isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6, Issue: 3,Special Issue: 2 ,Apr,2023 ,ISSN_NO: 2321-3337

A SECURED HEALTH RECORDS WITH ANONYNMOUS ACCESS DETECTION WITH CLOUD TRANSFER USING BLOCK CHAIN

Balaji.M[1], Kamal.R[2], Kartheesan.B.S[3], Vijay.B[4], Kamal.N[5]

UG Scholar[1,2,3,4] –Department of Computer Science, GRT Institute of Engineering and Technology, Tiruttani, India.

Professor[5] & Head- Department of Computer Science, GRT Institute of Engineering and Technology, Tiruttani, India

bm.becse@gmail.com, kamal25022002r@gmail.com, kartheesansurendran5@gmail.com, vijaybarathan2000@gmail.com, kamal.n@grt.edu.in

Abstract - In the existing system, hospital; details are maintained as a hardcopy like report. In most of hospital records are maintained as a hard copy due to huge volume and complexity, it is difficult to manage those data sets using traditional software and hardware. in this paper we propose an efficient storage system for patient information. Through this system we providing a security system for patient and hospital details. To secure the record we are implementing an efficient system by crypto stegano system. Patient details are stored in cloud for memory management and it will easy way access the data. We are providing permission key to access the patient details. No one can access the information without the knowledge of doctor. So, through this a security level is increased by storing data using crypto steganography.

Keywords: Private key, public key, steganography and encrypting the data storage

1. INTRODUCTION

The development of computer and communication technology, EHR has become an indispensable tool for medical services [1]. The system utilizes some electronic devices such as the computer to deal with digital medical records, and it has the advantages of easy to use, stronger timeliness, and low cost. EHR not only provides the most useful data for diagnosis and scientific research but also it gives one kind of judgment basis for handling medical disputes. So, it has attracted a wide range of attention including the government, the medical community, cybersecurity department, and so on [2], [3]. Because the medical data is crucial for the diagnosis, and it is personal and sensitive for patients. Thus, data sharing and privacy preservation issues are critical in EHR. The medical data should be stored, managed, and accessed securely. Notably, the doctor usually needs to know the medical history of the patient when he/she makes the diagnosis or treatment. However, the patient cannot professionally describe his/her medical history, which will affect the latest treatment. Thus, in EHR, historical medical data generated by different doctors in different hospitals should be capable of being securely and timely queried by a legitimate doctor with the patient's consent, please see [4]– [7] for more details. In recent years, the EHR system is markedly developed with the rise of cloud computing. For example, in [8], authors first expounded the security requirements of the EHR system based on cloud computing. Also, some suggestions are suggested to ensure the security of medical data in the cloud. In [9], the attribute-based encryption is utilized to protect the data in the cloud, and then the proposed EHR system is implemented in an android phone. In [10], Xhafa et al. proposed an attribute-based EHR with privacy awareness in cloud computing. However, as mentioned in [11], [12], these cloud-based schemes have some flaws. For example, they have a dependency on the cloud provider. If some targeted attacks to cloud provider are carried out, then the information leakage is likely to occur. Additionally, the server may suddenly stop if the cloud providers would go bankrupt or be swallowed up by the larger companies. That is, the security of EHR will be threatened. In 2008, the blockchain structure was proposed [13]. It can be viewed as a distributed database and satisfies the features of decentralization, tamper resistance, and asymmetric encryption. This technology can provide a reliable way to manage and store data. So, it may be a promising solution for EHR. At present, the blockchain based researches for EHR have already started attracting attention from medicine.

2. SECURITY POLICY

Access control is concerned with permitting only authorised users (subjects) to access services and resources (targets). It limits the activity of legitimate users who have been successfully authenticated. Authorisation or access control policy defines the high-level rules specifying the conditions under which subjects are permitted to access targets [14]. However, in many systems there is no real policy specification, only the implementation in terms of low-level

mechanisms such as access control lists. The study of access control has identified a number of useful access control models, which provide a formal representation of security policies and allow the proof of properties about an access control system.

2.1 Block chain is an undeniably ingenious invention – the brainchild of a person or group of people known by the pseudonym, Satoshi Nakamoto. But since then, it has evolved into something greater, and the main question every single person is asking is: What is Block chain? By allowing digital information to be distributed but not copied, block chain technology created the backbone of a new type of internet. Originally devised for the digital currency, Bitcoin, (Buy Bitcoin) the tech community is now finding other potential uses for the technology.

2.2. **Cryptography** is the process of hiding or coding information so that only the person a message was intended for can read it. The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and ecommerce**.**

2.3 **Steganography** is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

3. PROPOSED SYSTEM

We propose an efficient storage system for patient information. Through this system we providing a security system for patient and hospital details. To secure the record we are implementing an efficient system by crypto stegano/ Watermarking system. Patient details are stored in cloud for memory management and it will easy way access the data. We are providing permission key to access the patient details. No one can access the information without the knowledge of doctor. So, through this a security level is increased by storing data uploading crypto steganography / Watermarking.

4.MODULE

4.1 CASE DEFINE ADMIN MODULE

In general, case can be defined as a course or principle of action adopted or proposed by an organization or individual.

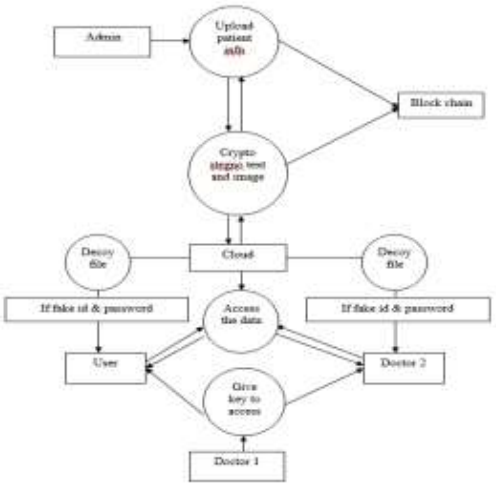

Fig. 4.1 Case Define Admin Module

4.2. LOGIN MODULE

Authentication is the process of determining whether someone or something is. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentication.

Fig. 4.2. Login Module

4.3 USER REGISTRATION:

In this module user/ patient have to register their personal information like name, address, mail ID, mobile number, address. And those details will be stored on database. After registration user will get user ID and password to access the application. This is ana application to view their hospital report from cloud. to access the hospital records we are creating user Id and password for authentication.

4.4 HOSPITAL SERVER:

Server is the main process for every application because it is the only way for communication it will establish the communication between client and corresponding website. In this module we are implementing hospital server to maintain both patient information, doctor information and other hospital details. All doctors have to register their designation and other details same like that other hospital have to register their details on this server. Because patient may change their treatment from one hospital to another that

is why hospital will also register their information. server will maintain all the details and provide details whenever user request for the query.

4.5 STEGNO ANALYSIS:

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. We are hiding the patient's personal information and their report about disease. Every data will be stored as a stegano format. when we stored the record as a stegano it will not hack or theft by anyone.

4.6 IMAGE CRYPTOGRAPHY:

In our system we are storing the patient scanning report like their x-ray, ECG and other images in encrypted form using ECC algorithm. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. Using ECC algorithm we are encrypting the image file and store it in cloud server.

4.7 FOG COMPUTING:

Fog computing is a term created by Cisco that refers to extending cloud computing to the edge of an enterprise's network. Also known as Edge Computing or fogging, fog computing facilitates the operation of compute, storage and networking services between end devices and cloud computing data centers. It is a separate to maintain the decoy information. Here we are decoy the patient information in secure way. Decoy is the process of creating a fake report of patient. For security we are creating this type of record.

4.8 DATA ACCESS:

In this module we are implementing accessing process for user as well as hospital. In this initially a patient detail will be maintained by a doctor who is the person patient met at first time. He had only the permission to access the patient information. If it any case patient change the hospital or he/she want to view his/her details they need some key to access the data which is stored in cloud. if the patient their hospital a new doctor has to give key to access the patient details. For both people they need one key to access the file. That key will be provided by a doctor from hospital 1. Bothe patient and doctor have user id and password to access the file. System will check their ID and password if it matches with previous data base, they will get key from doctor and view the details. if it will not match with previous database server will provide decoy file and alert will be send to the patient.

4.9 BLOCK CHAIN IMPLEMENTATION:

A block is a container data structure. The average size of a block seems to be 1MB (source). Here every certificate number will be created as a block. For every block a hash code will generate for security. Patient records are created as a block chain.

5. N-Tier Architecture

Figure 5.1 N-Tier Architecture

6. EXPERIMENTAL RESULTS

This result discusses about the implementation of the policy-based security for various cases are identified and the below Fig. 5.1., Fig. 5.2. and Fig. 5.3 Shows the implementation of admin policy based on the proposed methodology.

Fig.6.1. Shows the Admin Policy

Fig.6.2. Shows Patient Registration

Fig.6.3. Shows Patient Info

Feature	MyISAM	Memory	InnoDB	Archive	NDB
Storage limits	256TB	RAM	64TB	None	384EB
Transactions	No	No	Yes	No	Yes
Locking granularity	Table	Table	Row	Row	Row

FIG.6.4.

7. CONCLUSION & FUTURE WORK

In this paper we infer that crypto stegano technique will be more secure for Patient information. For that ECC algorithm is used. They can view their information anywhere but by providing to access the data. So, security level increased by comparing with existing work.

Future enhancement:

The future work of this paper is we can secure the content in two different cloud server and also, we can divert the cloud server while third party try to accessing our patient's information. Try to implement this system in mobile application for user feasible.

REFERENCES:

[1] M. Chen, J. Yang, Y. Hao, S. Mao, K. Hwang," A 5G Cognitive System for Healthcare", Big Data and Cognitive Computing, Vol. 1, No. 1, DOI:10.3390/ bdcc1010002, 2017.

[2] Frost & Sullivan: Drowning in Big Data? Reducing Information Technology Complexities and Costs for Healthcare Organizations. http://www.emc.com/collateral/analyst-reports/ frost-sullivan-reducing-information technology-complexities-ar.pdf

[3] M. Chen, S. Mao, Y. Liu," Big Data: A Survey", Mobile Networks and Applications, Vol. 19, No. 2, pp. 171-209, April 2014.

[4] M. S. Hossain, and G. Muhammad," Healthcare Big Data Voice Pathology Assessment Framework," IEEE Access, vol. 4, no. 1, pp. 7806-7815, December 2016.

[5] M. Chen, Y. Hao, K. Hwang, L. Wang, L. Wang," Disease Prediction by Machine Learning over Big Healthcare Data", IEEE Access, Vol. 5, No. 1, pp. 8869-8879, 2017.

[6] M. Chen, P. Zhou, G. Fortino," Emotion Communication System", IEEE Access, Vol. 5, pp. 326-337, 2017.

[7] M. Chen, Y. Ma, Y. Li, D. Wu, Y. Zhang, C. Youn," Wearable 2.0: Enable Human-Cloud Integration in Next Generation Healthcare System", IEEE Communications, Vol. 55, No. 1, pp. 54-61, Jan. 2017.

[8] Bian J, Topaloglu U, Yu F, Yu F. Towards Large-scale Twitter Mining for Drug-related Adverse Events. Maui, Hawaii: SHB; 2012.

[9] M. S. Hossain and G. Muhammad," Cloud-assisted Industrial Internet of Things (IIoT) - enabled framework for Health Monitoring," Elsevier Computer Networks, Vol. 101, No. (2016), pp.192-202, June 2016.

[10] Raghupathi W, Raghupathi V. An Overview of Health Analytics. 2013.

[11] M. S. Hossain, G. Muhammad, Sk. M. M. Rahman, W. Abdul, A. Alelaiwi and A. Almari," Towards End-to-End Biometrics-Based Security for IoT Infrastructure," IEEE Wireless Communication magazine, vol. 23. no. 5, pp. 45-51, October 2016

[12] I. Foster, Yong Zhao, I. Raicu, and Shiyong Lu. Cloud Computing and Grid Computing 360-Degree Compared. Grid Computing Environments Workshop, Austin, 2008.

[13] P. T. Grance. (October 2009) The NIST Definition of Cloud Computing. Available online: http://csrc.nist.gov/groups/SNS/cloud-computing

[14] Das Sargita, Chandrakar Ankita, and Pradhan Reshamlal. A Review on Issues and Challenges of Cloud Computing. International Journal of Innovations and Advancement in Computer Science 2015, Volume 4, pp. 81-88.

[15] Akyol BA. Cyber Security Challenges in Using Cloud Computing in the Electric Utility Industry. Pacific Northwest, Washington, 2012.