Middle-East Journal of Scientific Research 23 (10): 2552-2558, 2015
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2015.23.10.22764

Secured Medical Information Transmission Using Chaos Through Cloud Computing

I. Bremnavas

Department of Computer Engineering and Networks,
College of Computer Science and Information Systems, Jazan University, Jazan, Saudi Arabia

Abstract: The next generation platform cloud provides virtualization, dynamic resource pools and high availability. The user enables the cloud storage remotely to store their data and enjoy the on-demand service and such a service also leaving users' physical control of their outsourced data. This problem can be addressed by achieving a secure and dependable cloud storage service. The proposed system uses the secured medical information transmission using chaotic technique through the cloud computing system.

Key words: Cloud storage · Chaos · Cloud computing · Chaotic random key generation

INTRODUCTION

Cloud computing is the new era of internet based computing system, which provides to user working with the cloud applications in simple and customizable. It offers to store and access the cloud data from anywhere by connecting the cloud application using internet [1]. Users are able to store their local data in the remote server using the cloud service [2]. In this service oriented computing environment, the cloud computing have progressed as a most popular paradigm which resolves the infrastructures are delivered as a service. Most commonly used cloud service is data storage among other services, where end users can outsource any data to cloud servers, to enjoy and access the hardware/software resources virtually without investment. A set of cloud computing services such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) can be accessed by the cloud computing model. In SaaS services are provided through the service providers and customers to run applications on a cloud infrastructure. It can be accessed through web browsers. In PaaS services are a mode to rent hardware, operating system, storage and capacity of network over the internet. In IaaS services the consumer is provided with storage management and network, power to control process and other fundamental computing resources which are helpful to manage arbitrary software. The popular cloud service providers such as Microsoft SkyDrive, Amazon, Dropbox, Apple iCloud and Google Drive are all services initiated few years back. The cloud computing models and characteristics are shown in Figure 1.

The rapid development of cloud computing is increasing severe security concern. Lack of security is the problem in widespread adoption of cloud computing [3]. It bounded various security issues such as securing the data, virtualization and examining the utilization by the cloud computing dealers. Various security and privacy concern are in the unique cloud environment [4].

Shared and Extensible Responsibility: Shared and extensible responsibility is compromised between customers in different delivery models.

Outsourcing: Cloud providers should have appropriate mechanisms to prevent the control of users data lose.

Heterogeneity: Security and privacy mechanism has satisfied different cloud providers which may access the different approaches, thus generating integration challenges.

Multi-Tenancy: Policies, protection, data access and deployment of application must be the considered as major issues of a secure multi-tenant environment.

Corresponding Author: I. Bremnavas, Department of Computer Engineering and Networks, College of Computer Science and Information Systems, Jazan University, Jazan, Saudi Arabia.

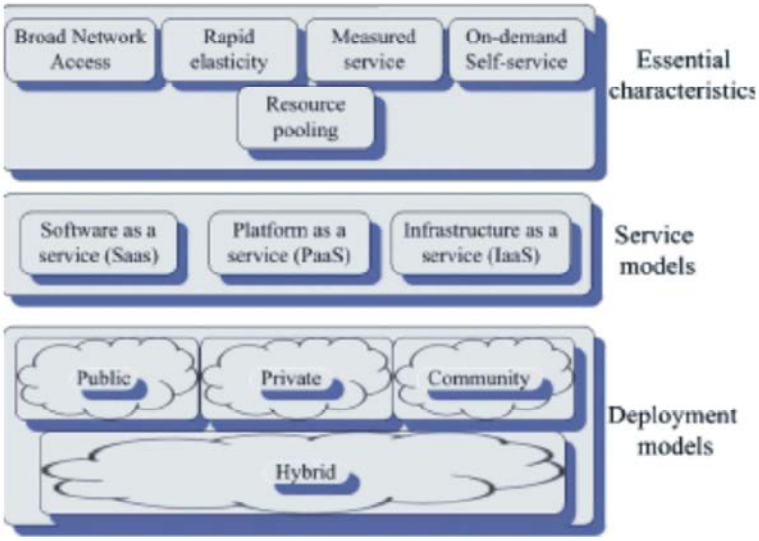


Fig. 1: Cloud computing – NIST (National Institute of Standard and Technology) Definition

The tremendous technical advantage of the cloud, security and privacy concern has been major problem preventing its adoption. Cloud users store the sensitive and privacy information in cloud instances. From security and privacy concerns, cloud providers need to ensure the confidentiality of the service. Any cloud service, user is supposed to know the risk associated with the data security, e.g., user data loss and data theft. Authentication, data encryption, integrity, recovery and user protection are all the important components to cover the data security model in cloud. To avoid unauthorised person access of the data, applying encryption mechanism on data, that data is totally unusable. Encryption is always a powerful scheme whenever storing the sensitive and privacy information. To confirm the basic security model components like *confidentiality*, *integrity* and *availability* (CIA), the cloud storage provider need to include a security scheme to ensure that the shared storage environment safeguards for the data [5]. This survey have been discussed some security issues in cloud computing. E.M. Mohamed *et al.* [6] discussed the data security model of cloud computing and also implemented data security model for cloud computing.

M. Balduzzi *et al* and C. Rong *et al*. [7, 8] presented the security issues review of the cloud computing. Akhil Behl [9] has discussed the exiting security approaches and security issues related to the cloud environment. E.Mathisen [10] presented few key security issues of cloud computing. Sabahi [11] focussed the security issues, reliability and availability for cloud computing and also given some solutions for security issues.

Cloud Based Medical Information System: Businesses, organizations, medical information system and the consumers are adopting cloud technologies. Nowadays, the serious problem in e-health care environment is medical information security. The security tool can protect medical information from attackers. L.M. Vaquero *et al*. focused only on e-health security and privacy protection in the cloud [12]. Cryptographic algorithm like Rivest Shamir Adleman (RSA) and Data Encryption Standard (DES) were used for medical information security. But it is not effective for medical information security because of the high data capacity and correlation among pixels. Chaos have been explored in last two decades for medical information security, it has some suitable intrinsic features of medical image processing. Chaos can be well applied in cryptography [13, 14]. Because it has many characteristics which can be connected with the confusion and diffusion property in cryptography, such as sensitive dependence on initial conditions and parameters, broadband power spectrum, randomness in the time domain and ergodicity etc.

Cloud based medical information system is becoming more predominant in medicine. Still, in e-health care environment some medical information systems have concerns about transferring their data storage, computing capacity to the cloud providers. Collaboration among the hospitals and medical society is required for sharing patient medical data and images. Patient medical data stored in virtual environment are easily accessible by different healthcare providers, thus the advantage of process is facilitating sharing of data and considerably reducing local storage requirements.

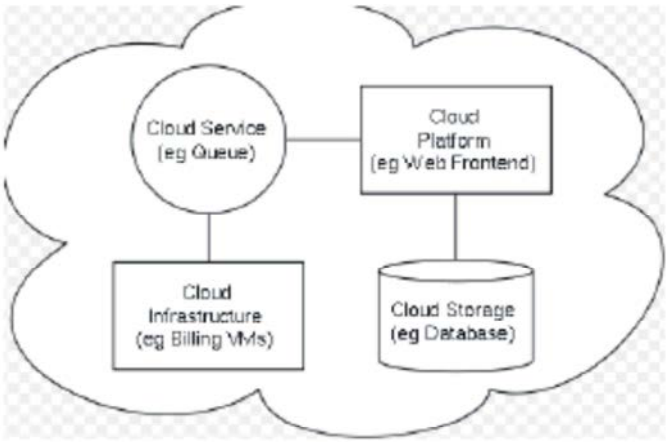


Fig. 2: Cloud computing general architecture

Ultimately what system allows physicians to build networks for storing the high volume of patient medical information and open platform for sharing and accessing of patient medical information.

The proposed system uses the secured patient medical information transmission using chaotic map over to cloud computing system. The first process is to provide the security for patient medical data using chaos and sharing and exchanging with the available "Cloud". The patient medical information will be available in the cloud, which can provide the required details to the doctors and the patient can seek the treatment in other branch hospital, reduce the computational resource maintenance in the hospital. The cloud computing general architecture is shown in Figure 2.

Secured Medical Information Transmission Using Chaotic Map in Cloud: From security perspective, for secure communication the encryption is a better mechanism. Better to secure the data before storing in a cloud server. User can give the permission to their members such that data can be easily accessed by them. In a public cloud, users are sharing medical information with other medical hospitals. In a shared pool outside the hospitals, users don't have any knowledge or control of where the resources are located. Because users share the medical environment in the cloud, may put your data at risk of seizure. Data integrity is assurance that the data is consistent and correct. Ensuring the integrity of the data really means that it changes only in response to authorized transactions.

The dynamic nonlinear system is chaos, has brought out the consideration of these facts such as low-dimensional dynamical systems are capable of handling complex and unpredictable behaviour. Chaos seems to be a good technique for encryption algorithm, characterized by sensitive dependence on initial conditions and similarity to random behaviour.

Here, we consider one dimensional chaotic logistic map. It is a simple model which yields chaos, can be written as:

$x_{n+1} = a\, x_n\, (1-x_n)$ (n=0, 1, 2…∞) where 0<=a<=4

This is a discrete time map which receives a real number between 0 and 1 and returns a real number in [0, 1]. " n" denotes a discrete time step and "x_n" denotes a data at "n". Time series x_n (n=0, 1, 2…) is deterministic. Using the above simulator, we can get these sequences x_0, x_1, x_2... dramatically and "a" is the control parameters governing the chaotic behavior.

In the above logistic difference equation initial key a = 0.3 as the user perception. The difference equation is evaluated to generate a sequence of random numbers which are sorted and their index value is used. This value 0.3 acts as an encryption key 'K' for the encryption process. The image pixel in the one dimensional array format is being encrypted with the pseudo random numbers generated by the logistic map as the key in the chaotic region i.e., a value 0 and 4. It has been applied to security and increases the hiding capacity of the embedding positions. This proposed algorithm has been put forward for Least Significant Bit (LSB) based image steganography in which the last bits of the cover image are replaced by the bits of the message image which is encrypted using index based logistic chaotic map. Now the image is encrypted in the chaotic region and it is ready to send across the transmission channels with more number of attackers. Figure 3 is the proposed flow diagram of secured medical image transmission using chaos in distributed cloud environment. Figure 4 is the flow diagram of proposed embedding algorithm.

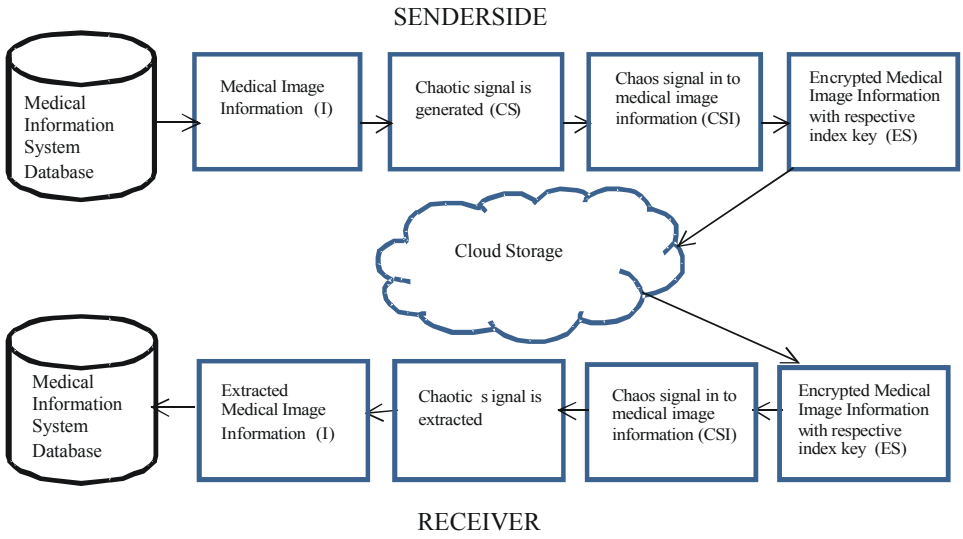


Fig. 3: Secured medical image transmission using chaos in distributed cloud environment

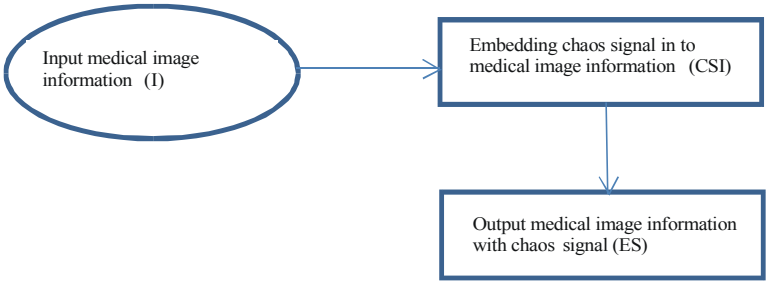


Fig. 4: Embedding Process

The medical information system has a patient medical database, where "n" number of patient medical information in the database. It extracts the features from medical information and generates a key. To protect what the sensitive patient medical information are encrypted before outsourcing to the cloud server. During the encryption process, the unique index key value is assigned for each patient medical data. Then, the encrypted query is submitted to the cloud server. Finally, the authorized user decrypts the received medical information. Working example of sender side encryption process is shown in Figure 5.

Proposed Embedding Algorithm:

I/P and O/P: Medical image information, I: Encrypted Signal, ES

Step 1: Load an medical image information from the database and store an image in one-dimensional array named as I.

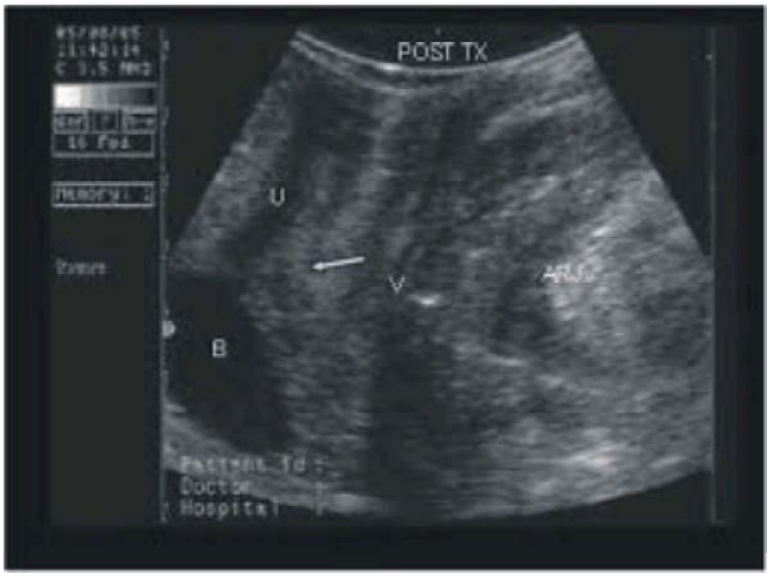
Step 2: Generate the chaotic signal S using logistic equation.

$$x_{n+1} = ax_n (1- x_n)$$

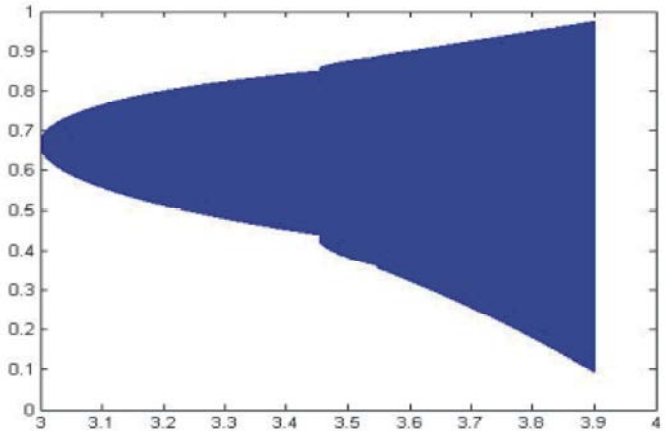
Step 3: The medical image information I is embedded within the chaotic signal S using the following steps

- Fix the covered boundary region based on the size of an medical image information I.
- The signal is assumed to be generated from the starting position of the boundary region.
- Set a key value K dynamically as user perception within the boundary region for representing the initial position.
- The medical image information value I is embedded with chaotic signal S from K.
- The sort actual indexes of the sorted key values should be stored.

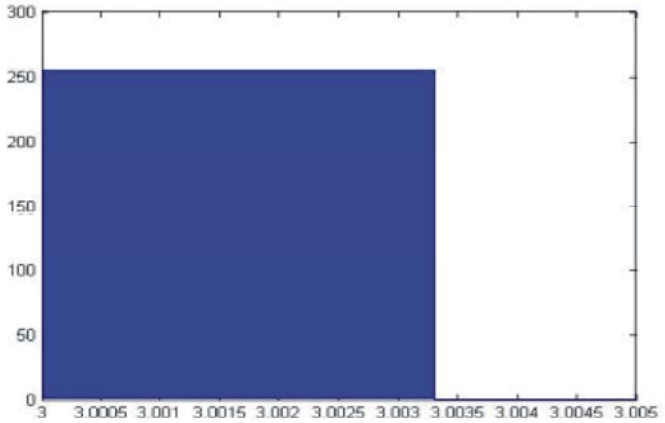
Step 4: The Encrypted signal (ES) is transferred along with the key value K. (The key value is embedded in a standardized position of the signal ES).



Medical Image Information (I)



Generate the signal based on the logistic equations (CSI)



Medical Information and chaos signal with the cover region (ES)

Fig. 5: Working example of sender side encryption process

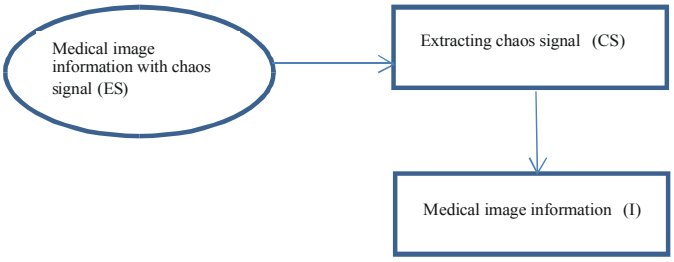
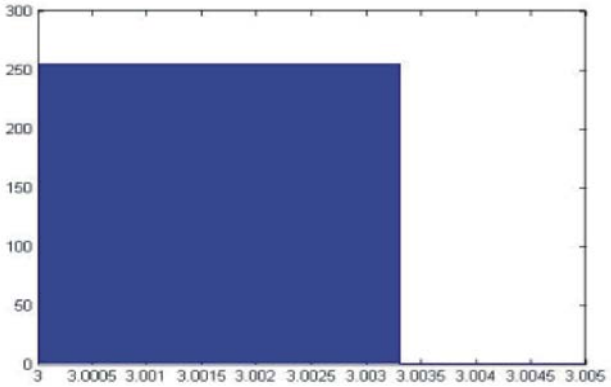
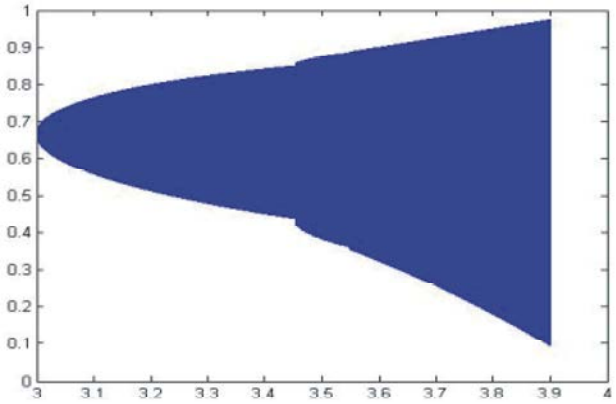


Fig. 6: Extraction Process



Medical Information and chaos signal with the cover region (ES)



Extracting the Chaotic signal (CS)

Medical Image Information (I)

Fig. 7: Working example of receiver side decryption process

Figure 6 is the flow diagram of proposed extraction process. The encrypted image is received by the trusted receiver. The indexing key value and the key is also embedded in the same cover region with secret coding. The receiver generates the random numbers using same logistic equation. The encrypted logistic map is subtracted from the raw logistic map thereby the image is being retrieved from the encrypted source of information. Working example of receiver side decryption process is in Figure 7.

Proposed Extraction Algorithm:

I/P : Encrypted signal, ES
O/P : Medical image information, I

Step 1: Receive the encrypted signal, ES from the open communication channel.
Step 2: Retrieve the actual indexes of the stored key value K from encrypted signal ES.
Step 3: Generate the chaotic signal S using logistic equation.

$x_{n+1} = ax_n (1- x_n)$

Step 4: Subtract the received encrypted signal, ES with the raw logistic signal, S using the key value K, to obtain a one-dimensional array for medical image information, I
Step 5: The resultant medical image information, I from the one-dimensional array.

CONCLUSION

In this work, we proposed a secured medical information transmission using chaotic map through cloud computing system. The proposed method considers the techniques from chaos security and image processing domains to perform secure medial information outsourcing problem.

REFERENCES

1. Vaquero, L.M., L. Rodero-Merino, J. Caceres and M. Lindner, 2008. 'A break in the clouds: towards a cloud definition', in: ACM SIGCOMM Computer Communication Review, pp: 50-55.
2. Mollah, M.B., K.R. Islam and S.S. Islam, 2012. 'Next generation of computing through cloud computing technology', in: 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE), pp: 1-6.
3. Fernandes, D.AB., L.FB. Soares, J.V. Gomes, M.M. Freire and P.R.M. Inacio, 2014. 'Security issues in cloud environments: a survey', Int. J. Inform. Sec., 13(2): 113-170.
4. Takabi, H., J. Joshi and G.J. Ahn, 2010. 'Secure cloud: Towards a comprehensive security framework for cloud computing environments', In: Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual, pp: 393-398.
5. Xiao, Z. and Y. Xiao, 2013. 'Security and privacy in cloud computing', IEEE Commun. Surveys Tutorials, 15(2): 843-859.
6. Mohamed, E.M., Hatem S. Abdelkader, Sherif E.I. Etriby, 2012. 'Enhanced Data Security Model for Cloud Computing', in: 8th International Conference on Informatics and Systems (INFOS), Cairo, pp: 12-17.
7. Balduzzi, M., J. Zaddach, D. Balzarotti, E. Kirda and S. Loureiro, 2012. 'A Security analysis of amazon's elastic compute cloud service', in: Proceedings of the 27th Annual ACM Symposiumon Applied Computings, pp: 1427-1434.
8. Rong, C., S.T. Nguyen and M.G. Jaatun, 2013. 'Beyond lightning: a survey on security challenges in cloud computing', Comput. Electr. Engg., 39(1): 47-54.
9. Akhil Bhel, 2011. 'Emerging Security Challenges in Cloud Computing. Information and Communication Technologies', in: World Congress on, Mumbai, pp: 217-222.
10. Eystein Mathisen, 2011. 'Security Challenges and Solutions in Cloud Computing', in: *International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011)*, pp: 208-212.
11. Farzad Sabahi, 2011. 'Cloud Computing Security Threats and Responses', in: IEEE 3rd International Conference on Communication software and Networks (ICCSN), pp: 245-249.
12. Abbas, A. and S.U. Khan, 2014. A 'Review on the state-of-the-art privacy preserving approaches in e-healthclouds', IEEE J. Biomed. Health Inform.
13. Maniccam, S.S. and N.G. Bourbkis, 2003. Pattern Recognition, 37: 725-737.
14. Kocarev, L., 2001. IEEE Circuits and System Magazine, 3: 6-21.