, one is key expansion part and second data encryption part. Data encryption is done by completing 16 rounds fiestel network.The function splits the 32 bit input into four 8-bit quarters, and uses the quarters as input to S-boxes. The outputs are added (Mod) modulo 232 and XOR ed to produce the final 32-bit output i.e. encrypted data. For Decryption at another end the same process takes place, but in reverse order

4. Twofish:

Twofish is also a symmetric block cipher having fiestel structure. Twofish also uses block ciphering like Blowfish. It is efficient for software that runs in smaller processor (smart cards) and embedded in hardware. It allows implementers to customize encryption speed, key setup time, and code size to balance performance. Twofish is license-free, un-patented and freely available for use. In twofish encryption it uses key sizes of 128, 192 and 256 bits. It uses the block size of 128 bits and there are 16 rounds of encryption in this encryption algorithm.

5. AES (Advanced Encryption Standard):

The Advanced Encryption Standard (AES) is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world for sensitive data encryption. AES is actually, three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128 bits, 192 bits and 256 bits, respectively. In Advanced encryption standard there are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128 bits, 192 bits and 256 bits, respectively. In Advanced encryption standard there are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

Other different algorithms used for encrypt data are:

6. DSE (Data Encryption Standard):

Data encryption standard is a symmetric encryption system that uses 64-bit blocks. Out of these, 8 bits are used for parity checks i.e. to validate the integrity of the key. Each of the key's parity bits (1 every 8 bits) is used to check one of the key's octets by odd parity. Basically, each of the parity bits is used to have an odd number of '1's in the octet it belongs to. The key is 56 3bits long, out of which only 56 bits are mainly used in the algorithm. So in order to find the correct key, a maximum of 256 or 72,057,594,037,927,936, attempts will be required. It is basically a combination of two basic techniques of encryption i.e. confusion and diffusion. There is no strong limitation found rather than its small key size which offers less security.

7. ECC (Elliptic Curve Cryptography Algorithm):

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields i.e. elliptic curve theory. ECC Create Faster, Smaller and more efficient keys as compared to other encryption algorithm. In this, encryption is done in elliptic curve equation form. ECC is considered so efficient that it can even yield a level of security with 164 bit key that other system require a 1,024-bit key to achieve that security level i.e.it offers the maximum security with smaller bit sizes that is why it consumes less power and hence, Elliptic curve cryptography is good for battery backup also.

Basically, an *elliptic curve* is a plane curve over a finite field (rather than the real numbers).

Which consists of the point values satisfying the equation,

$y2 = x3+Ax+B,$

Where a, and b are the constant point values.

In the encryption process of Elliptic curve cryptography, we have many options to use ECC cryptography but we will discuss simplest way.

According to this encryption technique,

- The sender must first encode any message M as a point on the elliptic curve Pm.
- The user must first encode any message M as a point on the elliptic curve Pm.
- Select suitable curve & point G as in D-H.
- Each user chooses private key nA<n and computes public key PA=nAG
- For encryption encrypt: Pm: Cm={kG, Pm+kPb}, where k is a random number
- For decryption decrypt Cm compute: $Pm+kPb–nB(kG) = Pm+k(nBG)–nB(kG) = Pm$

8. IDEA (International Data Encryption Algorithm):

IDEA is one of the strongest secret-key block ciphers that work on 64-bit plain text and cipher text (at one time).For encryption, 64 bit plain text is divided into four 16 bits sub blocks. Each block goes through eight rounds and one output transformation phase.In each of these eight rounds, some (arithmetic and logical) operations are performed. Throughout the eight rounds, the same sequences of operations are repeated. At the beginning of the encryption process, the 64 bit plain text is divided in four equal size blocks and ready for round1 input. The output of round1 is the input of round2. Similarly, the output of round2 is the input of round3, and so on. Finally, the output of round8 is the input for output transformation, whose output is the resultant 64 bit cipher text

9. Diffie–Hellman (DH) Algorithm:

Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. Using this method, two parties that have no previous knowledge of each other can together establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. The algorithm is itself limited to the exchange of keys.

The Diffie-Hellman key exchange algorithm works as follows.

Firstly, A and B agree on two large prime numbers n and g.

These two integers need not be kept secret. A and B can use an insecure channel to agree on them.

- ➢ A chooses another large random number x and calculates c such that c=g x mod n
- ➢ A sends the number c to B
- ➢ B independently chooses another large random integer y and calculate d such that d=g y mod n
- ➢ B sends number d to A
- ➢ A now compute the secrete key K1 as follows: K1= d x mod n
- ➢ B now computes the secret key K2 as follows: K2=c y mod n

Conclusion

Cloud based data is safer than client based servers and papers. Now, medical practices are willing to look to the cloud for the future of healthcare. Adopting cloud computing in the medical field/healthcare can enhance and solve several collective information concerns in healthcare organizations as well as cost optimizations. Personal health records are now considered as the emerging trend in the personal health information exchange field. So, cloud computing storage is highly utilized by the users. Hence, the attribute based encryptions and its variation such as distributed attribute based encryptions are applied for key management and for maximizing security purpose.

References

[1] Global Journal of Health Science; Vol. 9, No. 3; 2017 ISSN 1916-9736 E-ISSN 1916-9744 Published by Canadian Center of Science and Education (2016). “Security Challenges in Healthcare Cloud Computing: A Systematic Review”.

[2] Prashant Kumar Arya et al, International Journal of Computer Science & Communication Networks, Vol 5(1), 17-21. “Comparative Study of Asymmetric Key Cryptographic Algorithms”.

[3] G.Rathi, A. M. (2015). “Healthcare Data Security in Cloud Computing”. International Journal of Innovative Research in Computer, 1807-1815.

[4] “Comparative Study of Asymmetric Key Cryptographic Algorithms”. Rajdeep Bhanot and Rahul Hans, International Journal of Security and Its Applications Vol. 9, No. 4 (2015), pp. 289-306.

[5] “Healthcare Data Security in Cloud Computing”. G. Rathi, Abinaya. M, Deepika. M¸ Kavyasri. T, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 3, March 2015.

[6] “Cloud computing for healthcare organization”. Priyanga.P and MuthuKumar.V.P, International Journal of Multidisciplinary Research and Development, Volume :2, Issue :4, 487-493 April 2015.

[7] “A Survey on Security and Privacy of Healthcare Data”. Ruchika Asija and Rajarathnam Nallusamy, Conference Paper , ResearchGate, July 2014.

[8] “Secure Sharing of Medical Records Using Cryptographic Methods in Cloud”. M.P.Radhini, P.Ananthaprabha, P.Parthasarathi , International Journal of Computer Science and Mobile Computing, Volume 3, Issue 4, April 2014.

[9] “Security and Privacy Issues and Requirements for Healthcare Cloud Computing”. S. Markovski, M. Gusev (Editors): ICT Innovations 2012, Web Proceedings, ISSN 1857-7288, 2012.