CHAPTER 6

APPLICATIONS

6.1 INTRODUCTION

This chapter concerns about some of the application of the proposed digital signature schemes presented in Chapters 2 and 3. The proxy blind distributed signature scheme can be applied to polling station based automated electronic voting scheme and the Identity Based proxy blind distributed signature scheme can be applied to health care insurance service management system.

6.2 APPLICATION TO ELECTRONIC VOTING

Julie Ann Staub (2005), Avi Rubin (2004), Burmester and Magkos (2003), Chou-ChenYang and Hang Wen Yang (2005), Lin et al (2003) studied the security enhancement for anonymous e-voting over a network. There are various kinds of voting schemes available in the literature and also in practice. They are paper based voting scheme and automated voting scheme. The automated voting scheme is subdivided into two kinds. They are polling station based voting and internet voting. Again the Internet voting is subdivided into poll station internet voting and remote internet voting.

The polling station based internet voting scheme is considered to fit the model Proxy Blind Distributed Signature Scheme discussed in Chapter 2. It is assumed that the polling station or a vote branch server $\mathbf{B}$ is connected with n secured proxy servers $\mathbf{B}_1, \mathbf{B}_2, .. \mathbf{B}_n$. The voters will cast their votes

through the vote branch which it in turn send to the Vote Manage Center A and the voters can verify whether their votes are casted by verifying the signatures generated by **B** on behalf of A .

In an electronic voting scheme, the vote managing center commission a vote branch to act as a proxy signer. A voter can cast his/her vote in the vote branch. Since the vote branch does not know anything about the voting message during voting, the proxy blind signature scheme can be used in it. To achieve anonymity, blind signature scheme are normally used by e-voting schemes. Since a single vote manage center cannot blindly sign the vote messages from various branches, it can delegate its signing power to the proxy servers. Moreover, to achieve robustness the proxy delegation is distributed to the group of servers and a threshold number of servers lesser than the group members can generate the signature. Hence the proxy blind distributed signature scheme can be used to this electronic voting scenario. Figure 6.1 shows the Proxy blind distributed signature scheme in electronic voting scenario.

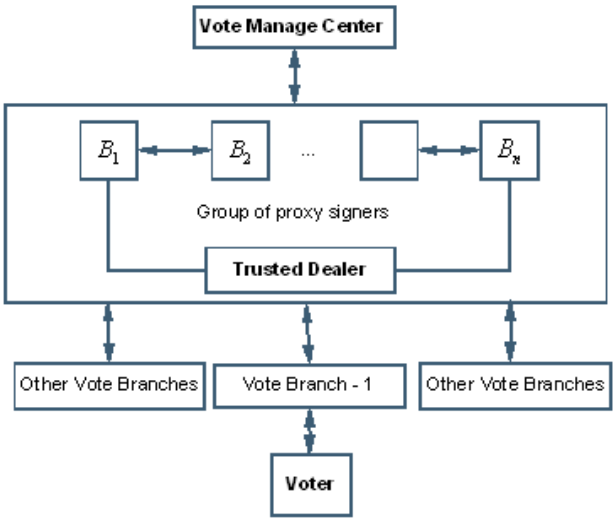

Figure 6.1 Proxy blind distributed signature scheme use in polling station based internet voting scheme

As the vote branch server $\mathbf{B}$ is distributed to n secured servers and the threshold version is followed, the joint generation of key requires only the threshold number t of the participating servers. If any one of the servers $\mathbf{B}_j$ where $j = 1,2,...n$ is busy or corrupted due to some malicious programs, then the rest of the servers can successfully complete the task. Therefore this model satisfies the robustness condition of the e-voting

6.3 APPLICATION TO HEALTH CARE INSURANCE SERVICE MANAGEMENT SYSTEM

A health insurance claim is a bill for health care services that the health care provider turns in to the insurance company for payment. With many insurance policies, when the patient go to the doctor for a routine checkup if the bill is Rs.100, then the patient has to pay a co-pay of Rs.25 to the hospital and the doctor bills the remaining amount of Rs. 75 to the concerned insurance carrier . The insurance claim begins before the patient make an appointment. Insurance carrier is responsible only for paying benefits that are covered under the policy. After the coy-payment is made, the doctor sends the bill to an insurance claims processing center. The processing center gathers all relevant information from the doctor including the patient information sheet, intake forms and the proper services documentation. These are compared to the insurer's explanation of benefits to see whether the policy covers the services. If it does, then the insurance carrier will submit payment for the remaining balance. If not, the patient is responsible for whatever balance is left after the co-pay.

Most claims processes are smooth, but there are some bumps will also encounter and they are termed as dread denied claims. The claim can be denied or can be rejected because of the following reasons:

- Treatment sought without prior authorization
- Improper claim filing (missing information, illegibility)
- Claims not filed within time limits
- Treatment not covered by policy

The health care management software system is one of the recent technologies focusing the health care insurance service management. The processes involved in this system are completely automated, the process included policy correction, endorsements, renewals and non-renewals, detailed policy transaction history and claims processing. Claims module is designed to handle simultaneous claims by sharing data between the policy and claim modules. When a new claim is created within the claim modules, the system automatically verifies coverage, coverage limits, deductibles, and aggregates based upon the date of loss. The Claim modules allows complete tracking of the payments, expenses, salvage, losses by peril and sub-peril and integrated claim letters that automatically incorporate and merge claim and policy information into the letter.

Health insurance fraud and abuse encompasses a wide range of practices, such as overcharging for services, billing for services not rendered, and rendering services that are unnecessary or inappropriate. Dowland et al (1999) presented a survey on computer crimes and abuses.

Information security plays a vital role in the Health Care Insurance claim module due to the following fraudulent activities. There is a possibility for a person who does not have a valid insurance card to use someone’s card. A dishonest hospital may give a forged receipt to an insurance card holder stating that medical treatment was given to that person who has not undergone any treatment. In these two fraudulent activities, the first one lacks the Identity of the Insurance card holder and the second lacks decentralization of

signing power. The Identity Based Proxy Blind Distributed Signature Scheme discussed in Chapter 3 could be applied to the health care insurance service management system for the secured and robust signature generation for the customer health insurance claims module.

6.3.1 Claim Module

The health care management software system setup of the insurance company is as follows. The company's health insurance server is connected to the registered hospital servers $S\_H_1, S\_H_2, ...S\_H_k$ and each hospital server is connected to a finite number of doctor's system $D\_1, D\_2, ...D\_m$ and each doctor's system is interconnected with n number of proxy systems $\Pr ox\_1, \Pr ox\_2, ...\Pr ox\_n$ in various internal departments like pharmacy, test labs, X-ray center, ECG center, etc. The identity based proxy blind distributed signature scheme for health insurance claim is shown in Figure 6.2.

The patient claim bill plays a vital role in the reimbursement of money for the insurance holder and hence the message to be signed here is the patient's bill. Unique identity will be given by the company to each individual registered client. Hence the message consists of the Bill amount and the identity of the patient. Using the digital signature scheme discussed in Chapter 3, the patient will get the signature for the message and produce it to the insurance company along with his unique identity. If the validity holds well, the claim amount will be accepted by the company and the amount will be paid by the insurance company.

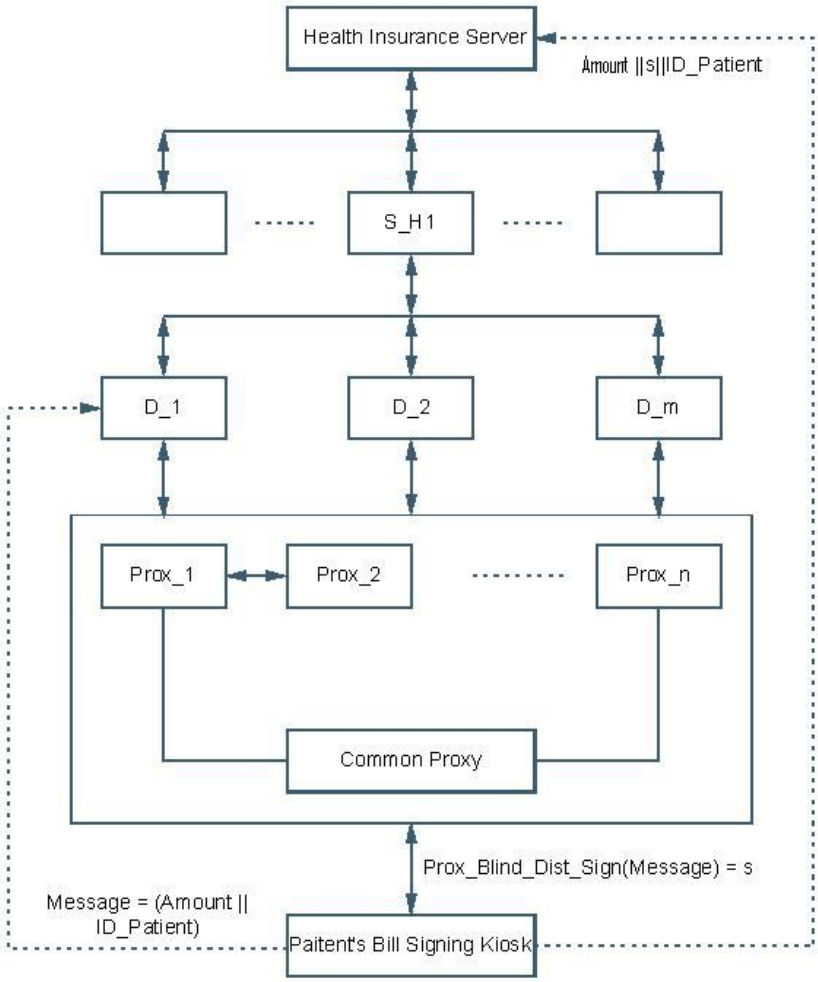

Figure 6.2 Identity based proxy blind distributed signature scheme fitted to health care insurance claim module

The advantage of using the Identity based proxy blind distributed signature scheme in the claim module is that it will over come the fraud of using other's identity. Since $message = billamount + ID\_patient$ and $\Pr ox\_Blind\_Dist\_Sign_{S_{prox}}(message) = (S^1 \| c^1) = signature$, for the verification process the insurance server will check for the identity of the patient along

with the message and signature and then the claim is accepted if and only if $c^1 = H(message \| e(S^1, P)e(Q_{prox}, P_{pub})^{-c^1})$.

Moreover, in this scheme the proxy signing delegation is distributed to the group of servers and threshold version is followed. Therefore the health insurance fraud and abuse of practices, such as overcharging for services, billing for services not rendered.