Available Online through  
www.ijptonline.com

SECURED HEALTHCARE DATE EXCHANGE USING PROPOSED SECURITY SCHEME

P.M. Durai Raj Vincent*
Assistant Professor (Senior), School of Information Technology, VIT University, India.
Email: pmvincent@vit.ac.in

Received on 04-05-2016  
Accepted on 30-05-2016

Abstract

Security providing is the most important agenda for any application depends on the sensitivity of the information shared. Security and confidentiality is the prime requirement for any information shared in internet. In order to share the health records under computing network environment is gaining its momentum as the need of such reliable system is always growing. When a system connected over internet always offers unlimited risks. If the connected system is deals with very sensitive information like patient health records then a reliable system should make sure the security and confidentiality for the data transferred between. This effective transmission will create an environment in which a patient can continue his treatment anywhere in the world under a networked scenario. This work aims to provide a security solution to such data transfer with the novel procedures for encryption and digital signature. The proposed approach uses public key cryptography as this approach will ensure complete security along with digital signature. Thus this paper will present the proposed approach to ensure the security for the data transfer.

Keywords: PKI, RSA, authentication, TLS.

1. Introduction

Internet is the gift of last century which rules this century where as an integrated hospital system will always provide a better treatment for the patient irrespective of the geo location of the availability of the patient in different time period. Especially in the modern world the types of diseases are keep on increasing and in emergency cases such type of system is required to save the lives. Thus integrating internet along with the health care is need of this millennium. This system will affirm the patients to travel across, irrespective of their health conditions. Because of the above said advantages health care applications are growing rapidly.
On the other hand such system will always require very strict security and privacy requirements. The requirement of such system will differ as the practical scenarios are vary like the data requirement in different scenarios like inside the hospital, pre hospital scenario as well during emergency and in the monitoring in home itself. It is always very dangerous if the record of any patient is tampered or corrupted. So very genuine and secured system is required to provide the security and access control. A secured network requires proper key establishment, confidentiality and privacy, integrity and authentication of the usage, availability of such system all the time, secure routing, setting up trust etc. The system will be available to the physicians to access the records of any patient from any particular location. During the requirement the physician will access those required information through internet and the actual data will be available in the data base. To access the data the data needs to be transmitted in which the potential vulnerability will be there to attack to tamper which may be intended to spoil the name of any popular hospital. But it will directly plays with one’s life. So such kind of tampering will not be allowed at any cast. Figure 1 shows the architectural diagram of the overall function in which the internet connects various systems which are located in remotely.

**Fig 1: Architecture Diagram**

Encryption is the process of converting plain text in to cipher text in order to hide the information during its transmission. The same mechanism can be incorporated here to protect the information. Such type of encryption will be
normally termed as symmetric approach and asymmetric approach. Symmetric approaches will use same key for encryption as well as for decryption where as asymmetric approaches uses two different keys for the above said processes. The later is the better approach because of the two different keys used. Even one key is compromised; it will not affect the security of the whole system as it cannot be used for both encryption as well as decryption. Either one is possible by a particular key. But this approach is not considered for any online application because of the huge execution time it takes compared to the other encryption system.

Because of the above said reason the symmetric approaches are considered for any online applications including health care. But the possibility of this approach is completely depends on the successful key sharing. Apart from data confidentiality it is necessary to verify the authenticity of the information received along with its integrity. In general digital signature algorithms are utilized to provide the same. Hash or MAC algorithms will provide this. Further to encryption process, the cipher text will be sent along with the hashed output which will be verified at the other end to ensure the security requirements.

Key sharing algorithm is an important requirement in this communication. As most of these approaches adopted with symmetric encryption algorithms, a secure key sharing process is required to ensure the secrecy to the data transferred. Many existing key sharing procedures are there which includes asymmetric key exchange algorithms because of its secured nature of data transfer.

By considering all the above discussed aspects a new security model will be proposed in this paper to secure the data exchange done for health care applications. The proposed approach will provide data confidentiality as well data authentication along with data integrity which is the required measures in order to facilitate any secured communication.

This paper will be organized as the second part will illustrate some of the related works done in this field followed by the proposed algorithm and the secured framework for the health care applications will be presented in the next chapter.

2. Related Work

This chapter presents the related work done in the field of health care to transfer data in order to facilitate an uninterrupted treatment to patients.

For medical analysis outsourcing of data is required which requires secure data transfer [13]. Fast algorithms are always required where such transfers should be done quickly. Here a search algorithm was proposed based on bloom filter by
which the privacy of the data is maintained. Public key based health care system was introduced in wireless sensor networks [5]. Patient’s privacy is ensured by this proposed approach. Since the patients are under continuous monitoring which requires authenticity of the information. This authentication and access control was the prime aim of this work which was proposed based on elliptic curve cryptography.

A secure mobile agent was introduced for telemedicine based on P2P networks [6]. Transmitting patient health information in telemedicine application was the aim of this work. This was tested in peer to peer networking environment. This was an agent based approach which was proved as a secured one.

Public key cryptography along with watermarking technique was introduced [7]. This is to securely transfer the images in which the keys will embedded in an encrypted image. The proposed approach was tested its results with the collected medical images. Secured web based medical applications were developed [8]. This one offers variety of security functionalities. A trusted third party was involved in this approach in order to generate and distribute digital certificates. PKI based secure mobile access to electronic health services data was presented [9]. This work incorporates public key cryptography in health care. Public key approach enabled protocol like Transport Layer Server provided various services required like confidentiality, authentication. Attribute certificates will ensure this trust model.

Healthcare Public Key Infrastructure was created for data exchange in health care [10]. This was to share health records by OCHIS an organization originated in Japan. It also proposed that a nonprofit organization can act as a trusted third party to be operated as a data centre for health care data communications. Privacy and integrity are the most important expectation of any patient of their medical records [11]. As these data storage got shifted from paper to digital, digital cryptographic methods were proposed to secure the data stored. Security issues of wireless networks in healthcare applications were discussed [12]. Some of its challenges which includes dynamic network topology, possibility of various attacks etc. Security solution also proposed again it is based on public key cryptography which will fight against any kind of message disclosure. Also this has ensured the complete security requirements. A fast approach was proposed [13] to transfer medical images. This was proposed based on visual cryptography for black and white images. Important advantage in this approach was there was no requirement for post processing of the image. The quality of the image is not get affected by this approach. Thus the various views on health care data protection during its transmission has presented and in the next chapter the proposed work will be presented.
3. Proposed security model

The proposed security model will be presented along with the algorithm to be used for providing data confidentiality.

This algorithm was already proved[2] as an efficient one compared to the other public key crypto systems.

The steps for executing the algorithm are given below.

**Algorithm: Public Key Generation**

**Input: Input variables ‘p’, ‘q’, ‘r’**

**Output: ‘s’, ‘e’ and ‘t’ values.**

Randomly select three numbers p,q,r and among this ‘p’ must be a prime number as also p should be less than the product of q and r (p<qr).

Based on the conditions given in the previous steps the corresponding values will be selected. Afterwards the given steps will be followed and the corresponding values calculated.

\[
s = qr - p \quad \text{(1)}
\]

\[
e = ps + r \quad \text{(2)}
\]

\[
t = p^2 s + q \quad \text{(3)}
\]

Now the public key will be calculated based on the step given below. Let the public key be ‘n’ and the calculation goes with,

\[
n = et - p \quad \text{(4)}
\]

After completing the tasks given in these steps, we will end up with various values like s, e, t and n. Now the key is generated and the public key is going to be <e,n>.

This value will be now shared with the sender in order to perform the encryption process. For this processing, any existing public key sharing technique can be used.

After receiving the public key pair <e,n> the sender will be going to encrypt the message. The sender is ready with the plaintext ‘M’ and performs the given step to perform the encryption process.

**Algorithm: Encryption**
Input: Plaintext

Output: Ciphertext

Let ‘M’ be the plaintext, Calculate the cipher text using the given formula

\[ C = M \times e \pmod{n} \]  \hspace{1cm} (5)

Thus the cipher text is generated from the plaintext. Now it is ready to transmit to the other end.

After encrypting the plaintext the sender will send the cipher text to receiver. Now the receiver needs to generate the private key in order to get back the original plaintext. Thus the decryption process starts with private key generation.

Unlike the traditional approach the proposed algorithm takes two steps to solve the equation to get back the private key.

**Algorithm:** Private Key Generation

**Input:** p, n and t

**Output:** Private key ‘d’

By solving the given equation ‘u’ will be calculated

\[ p \times u \pmod{n} = 1 \text{ and } 0 \leq u \leq n \]

calculate, \( d = u \times t \) \hspace{1cm} (6)

Now the private key is going to be \( <d, n> \)

Now comes the final step of getting back the original plaintext by performing following operation with the cipher text received from the sender and private key calculated in the previous step.

**Algorithm:** Decryption

**Input:** cipher text ‘c’, private key ‘d’ and ‘n’

**Output:** Plaintext ‘M’

Get back the original message by the given formula.

\[ M = C \times d \pmod{n} \] \hspace{1cm} (7)

Thus the whole algorithm is complete with this decryption process.
Further to this algorithm the procedure for securing the data transferred is given below. Normally symmetric key approach will be applied along with key sharing algorithm and digital signature algorithm will be used for ensuring data confidentiality along with message integrity and data authentication. Many familiar algorithms will be used in proving security for the content to be transferred over internet like RC4, Blowfish, AES. Similar to that digital signature algorithm like SHA versions used to be applied for having digital signatures. But here the proposed approach is different from this traditional procedure, The complete procedure will be explained in two different perspectives. The first one will be the operations should be done at the server side and the other one at the client side.

**Algorithm: Proposed framework steps at the server side**

**Step 1:** The required public and private key will be generated by both the sides.

**Step 2:** The key pairs will be shared mutually using public key sharing approach.

**Step 3:** Encryption of the data will be done with the public key of receiver’s using the algorithm given.

**Step 4:** Cipher text will be generated after the encryption will be applied to the same algorithm with the private key of its own.

**Step 5:** The final output which is generated after double encryption in the last step will be sent to the receiver.

The server side procedure is explained above. The double encryption is possible in this proposed model because of the algorithm used as the approach is based on public key cryptography. The first encryption is providing data confidentiality where as the next one providing digital signature because the second encryption is done with the private key of sender. Thus the operations done at the server side ensures the entire security requirement.

By sending the cipher text to the other end the process at the server side ends where as the given steps should be performed at the client side to get back the original information along with the proper verification.

**Algorithm: Proposed framework steps at the client side**

**Step 1:** The cipher text will be decrypted with the public key of the sender

**Step 2:** Further to the first decryption, next decryption will be done with the private key.

**Step 3:** After first two steps the information will be retrieved.

By applying the above steps shown the received information will be verified with data authentication and integrity.
Thus the proposed model receives the information with all the security requirement verifications and the data can be utilized for further treatment with 100 percent assurance.

4. Results and Analysis

This chapter will analyze the proposed framework with existing approaches. The proposed model mainly aims to reduce the response time in terms of lower execution time without compromising the security of the information transferred. The first comparison will show the efficiency of this algorithm with other public key encryption algorithms.

![Execution Time Comparison with RSA and ECC](image)

**Fig 2: Comparison with other public key techniques**

The above figure shows the comparison results between other two algorithms considered. Horizontal axis takes the input data size from 128 bits to 1024 bits which is represented in the graph. The results shows that the proposed algorithm is taking considerably lesser time compared to the other two algorithms taken. So it can be considered for the online applications on the other side the security of the algorithm also already proved.

The next comparison shows the proposed approach with the other possible combinations already in use for secured health care data exchange. All such familiar approaches are considered for this comparison is shown in the given figure.

![Comparison Results](image)

**Fig 3: Comparison with other approaches**
The above diagram shows the comparison of the proposed model with the other approaches which are used widely. From the figure it is proved that the proposed model will work faster than the other familiar approaches which is the desired property for any system which runs online. The execution time was taken in seconds. As various algorithm combinations taking different execution time, a constant input data size was fixed for this analysis say 1024 bits. This results were taken in a configuration of i3 processor with 2.4 GHz and 4 GB of RAM and for a fair analysis each combinations were executed for five times in order to optimize the results in a better way and average of time was considered for analysis.

Thus the proposed model proves its fast execution as well as secure nature over other algorithms which are currently utilized for providing security in health care applications. So the proposed model should be considered for applications which are used for human lives.

**Conclusion**

Any online application requires trust over it to succeed which is quite possible if such system is secured. When it comes to health care data exchange such secured data transfer is the top most priority as the process involves with human lives. In this we have presented a secured model which will ensure data confidentiality, data integrity as well data authentication. The proposed model’s efficiency was already proved through various results shown. Thus the proposed model should be considered for transferring data in health care industry. In part of future work we will consider including certifying authority to facilitate the whole process.

**References**


**Corresponding Author:**

**P.M. Durai Raj Vincent,**

**Email:** pmvincent@vit.ac.in