Conclusions and Future Work
CONCLUSIONS AND FUTURE WORK

The introduction part of the thesis projects, the idea of health insurance and the importance of security to insurance data, the thesis presents its decisions regarding insurance company selection and protocols employed in exchange of data among client, insurer and the third party. The possible approaches and presented in this work. Various solutions arrived contemporary problems of security and confidential in various areas of computer science are discussed with comparison between older to latest technologies. In final chapter, I will conclude by describing how my work was developed and implanted through third party managed web portal. Finally suggestions regarding some future research directions are given which could enhance value of the work along with the path to a practical and widely used application.

7.1 Conclusions

Security is major concern in various walks of life including insurance. In health insurance organizations there is a possibility of copying and keeping patients electronic health records (EHRs) through portable storage media, they will encounter new risks to the protection of their private information which should be dealt carefully along with their decisions in this competitive insurance market. So as to ensure security to insurance data is to new techniques of security is studied and proposed.

Health insurance, a vital aspect posing and drawing much attention in the contemporary society, modern man with the help of medical aid support extending the longevity compared to the days before, the technological advancements in the areas of biomedicine and the supportive computation techniques in this areas improves the potency of biomedicine application to the human kind to enhance the longevity and provides means for comfortable and peaceful life, with a view to support the present work is undertaken The Design And Development Of Secure e-Health Insurance Decision Making Protocols. The basic RSA employed encrypt and decrypt the health data obtained from sources like public and private hospitals then secure field RSA of the proposed present work enhanced the health management data by the insurance and allied companies for the benefit of the patients under health coverage insurance areas.
Health insurance is part of health care data which faces following threats such as unauthorized access to physician pages, unauthorized access to patient pages, confidentiality and integrity of patients insurance data, the patient information may be given to other people in which case patient privacy is violated, an insured person may give his card and information to a non-insured person. If a physician is cheated or agreed, a person who has no right to benefit from HIC may use health services, an insurance company may give client’s data to another company, third party service provide may leak unnecessary information or clients decisions to insurance company which may lead to violation of privacy of patient.

In the course of this research work, efforts are made to address above threats discussed we have designed and develop a new cryptosystem Selective Secure Field RSA (S²FRSA) for insurance data where a limited data only will be exposed to insurance company by third party service provider to provide security services like confidentiality, integrity, authentication, and non-repudiation for client’s data for applications running on internet.

In this thesis the aim is to propose security solutions for design and development of protocols. Further it is to safeguard the transactions in E-Health Insurance System to avoid patients and doctors to overcome the distrust in engaging in ad-hoc e-Health Insurance transactions with other Insurance Company’s over the Internet.

The following objectives of this thesis are formulated to achieve the above aim:

1. Propose a threshold decision making algorithm for selecting Insurance company/Policy,
2. Propose efficient threshold public key cryptosystem for secure e-Health Insurance service protocols,
3. Design a system for generation of symmetric secret key by the parties (Third Party, Client, Hospital, Insurance Company) themselves
4. 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. Publication of public keys and Distribution of private keys among Third Party, Client, Hospital, Insurance Company, and

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.

The proposed Selective secure Field RSA($S^2$RSA) public key Cryptosystem is implemented in Java language which contains three phases viz. Key generation, Encryption and Decryption. The Cryptosystem can be applicable to the computer applications which require security to the data during transmission over the networks, Data sharing, and the data storage. $S^2$RSA algorithm is implemented and the analysis compared with existing security techniques and results are published.

For purpose of decision making a new algorithm Threshold Multi Attribute Secure Decision Making Algorithm (MASDMA) with $S^2$RSA used to secure decisions with multiple attributes are chosen for making decision for clients in selecting insurance companies like Hospital, location, equipment, success rate, doctors experience, insurance companies services etc.

The above contributions of the research work justified the aim and scope of thesis.

In order to support our argument, the proposed threshold Multi Attribute Secure Decision Making Algorithm (MASDMA) with $S^2$RSA cryptosystem is applied in Health Insurance Portal which is third party health party service provide from which the clients (both patients and insurance companies) can register and securely exchange the data for availing of insurance compensation. Health insurance web portal is designed basing on E-Health insurance framework which contains various service layers like

1. Patient/Insurer Registration Service
2. Expert Verification Service
3. Insurance Scheme Selection Service (ISSS)

4. Expert Security Service System for Data Module

5. Exchanging Client data between HIC and HC Service Module (ECHHM) Payment Module.

A e-health insurance framework comprising of various services using Java technologies like JSP, JDBC with backend MYSQL were discussed and sum of the examples are verified with the developed protocols. In a nutshell the work carried out by the author enhances the potentiality of applications of medical aid to patients through various agencies using several computer techniques. The web portal uses the proposed protocols for exchange of data between clients, insurance company third party health service provider web server. Health Insurance web portal application is designed in Java Sever Pages technology with Apache Tomcat web Server using MySQL database.

7.2 Suggestions for Future Work

Several directions are identified that the research presented in this thesis can take further. Some of the recommendations for further work include:

The Proposed $S^2$FRSA cryptosystem can be analyzed and modified to be used for Mobile Applications so that M-Commerce applications be developed with enhanced security which required only part of data to be visible like patient-doctor diagnosis system. MASDMA algorithm can be used in applications where multiple decisions are to be taken.

Finally the Health Insurance application developed can be extended to mobile/cloud technology so that clients can use it with a smart mobile devices pulling data from cloud can use or process the requests in natural language as they are familiar with native language and can give benefits to Insurance companies to improve client's occupancy in their business in this competitive world.
It is envisaged that extension of the present work from the patient, health insurer, hospital authorities and better potentiated with the available fast developing computational methods and provide best global available medication for low cost for common people. This is essential countries like India to enrich their human resource and to enhance the scientific and technological areas this posing competition to develop countries like USA.