Chapter 5

Design and Development of Threshold Protocols for E-Health Insurance System
DESIGN AND DEVELOPMENT OF THRESHOLD PROTOCOLS FOR E-HEALTH INSURANCE SYSTEM

This chapter discusses about the Protocols proposed for secure transactions in e-health insurance system. Section 5.1 gives information about protocols and their necessity in transactions with third party for client or insurance company. Section 5.2 to Section 5.5 discuss about protocols designed and implemented using Proposed MASDMA and $S^2$FRSA algorithm. Finally conclusions are drawn from this chapter are stated.

5.1 Introduction

This chapter presents the design of a family of e-Health insurance transaction protocols based on Multi Attribute Secure Decision making algorithm and $S^2$FRSA cryptosystem for e-Health Insurance System. The transactions mainly focuses on the Registration of an Insurance Company with Third Party, Registration for Client with Third Party, Security Protocol for Exchange Clients data between Third Party and Health Insurance Company (HIC), Security Protocol for Exchange Clients data between Third Party (Health Services Portal Server (HSPS), and Hospital Server (HS), Security Protocol for Exchange Clients data between HIC and Hospital Server (HS) for payments or verification and sharing the data[27]. These protocols satisfy the following things.

1) Non-repudiation—to provide protection against false denial of transmission or reception of electronic items (contracts signing, certified e-mail delivery, e-payment and e-Medical-diagnosis delivery, e-decisions regarding health insurance in this context);

2) Strong fairness—to ensure that all parties like insurance company, third party, hospital participating in an exchange process receive either the expected items or neither party receives anything valuable. In addition, the following requirements have been identified in order to provide end-to-end security for transactions:
(3) User authentication and access control – to ensure that the transfer and exchange services can only be accessed by authenticated third part or client or insurance company authority.

(4) Accountability – to allow secure logging and management of records of client medical diagnosis and transactions undertaken within the system, so that all users are accountable for their actions. This requirement is necessary for potential dispute resolution.

(5) Data confidentiality – to prevent parties other than IC, Client, TP to involve in exchange process from gaining any information of data being transferred.

(6) Data integrity – to prevent parties other than IC, client, TP involve in exchange process from unauthorized alteration of data of client medical data being transferred.

This chapter proposes protocols [27] between Insurance Company, third party, client and Hospital for secure exchange of data in e-health insurance.

5.2 Registration protocol for Insurance Company with Third Party

This protocol is designed for secure registration of Insurance Company(IC) with Health Services Portal Server (HSPS). This protocol allows the Insurance Company to register itself in HSP Server which allows clients to select the company for health insurance benefit[27].

The sequence diagram Fig: 5.1 shown below represents the communication between the each object is as follows. There are four objects they are Insurance Company, HSP server, Session, HSPDS server.

1. Insurance Company (IC) Request for Connection establishment to HSP Server

2. HSP Server Creates the Session for Insurance Company for future Communication

3. HSP Server responds to IC by establishing the Connection.

4. Insurance Company IC will send its data to HSP server.

5. HSP Server will generate unique-Id ‘h’ for IC which acts as UserId for further communication.
6. HSPS server generates the prime number 
set \( P_i \) by using data of IC.
7. HSPS uses the largest prime \( P_i \) and uses fields to compute \( f^* \).
8. HSPS uses S^{2}FRSA to encrypts data and generates key \( V_k \)
9. HSP Server uses \( V_k \) for verification of Insurance company
10. HSPS sends \( V_k \) as IC Verification Card with photo identity and encrypted data to IC and stored in HSPDS.
11. IC sends response Ack to the HSP Server
12. HSP Server closes the Session with IC.

Figure 5.1 Represents the Registration protocol for Insurance Company with Third party portal

102
The following Activity diagram represents the step by step process of Insurance Company registered with the third party portal.

Fig 5.2 Activity Diagram for Registration Protocol for Insurance Company with Third Party
The Insurance Company Sends request to HSP Server for establishing connection, HSP server creates the session for Insurance Company for future Communication. HSP server creates and sends $V_k, h$ to Session and Insurance Company and establishing the Connection. Then starts the communication between the IC and HSP server, the IC sends data to HSP server, the server Authenticates the who’s data using unique-Id ‘$h$’. HSP Server generates the prime number set $p_i$ from that it selects the largest primes $P,Q$, then generate the verification key $C_k$

HSP Server verifies the users using the verification key $C_k$ and give the appropriate response to the request and finally close the session.

The above activity diagram in figure 5.2 represents the steps executed as part of protocol between the Insurance Company and third party health services portal. The Insurance Company registered with the complete details regarding the company like establishment year, customer strength, employee strength, profit of the last year, success rate, company Email, mobile number etc. this information is helpful to insurer to select the best company based on the success rate of the company.

The third party Health service portal helps to insurer/customer to select the best company, it suggests the list of the companies is preferable and list of the companies are not preferable. The insurance company registration is very benefit to itself, because it gains the customers very easily based on their success rate.
5.3 Registration Protocol for Customer/Client with Third Party[27]

This protocol is designed to secure registration of Client with Health Services Portal Server (HSPS). This protocol allows the Client to register itself in HSP Server which sends required clients data to client selected the company for health insurance benefit.

Fig 5.3 Represents the Registration protocol of client with Third party portal
The above sequence diagram represents the communication between each object as follows. There are three objects, they are Client, HSP server, Session.

1. Client Request for Connection establishment to HSP Server
2. HSP Server Creates the Session for Client for future Communication
3. HSP Server responds to Client by establishing the Connection.
4. Client will send his data to HSP server regarding registration.
5. HSP Server will generate unique-Id ‘k’ for Client which acts as User ID for further communication for secure data exchange.
6. HSPS server Generates the Prime number set P by using data of client
7. HSPS Select the Largest Prime Q relatively prime to P and also finds \( f^* \).
8. HSP Server uses \( S^2 \text{FRSA} \) Generates the Verification key \( C_k \)
9. HSPS sends \( C_k \) to client as Health Insurance card with photo identity and encrypted personal data
10. Client sends response Ack to the HSPS Server and stores HI card in HSPD server.
11. HSP Server closes the Session with Client.

The following Activity diagram represents the step by step process of Client registered with the third party portal.

The Client Sends request to HSP Server for establishing connection, HSP server creates the session for Client for future Communication. HSP server creates and sends Unique-ID for exchange of data between Session and Client after establishing the Connection. Then starts the communication between the Client and HSP server, the Client sends data to HSP server, the server authenticates the data using unique-Id ‘h’. HSP Server generates the prime number set \( p, q \) from that it selects the largest primes \( P, Q \), then generate the verification key \( C_k \) along with \( f^* \) from \( S^2 \text{FRSA} \) and sent to Client as HI card.

HSP Server verify the users using the verification key \( C_k \) Health Insurance Card (HICard) and give the appropriate response to the request and finally close the session.
**Fig 5.4 Shows Activity diagram of Registration process of Client with Third party.**

The above activity diagram shows sequence of steps representing the Registration protocol between the client/insurer and Health Service portal. This implements the above protocol (Registration Protocol for Client with Third Party) The client registered with his/her simple information like name, email, Date of birth, mobile number. The registered clients only use this portal to apply the insurance in the online for different companies. This portal combines together the insurance
companies and clients. The third party Health Service portal helps to client to select the best company and best hospital and suitable insurance for your bio-data. The client don’t bothering about the decision to select the hospital and insurance company, it provides the more suggestions with clear information. So the clients easily select the insurance company and hospitals.

5.4 Registration Protocol for Hospital with Third Party[27]

This protocol is designed for secure registration of Hospital with Third Party which has agreement with Insurance Company which is already registered with Health Services Portal Server (HSPS). This protocol allows the Hospital to register itself in HSP Server which can access clients data registered with third party when he becomes patient in Hospital. At the time of registration HSP Server generated Hospital Identification Card which is used by Hospital authorities to access Clients data at HSP server.

![Diagram of Registration Protocol](image)

Fig 5.5 Represents the Registration process of Hospital with Third party portal
The above sequence diagram represents the communication between the each object is as follows. There are three objects, they are Hospital, HSP server, Session.

1. Hospital Client (Hospital Server) HS Request for Connection establishment to HSP Server
2. HSP Server Creates the Session for Hospital Server (HS) for future Communication
3. HSP Server responds to Client by establishing the Connection.
4. HSP Server will generate unique-Id for Client which acts as User ID for further use.
5. HS will send its data to HSP server regarding registration.
6. HSPS server uses $S^2$FRSA to encrypt hospital details.
7. HSPS server generates Hospital Identification Card to verify to access patients data by hospital authorities.
8. HSPS sends Hospital ID cards with photo identity and encrypted details of hospital.
9. HS sends response Ack to the HSPS Server
10. HSP Server closes the Session with Client.

The Hospital authority/Client Sends request to HSP Server for establishing connection, HSP server creates the session for Client for future Communication. HSP server creates sends Session ID (as OTP) to Client after establishing the Connection. Then starts the communication between the Client and HSP server, the Client sends data to HSP server, the server Authenticates data using unique-Id ‘h’. HSP Server generates the prime number set $p$, from that it selects the largest primes $P,Q$, then generate the verification key $C_h$ by using $S^2$FRSA and creates Health Card with ID and encrypted data which can be used by HSP Server verify the user with verification key $C_h$in it and give the appropriate response to the request and finally closes the session.
5.5 Security Protocol for Exchange Clients data between Third Party and Health Insurance Company (HIC).[27]

This protocol is used for exchange of client’s data between HSPS and Health Insurance Company HIC, HSPS uses Secure Field RSA (S^2FRSA) to generate key which is used to decrypt only fields required for insurance processing and thus hiding remaining fields that are not required for security purpose.

The above sequence diagram represents the communication between the each object is as follows. There are three objects; they are HIC, HSP server, and Session.

HIC requests for connection establishment with Health Services Portal Server(HSPS)
1. HSPS creates a session for HIC for further communication.

2. HIC acknowledges and requests the Clients details for insurance processing.

3. HSPS validates personal data of Client from clients health card and generates ‘p, q’ value to compute e and φ (n)(uses $S^2FRSA$)

4. HSPS computes d value such that $d = e^{-1} \mod (\phi(n))$, public key for decryption purpose for HIC

5. HSPS chooses random integer ‘h’ such that $x = (f^h)^c \mod (n)$ used for sending data securely.

6. HSPS accepts fields r,s,t of data required for HIC for generating key.

7. HSPS uses $S^2FRSA$ to generate key $d = fd + rst + sd$ where fd,sd are part of private key $k$.

8. HSPS sends private key is (x, d, n) to HIC

9. HIC acknowledges the key which is used for secure exchange of data.

10. HSPS closes the session with HIC.
The following sequence diagram represents the step by step process of the security protocol for exchange the Client data between HIC Hospital Server for Payments.

Fig 5.7 Represents the Exchange Clients data between Third party and Health Insurance Company.
Fig 5.8 Activity Diagram showing the Exchange Clients data between Third party and Health Insurance Company.
5.6 Security Protocol for Exchange Clients data between Health Insurance Company and Hospital Server (HS) for Verification/Payment.[27].

The above protocol is used in secure exchange of data between Health Insurance Company and Hospital authority for payments or other verification purpose by Insurance Company. The Health Insurance Company requests for the connection to Hospital Server, then the Hospital Server verify and create the Session. Once establish a connection, the HIC Requests the Patient data from Hospital Server. after verification with its Insurance Company ID card, Hospital Server sends the patient data in an Encrypted format and also specified attributes (columns) only using S^FRSA.

![Diagram of the Security Protocol]

*Fig 5.9 Represents the process of exchanging the Clients data between Hospital Server and Health Insurance Company.*
This protocol is used for exchange of client’s data between HIC and Hospital Server (HS), Health Services Portal Server (HSPS) uses Selective Secure Field RSA (S²FRSA) to generate key in form of Health Card which is used to decrypt only fields required for Hospital and thus hiding remaining fields that are not required for security purpose.

The sequence diagram above represents the communication between the each object is as follows. There are three objects; they are HIC, HS server, and Session.

1. HIC requests for connection establishment with Hospital Server(HS)

2. HS creates a session for HIC for further communication.

3. HIC acknowledges and requests the Patients/Clients details for health diagnosis data for payment.

4. HS sends the patient data which is encrypted by using S²FRSA.

5. HIC uses secret key (x, d, n) given in Health Card to decrypt Clients Data(CD) which is decrypted as \( y = x^d \mod (n) \)

6. HIC obtains \( CD = C^d \mod (n) - y \)

7. HIC verifies and computes Payments and S acknowledges the HS

8. HIC closes the session with HS.

The HIC receiving the patient data then it will be decrypt using the key of that patient, that key holds the restricted fields, those fields are not visible to the HIC, and finally close the session.
Fig 5.10 Represents the each activity of Exchanging of Clients data between Hospital Server and Health Insurance Company for verification.
The above Figure represents the Health Insurance Company request the Hospital Server for viewing the customer details as select the “View Customer Details” option in the figure. When it selects that particular option then the server provides only specific fields because some fields are restricted. Where HSP server validates the client’s data and restricts the some fields, so the remaining fields only available to insurance company by verifying its Health Card.

The HSP server generates the primes \( p, q \) and computes the \( e, d \) and \( \phi (n) \) are used in the \( S^2\)FRSA (Select Secure Field RSA). The HSP server restrict the fields is as follows. The above figure 5.8 represents the client fields are restricted by the HSP server (ADMIN). These fields are not available to Insurance companies as the Admin restrict the fields based on their insurance type.

5.7 Conclusion

In this chapter we have proposed protocols for registration of Insurance company or Client or Hospital with Third Party, exchange of data regarding decision making or for verification of clients data between stake holders in the health insurance process securely which is depicted in sequence diagrams and activity diagrams. The proposed protocols ensure a secure transactions in e-health insurance system.