Enhancing the Security in Health Data using Attribute Based Encryption

Pooja H. G[1]
PG student ,Dept of CSE,CIT , Gubbi ,
Karnataka ,India

Mrs. Sharayupradeep[2]
Associate Prof, Dept of CSE
CIT , Gubbi ,
Karnataka, India

***Abstract*— My Health Register (MHR) contains the details of the patient health which is monitored and handled by the patients.MHR contains the sensitive data about the patient health and this information is shared across the internet with doctor, health provider. So the data should maintained secure hence the data are stored in encrypted format with in the cloud. The data stored in CP-ABE (cipher text policy attribute based encryption) encryption technique. Even data is encrypted, the network and devices with in the health organization are suffering from blitz of malicious attacks leaving the patient data at risk, along with patient data , internet connected device from billing system are getting hammered by malicious attack. In this paper to overcome the authentication attack we propose a session hijacking prevention technique to eliminate the data hacking and man in the browser attack to prevent the fraud transaction happening in the billing system. And provide secure sharing of information**

Keywords—PHR, Attribute based encryption,Session hijacking.

I. INTRODUCTION

Recent technology advances in healthcare system patient health information are stored and managed as a My health register by the patient this personal health information are stored manage and control in one place in the web. This makes the easy sharing of medical information efficient. This health information are stored and maintained by the health organization, third party service provider the data should be secure since it contains the crucial and sensitive data related to the patient. In early days the patient information are stored in paper document this may lead to loss of data to overcome this in recent times new architectures are designed to store the patient information in cloud. The main aim of using cloud to store the data is easy available and sharing of the data across the internet. The main challenge in cloud is providing the security and privacy of the data stored in the cloud. MHR contains the sensitive data so the data in the cloud should be secure to provide the security the patient could able to control over the data so that only legitimate patient can access the data.

A possible approach to maintain data secure in cloud is to encrypt the data before storing it in the cloud. encryption of the data is decide by the MHR owner and they are capable of giving permission to other to access the file only authorized person can access the patient data using the decryption key which are provided to them. Even the data are stored in the encrypted format the data is hacked during the time of authentication of the user. The network and devices are suffering from an malicious attack like viruses, worms and different authentication attack like phishing attack, session hijacking attack, replay attack using this hackers can hack the sensitive data of the patient. In modern healthcare organization the billing system are directly connect to the internet and different machines in the health system so the attacker can attack like main in the browser attack and can make fraud transaction .

In this paper we propose a technique for encryption and secure sharing of information using [1] CP_ABE technique. (1) The main idea of CP_ABE is The idea of Attribute-Based Encryption (ABE) was first proposed by Sahai and Waters On the contrary to the traditional identity-based encryption, a user is able to decrypt a ciphertext if there is some match between his private key and ciphertext in the ABE . Our scheme chooses CP-ABE .In the CP-ABE, the private key is distributed to users by a trusted central issuer only once. The keys are identified with a set of descriptive attributes, and the encrypter specifies an encryption policy using an access tree so that those with private keys which satisfy it can decrypt the cipher text. To overcome the authentication attack and fraud transaction we uses the concept of session hijacking and main in the browser attack technique respectively.(2) In [2]session hijacking an attacker usually takes over the web server and therefore hijacks all subsequent legitimate user sessions to launch attacks. (3) Man-in the- browser is a Trojan horse that exploits the vulnerabilities in browser security to alter web pages transactions or insert extra transactions, in a secret way invisible to both the client and hosting.

II. RELATED WORK

In the recent healthcare system the patient data are stored within the cloud hence the data should be secure with in cloud. In the existing system the data within cloud are encrypted and stored within the cloud. [3]Health vault, medcloud provide health services where the patient data are stored within cloud since the patient data are sensitive it should be secure even the data encrypted and stored the data within the cloud is not patient-centric instead the data is server-centric the data are controlled within the server so there is chance data loss. [4] As a famous incident veterans affairs database containing PHI of 26.5 million military veterans, including their social security numbers and health

problems was stolen by an employee who took the data home without authorization. To ensure privacy control on the MHR the data should be patient-centric so there will be control on their own data and even the data are shared in public and private domain the data should be secure. To ensure security and Patient-centric access of data we adopt the concept of attribute based encryption as the encryption primitive. Using[5] ABE, access approach is defined based on the attributes of patient or data, which provide the patient to share their MHR among a group of users by encrypting the file using attributes. The main complexities involved are the encryption, key generation and decryption with the number of attributes declared.

ABE works in four phase initially *: Setup* : A randomized algorithm which must be run by some trusted party (e.g.central authority). Takes as input the security parameter. Outputs a public key, secret key pair for each of the attribute authorities, and also outputs a system public key and master secret key which will be used by the central authority.

Attribute Key Generation : A randomized algorithm run by an attribute authority. Takes as input the authority's secret key, the authority's value dk, a user's GID, and a set of attributes in the authority's 1domain Ak C. (We will assume that the user's claim of these attributes has been verified before this algorithm is run). Output secret key for the user.

Central Key Generation : A randomized algorithm run by the central authority. Takes as input the master secret key and a user's GID and outputs secret key for the user.

Encryption : A randomized algorithm run by a sender. Takes as input a set of attributes for each authority, a message, and the system public key. Outputs the ciphertext.

Decryption : A deterministic algorithm run by a user. Takes as input a cipher- text, which was encrypted under attribute set AC and decryption keys for an attribute set Au. Outputs message m if |Ak C ∩Ak u| > dk for all authorities k.

Even the data is encrypted and stored in cloud still there is security problem in healthcare system the existing system concentrate on security within the cloud and while transmitting the data . The loss of data can happen when user login in into account, at that time attackers can hack the user session and get access to the patient information. [6]An incident that networks and devices operated by U.S health organizations are suffering from an onslaught of malicious attacks, leaving patient data at risk. The new SANS Institute-Norse corp. Health care cyber threat Report found that internet connected devices from billing systems to dialysis machines are getting hammered by malicious attacks. So security must be consider on the authentication attacks several attacks can happen when user login an attacker can hack the user session and can get username and password and get access to user data so security should be given on session hijacking. other authentication attacks man-in –browser attack can happen within the network where attacker can alter the information and fraud transaction can happen within the healthcare system this are the drawbacks in the existing system .

.

III. PROPOSED SYSTEM

. My health register is internet based application that provide people to access and co-ordinate their health information and make if suitable parts of its information available to those who need. In order to provide security and privacy in the proposed system it uses the concept of ABE encryption along with that it concentrate on the authentication attacks that happens within the network like session hijacking to avoid hacking of user session and man–in-the-browser attack to avoid fraud transaction happens in the healthcare system.

In the proposed system it mainly concentrate on the security of the patient data within the cloud and provide a mechanism to avoid authentication attack. It mainly concentrate session hijacking and man-in the-browser attack , where attacker hijacks the user session and can get access to the user data and can alter the data. So it provide mechanism to overcome the attacks.

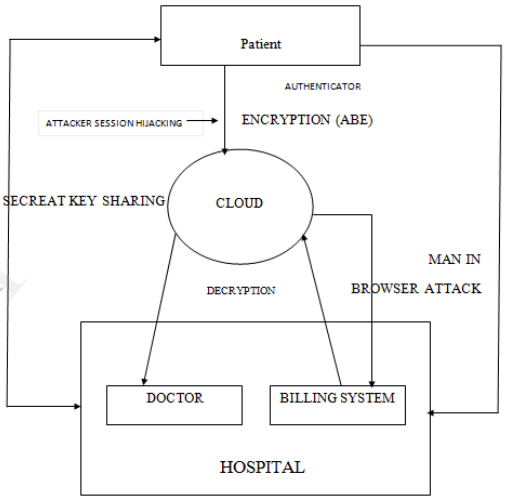

FIG: System Architecture

1)*Session hijacking*: an attacker usually takes over the web server and therefore hijacks all subsequent legitimate user sessions to launch attacks. Attacker hack the user sessionId and try to logging into their account using particular sessionid and the attacker can eavesdrop, send spoofed replies and/or drop user requests. To avoid this there should me a mechanism that identifies the and prevent the hacking of user session . This can done using IDS (intrusion detecting system). When attacker try to login to user account using sessionId IDS system will map with the user information and try to find the valid user , if the user is not valid IDS system will prevent the logging into user account and shows the error message and identify the attacker and indicates to the admin about the attack .

2)*Man-in the Browser-Attack*: [7]Man-in the- browser is a Trojan horse that exploits the vulnerabilities in browser security to alter web pages, transactions or insert extra transactions, in a secret way invisible to both the client and hosting. In the healthcare system machines which are directly connected to the billing system are hacked by the attacker and they try to change the values or alter the information within the system to avoid this there should be mechanism that

identify the changes within the data. To avoid this attack within the server there should be a guard that identifies the changes. IDS will verify the data send from source to the destination. In destination verification module will identify the source Id and it will compare the data that it send from the source if there is any changes IDS sends error message reporting that the data is altered.

$$\alpha + \beta = \chi. \qquad (1)$$

IV. CONCLUSION

In this paper we propose privacy for the healthcare system using ABE technique in which the patient data is encrypted and to access the data it provide secret key which are generated using the attributes of patients and provide the access to information for the authorized user and in this it also concentrate on the authentication attack .where attackers hack the user session and get access to the user data and it provide the mechanism to over com the session hijacking attack and in the healthcare system the billing system which are directly connected by the machine are getting hacked and the data and information are altered in this it provide the mechanism to overcome man-in-browser-attack .in this paper it provide the security for the healthcare system and it overcomes some of the existing security issues and provide the solution. which the patient data is encrypted and to access the data it provide secret key which are generated using the attributes of patients and provide the access to information for the authorized user and in this it also concentrate on the authentication attack .where attackers hack the user session and get access to the user data and it provide the mechanism to over com the session hijacking attack and in the healthcare system the billing system which are directly connected by the machine are getting hacked and the data and information are altered in this it provide the mechanism to overcome man-in-browser-attack .in this paper it provide the security for the healthcare system and it overcomes some of the existing security issues and provide the solution.

V. REFERENCES

[1] Privacy Preserving Cloud Data Access With Multi-Authorities Taeho Jung§, Xiang-Yang Li§, Zhiguo Wan† and Meng Wan ‡ §Department of Computer Science, Illinois Institute of Technology, Chicago, IL †School of Software, TNLIST, Tsinghua University, Beijin ‡Center for Science and Technology Development, Ministry of Education, Beijing
[2] http://www.cleverlogic.net/tutorials/session-hijacking-0
[3] https://www.healthvault.com/in/en
[4] AT RISK OF EXPOSURE IN THE PUSH FOR ELECTRONIC MEDICAL RECORDS, CONCERN IS GROWING ABOUT HOW WELL PRIVACY CAN BE SAFEGUARDED.
http://articles.latimes.com/2006/jun/26/health/he-privacy26
[5] Multi-Authority Attribute Based Encryption Melissa Chase Computer Science Department Brown University Providence, RI 0291 mchase@cs.brown.edu.
[6]http://searchnetworking.techtarget.com/news/2240214827/Study-Malicious-attacks-at-hospitals-risk-patient-data
[7] Article: Man in the Browser Attack Aakash Goyal Assistant Professor, Jind Institute, Engineering and Technology, Jinds, Kurukshetra.