International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 32557-32575
© Research India Publications
http://www.ripublication.com

A Novel Framework for Securing Health Data in Pervasive Environment Using Hybrid Cryptography

Blessed Prince. P [1] Dr.K.Krishnamoorthy[2] Ananda Raj R[3] Jeno Lovesum S.P[4]

[1]Department of Information Technology, Karunya University, India
[2]Department of Computer Science and Engineering, Sudharsan Engineering College, India
[3] Department of Information Technology, Karunya University, India
[4] Department of Computer Science and Engineering, Karunya University, India
[1]blessedprince@gmail.com
[2]kkr_510@rediffmail.com
[3]anandaraj3121@gmail.com
[4]jenolovesum@gmail.com

Abstract

Advancement in mobile technology along with various computing models like cloud computing brings drastic changes to the e-healthcare sector. Various e-healthcare applications have been proposed to allow the patient to submit their health information to the third party cloud storage. However, the acceptance level of users towards these health care applications is limited in concern with security issues. In this paper, we have proposed a secure e-healthcare protocol using hybrid cryptography that allows the patient to securely upload the health information to the cloud storage. We perform cryptographic activities such as key generation, encryption and decryption in the client side with minimum encryption and upload time. Also the proposed protocol complies with the HIPAA privacy and security regulation policies and performs efficient user authentication and revocation.

General Terms: User authentication, Hybrid cryptography, e-Healthcare, HIPAA privacy constraints

Additional Key Words and Phrases: Cryptology, encryption, cloud storage, data upload, privacy and security.

1. INTRODUCTION

Recent advancements in mobile technology along with the converged infrastructure and shared services of cloud computing, drastically changes the field of health sciences [Nabil. 2014]. Innovation in the technology allows developers to offer services in the health care domain. Lot many cloud based e-healthcare applications are available that assists their remote users to monitor and exchange their real time health information. These applications plays a major role in electronic healthcare system in which a patient who is incapable of meeting the physician in person can use their personal digital assistant like mobile or laptop to collect the health information through wearable sensors and the information can be uploaded to the cloud server for the diagnosis by the physician (Figure. 1.1). However, cloud based e-health technologies are not much embraced by common users or health communities citing issues with privacy and security [Eman et al. 2012]. The primary issue with cloud is lack of confidentiality and privacy of the patient's health data, as the sensitive health information is stored with the third party server.

We have analyzed various security and privacy issues related to electronic health care system in correspondence to the Health Insurance Portability and Accountability Act (HIPAA), recognized by US congress in 1996 as Federal Law [http://health.state.us/hipaa/]. In this paper we propose a secure e-healthcare protocol using hybrid cryptography which accredits the patient to securely exchange the health data with cloud. The proposed secure e-healthcare protocol encompasses user authorization, data exchange with cloud. The proposed protocol corroborates hybrid cryptography gimmick that enciphers the health data preceding cloud sync. In disparity with the existing encryption modus, our proposed protocol securely exchanges the data with less encryption time, abiding the requirements of the regulatory agents like HIPAA.

The rest of the paper is organized as follows; section 2 discusses the related works. Section 3 describes proposed secure e-healthcare protocol. Section 4 illustrates the competence of the proposed e-healthcare system persistently abiding HIPAA constraints. Section 5 expounds and analyses various belligerent attacks. Section 6 discusses the implementation and experimental results. Section 7 concludes the paper and gives idea for further research and scope.

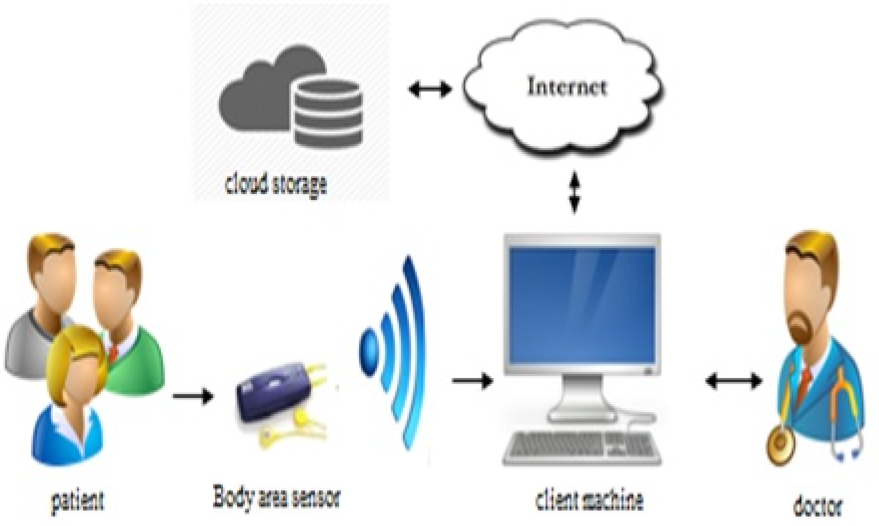


Fig. 1.1 Basic e-Healthcare architecture

2. RELATED WORKS

[Dawei et al. 2011] defines the security as 'Absence of unauthorized access to the system and divides the security, privacy and trust issues related to cloud environment into following six segments: providing safety mechanism, data confidentiality, preventing malicious insiders, service hijacking and phishing, data management over virtual environment. [Pandey et.al. 2012] proposed an autonomic cloud environment for hosting ECG data analysis service. Pandey et al illustrated the challenges faced by end-user while running their application in the traditional cloud computing model. The paper addresses the two major issues related to the cloud environment namely scalability and economy. [Sandeep. 2012] proposed a framework focusing confidentiality, availability and integrity to ensure secure data transfer over cloud environment. The specified model make use of secure socket layer (SSL) certificate to prevent the data access for unauthorized users, also the data is encrypted using the secret key of the user to provide higher degree of security. Even though this proposed system offers higher security, it squanders more system resources by performing two phases of encryption during data exchange.

[Farrukh. 2014], proposed a framework for security and patient's privacy using wireless body area networks. This model implements security to the user's health information by generating a 360 bit long key by combining ECG and EEG signals. Patient wears the body area sensors and connects to the remote base station to upload the health information to the hospital community server. Also key generation involves three phases: feature generation, quantization and block exchange. This model generates a 360 bit key depending on patient's ECG information, leading to lack of integrity as there is a contingency of two or more messages encrypted with the same key, also takes more time and resources, considering the key size. [Ray et.al. 2012] proposed a new contract oriented and smartcard based healthcare system using RSA-CA abiding HIPAA privacy-security regulations. This scheme authenticates the system user's through certificates, and offers strong data encryption. This system reveals the patient's health information during emergency situation. Although Sangram's model offers high data security through public key certificates, the patient have no control over their health data, instead uploaded by medical staff to the MCS. [Danan Thilakanathan et.al. 2014] proposed a platform for secure monitoring and sharing of health data in cloud. This model allows the patient to collect the health information using body area sensors and deliver it to the patients' handheld devices through Bluetooth connectivity, encrypt the data with the patient's random key which in turn is encrypted with the public key generated by cloud server. In this model, user revocation and encryption leads to high computational time, which is a constraint in mobile devices.

Authentication can be described as the act of granting permission to the authorized user to access the system resources [Sharma et.al. 2010]. The existing authentication techniques are as follows, (a) username and password based authentication, (b) one time pass-code based authentication, (c) Biometric based authentication and (d) certificate based authentication. Table II compares the merits and demerits associated with the traditional authentication techniques.

In the proposed secure e-healthcare model, password based authentication technique is enhanced by adopting intermediate data generation and integrity check using one way hash function. Also the proposed model is staunchly against the prevailing attacks like sniffing attack, replay attack, collision attack, repudiation mechanism and identity theft. Our proposed secure e-healthcare protocol addresses safety mechanism, data confidentiality and also prevents malicious insiders by providing hybrid encryption and access control to the data owner. Our proposed e-healthcare protocol uses java based client interface, hosted in the Novell powered open SUSE cloud server. The proposed system craves no further software for data encryption, key generation and data exchange; in turn the economy issue is addressed. Our proposed model achieves tantamount of security by encrypting the health data with 256 bit symmetric key and a message authentication code (MAC) to authorize the user with minimum time. The proposed system makes use of body area sensors to collect the health data and PHI is directly dumped into the patients' personal digital assistant like laptop or mobile devices rather sending to the remote base station; The hospital community server is replaced by the cloud server for effective data storage and retrieval without compromising security. Also our model doesn't enforce the user to sign a contract for registering with the system in contrast with Sangram's model. Our proposed model, coalesce both private and public crypto system to encipher the PHI prior uploading to the cloud server. Our performance analysis reveals that data encryption and user revocation is done in a lesser time. Table I illustrates the summary of literature review.

Table I. Survey on e-Healthcare Architectures

	Sandeep et al (2012)	Danan et al (2013)	Sangram et al (2013)	Farrukh et al (2014)	Proposed model
Registration & Authentication	✓	✓	✓	✗	✓
confidentiality	✓	✓	✗	✗	✓
Integrity	✓	✓	✗	✗	✓
Encryption	✓	✓	✓	✓	✓
HIPAA constraints	✗	✗	✓	✗	✓
Computational time	High	High	High	High	Low
Emergency data retrieval	✗	✓	✓	✗	✓
Non repudiation	✗	✗	✗	✗	✓
Key size	128	Not specified	Not specified	360	256
Cryptosystem	private	Public-private	Public-private	private	Public-private

3. PROPOSED SECURE e-HEALTHCARE PROTOCOL

The proposed secure e-healthcare system (Figure. 3.1) allows the patient and doctors to register with the cloud server by providing their credentials and a secret personal identification number (PIN). On reading the credentials from the user, the system generates a 128 bit hash value using one way hash function [Ralph. 1998], which is in turn used to authenticate the user. The system acquiesce the authenticated data owner to encrypt the health data by generating a random session key, which in turn is encrypted using receiver's public key and the health data is uploaded to the cloud server and can't be accessed without the permission of the data owner. The physician is allowed to decrypt the random session key by using his secret private key which is used to decrypt the original health information. The proposed system assumes that the health information is collected using body area sensor and dumped into the mobile device which is ready to be uploaded to the cloud server. The proposed scheme is detailed in the following section, which uses few notations as listed below (refer Table III),

Table II. Merits & Demerits of various authentication schemes

Authentication technique	Merits	Demerits
Username & password based authentication	Easy implementation User friendly cost effective Commonly used in various web applications [Steve. 2010]	Highly sensitive to various attacks [Steve. 2010] like password cracking, packet sniffing, replay attack, identity theft, pattern recognition etc...
One time pass-code authentication	Strong against Man-in-the-middle attack [Haung et.al. 2013] Provides complete protection during login phase.	Vulnerable to masquerading (stealing the password from the storage location [Cullen. 1995]) attack [Unar et.al. 2014]
Biometric authentication	User need not to remember any cryptographic words Sole property of an individual	Selection of human organ is very important.
Certificate based authentication	Minimal involvement of end user No extra hardware is required Highly compactable.	Performance degradation due to large user groups (SSL SPIKES) Not suitable for bulk file transfer.

The proposed e-healthcare system can be divided into following phases (refer Table IV): Registration and Login phase, Data encryption and upload phase, Access control phase, data download and decryption phase. The proposed protocol ensures that, all the phases abide with HIPAA constraints.

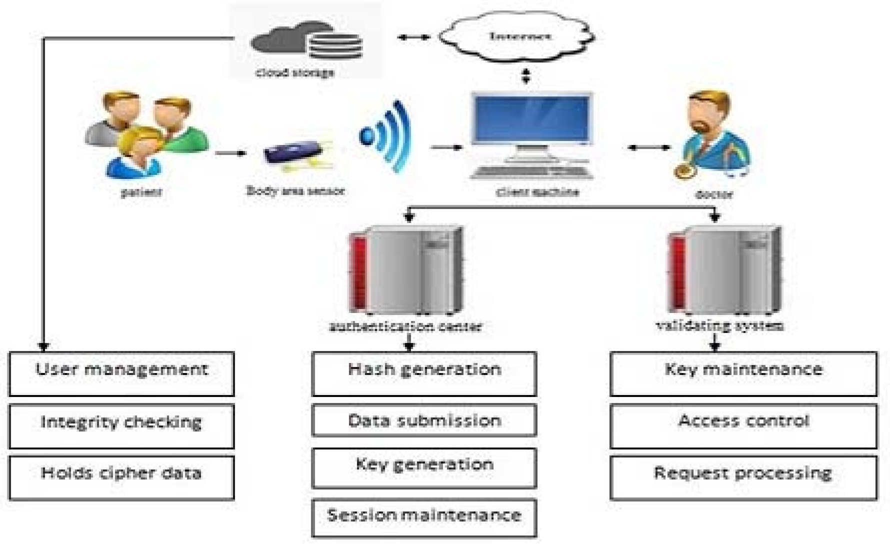


Fig. 3.1. Proposed e-Healthcare architecture

3.1. Registration and Login Phase

The registration phase allows the system user to register with the cloud server by providing the username (ID), password (P) and a four digit personal identification number (PIN). The user credentials are transferred to the authentication center (AC), the AC shifts the credentials to radix$_2$ format and generates a hash value (h_v) [Guido et.al. 2013] after processing the input data (ID, P, PIN). Intermediate data generation process is done during the registration phase by the AC in order to increase the complexity of the hash value.

Step 1: User → AC: Register (ID, P, PIN)
Step 2: (ID, P, PIN) → Radix$_2$
Step 3: h_v = SHA3(Radix$_2$ >> PIN)
Step 4: AC → CS: (h_v, ID)

Login phase verifies the authenticity of the user with the following mechanism. Once h_v is generated by the AC, it appends the client side nonce N_c and username along with h_v and posts it to the cloud server (CS) for verification.

User → AC: login(ID, P, PIN);
AC: gen_hash(ID, P, PIN);
AC → CS: post(h_v | | N_c | | ID);

On the receipt of hash value with the user’s identity, the cloud server verifies and authorizes the system user. Nonce value [Phillip. 2004] along with hash code avoids replay attack by malicious invaders.

3.2. Data Encryption and Upload Phase

After successful login, the data owner can encrypt their health data with a random 256 bit session key (k) using AES [NIST. 2001], a private-key cryptosystem, the session key is encrypted using a public key of the data consumer which is generated and registered with the validating system (VS) which is responsible for maintaining the entire receiver's public key, which in turn can be decrypted using the data consumers private key. Both public and private key of the data consumer is generated using ElGamal algorithm, a public key cryptosystem (Figure 3.2). The encrypted data is uploaded to the cloud server which can't be accessed without the knowledge of the data owner.

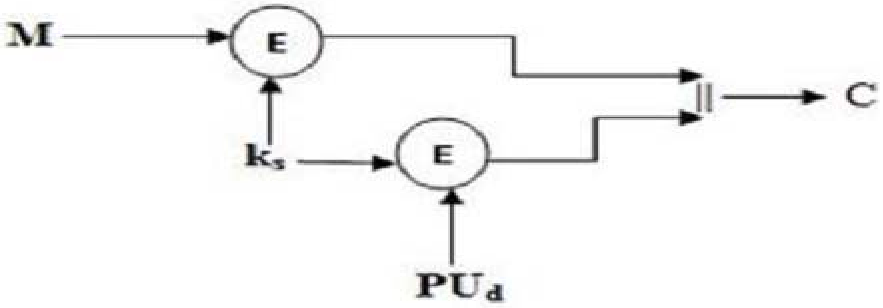


Fig. 3.2. Encryption mechanism

3.2.1 ElGamal Encryption

ElGamal encryption proposed by T.ElGamal, a public key cryptosystem [Taher. 1985], efficient, simple and doesn't depend on public key infrastructure (PKI), which makes ElGamal a perfect candidate to perform client side computation It has been analyzed that the cipher of ElGamal encryption scheme doubles the size of plaintext, which increases the upload time and may be not suitable for mobile environment. Hence the proposed secure e-healthcare protocol encrypts only the session key using ElGamal encryption instead of encrypting the health data. ElGamal encryption is detailed as follows:

Initialization

Select a prime number p, compute the primitive root g of p, $B=g^b$ mod p and $A=g^a$ mod p. Select a private key x, and the public key is [p, g, B].

Encryption

The message M can be encrypted using the public key
E (M) = M. B^a mod p = M. g^{ab} mod p, where M is the Session key(S_K)

Decryption

The cipher text **C** can be decrypted using private key x as
$D(E (M)) = C = M. k \bmod p$
$M = C^{-k} \bmod p$, Where $k = A^{b} \bmod p$

The desideratum of the proposed model is to offer a reliable and secure data exchange with minimum cost. The rest of the paper assumes that the health data is collected using body area sensors and it is ready to be uploaded to the cloud server.

Table III. Symbols used in proposed protocol

Symbol	Description
h ()	one way hash function (SHA3)
h_v	128 bit long has value
k_s	secret session key of the patient
ID_p	identity of the patient
P	password of the system user (of any length)
ID_b	user id in binary form
DO	data owner
M	health data
P_b	password in binary form
PIN	personal identification number
| |	append operation
$\oplus$	Exclusive OR (XOR) operation
(PU_d, PR_d)	public and private key of the doctor
ID_d	identity of doctor
E	encryption
D	decryption
N_c	nonce value
C	encrypted health data (cipher)

Our proposed system encrypts the health data and securely uploads to the cloud server for physician access. As the data owner enters the encryption phase, AC computes the public and private key for the data owner and the public key is maintained with VS. The data owner requests the VS to get a public key of the recipient Public key is obtained only after verifying the identity of data owner by verifying unique ID of the data owner and the recipient and the nonce value. On receiving the public key of the recipient, system generates a 256 bit session key and encrypts the health data with AES and the key is only valid for the current session, the generated key is not maintained with the system. Before uploading the encrypted health information to the cloud server, data owner encrypts the

session key with the received public key. This operation is performed using ElGamal, a public-key cryptosystem. The encrypted key is appended with the cipher C on uploading to the cloud server. Similarly for the physician, the public key generation process starts once the physician ought to access the health data.
Step 1: patient ← sensor
Step 2: patient → AC: keyGen(P,g,x) → VS: storeKey(P,g,B);
Step 3: Patient → VS: get_pub_key($\mathbf{ID_p}$ | | $\mathbf{ID_d}$ | | $\mathbf{N_c}$);
Step 4: VS → patient: return($\mathbf{PU_d}$);
Step 5: patient: gen_sec_key(); C: E(**M**, $\mathbf{k_s}$);
Step 6: Patient → CS: E_2($\mathbf{k_s}$**,** $\mathbf{PU_d}$); upload(C | | E_2($\mathbf{k_s}$**,** $\mathbf{PU_d}$));

3.3 Access Control Phase

According to privacy constraints of HIPAA, no information should be accessed without the permission of data owner [HIPAA. 1996]. To achieve this, our model allows the data owner (patient) to configure the access rights of his/her health information. Even though the health information is intended for the desired doctor, the data owner can prevent his/her health data being accessed by the recipient using the access control phase. This adds data integrity to the health information which is uploaded to the cloud server.
Patient → VS: enable ($\mathbf{ID_p}$, $\mathbf{ID_d}$, access_right);
VS → Patient: return access_ privilege;

3.4 Data Download and Decryption Phase

Any physician requesting access to the health data must be validated by the system verifying their identity, patient identity, time stamp (T_s). VS verify the access rights for the doctor with the privilege assigned by the data owner. On successful authorization, the encrypted health data is made available to the doctor. The decryption process starts after downloading the health information completely into the physician's device. Each decryption initiated by the physician will be acknowledged by the system after verifying the access rights.
Doctor → VS: request($\mathbf{ID_d}$, $\mathbf{ID_p}$, T_s); VS: search($\mathbf{ID_d}$);
check_privilage($\mathbf{ID_d}$, $\mathbf{ID_p}$); VS → Doctor: return privilege;

The decrypting process rips the encrypted session key from the cipher, decrypts the session key by the receiver's private key, decrypts the original health information with the session key.
Doctor → CS: download();
Doctor: D(E2($\mathbf{k_s}$, $\mathbf{PU_d}$), $\mathbf{PR_d}$); D2(**C**, $\mathbf{k_s}$); return M;

However, if the patient wants to perform any revocation of the doctor, the data owner can restrict the access for the doctor. Further request by the doctor to the VS ignores the request.

Table IV. Proposed secure e-Healthcare protocol

Actor(s)	Action performed	Phase

DO → AC
AC → CS
	Register(ID,P,PIN)
	Gen_hash(intermediate_data)
	Register with cloud database
		Registration

DO → AC
AC
AC → CS
CS → DO
	Login(ID,P,PIN)
	Gen_hash(IG,P,PIN)
	Post(h_v | | N_c | | ID)
	Verifies the integrity of hash code and compares the received hash value with registered data
	Return 'access_permission'
		Login

DO ← sensor
AC → VS
	Get_health_data()
	Generate(p,g,B)
	Choose a random value x, (private key)
	Store ([p,g,B] | | IDp)
		Key generation

DO → VS
VS → DO
DO → CS
	Get_public_key(ID_p||ID_d||N_c)
	Return 'PUd'
	Ks=gen_sec_key()
	C=((E(M,k_s)), E(k_s,PU_d))
	Upload(c | | E(k_s,PU_d))
		Encryption

DO → VS VS → DO	Enable(ID_p,ID_d,access_right) Return 'success'	Access configuration

DC → VS
VS → DC
DC → CS
DC
DC → AC
	Request(ID_d,ID_p,T_s)
	Search(ID_d)
	Chk_privilage(ID_d,ID_p)
	Return 'privilege'
	Download(privilege)
	D(E(k_s,PU_d),PR_d)
	D(C,k_s)
	Get M
	Logout(ID_d)
		Decryption

DO → VS VS → DO	Disable(ID_p,IDd,access_right) Return 'success'	User revocation

4. COMPARISION WITH HIPAA CONSTRAINTS

The proposed secure e-healthcare model have satisfied the guidelines of HIPAA related to the privacy and security regulations of the patient who is uploading their sensitive health information to the third party server. This section compares the proposed model with HIPAA constraints in detail. The major security constrains described by HIPAA were as follows [Jiankun et al. 2010].

4.1 Patients' Knowledge

It is obligatory to allow the patient to know, how his/her personal health information along with their name, identity, phone number and contact address were used by the physician and cloud administrator. To improve patient's knowledge about the health information, the proposed secure e-healthcare protocol have been implemented using a java based application, which enables the cloud administrator to convey access details about the patients' health information to it's users.

4.2 Confidentiality

As per the confidentiality constraint of HIPAA, it is mandatory for e-healthcare system to ratify encoding of the health data to preserve confidentiality. Our proposed e-healthcare protocol encodes the data using public and private cryptosystem, enhancing confidentiality.

4.3 Patient's Control

Data owner should be able to control the access rights over their health information. The proposed healthcare system grants the data owner to configure the access permissions, either to allow or deny access over their health information through a simple web interface.

4.4 Data Integrity

Any malignant activities alike tampering, unauthorized destruction, or anything leading to loss of integrity must be eliminated. Assuaging this HIPAA constraint our proposed model performs key generation and encryption in the client side. Any endeavor to alter or access the health data is imparted to the data owner through mail service.

4.5 Consent Exception

Any e-healthcare system should offer an option to retrieve the patients' medical record along with his/her contact amid emergency situation. The proposed healthcare protocol allows the data owner to register their contact info with the cloud server during the registration phase which helps the system to impart the health data to his/her emergency mail id and the access is granted after verifying the identity.

5. SECURITY ANALYSIS

The proposed secure e-healthcare protocol has been analyzed by performing malicious activities in order to determine the security flaw. The security analysis is detailed in the following section.

5.1 Collision Attack

Hash function resulting with same hash output for two different input messages is known as collision, and the likelihood of collision over SHA 3 hash algorithm [Chang et al. 2012] is limited. Performing collision attack over the proposed secure e-healthcare protocol would fetch an intermediate data, which is clueless in regard to user credentials. For a malicious attacker, retrieving the credentials from the intermediate data is unattainable, without knowing the data generation mechanism which is proposed in our e-healthcare protocol. Table V shows the intermediate data generated for various input along with the generation time, length of the password, PIN chosen by the user.

Table V. Intermediate data generation

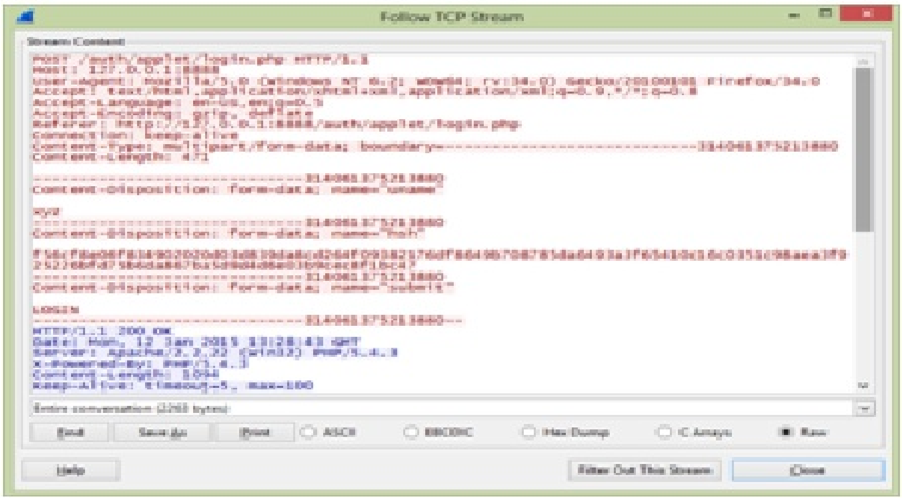
Input	Length	PIN	Intermediate data	Generation time (ms)
abcABC	6	10	Vtsoacklfsibel	0.21
AbcABC123	9	20	P8Xp0xzFF	0.29
Abcdefgh	8	50	IKMOQCEG	0.26
ABCDEFGH	8	70	GHABCDEF	0.33
ABCzxy1230#$^&!	15	99	Syn<DC1d^mackacksi	0.56

5.2 Replay Attack

During the authentication phase the proposed secure healthcare protocol generates a hash value and transferred to the server for authenticating the user, which may lead to the replay attack. Consider if Alice, a registered user is trying to get access to the system by posting a hash code to the server. On receiving the hash value server verifies with the previous hash values and grants the access permission for Alice. In this scenario if Bob, a malicious invader captures packet of Alice along with the hash value and retransmits to the server, in turn the server grants the permission to an attacker assuming as Alice. This replay attack is eliminated by adding a timestamp to the hash values which is indented for the server. Hence if Bob retransmits the same packet which is generated by Alice, the server denies permission since the timestamp gets expired.

5.3 Packet Sniffing Attack

The environment for sniffing attack [Edgar. 2001] has been simulated using an open source tool Rawpcap and a packet analyzing tool Wireshark. During the analysis, an authentication packet composed of user credentials is forwarded to the server, captured and verified to know that the packet contains hash value computed in the client side.



```
POST /auth/applet/login.php HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:34.0) Gecko/20100101 Firefox/34.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1:8888/auth/applet/login.php
Connection: keep-alive
Content-Type: multipart/form-data; boundary=---------------------------314065375213880
Content-Length: 471

-----------------------------314065375213880
Content-Disposition: form-data; name="uname"

xyz
-----------------------------314065375213880
Content-Disposition: form-data; name="hash"

[illegible]
-----------------------------314065375213880
Content-Disposition: form-data; name="submit"

LOGIN
-----------------------------314065375213880--
HTTP/1.1 200 OK
Date: Mon, 12 Jan 2015 13:28:43 GMT
Server: Apache/2.2.22 (Win32) PHP/5.4.3
X-Powered-By: PHP/5.4.3
Content-Length: 1094
Keep-Alive: timeout=5, max=100
```

Entire conversation (2268 bytes)

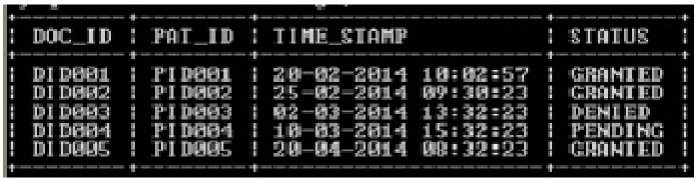
○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Fig. 5.1. Authentication packet posted to server

However, there is a chance that attacker may retransmit the obtained hash value to the server; the proposed authentication protocol regenerates the hash code for the given input. Figure. 5.1 represents the authentication packet which is posted to cloud server, and it is clear that the information contained in the packet is 128 bit hash value of the user credential, thus sniffing attack is avoided in the proposed model.

5.4 Non Repudiation Mechanism

Either the sender or the receiver should deny that they haven't transmitted or received the data; such mechanism termed as non repudiation mechanism [Steve et al. 2002]. To ensure non repudiation mechanism, the proposed model logs all the activity of the data owner while uploading the health data into the cloud server similarly the doctor's access request also recorded in the cloud server (refer Figure. 5.2). Hence, later the physician cannot deny that he haven't downloaded or accessed the health information of a patient.



```
+---------+---------+---------------------+---------+
| DOC_ID  | PAT_ID  | TIME_STAMP          | STATUS  |
+---------+---------+---------------------+---------+
| DID001  | PID001  | 20-02-2014 10:02:57 | GRANTED |
| DID002  | PID002  | 25-02-2014 09:30:23 | GRANTED |
| DID003  | PID003  | 02-03-2014 13:32:23 | DENIED  |
| DID004  | PID004  | 10-03-2014 15:32:23 | PENDING |
| DID005  | PID005  | 20-04-2014 08:32:23 | GRANTED |
+---------+---------+---------------------+---------+
```

Fig. 5.2. System recorded access requests

The proposed secure e-healthcare protocol is tested for the common security attacks, and the results infer that the proposed protocol resists the malicious attacks by the invaders.

6. IMPLMENTATION AND EVALUATION

6.1 Scenario

Following scenario is considered for the implementation of proposed secure e-healthcare protocol. A patient who is incapable to contact the physician in person, gather their health information thru sensors, in turn the health information is dumped to the patients' hand held devices like laptop or mobile through Bluetooth and uploads the health data to the cloud server. The proposed system helps to securely upload and access of the health information to and from the cloud server.

6.2 Implementation

The proposed protocol is implemented with a Novel powered Open SUSE cloud based java application which can be accessed thru any handheld device. The client side application interacts with VS and performs key generation; encrypts the data; authenticate the user. The e-health system allows the user to configure access control upon their data; secure upload and sharing of the health information.

6.3 Experimental Results

The proposed secure e-healthcare protocol is evaluated with samples of ECG (Electrocardiogram) data, each of 30s, 60s, 90s, 120s and 150s. Initially the collected test samples were encrypted using AES 256 bit encryption scheme alone and the performance were analyzed in terms of encryption time. Figure 6.1 depicts the results of AES 256 bit encryption. The results infer that the data samples were encrypted at a faster rate, 35 ms to encrypt 150 second ECG sample, an optimal encryption time. Figure. 6.2 shows the performance of ElGamal (asymmetric cryptosystem) encryption scheme. Compared with AES, the ElGamal encryption scheme consumes 26 seconds to encrypt the ECG sample of 150 seconds, which clarifies that the entire encoding of the heath data with ElGamal encryption scheme is not affordable.

However, Elgamal provides an efficient channel to securely exchange the keys among users. The proposed secure e-healthcare protocol depends on the ElGamal encryption for key exchange rather data encryption.

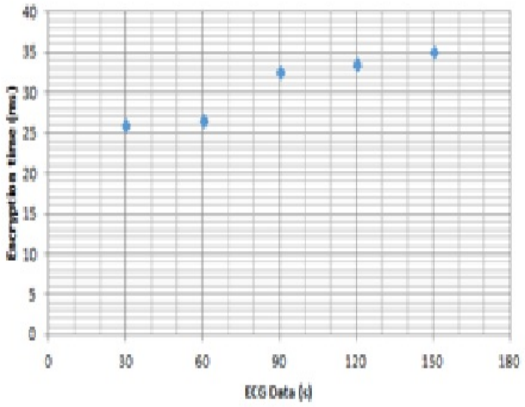


Fig. 6.1. AES Encryption Time

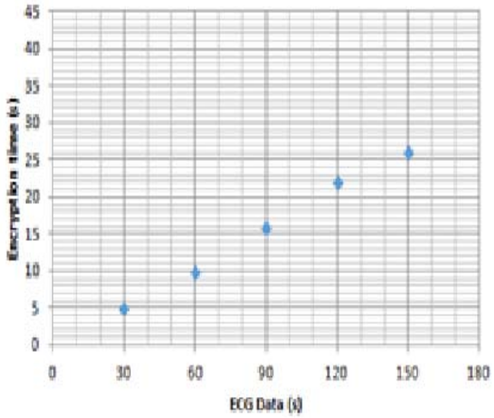


Fig. 6.2. ElGamal Encryption Time

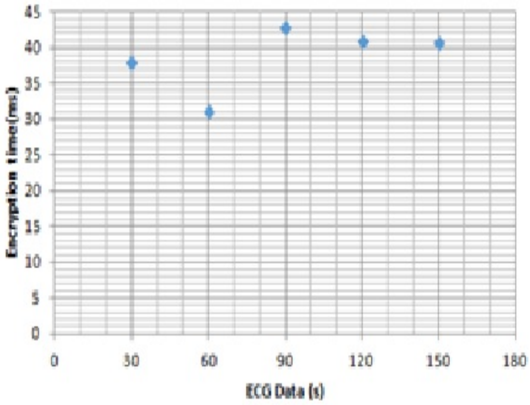


Fig. 6.3. Hybrid Encryption Time

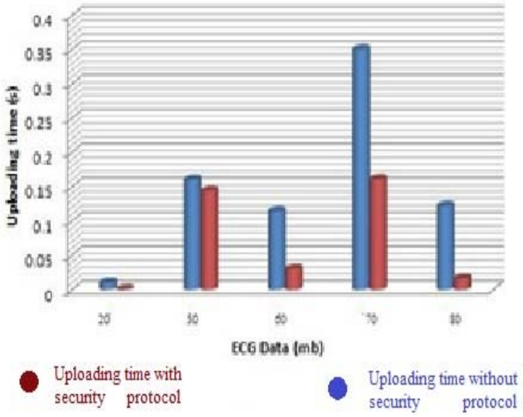


Fig. 6.4. Uploading Time of proposed protocol

The proposed hybrid model make use of AES 256 bit encryption for encrypting the health information and the random session key is securely shared among the cloud users through ElGamal encryption scheme(see Figure.6.3).The encrypted session key is uploaded to the cloud server, which can be decrypted using receiver's private key. The strength of the ElGamal encryption algorithm depends on the size of prime number selected during the generation of key pairs; the proposed model uses 1024 bit long prime number.

The proposed model limits the prime size to 1024 in order to maintain the performance of computing device, as the handheld devices are resource constraint. Table VI compares the encryption time of the proposed model with AES 256 bit encryption and ElGamal encryption scheme. Also the proposed secure e-healthcare model generates the cipher data; size identical to the original data; hence reduces the network overload while uploading to the cloud. Figure. 6.4 depicts upload time for various sized cipher data. Figure. 6.4, it is infers that the proposed model takes less time to upload the cipher data than one without security protocol. The proposed security protocol converts the encrypted health information to plain text format, results in less upload time (illustrated in the graph).

Table VI. Encryption time of proposed protocol

Test Cases (s)	AES256 Encryption (ms)	ElGamal Encryption (s)	proposed Model (Hybrid) (s)
30	26.17	05.00	0.0378
60	26.64	10.00	0.0310
90	32.74	16.00	0.0427
120	33.74	22.00	0.0409
150	35.13	26.00	0.0407

7. CONCLUSION

Healthcare applications in cloud environment being the repository of sensitive information, it is the foremost objective to consider security as a primary parameter. Cloud based e-healthcare applications demands for privacy, confidentiality, data integrity and resource availability. Hence a secure e-healthcare protocol is proposed with the aim of offering a secure platform by merging public and private cryptosystems. Proposed hybrid cryptosystem provides an overhead less key exchange channel combines with increased encryption pace. Highlights of proposed model enhances user authorization with intermediate data generation; reduces encryption time, leading to minimal resource consumption, apt for resource constraint environment; converts the encoded data to plain text format, resulting in less upload time; provides data integrity with digital signature and verification process; helps the data owner to permit or restrict access to the health data; robust to malicious attacks; and abides to HIPAA privacy and regulation act. As our future work we eliminate the constraint over prime size to optimize system resource utilization in resource constraint devices.

8. REFERENCES

1. Nabil Sultan, "Making Use of Cloud Computing for Healthcare Provision: Opportunities and Challenges," International Journal of Information Management, Elsevier, 34(2014) 177-184, 2014.

2. Eman AbuKhousa, Nader Mohamed and Jameela Al-Jaroodi, "e-Health Cloud: Opportunities and Challenges," Journal of Future Internet (2012) 621-645, 2012.
3. Documentation for Health Insurance Portability and Accountability Act, http://health.state.tn.us/hipaa/.
4. Dawei Sun, Guiran Chang, Lina Sun and Xingwei Wang, "Surveying and Analyzing, Privacy and Trust issues in Cloud Computing Environments," Advanced in Control Engineering and Information Science, Elseiver, 15 (2011) 2852 – 2856, 2011.
5. Suraj Pandey, William Voorsluys, Sheng Niua, Ahsan Khandoker and Rajkumar Buyya, "An Autonomic Cloud Environment for Hosting ECG Data Analysis Services," Journal of Future Generation Computer Systems, Elseiver, 28(2012) 147-154, 2012.
6. Sandeep K. Sood, "A Combined Approach to Ensure Data Security in Cloud Computing, Journl of Network and Computer Applications," Elseiver, 35 (2012) 1831–1838, 2012.
7. Farrukh Aslam Khan, "A Cloud-Based Healthcare Framework for Security and Patients' Data Privacy Using Wireless Body Area Networks," The second International workshop on Communication and Sensor Networks (ComSense-2014), Elseiver, 34 (2014) 511 – 517, 2014.
8. Sangram Ray, G.P. Biswas, "Design of RSA-CA Based e-Health System for Supporting HIPAA Privacy-Security Regulations," 2nd International Conference on Communication, Computing and Security, Elseiver, 6 (2012) 954 – 961, 2012.
9. Danan Thilakanathan, Shipping Chen, Surya Nepal, Rafael Calvo, Leila Alem, "A Platform for Secure Monitoring and Sharing of Generic Health Data in the Cloud," Future Generation Computer Systems, Elseiver, 35 (2014) 102–113, 2014.
10. Sharma A, Ojha V, Belwal RC and Agarwal G, "Password Based Authentication a Philosophical Survey," IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS), volume 3, 2010.
11. Steve Gold, "Password Alternatives," Journal of Network Security, Elsevier, 2010.
12. Yun Haung, Zheng Haung, Haron Zhao and Xuejia Lai, "A New One-Time Password Method," International Conference on Electronic and Computer Science, 2013.
13. Cullen C, "Inherent Vulnerabilities of One-Time Pass-code Mechanism," Conference on Local Computer Networks, 1995.
14. Unar JA, Woo Chaw Seng, Almas Abbasi, "A Review of Biometric Technology Along With Trends and Prospectus," Journal of Pattern Recognition, Elseiver, 2014.

15. Ralph C. Merkle, One Way Hash Function and DES, Lecture notes in computer science, Springer-Verlag 435,428-446, 1990
16. Guido Berton, Joan Daemen, Michael Peeters, Gilles Van Assche, “KECCAK and the SHA-3 Standardization”, National Institute of Standards and Technology (NIST), 2013.
17. Advanced Encryption Standard (AES), National Institute of Standards and Technology (NIST), FIPS Publication 197, 2001
18. Taher Elgamal, “A Public Key Cryptosystem and A Signature Scheme Based on Discrete Logarithms,” Lecture notes in computer science, Springer 196, 10-18, 1985.
19. Phillip Rogaway, Nonce-Based Symmetric Encryption, Fast Sotware Encryption, Lecture notes in computer science, Springer 3017, 348-358, 2004
20. Health insurance portability and accountability act of 1996, public law, 104-191, 1996
21. Jiankun Hu, Hsiao-Hwa Chen, Ting-Wei Hou, “A Hybrid Public Key Infrastructure Solution (HPKI) for HIPAA privacy/security regulations,” Journal of computer standards and interfaces, Elseiver, 32 (2010) 274-280.
22. Shu-jen Chang, Ray Perlner, William E. Burr, Meltem Sonmez Turan, John M Kelsey, Souradyuti paul, Lawrence E. Bassham,Third round report of the SHA-3 cryptographic hash algorithm competition, NISTIR 7896, 2012
23. Edgar Danielyan, Avoiding sniffing attacks through encryption, Chapter 7, sciencedirect, 2001
24. Steve Kremer, Olivier,arkowitch, Jianying Zhou, “An Intensive Survey of Fair Non-Repudiation Protocols,” Journal of computer communications, 2002.