ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Access the Personal Health Records by checking the DES key DNA encryption algorithm

Al.Jeeva[1], Dr.V.Palanisamy[2]

Research Scholar[1], Professor & Head [2]

Department of Computer Science & Engineering, Alagappa University, Karaikudi-630003. Tamilnadu, India

[1]jeevamrp@gmail.com,[2]vpazhanisamy@yahoo.co.in

Abstract: **Nowadays, Personalized medicine is an promising way of treatment for the patients. Medical records make into standardize and manage in the form of Electronic Medical Record.(EMR). Personal health record (PHR) is essential for continuing the treatment, tracing the previous clinical reports and in taking drugs. The management of PHR by hand increases the time of processing and arise the complexity in storage problem. The health information exchange often outsources the data to be stored at a third party. Third party implements the encryption techniques for access control mechanism. The access control mechanism provides the security against intruders and unauthorized person. Third party assures the patients' be in the charge of access their own PHRs. The privacy risk, unauthorized access are the most important issues achieving the enforced access control. Sometimes PHR owner can't able to access the medical record regarding severe health problem, environmental issues. In those situations, The owners' blood relationship take care of the PHR owner. So the blood relations become authorized person for accessing the PHR record. In this paper, the access control mechanism design for accessing PHR of owners and their blood relationship through their encrypted DNA matching.**

Keywords— **Access Control Mechanism, cryptography, DNA Encryption, DNA Cryptography.**

1. INTRODUCTION

In current decade, the collection of patient information manages in electronically-stored information in digital format. Due to the high cost of data storage servers and data centers, hospitals outsource their patient record to third party. The third party stores the PHRs and provides the service to access the PHR through web. The patients allow to access, modify and manage their personal records through PHR service. Each patient shares health data to family members' health care providers, health care insurance with limited access control. Here, the third party assures the uncompromised access control to get the PHR. In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. A PHR service allows a Patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each Patient is promised the full control of her medical records and can share their health data with a wide range of users, including healthcare providers, family members or friends. Due to the high cost of building and maintaining specialized data centers, the hospitals outsource the PHR into third party. Many PHR service providers service to access and manage the records by PHR owner. For example, Microsoft HealthVault.1 Recently, architectures of storing PHRs in cloud computing have been proposed PHR owners is setup the access roles for accessing their own records to other people like hospitals, insurance company and friends. The third party service providers assure the security and privacy of PHR. They design the access control mechanism to stored records in the centralized database. The centralized database keeps into cloud computing environment [1]. Generally, the data sharing performs in secured manner that attain by encryption techniques which has applied into the information. Commonly, the users access the encryption information through the access control mechanism and that is design from cryptography techniques. Some times PHR owners can't able to access their records because of health issues. In hard situation, PHR own permits the blood relationship to access the health records. But third party doesn't know the person who is the blood relationship of PHR owner. For avoiding this issue, in this paper, apply the DNA based cryptography techniques for generating the key from DNA data. It assures the high security and identifies the relationship without human intervention.

A. DNA Computing and Cryptography techniques

In Biology, DNA (Deoxyribonucleic acid) is the main molecule whose structures reflect the chemical reaction of the body and characteristics of human. In biology, a Deoxyribonucleic acid (DNA) is the master molecule whose structure encodes all the information needed to create and direct the chemical machinery of life [6]. Watson and Francis Crick were predicted the DNA molecule on 1953. DNA structure constructs with two long polynucleotide chains which are made from subunits that is called nucleotides. Sugar –phosphate molecule and nitrogen containing group present in the DNA base. There are four types of bases (adenine, guanine, cytosine, and thymine) labeled A, G, C, and T. The DNA-based cryptography is a latest and very hopeful direction in cryptography research. The cryptography concept applies in to DNA sequence to store and sharing the information as well as computation. Currently many Researches have been proposed to implement the cryptography techniques into DNA format. Some of the techniques are such as Onetime pads [8], RSA Algorithm [9, 10], Playfair cipher [11], DNA-based Encryption using pointers [12] and DNA Encryption using PCR [13]. There are two types of cryptography such as symmetric cryptography and assymmentric cryptography. Adleman proposed the DNA computing in 1994 to build the association between DNA molecule and computer. He analyzed that DNA computing is faster than electronic circuit. By using DNA computing he found the solution for Hamilton path problem [5] then Lipton enchanced the work of Adleman and examined the solution of NP-complete problem and he found the new concepts of DNA computing [6]. Boneh contributed an approach of DNA cryptography and he break the DES in 1995 [7]. In 1999, C.T.Chelland delivered a new method by steganography association with DNA to hide secret message encoded as DNA strands [8]. In 2000, Prof.Gehani proposed an encryption method using one-time pad and substitution method [9]. Andre Lier designed two different method. First method is to hide the information and second method is to design molecular checksum [10]. In 2003, Jie chen contributes carbon nano-tube based message transformation and DNA-based cryptosystem [11]. Lumingxin extended a symmetric key cryptosystem using DNA biotechnology and microarray [12]. Zheng zhang designed a technique to secure the information using bio molecular automaton [13]. Xingwang approach a new encryption scheme by using DNA computing and traditional cryptography and RSA algorithm [14]. G.cui implemented the technologies of DNA synthesis, PCR amplification, DNA digital coding and traditional cryptography to design a new encryption scheme [15].LAI Xuejia ,made an asymmetric encryption method and signature cryptosystem by associating genetic engineering and cryptology [16].

B. Symmetric cryptography

Symmetric key cryptography is simple and quite faster. The sender and receiver share a single common key to encrypt and decrypt the message. It only needs one key to encrypt the message. And both user only need the same key to decode the message. And the in order to create the key is by moving the bit. An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. So the sender and receiver keep the key in safe any ways. Symmetric-key cryptography is sometimes called secret-key cryptography. The most popular symmetric-key system is the Data Encryption Standard (DES). In this paper, the DES is applied over DNA encryption.

II. PROPOSED METHOD

In our access control mechanism, the DNA encryption process append to checking the DNA matching between PHR owners to family relation. Generally, the structure of DNA sequences are similar to family members. Here the DNA sequence is the key point of our proposed access control mechanism.

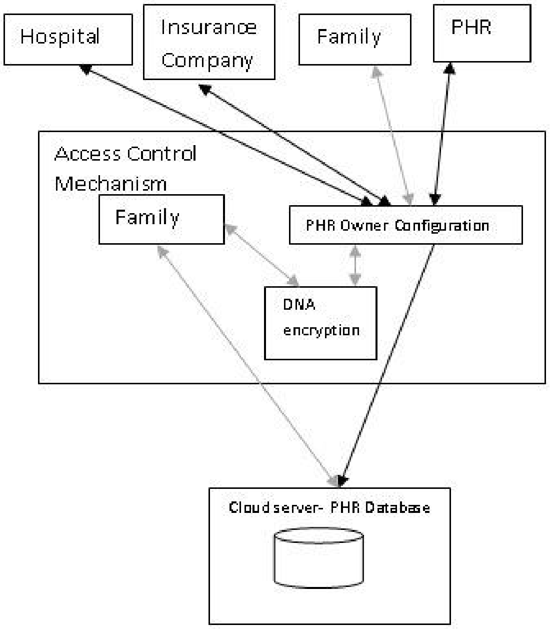

Fig1. Framework of access control mechanism

In fig1, the framework is to offer secure patient-centric PHR access and authenticate the family member based on key of encrypted DNA. There are three users can access the PHR with PHR owner permission, PHR owner configure the access control mechanism to assign the roles and decide the authentication level. The role of nurse or medical practitioner is to access clinical reports in detail. The role of insurance company is to access the summary of clinical report. So the access level varies in different domain. Sometimes PHR owner can't access the records due to severe illness or critical situation. Family members of PHR owner take care of his health and communicated with medical practitioner and also family member act as super user. They can access all records. Third party check the person who is the family member of PHR owner, through encrypted DNA. The structure of DNA sequence is in string format and its length is too large. If apply comparative operation between two DNA strings in authentication process. The time complexity will go increase. Encryption technique is the best way to secure the DNA sequence. The encryption process execute in one time when the PHR owner feed the DNA sequence into the server.

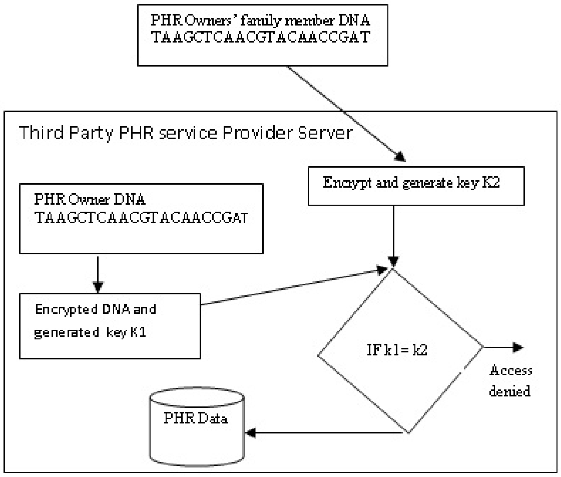
PHR Owners' family member DNA TAAGCTCAACGTACAACCGAT
Third Party PHR service Provider Server
Encrypt and generate key K2
PHR Owner DNA TAAGCTCAACGTACAACCGAT
Encrypted DNA and generated key K1
IF k1= k2
Access denied
PHR Data

Fig 2. Process of accessing PHR by family member

Fig2 shows the family member authentication mechanism. In the mechanism the family member feed his DNA sequence into encryption process. DES symmetric key algorithm applies into encryption process. It is simple and quite fast in hardware and software. The DES algorithm encrypts the DNA and generates the 64 bit key. Already PHR owner's encrypted DNA has stored in the system. The authentication mechanism checks the key value of family member and PHR owner. As per DNA sequence analyzing, the DNA sequence of PHR owner and family members DNA are equal. Hence the key values are also equal. Therefore, the Family member becomes the super user of PHR records.

III. CONCLUSION

In this paper, we have proposed access control mechanism of secure accessing the personal health for family members. The patient-centric concept, Patient configures the access control mechanism for sharing their medical record to others. In this paper, authenticate the family member through encrypted DNA key matching mechanism. This mechanism achieves the security of PHR records and identity the family member of PHR owner exactly. This mechanism assures the confidentiality and security of PHR records.

REFERENCE

[1] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010.

[2] H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10),pp. 220-229, 2010.

[3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), June 2011

[4] Ming Li, Shucheng Yu, Yao Zheng,et.all," Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", IEEE transactions on parallel and distributed systems, vol. 24, no. 1, january 2013,pp-131-143

[5] L.Adleman, "Molecular computation of solutions to combinational problems",science, JSTOR,vol.266,1994,pp-1025-1025.

[6] R.J.Lipton "Using DNA to solve NP-complete problems",science
vol.268 pp.542-545,1995

[7] D.Boneh,C.Dunworth and R.Lipton, "Breaking DES using a molecular computer", In proceeding of DIMACS workshop on DNA computing,1995,pp.37- 65

[8] C.T.Celland,V.Risca and Bancroft C., "Hiding message in DNAmicrodots",Nature ,vol399,pp.533-534,1999

[9] A.Gehani,T.H.Labean and J.H.Reif, "DNA based cryptography-
DNA based computers v.providence American Mathematical society,vol54,2000. pp.233-249

[10]A.Leier,C.Richter and W.Banzhaf, "cryptography with DNA binary strands",Biosystems,2000.pp-13-22

[11]J.Chen, "A DNA-based,biomolecular cryptography design",circuits and systems ISCAS apos,2003,pp.822-825.

[12] M.X.Lu, "Symmetric - key cryptosystem with DNA technology",science in china series information science,vol.3,2007,pp.327-333

[13] Zheng Zhang,Xiaolong shi,JieLiu,"A method to encrypt information with DNA computing",3rd international conference on bio-inspired computing.Theories and application 2008.pp.155 -160

[14] Xing wang,Qiang zang "DNA computing based cryptography",Fourth international conference on bio-inspired computing BIC-TA2009 pp1-3.

[15] G.Cui,L.Cuiling,L.Haobin and L.Xiaoguang, "DNA computing and its application to information security field",IEEE 5th international conference in National computation,Tianjian china,Aug 2009,pp.148-152.

[16] L.Xuejia,L.Mingxin,Q.Lei,H.Junsong and F.Xinven, "Assymmetric encryption and signature method with DNA technology",science in china: Information Science,vol.53,2010,pp.506-514.

[17] Deepak singh chouhan,R.P.Mahajan, "An architectural framework for encryption and generation of digital signature using DNA cryptography",International Conference on Computing for Sustainable Global Development(INDIACom),2014

Authors Profile

Dr.PalanisamyVellaiyan obtained his B.Sc degree in Mathematics from Bharathidasan University in 1978.He also received the M.C.A., and ph.D Degree from Alagappa University in 1990 and 2005 respectively. After that working as Lecturer in AVVM Sri Pushpam College, Poondi from 1990 to 1995, He joined Alagappa University as Lecturer in 1995. He is currently working as Professor and Head of thedepartment of Computer Science and Engineering. He also received the M.Tech. Degree from Bharathidasan University in 2009. He has published over 20 journals and conferences and his research interest includes Computer Networks & Security, Data Mining & Warehousing, Mobile Communication and Computer Algorithms.

JeevaAlagarsamy received his Diploma in EEE from Alagappa Polytechnic, Karaikudi. He also received B.C.A., and M.Sc., Degree from Alagapppa University, Karaikudi in 2008, 2011and respectively. and M.Phil Degree received from Alagappa university, He is doing Ph.D Degree in the area of information security and cryptographyce, Department of Computer Science and Engineering, Alagappa University, Karaikudi, Tamil Nadu, India. His research interest includes ad hoc wireless Networks &Security, Cloud Computing Data mining and Computer Algorithms.