Chapter- 1

Introduction
INTRODUCTION

1.1 Introduction to Health Insurance

Health component plays a vital role in human society for comfortable and convenient living various health technologies are on the use today to provide good health and a lot of health care institutions are extending their services to human kind. The computerized health management attracting more attention in the contemporary society to provide much better health care at low-cost for a common man. The term health insurance is the facility that covers medical expenses for an individual or entire family group. A health insurance policy is a contract between insurer and an individual/group in which the insurer agrees to provide specified health insurance coverage for financial assistance at a particular “premium” for over a period of time. The health insurer usually provides either direct payment to hospital (cashless facility) or reimburses the expenses associated with illnesses and injuries or disburses a fixed benefit on occurrence of an illness after providing the proof. The number of people, amount of health care costs and time of policy coverage will vary according to the health plan which the client opts for.

In countries like India where middle class occupies more than 60% of population, health insurance is essential which will give financial coverage against the medical expenses among individuals and groups due accidents or sudden illness. By estimating the overall risk of health care and health system expenses, among a targeted group, an insurer can develop a routine finance structure, such as a monthly premium or payroll tax. It was to ensure that money is available to pay for the health care benefits specified in the insurance agreement. The benefit is administered by a central organization such as a government agency, private business, or not-for-profit entity. It is necessary to have a Medical Health Insurance Policy against crippling illnesses or death. Moreover, in such cases hospitalization and medication expenses can be unaffordable. Medical Health Insurance to every common man can prove to be a source of relief by taking care of financial burden, your family may have to go through.
The accurate and comprehensive health care information is critical to the quality of health care delivery for physician-patient relationship. The efficacy of the health care relationship depends on the client's understanding that the information recorded by Insurance Company or physician will not be disclosed to third parties. Without these assurances, many clients applied for health care facilities might refuse to provide physicians with certain types of information needed to render appropriate care [7]. Currently there are large insurance companies offering various health care services for customers to choose best among them. So the companies are offering expert system advisor which helps customer to calculate the risk involved in making decision and taking on or endorsing a particular insurance policy. Expert system based on simple attributes like premium, salary of client will come to decision for suggesting best policy for client [8] but not the hospital for which the client offering.

For online Insurance activities E-Health Insurance System (EHIS) refers to a range of transactions undertaken among Patients, Doctors, Health Insurance Providers and Third party Health services provider. If these services are involved, which are at least supported by an electronic communication network such as the Internet. These activities include payment of medical health insurance premium installments (e-payments [9]), payment of patient's medical treatment bills (e-payments), and transfer of patient's laboratory, clinical reports and medical treatment report (e-Medical-diagnosis).

Use of Internet as an underlying communication facility for EHIS, has many advantages. It is a relatively cheap and widely available medium. Internet has enhanced the accessibility of a large number of Patients base to on-line services. Further it enables Doctors, insurance companies to reach out to more Patients. The Internet provides five advantages: saves time saves money by cutting appointment trips; reduces paperwork; time to negotiate; and to quick performance of needy transactions.

The main disadvantage of Internet is being an open and inherently insecure environment. Committing fraud over the Internet is relatively easier: as attacks can occur remotely. Further the parties (Patients, Doctors, insurance companies and Third Party Service providers) may easily act under false identities
and can disappear during or after transaction. In addition, dispute resolution over the Internet is time consuming because many countries still do not have legal on-line regulations. The exchange of data between parties involved in insurance is based on protocols. It should be secure in terms of data storage and decision making. Each stakeholder in transaction should be given authenticity only on data required, while the remaining data should be kept in secret. In healthcare systems security plays a crucial role in various aspects. The authentication of patient who has right to benefit health services and privacy of patient health are some of well-known ones. Health Insurance Companies (HIC) purchasing health service for their customers face with serious security breaches [19]. With flaws in security has resulted in the threat of e-crime [20] becoming bigger than that from old-fashioned robberies. Consequently, a serious lack of trust is present between Patients, doctors and Insurance companies.

The need to increase level of trust among Patients, doctors, Insurance companies and Bank on the Internet and counter security threats has increased the dependency of e-Health Insurance System on security technologies. The protocols for Secure e-Health Insurance System facilitates trustworthy of communications, where transactions are exposed to attacks from external as well as internal entities. If parties feel that they are likely to get involved in disputes with other parties due to online transactions, their interests should not only be protected but also should attract more clients to use EHIS in a satisfactory manner. Fairness and non-repudiation [1] are the two services required to addresses this problem.

1.2 Preliminaries of Security

Various Security attacks on data through the network like passive attacks, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider, phishing attacks, spoofing have proliferated in recent years. Hence securing the data is a major issue with a serious concern in many fields, since the data being shared among different services (users) through distinct computing techniques. Various security mechanisms have proposed to ensure the data security which relies on cryptographic techniques like symmetric encryption, asymmetric encryption, data integrity techniques, authentication protocols etc. We define security as, “the combination of confidentiality (the prevention of the unauthorized disclosure
of information), integrity (the prevention of the unauthorized amendment or deletion of information), and availability (the prevention of the unauthorized withholding of information)." [33] The various techniques of security assure five important aspects:

- Confidentiality
- Integrity
- Availability
- Authentication
- Nonrepudiation

Large amounts of data are produced by Health Insurance Companies daily by adding new clients or storing reports of existing clients which should be protected by stronger security measure. Even though various security techniques have been used for protecting patient data, insurance data, decisions of client but they are not sufficient as technology improves day by day. Use of information technology allows atomization of process for extraction of data. It helps to get interesting knowledge and regularities. It also means the elimination of manual tasks and easier extraction of data directly from electronic records. It is by transferring onto secure electronic system of medical records which will save lives and reduce the cost of health services. Further it enables early discovery of contagious diseases with advanced collection of data. Various expert decision making systems use various Data mining techniques to predict trends in the clients conditions and their behaviors. It is accomplished by data analysis from different perspectives and discovering connections and relations from seemingly unrelated information. Health Insurance data mining provides countless possibilities for hidden pattern investigation from these data sets [6]. The decision making systems should be secure enough to make clients decisions secret and hidden, and not to be used by other Insurance companies for attracting customers. The expert system which makes decision regarding e-health insurance can be implemented as service in cloud [10] which is the latest computing technology.

1.3 Problem Context

In general, an E-Health Insurance System transaction represents an exchange on patient’s data, e-Medical-diagnosis (i.e. all laboratory, clinical reports and medical treatment report with respect to a patient) and e-payments (the premiums that a patient pays to insurance company and the payments it pays to a doctor). Leaking of
information to insurance company may lead to problems, which in turn may sell the data to other companies which may cause problems to clients. Also for instance, a patient pays his Medical Health Insurance premium installment and if he finds later on that his premium installment is not credited into his account, then it is not an e-medical transaction [33,28]. In e-health insurance the customer who is in need of insurance, this system will assist him to take decision in selecting appropriate Health insurance organization and Insurance policy according to his requirement given in training dataset which is not present in existing Insurance expert systems. The decision making system by the third party will allow clients to execute protocols securely between Patient / client and Insurance Company (IC), Insurance company and Hospital Management, Hospital and Patient.

Most popularly used Asymmetric cryptosystem is RSA named after authors Ravest,Shamir,Addleman [25] which specifies key up to size of 512 bits for secure exchange of data in protocols. In RSA there is no restriction to display data depending upon requirements i.e., patients data that is required for Doctor, Patient data that is required for IC. Patient’s personal data is essential for IC except the diagnosis report from hospital to which IC will pay. In an era where consumers are increasingly concerned about the privacy of their personal information. The health privacy protections are intended to provide consumers with similar assurances that their health information, including genetic information, will be properly protected. Under the Privacy Rule, health plans, health care clearinghouses, and certain health care providers must guard against misuse of individuals’ identifiable health information and limit the sharing of such information, and consumers are afforded significant new rights to enable them to understand and control how their health information is used and disclosed.

The thesis focuses on secure protocols for exchange of Clients / Patients data between Third party, IC and Hospital for decision making and payments. It is crucial to ensure that such exchanges are fair. Either E-medical transaction is a security service that guarantees that at the end of an exchange process, all parties receive the items that they expect or none of them receive anything. For example, e-medical transaction involves securing patients data secure, and only reveals required data or fields in to either IC or Doctor who is responsible. Similarly, to ensure fair contract-
signing scenario, or in making decision for selecting hospital or patient we must ensure security. They require fairness and non-repudiation protections in order to make the overall e-Medical-diagnosis process secure. Moreover, apart from being substantial parts of more complex processes, contract signing and certified delivery are also important transactions on their own. Our thesis focuses on providing solutions for decision making in E-Health insurance by designing protocols for achieving e-medical transaction securely for these transactions.

1.4 Research Hypothesis

In this dissertation, it is designed and implemented a threshold Public Key Cryptosystem known as Selective Secure Field RSA (S²FRSA) for encryption and decryption of required fields of data in transmission and storage instead of RSA which reveals entire patient record when private key is given. In this thesis third party provides EHIS services allowing client to make decisions regarding IC, Policies and even hospitals depending upon multiple attributes of clients like occupation, location, premium, group coverage etc. by using EHDMA(E-Health Decision Making Algorithm). For a secure decision of clients at third party portals it is developed Multi Attribute Secure Decision Making Algorithm (MASDMA). The prime focus is to view only specific data intended for party for completion of transaction. The protocols have been designed for data exchange between Client and IC, Patient and Hospital management, Third party service provider and Hospital securely. The above protocols are provided security based on work related to protocols in E-commerce using dual signature schemes in [30].

It is examined about the main problems that are to face with achieving e-Health insurance system transaction over the Internet. It is considered of traditional treatments, fairness in such treatment is achieved trivially. For instance, when a doctor prescribes a treatment to a patient for a course (i.e. week time), the patient may take course for two or three days and claims for full treatment expenses from IC or entire patients data if revealed to insurance company or Hospital authority there may arise a chance of manipulation in payment to Hospital by IC. At the time of registration with IC, the patient should select various schemes available depending upon ones income, occupation, number of family members
etc. Use the solicitor as Insurance Server to make sure that client has rightly selected the scheme and data is exchanged fairly. In all these cases, fairness is achieved by exchanging the items simultaneously.

Secure EHIS, on the other hand does not have the support for these facilities. In such circumstances, it is difficult to guarantee transaction between mutually distrustful parties. For instance, if a doctor after giving treatment to a patient but the PMHIP may reject for e-payment by aborting the communication. Resolving a dispute over such a e-medical transaction is difficult due to yet undefined e-Medical Health Insurance System regulations and difficulty in tracking down the culprit of the transaction.

It is termed Third party as E-Health Services and the server as Health Services Portal Server (HSPS) has to be employed to help the parties (Client/Patient’s, Doctor’s, and IC) for exchanging data between them securely. Generally, the role of the EHIS is to re-balance unfairness for the party (Patient, Doctor’s, and IC) that releases his items first. However, the level of the EHIS’s involvement was high, and its availability was crucial for the correct functioning of the exchange. Furthermore, the EHIS needed to have full access to the exchanged items, which therefore did not enjoy the confidentiality protection.

It is to analyse the above-mentioned transaction; we have noticed a common feature that they involve an exchange of a digital signature for either another signature. Our research hypothesis was to design and develop appropriate protocols to implement e-Health Insurance transaction and to achieve encrypting data by using our threshold $S^2$FRSA signature scheme with single public key and private key which will display only a specific data in a specific way for a specific user. So that the recipient could verify that encryption [27] contains the correct signature, but cannot obtain it before releasing his item, at which point he would in turn receive the signature decryption key from the sender. If the key could also be made recoverable by an agreed EHIS, then the receiver would be safe to release his item first, as-even if the sender refused to surrender the key after receiving the recipients item- the EHIS could recover the key for the recipient. In addition, by making EHIS deal only with decryption keys and not with items themselves we could prevent disclosure of the exchanged items to it, thereby preserving their confidentiality.
1.5 Aim and Objectives

The aim of this thesis is to develop threshold cryptosystem which is used to provide security solutions for design and development of protocols. These are meant to provide fairness and non-repudiation services required. Further it is to safeguard the transactions in E-Health Insurance System. By ensuring these services, it is aimed at helping patients and doctors to overcome the distrust in engaging in ad-hoc e-Health Insurance transactions with other IC’s over the Internet. There by it increases their confidence in securing Insurance System protocols by using \( S^2F\)RSA cryptosystem.

In order to achieve above aim the following objectives of this thesis are formulated. It is to

1. Propose a threshold decision making algorithm for selecting Insurance company/Policy

2. to propose efficient threshold public key cryptosystem for secure e-Health Insurance service protocols,

3. to design a system for generation of symmetric secret key by the parties (Third Party, Client, Hospital, Insurance Company) themselves,

4. to design a system for making decisions at third party for client with EHIS for selection of insurance scheme and hospital suitable for him depending upon the client data set,

5. the Publication of public keys and Distribution of private keys among Third Party, Client, Hospital, Insurance Company, and to

6. Design and development Protocols for exchange of data between parties (Third Party, Client, Hospital Management, Insurance Company) and during decision making at selection of insurance schemes and hospitals. The above Protocols are implemented as web application based on Secure E-Health Insurance Model as given in [29].
1.6 Scope of the Research Work

The scope of the research work is to design and develop a secure protocols during transactions between Third Party, Insurance Company, Hospital and Client, during decision making purposes for client in selecting hospital and insurance plans. In this research it is aimed to develop a secure Cryptosystem namely Selective Secure Field RSA (S²FRSA) for securing clients data from insurance company as well as with hospital management. The proposed public key can be used to tackle the vulnerabilities existing in E-Health Insurance to some extent.

The outcome of the thesis and its applicability is framed as follows:

1. In the first phase, it is designed and implemented Selective Secure Field RSA (S²FRSA) Public Key Cryptosystem which contains three phases viz. Key generation, Encryption, and Decryption. In the Key generation phase, we obtain a public key and private key pairs for each Insurance company/Hospital for which limited patients/clients data is visible. By Combining S²FRSA and decision making algorithm we have developed a new algorithm MASDMA (Multi Attribute Secure Decision Making Algorithm) which allows client to make decisions regarding Hospital and Insurance scheme.

2. In the second phase, it is to examine the important contributions of existing decision making protocols in E-Health Insurance which have led us to design and develop protocols for E-Health Insurance [27].

3. In the final phase, it is designed to a model for Secure E-Health Insurance System [29] by ensuring security to the data in storage as well the protocols that used in authenticating users, data sharing between Third party, Hospital and Insurance Company.

It implements the S²FRSA Public Key Cryptosystem along with MASDMA in Java and tested the same with sample data and obtained the results as per the hypothesis and applied in the E-Health Insurance System web portal which is developed by using JSP.
1.7 Dissertation Organization

The contribution of the thesis entitled "Design and Development of Secure E-Health Insurance Decision Making Protocols", introduces a $S^2$FRSA cryptosystem for securing data during transactions between various entities participating in process and developing protocols used for decision making by client for opting for insurance. The thesis is organized as stated below:

CHAPTER 1

This chapter explains the overview of the problem and discusses about the necessity for a Medical Health Insurance policy, and gives outline about our current problem context and the need for Third party in EHS. Aim and objectives of this research work are given along with our achievements and novel contributions. This chapter presents the outline of the thesis.

CHAPTER 2

In this chapter, is to thoroughly examine and exercise earlier research works done in the field of Health Insurance regarding decision making and security which figures out some gaps in the current context. The study of various research works and HIPAA (Health Insurance Portability and Accountability Act) have led us to think a solution to the problem of data threat by ensuring the Confidentiality, Integrity, Availability, Accountability, and Nonrepudiation [10]. Some research results have motivated the researcher to design this new cryptosystem to give solutions to the existing security issues which can be applied in protocols designed for Data exchange and decision making.

CHAPTER 3

In this chapter, we examine the RSA algorithm and its usage in decision making to withstand attacks for achieve possible solutions in handling the threats, a new threshold Selective Secure Field RSA($S^2$FRSA) Public Key Cryptosystem in contrast to RSA is given in detail along with results and graphical analysis. In this Chapter we disclose a new threshold algorithm (MASDMA) is designed by combining with cryptosystem proposed ($S^2$FRSA) to address existing problems in protecting client’s decisions and data from Insurance agents and hospitals. Here, the results of proposed designed algorithm is given with sample data sets regarding client’s decisions.
CHAPTER 4

This Chapter gives a description and study of existing decision making algorithms in Health insurance System along with their pros and cons in current context. By analyzing the above facts in this chapter it is explained the proposed threshold decision making algorithm along with the results and analysis using available data sets.

CHAPTER 5

This chapter is dealt with design, development and analysis of the proposed protocols [12] used in data exchange and decision making using S²FRSA cryptosystem. The protocols designed are

✓ A Health Services Portal (THIRD PARTY) and Insurance Company
✓ Health Services Portal and Client
✓ Third Party ,Health Insurance Company
✓ Third Party, Hospital
✓ Health Insurance Company, Hospital

CHAPTER 6

In this chapter, the new model of Health Insurance is designed to be given with necessary implementation details. The proposed new model "Secure E-Health Insurance Model "[27, 28,29] is designed and implemented as a web application. It encompasses designed protocols with the application of MASDMA, S²FRSA Cryptosystems for securing the storage and exchange of data between Third party, Client, Health Insurance Company and Hospital management.

CHAPTER 7

This chapter is intended for the conclusions related to the entire thesis and suggestions for further openings.

Thus the thesis is designed to have seven chapters. It also provides a compact/detailed bibliography besides charts, tables and other illustrations to strengthen the present thesis.