Protecting Medical Images by Using Fused Cryptographic Technique with Fog Computing

Lipsa Nayak
Research Scholar, Dept. Of computer Science
Vels Institute of Science, Technology and Advanced Studies (VISTAS)
Chennai, India
Email: info.lipsa@gmail.com

V.Jayalakshmi
School of Computing Sciences
Vels Institute of Science, Technology and Advanced Studies (VISTAS)
Chennai, India
Email:jayasekar1996@yahoo.co.in

2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS) | 978-1-6654-1272-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICICCS51141.2021.9432356

***Abstract*—Medical Service providers are moving towards Cloud Computing as information sharing is a prevalent stage for any medical organization. With the enhancement of innovation, a titanic measure of information is creating with time. Cloud Computing gives a tremendous information stockpiling limit with the adaptability of getting to it without the time and place limitations with virtualized assets. To access information from any topographical area, the medical services industry is moving towards cloud processing. Tremendous expansion in clinical pictures presents a major test for medical services suppliers as they need to oversee, process and share these data with low cost. Medical images show restraint's computerized records, which incorporate touchy data of patients. Apart from all the capable assistance given by cloud processing, security is an essential worry for different associations. To address the security issue, a few cryptographic strategies carried out by analysts around the world. In this paper, an efficient fused Cryptographic technique which is a combination of Elliptic Curve Cryptography and DNA Cryptography with Fog computing facility is discussed.**

Keywords*—Healthcare, Cloud, Security, Medical images, DNA cryptography, Elliptic Curve Cryptography, Fog computing

I. INTRODUCTION

Development of healthcare industry is rising immensely by adopting advanced IT services. To revolutionize healthcare organizations, there is a vast replacement of traditional technology with advanced technology [1]. To modernize healthcare institutions, smart devices, innovative machines, sensors, IoT devices, Electronic medical record are in vast use. All these transformations in healthcare industries generates a huge quantity of data. These data are very useful for healthcare industry. By storing and analyzing these data healthcare industry can provide cost effective service, better health tracking of patients, prevent human errors, prevent some critical disease. Use of advanced imaging techniques such as magnetic resonance imaging (MRI),3D imaging, tactile imaging, thermography, nuclear medicine functional imaging, positron emission tomography (PET), single-photon emission computed tomography (SPECT) etc. are very useful to provide healthcare services. By storing and analyzing these data healthcare industry can provide cost effective service, better health tracking of patients, prevent human errors, prevent some critical disease. Growing size of these data make normal data to bigdata. Bigdata pierce almost all organization today. Huge set of multiple types of data refers to Bigdata. These huge data is a combination of structured, semi structure and unstructured data from various organizations. Medical images are usually unstructured data which is difficult to store and manage in traditional database. Earlier hard copies of these images were circulated for treatment, which are expensive and clumsy. After that compact disc (CD) were introduced to store data, which is insufficient to store these huge data consequently and difficult to maintain. Subsequently cloud computing enter to healthcare domain for its innumerable benefits like portability and flexible storage capacity of medical data. Cloud computing is valuable for healthcare organizations in many ways. Collecting patient's data is a hectic task for medical service providers as well as patients [2]. To move these data to cloud will be very beneficial for both of them. For Healthcare professionals it is simpler to follow a patient's health records and to take suitable decisions remotely from anywhere and any place using cloud computing [3]. With the interaction of cloud computing data sharing between doctors or healthcare experts has become significantly simpler and less difficult. Apart from all the fabulous benefits provided by cloud computing, it has few serious security challenges [4]. In this paper we used a multilayer security technique to protect medical images in healthcare cloud. A fusion of DNA cryptography and Elliptic curve cryptography is used with the help of fog computing [5]. DNA cryptography and Elliptic Curve Cryptography each on is a prevailing cryptography itself and by merging both these techniques we can protect medical images luminously. ECC is a public key cryptography, it is efficient like other public key cryptography but with a very small key size.

II. PRELIMINARIES

A. *Cloud computing*

Cloud computing allow to store and access data over internet. Cloud computing alludes the on-demand accessibility of data needed by client without time and place restriction. For its staggering features like coordinated effort, reachability, effectiveness, and security most of today's organizations are moving towards cloud computing. Medical institutions are always front liner when it comes to use any advanced technology. To manage, store and implement healthcare Bigdata, healthcare organizations also adopting cloud computing immensely. In healthcare industry, cloud computing provides benefits to both patients and healthcare provider. Organization that facilitates these cloud services are called cloud service providers. Cloud service providers are taking care of infrastructure. All resources are brought and maintain by cloud service providers. Healthcare organizations only have to access in pay-per-use service. Four cloud deployment models are there through which we can take cloud services.

1) Public Cloud: In this model the entire IT infrastructure is located in cloud service provider's location. Everything needed to provide service is owned by cloud service providers. Any individuals or organizations can store and manage their data over internet without investing in costly setup. Amazon, Google, Microsoft are some public cloud service providers.

2) Private cloud: Users, who choose private cloud gets a dedicated cloud which cannot be shared with anybody else. Cost and management also owned by that particular organization. Level of security is high in case of private cloud.

3) Hybrid cloud: Hybrid cloud provide service of both public and private cloud. Organizations those need dedicated cloud infrastructure with more scalability, demand for Hybrid cloud. Sensitive information of the organizations is kept in a private cloud.

4) Community cloud: This Cloud framework is worked in the wake of understanding the processing needs of a local area as there are numerous elements including compliances and security strategies which should be remembered for the local area Cloud foundation.

Cloud computing has three service model based on which it provides service to the customers.

1) Software as a Service (SAAS): furnishes customers with admittance to fundamental working programming also, discretionary administrations to create and utilize programming applications without programming establishment

2) Infrastructure as a Service (IAAS): It permits the client to use the infrastructure without referencing the hardware.

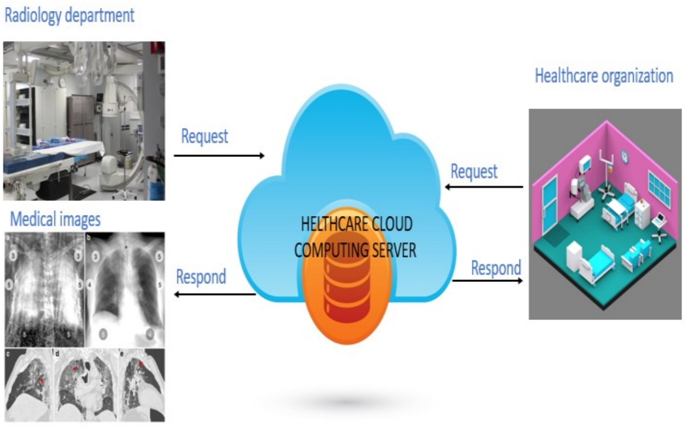
3) Platform as a Service (PAAS): This service permits customers to access some basic software and to develop and run software without installing it.

B. *Maintaining Cloud Computing for Healthcare Big Data*

By the help of cloud computing huge amount of healthcare data can be store in a nominal cost. Cloud computing provides service in pay- as-you -go method, so that healthcare institutions have to pay only for those facilities which they are benefiting. To store and keeping up huge volumes of data normally needs more staff to provide support, program design and IT equipment, which demands more expenditure. Presently, with cloud computing healthcare organizations can, reducing down additional expenses. Sometimes, for various reasons, loss of data is a most appalling part for any organization today. Without accurate data it is completely impossible for any healthcare organization to provide service to patients. Here, the Cloud gives flexibility of backup and restoration alternatives, limiting the possibilities harm due to loss of data. It is a very important factor for any institutions that how fast data can be updated. Cloud computing provides tools that can refresh data in a praiseworthy speed and health care systemcan get constant updates on all the important data. Cloud service providers stretches a large IT infrastructure and owes all service and maintenance of hardware. So, by adopting cloud computing medical institutions can be relaxed of any maintenance cost and time.

C. *Fog computing with Decoy images*

Fog computing is a rising that offers benefits to stockpile, process and communicate data nearer to the client. It is geographically disseminated and to which various diverse devices are pervasively associated towards the end of the institution. Produce information and putting them on the edge of an organization to be closer to the client are considered among the primary undertakings of fog computing. It is an elongate form of cloud computing [6]. Fog computing is an alternate methodology for getting information in the cloud applying hostile decoy technology. We screen information access in the cloud and identify unusual information access designs. We use fog computing in this paper to create and maintain decoy files so that it can give an appearance of real cloud of medical image. Generally, Decoy means a creature, which is kept by the hunters to attract other animals. Here same technique is used to misguide attackers those want to hamper or steal medical data. This fog of decoy files will be used as a trap for attacker. It will work as a honeypot to attract attacker and make them believe that they are accessing the actual image gallery of the medical institution. Whereas the real image gallery is stored safely in the cloud. By using this technique, we can be able to stop retrieving of the real cloud by the attacker. We can reduce the attempt of breaking the security of real cloud of images by using fog computing. Here fog computing is used to create these decoy file which resembles the replica of real image but contain some fake information in actual.



D. *DNA computing for for medical Image Encryption*

DNA Cryptography is an application of DNA Computing which was invented by Richard Adleman in 1994[fig 1].

Figure 1: DNA structure

The DNA cryptography is a new and advanced cryptographic technique for DNA sequences are used for medical image encryption. For its intricate double helix structure, it is difficult to break the security [7]. A (adenine), C (cytosine), G(guanine), and T(thymine), are nucleic acid bases. A and T complements each other, and C and G complements each other. We can represent these nucleic acids in binary numbers. We can take number 01 for A, 10 for T, 00 for G and 11 for C as shown in Table 1. Each pixel value of medical image can be expressed as binary streams. For example, if first pixel value of a medical image is 85, we can get a binary stream 1010101[8]. Again, by applying above rule we can convert binary stream to DNA sequence.

Table .1 Conversion table of DNA to Binary Sequence

E. *Elliptic curve cryptography*

Elliptic Curve Cryptography is one of the leading Public key cryptographies [fig 2][9]. With lesser key size Elliptic Curve Cryptography provides excellent security[10]. Elliptic Curve Cryptography or ECC was developed by Victor Miller and Neal Koblitz in year 1985[11]. Equation of Elliptic Curve Cryptography is in the form of

$$y^2 = x^3 + cx + d$$

where c and d are the constant with

$$4c^3 + 27d^2 \neq 0$$

We can get private key by multiplying G with the private key.

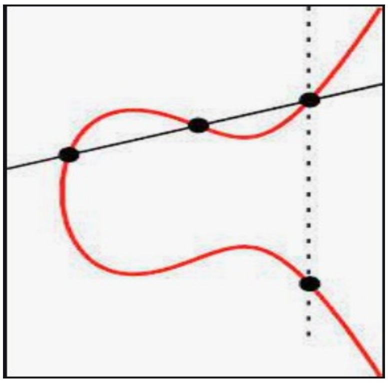


Figure 2 : Elliptic Curve

III. PROPOSED ALGORITHM FOR DNA ENCODING BASED ELLIPTIC CURVE CRYPTOGRAPHY WITH FOG COMPUTING FACILITY

To obtain a very protective security which cannot be broken easily, we fused DNA Cryptography and Elliptic Curve Cryptography. In the first phase of this technique, we store medical images in a fog of decoy images [13]. This step is taken in this paper to confuse attacker. Attacker might think this fog as real image gallery and access it. By using his technique, we can reduce attackers [14][15]. Whereas real images are securely stored with the protection of DNA Cryptography and Elliptic Curve cryptography.

DNA sequence	A	C	G	T
Binary sequence	01	11	00	10

```
Algorithm. Medical image encryption
Input: Input medical image as P (Q1, R1)
Output: Encrypted medical image as M(Q1,R1)
Step 1: Start
Step 2: The input digital medical image is represented as P (Q1,R1), where Q1 is the row size and R1 is the column size. Based on the input medical image's pixel value it is divided into odd pixel numbers and even pixel numbers.
Step 3: These Odd, Even Pixel values are converted into binary numbers.
Step4: Binary numbers can be converted into DNA Sequences.
Step 5: These numbers are converted into decimal points and represented in a elliptic Curve.
Step 6: Stop
```

IV. CONCLUSION

Medical services associations are getting gigantic advantages by moving their images to the cloud. It is an essential and truly going test to get medical care huge information in this circulated climate. In this paper, our examination depends on a complex staggered security procedure by utilizing DNA encoding and Elliptic bend cryptography [16][17]. Both these strategies give undeniable level security itself. To give complex insurance to the assailant, we consolidated a few highlights of DNA cryptography with Elliptic bend cryptography. This fused cryptography offers better security in less time, memory, and more modest key size than customary security methods.

REFERENCES

[1] Opportunities and Challenges of Cloud Computing to Improve Health Care Services; Alex Mu-Hsing Kuo; J Med Internet Res. 2011 Jul-Sep; 13(3): e67. J Med Internet Res. 2011 Jul-Sep; 13(3): e67.

[2] Kharat AT, Safvi A, Thind S, Singh A. Cloud Computing for radiologists. Indian J Radiol Imaging. 2012;22(3):150–4.

[3] Li, M, Yu, S, Ren, K, Lou, W. Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multiowner Settings. In: International Conference on Security and Privacy in Communication Systems, Singapore, Singapore, 2010, pp. 89–106.

[4] Liu, X, Deng, RH, Choo, KR, Yang, Y. Privacy-Preserving Outsourced Clinical Decision Support System in the Cloud. DOI 10.1109/TSC.2017.2773604, IEEE Transactions on Services Computing.

[5] Hongjun Liua, Xingyuan Wang, Abdurahman kadir," Image encryption using DNA complementary rule and chaotic maps," Applied Soft Computing 12 (2012), pp. 1457–1466.

[6] B. M. Bowen and S. Hershkop, "Decoy Document Distributor: htt p ://sneaker s .cs.columbia.ed u /ids/fog/," 2009. [Online]. Available: http : / /sneaker s .cs.columbia.ed u /ids/FOG/

[7] Wang, Qian, Qiang Zhang, and Changjun Zhou," A multilevel image encryption algorithm based on chaos and DNA coding ," Fourth International Conference on Bio-Inspired Computing, 2009.

[8] Ganesh Chandra Deka et.al., "Advances of DNA computing in cryptography," Taylor & Francis, 2018.

[9] N. Koblitz, "Elliptic Curve Cryptosystems," Math. Comput., vol. 48, 1987, pp. 203–209.

[10] Victor S. Miller, Use of Elliptic Curves in Cryptography, Advances in Cryptology. Springer, vol. 218, pp. 417–426, (2000).

[11] S. Sutikno, A. Surya, and R. Effendi, "An Implementation of El Gamal Elliptic Curves Cryptosystems," Proc. IEEE Asia-Pacific Conf. Circuits Syst., Chiangmai, Thailand, vol. 24–27, 1998, pp. 483–486.

[12] M. Van Dijk and A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing," in Proceedings of the 5th USENIX conference on Hot topics in security, ser. HotSec'10.

[13] Manreet Kaur and Monika Bharti, "Fog computing providing data security: a review," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 6, pp. 832–834, 2014.

[14] Liu, X, Deng, RH, Choo, KR, Yang, Y. Privacy-Preserving Outsourced Clinical Decision Support System in the Cloud. DOI 10.1109/TSC.2017.2773604, IEEE Transactions on Services Computing.

[15] Kester, Q, Nana, L, Pascu, A, Gire, S, Eghan, J, Quaynor, N. A Security Technique for Authentication and Security of Medical Images in Health Information Systems. In: 2015 15th International Conference on Computational Science and Its Applications, Banff, AB, Canada, 2015, pp. 8–13.

[16] Zhang Q, Guo L, Wei X (2010) Image encryption using DNA addition combining with chaotic maps. J Math Comput Model 52:2018–2035

[17] Xue XL, Zhang Q (2010) An image fusion encryption algorithm based on DNA sequence and multi-chaotic maps. J Comput Theory Nanosci 7:397–403