List of Publications
Protocols For Health Insurance System
G. V. Ramesh Babu1, Dr. M. Padmavathamma1
1. Assistant Professor, 2. Research Supervisor and Head, Department of Computer Science
1,2 S.V. College of CM&CS, S.V. University, Tirupati

Abstract
Health insurance companies (HIC) should provide health services to their customers in an efficient and secure way. Insurance companies are using modern technologies of IT to provide service to customers through E-Health Insurance, which is an Internet-enabled health insurance application involving management of Customers data electronically. Due to the ease of global access to the information systems, privacy and security is becoming a major concern in the e-health insurance systems. To achieve above criteria we have proposed protocols for Health Insurance System (HIS) which provides the services to customers in Secure manner in two phases. In each phase we propose protocols for secure communication. Phase - I consists of a) Client Registration service i.e., between Client (C) and Insurance Company (IC) b) Insurance Company Verification (Client data) and Health Card Generation service. In Phase-II we propose protocols between Insurance Company and Client for verification of health records and between Hospital (H) and Insurance company to ensure payment securely by using Expert Security Service.

1. Introduction

Group practice prepaid health care plans have been shown to operate in a business like way and to deliver high quality health care at lower costs. The number of people in developing countries in India covered by such plans, however, is very small. A well-formulated and well-managed Health insurance services could provide a comprehensive financial assistance. Generally a) Insurance companies negotiate rates with health care providers to provide financial coverage to clients b) It shields you from unexpected medical costs – Even if your health plan requires you to pay certain costs out of pocket, being covered can help, save you from bankruptcy in case of injury or hospitalization. c) It shields your business from personal medical costs – As a self-employed person or small business owner, unexpected personal medical expenses can cripple your business. By limiting your personal liability for medical costs, health insurance can help keep your business afloat.

Securing confidential patient data is more important than ever – and it requires more than good intentions. It demands a comprehensive security solution built around strong encryption, robust identity management, and policy-based data management. This is especially true as hospitals and healthcare providers, insurers, pharmaceutical companies and others grow their ranks of mobile workers who carry or remotely access personally identifiable health information and R&D data. Data centres should maintain Client’s data at Insurance offices should follow HIPAA Privacy Rule and the HIPAA Security Rule.

According to HIPAA the Privacy Rule protects all individually identifiable protected health information (PHI) maintained by the Covered Entity. It is not specific to electronic information and applies equally to written records, telephone conversations, etc. According to the Department of Health and Human Services, PHI includes data that relates to:
- the individual’s past, present or future physical or mental health or condition or
- the provision of health care to the individual or
- the past, present, or future payment for the provision of health care to the individual

According to HIPAA Security Rule the security of electronic protected health information (ePHI). It prescribes a number of required policies, procedures and reporting mechanisms that must be in place for
all information systems that process ePHI within the Covered Entity. It also prescribes a number of required and addressable implementation specifications designed to protect the confidentiality, integrity and availability of ePHI within the enterprise. These specifications fall into five categories:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures

Health Insurance System protocols should be well designed to meet requirements stated below to provide security, to access PIN b) digital certificates c)read/write by smart card readers d)access to basic patient's data e)access to health insurance data f)submission of data g) exchange of data h) Payment Billing and insurance.

- Have strong measures protecting confidentiality of the medical information they contain. \((\text{Requirement I})\)\(^{(6-9)}\)
- Prove the validity and accuracy of the HER so as to be able to protect the patient's rights. \((\text{Requirement II})\) \(^{(6-9)}\)
- Contain measures for the selective protection of privacy that allow for consultations with a trusted third party (TTP) on related medical information inquiries\(^{(6-9)}\).\((\text{Requirement III})\)

For ensuring security for clients data in Health Insurance premises we formulated a model and set of protocols to exchange data between client and Insurance agents/offices servers. Hospitals and health systems like insurance companies take measures for protecting the security of patient health information; yet, data breaches remain common in the industry. Health insurance companies must take following steps make data security a priority: 1. Conduct a HIPAA risk analysis 2. Implement encryption for all data as recommended by the AMA. 3). Choose the highest level of encryption without the lag. 4). Secure laptop data with encrypted portable storage devices. 5) Make sure you have disaster recovery and business continuity plan.

2. Literature Survey

Insurance Companies must deliver cost effective, quality health care to its members as well as address the key administrative and clinical issues. To do this, Insurance and hospital management relies heavily on its IS/IT (Information Systems/Information Technology), in particular, MARS (medical automated record system). Smart Cards are efficient for security for authentication \(^{(1)}\). In 1996, the Health Insurance Portability and Accountability Act (HIPAA) offered some general guidelines to enforce the protection of private medical information. One such guideline stated that patients must be able to view and obtain copies of their records, and request amendments to confirm they have the right of accessing their medical records to understand and monitor their health status and the process of diagnosis and therapy \(^{(2)}\).

Bhatti et al. \(^{(3)}\) proposed a policy-based system to address the following requirements: 1) the integration of privacy and disclosure policies with well-known healthcare standards used in the industry for the purpose of producing precise requirements of a practical healthcare system, and 2) the provision of ubiquitous healthcare services to patients using the same infrastructure that can enable federated healthcare management for organizations. More specifically, the disclosure and privacy policies have been designed by making use of requirements specification based on a set of use cases for the Clinical Document Architecture (CDA) standard. Also, a context-aware policy specification language has been proposed, which allows encoding CDA-based requirements use cases into privacy and disclosure policy rules. Unfortunately, the HIPAA security regulations are not covered in this framework.

Consequently, Health Insurance System should use modern technologies and must ensure quality information via internet\(^{(5)}\):

1) Cost savings: the provision of detailed, structured and extensive information to the insurer aims at avoiding costs for highly individual, time-consuming consultation. Therefore providing information by websites is cheaper than providing telephone-based customer services or individual services in a local agency.
(2) Competitiveness: as the fee for health insurances in Germany was harmonized to a uniform level, sickness funds need other major differentiating factors from their competitors than costs. One possibility that can also be found as a major differentiating factor in other industries is "quality of services". Consequently, information services provided by electronic means with a wide availability and a certain quality level could be a factor that distinguishes high-quality from low-quality from the point of view of insurant.

The private insurance system is based on an individual agreement between the insurance company and the customer. The fee depends on a range of individual characteristics, for example, the percentage of coverage, the amount of chosen services, the individual risk or the entrance age into the private system, and so forth.

3. Proposed Health Insurance System (HIS)

4. Protocols for Health Insurance System

In the Proposed model above in figure-1 we are proposing protocols between Client and Insurance company and, between Hospital and Insurance company to facilitate payment. In our architecture we divide working model into two phases and in each phase we propose protocols for secure communication. Phase - I consists of a) Client Registration service i.e., between Client (C) and Insurance Company(IC) b) Insurance Company Verification (Client data) and Health Card Generation service. In Phase-II we propose protocols between Insurance Company and Client for verification of health records and between Hospital(H) and Insurance company to ensure payment securely by using Expert Security Service.

In Phase-I, we propose Protocols for

1. Client and Insurance Company (IC) (C → IC)
   a) Secure decision making process for Client selecting Insurance Scheme
   b) Registration Process (for Client Registration/Authentication)

Secure authentication algorithms and digital signatures are used in the proposed scheme at the time of client data registration for ensuring data integrity.
2. Insurance Company (IC) and Client (C) 
(IC → C) 
   a) Secure Verification Process (for client Data Encryption and Decryption during storing) 
   b) Health Card Issuing Process (combination of Image Encryption and PKI) 

In Phase-II, we propose Protocols for 

3. Insurance Company and Hospital (IC → H) 
   a) Secure Verification Process (to verify client/Patients Diagnosis Reports) 
   b) Secure Payment Process (to release payment to hospital by Insurance Company) 

5. Conclusions

In this paper, we have proposed protocols for Health Insurance System to address the HIPAA privacy and security regulations in e-health insurance systems. Instead of adopting conventional manual procedures we have designed a Health Insurance System which is secure based cryptographic key management and ensures cryptographic authentication, encryption and non-repudiation, etc. The delegation of client's data to the insurance companies and hospitals are done securely and has avoided the problem of requesting a physical presence of the client/patient for each such access. The proposed scheme can address the HIPAA privacy and security regulations. 

6. References

Secure e-health insurance model

G.V. Ramesh Babu, M. Padmavathamma
Department of computer science, S.V. University Tirupati, A.P. India

Abstract: In the current era of modern health problems should be addressed with utmost importance and data should be secured in the competitive market in order to avoid misuse by third parties which are not responsible in this regard. In view of Health insurance which benefit patients economically should be effective and should also address the issue of providing privacy to their medical record. To address the above issues we are proposing architecture a new secure e-health issue system (SEHIS) model which allows to store patient's data in Smart e-Health Card (SEHC) which is given to patients by Health Insurance companies in turn used by medical practitioners to access patients data. SEHIS provides expert services to advice patients regarding insurance schemes selection (decision Support system) verify and secure patients data in SEHC. In this model, SEHC contains patients data like finger prints, photo and personnel data is encrypted by using PKI, Digital image encryption techniques. SEHIS model verifies counterfeit documents, if any of the patient to use insurance facility or an insured person and a physician may deviate from insurance company rules to get benefits illegally etc. in our proposed model, SEHIS will benefit insurance companies, patients and works accordance with HIPPA requirements.

I. Introduction

Enforcing of information technology in Healthcare System is essential it needs to make effective service oriented to the clients. In which, health care services like e-Insurance Health Care System is used to diagnosis through Doctor authority in order to get benefit from the health area. In which, expert system in health care for health insurance patient clients for better medical services. In the area of health care system for diagnosis and deals with expert system model which allows diagnosis of diseases and an expert evaluate the diagnosis processed by the system in Doctor authority diagnosis several diseases. It maintains information from past history and symptoms.

Security for e-Health Insurance has vital aspect. The authentication of patient who utilize the benefit of health insurance. In the e-Health Insurance field Digital Health Card which benefit to the patient for treatment. In which patient can communicate their health information through web service. In this process, image encryption can be maintained on patient photo, details and test reports. Insured patient is utilize through hospitals for treatment in which Doctor authority connect through web service of entering into the particular site for medical operations through expert verification system such as, Diagnosing etc., [5,6].

To verify client requirements for expert verification system is normally performed by testing. In this model SEHC contains patients data like finger prints, photo and personnel data is encrypted by using PKI, Digital Image encryption techniques. SEHIS model verifies counterfeit documents, if any of the patient to use insurance facility or an insured person and a physician may deviate from insurance company rules to get benefits illegally etc. in our proposed model, SEHIS will benefit insurance companies, patients and works accordance with HIPPA requirements.

II. Related Work

2.1 Digital Health Card System:

Smart Cards are efficient for security for authentication smart card which interconnect health care providers it is used for patient authentication and doctor authority for medical operations. To secure sensitive information electronic implementation of Digital Health Card and security interoperability like cryptography standards besides, to ensure authenticity of health card. Digital Health Card is used to maintain authentication it has data storage and processing capabilities. In a online based health care system individual data is kept in patient health card [7]

2.2 Expert System:

Expert system occurs to facilitate in different filed or areas such as medical. In which one of the prime areas i.e., medical analysis through decision making. Expert systems normally make different stages such as analysis and diagnosis through which patient status can be determined. Expert system diagnosis and suggest about particular diseases knowledge based management system. Expert system are a branch of Artificial Intelligence (AI) and were developed by the AI Community in the mid-1960s. an expert system can be defined...
Secure e-health insurance model

as "an intelligent computer program that uses knowledge and inference procedures to solve problems that are difficult enough to require significant human expertise for their solution". Expert systems have several applications in various domains. They are mostly relevant in order to develop an expert system the knowledge is converted into a computer program. Knowledge is represented in the form of IF-THEN rules. Health care professionals such as doctors, clinicians, pharmacists, diagnosis and treatment can be made through web service depending upon the data available in the patient details [8].

![Diagram of Expert System](image)

2.3 Image encryption

Image encryption process transforms plain - image information into cipher-image for involving the original image with one or more key. Technology that use the same secret key for encryption and decryption under private key techniques asymmetric key technique use two different keys, are public key for encryption and two private keys for decryption. Cryptosystem can be serve all types of attacks they try to violate the system such as, Plain text attack, cipher text attack [7, 8]

Encryption image:
1. Load the plain image (original image)
2. Calculate the width and height of the input image
3. Lower horizontal number of blocks = integer (Image - Width)/n
4. Lower vertical number of blocks = integer (Image - Height)/m

No of blocks = horizontal number of blocks x vertical number of blocks [7]

2.4 Biometric authentication:

Biometric authentication can be maintained by using fingerprinting.

III. Methodology

First and foremost client selects the scheme of insurance. After scheme selection client needs to register and furthermore, payments is to be paid. While process starts verification through insurance authority to be performed. After verification process completes Digital Health Card generated to the client. Then client patient submits his health card to the doctor authority. In the doctor authority diagnosis based on symptoms based on lab test results. During the transaction process secure communication essential between patient client and doctor authority through encrypted of image. In this scenario authentication and confidentiality are major concern to ensure security.

IV. Proposed Architecture

![Proposed Architecture Diagram](image)
IV. Conclusion

In this paper, we have developed architecture for e-health insurance system which serve patient communications with doctor authorities.

References

Medical Diagnosis Expert System as Service in Cloud

A. B. Rajesh Kumar, G. V. Ramesh Babu, C. Phani Ramesh, P. Madhura, and M. Padmavathamma

Abstract—With the technological advancements in information technology, cloud computing provides several opportunities and services to users like storing personal information, accessing various web services for online transactions, online diagnosis systems etc. But security in cloud is biggest challenge which poses threat to individual privacy and misuse without knowledge of data owner. In such a situation, secure decision making based on patient information through patienit enforec and using cryptography techniques need to be adopted to protect sensitive data for diagnosis. In this paper, we propose a novel approach development of cloud model for medical diagnosis expert system in which patient access is divided into two ways. Patient needs to access openly and other is to be provided security in terms of encryption techniques which secure patient information through decisions for diagnosis can be made based on personal information of the patient and to implement patient access to control using EAS [1] ID3 [2].

Index Terms—Cloud computing, SAAS, decision tree, ID3, expert system as service.

I. INTRODUCTION

Distributed computing environment that will collect authorized medical data store it securely within a networks to assist fast and efficient care. Cloud computing, health care services that benefit patients, doctors and hospitals for medical data analysis for the purpose of decision based on test reports [3]. In communication and information technology an increasing number of health services are available. Health care services provides patients’ safety less health care cost and improving quality of diagnosis [4]. Despite number of changes by industry and a number of standards under development provides patient information. Security and privacy are major difficulties with respect to patient information. Patients are expected to treat as confidential. To address these issues cryptographic techniques can be implemented to maintains security for personal information. The advent of cloud computing has permitted us to host the software pack that analyses patient personal information as w as as services, [5] PAAS layer controls the execution of the software. In this paper, we propose a novel approach development of cloud model for medical diagnosis expert system in cloud which provides secure patient information through decisions based on lab test reports of the patient and to implement patient access control using expert system as service and ID3 [6], [7].

II. RELATED WORK

A. Expert System

Expert system is computer programs that are derived from computer science reveals called artificial intelligence (AI). It is designed to diagnose patient data in developed to diagnose disease. Expert system includes both conventional such as DBMS and AI. [8] Medical Diagnosis DBMS are used to store and diagnosis patient personal information. In an interaction based expert system to assist the doctor for diagnosis process. Based on test reports and to bring out the appropriate information for consultation and with the results produce possible diagnosis and suggest treatment. To help doctors for disease associated with symptoms.

B. Decision Trees

Decision tree is a classification techniques that uses a series of questions or rules about the attributes of the class to classify data sets into classes. Training data set to establish a classifier is used for test data and this is based on the concept of measures of impurity of the data. These metrics can be entropy. Information gain is used to decide the class of each data item, which can be expresses as follows: [9], [10].

Gain (R, A) = Entropy (R) - \sum_{R_j \in \mathcal{R}} \text{Entropy} (R_j)

R is the subset of R that has attribute value of v.

\sum_{v} \text{over each attribute value of } A.

\mathcal{R} is the number of elements in the set R.

III. OUR PROPOSED ARCHITECTURAL REPRESENTATION

The objective of our architecture is to achieve decision based on patient information.

![Fig. 1. Medical diagnosis expert system as service.](image_url)

Manuscript received February 2, 2013; revised April 10, 2013.

The authors are with the Department of Computer Science, S.V. University, Tirupati, 517502, India (e-mail: a_b_rajeshkumar@yahoo.com, gvrameshbabu2003@yahoo.com, phani.eng@gmail.com, p_madhura@yahoo.com, prof.padma@yahoo.com).

DOI: 10.7763/IJCE.2013.V2.211
A. Our Architecture Consists of the Following Parts and Roles

A model of cloud expert system as a service provides on demand in internet, eliminating the need for installing and maintenance of the expert system software on the clients computer. PAAS offer development tools. Ex: AZURE IaaS Virtual machines are provided Ex: Amazon. The patient who has full access to the cloud server.

A specific diagnostic expert system based on test reports.

A specific doctor expert system module need to diagnosis using ID3.

A specific Hospital expert system is to make decisions based on patient test reports.

Patient - centric control through cryptograph techniques can be applied and to maintain confidentiality and integrity of patient personal stores in the cloud need to be protected information.

Data in cloud through cloud service provides and if patient wants to access openly and other is to be provided security in terms of encryption techniques which secure patient information through decision for diagnosis can be made based on personal information of the patient and the data base, sends a request to the cloud service provide and receives the original data. If data in is encrypted form that can be decrypted in his key.

B. Methodology of Expert System Service

To provide patient information that will help the doctor makes critical decision concerning a patient health.

- If (Serum = ‘Yellow’) then do CD4 count test.
- Else ‘No Disease Found’
- If (CD4 Count ≥ 500) then ‘patient in early stage’
- Else if (CD4 count < 500 and CD4 Count ≥ 200) and symptoms appears then ‘patient is in middle stage’.
- Else if (CD4<200 & Symptoms appears then ‘patient is critical stage’)
- Else ‘Patient is in Normal Stage’

C. Decision Tree

- Decision trees are simplistic.
- Decision trees and proven to be better classifier.

![Decision Tree Diagram]

Fig. 2. Decision tree

To provide on demand - resource provision according to the service level established between a patient, a Doctor and Hospital. Access control can be made through registration by patients Doctors and Hospital. During the process of decision making patient has to submit it his symptoms as input data. Diagnosis can be performed using Decision Tree. After disease prediction patient can choose specialized doctor. Selecting Hospital which chosen doctor treatment. And also can refer to medical insurance agents first and foremost patient has to submit his secret key to the cloud. Through which doctor can receives key data and suggests his views on that particular patient based on lab test reports. Diagnosis system is developed with the purpose of helping the doctor in diagnosis various diseases based on test reports Objective of this system into produce recovery data and information for decision making to the Doctor and with the results obtained to produce possible diagnosis.

IV. Conclusion

In this paper, we developed a novel approach development of cloud medical diagnostic expert system as service, which provides secure patient information diagnosis based on lab test reports.

REFERENCES


M. Padunaramanas is working as Head of Department of Computer Science, S V University, Tirupati, AP, India. She has vast experience of 26 years in teaching. She has guided 8 PhD’s, 12 M.Phil’s and published 35 articles in International/National Journals. She has attended and chaired many international conferences conducted by various international organisations at various places around the world. Currently she is director of projects funded by UGC, DST India. Her Areas of interest are Network Security, Cloud computing and Data mining.
A. R. Rajesh Kumar is a research scholar from S.V. University Department of Computer Science, Tirupati, AP, India and presented papers and attended international conferences in India and around Asia. His areas of interest are Network security and Data mining.

G. V. Ramana Babu is working as Asst. Professor, Department of computer science, S.V. University, Tirupati, AP, India. He has a teaching experience of 13 years and presented papers and attended international conferences in India and around Asia. His areas of interest are Network security, Ecommerce and Data mining.

C. Pinal Ramana is a research scholar from S.V. University Department of Computer Science, Tirupati, AP, India and presented papers and attended international conferences in India and around Asia. His areas of interest are Network Security, Ecommerce and Data mining.

P. Madhura is a research Scholar from S.V. University Department of Computer Science, Tirupati, AP, India. Her areas of interest are Network security and Data mining.
Data Mining Technique for a Secure Electronic Payment Transaction using MJk-RSA in Mobile Computing

Ramesh Babu G.V., Narayana G, Sulaiman A, Padmavathamma M

Research Scholars, Research Supervisor, Dept. of Computer Science, S.V. University – Tirupati, A.P, India

ABSTRACT

Due to the evolution of the Electronic Learning (E-Learning), one can easily get desired information on computer or mobile system connected through Internet. Currently E-Learning materials are easily accessible on the desktop computer system, but in future, most of the information shall also be available on small digital devices like Mobile, PDA, etc. Most of the E-Learning materials are paid and customer has to pay entire amount through credit/debit card system. Therefore, it is very important to study about the security of the credit/debit card numbers. The present paper is an attempt in this direction and a security technique is presented to secure the credit/debit card number supplied over the Internet to access the E-Learning materials or any kind of purchase through Internet. A well known method i.e. Data Cube Technique is used to design the security model of the credit/debit card system. The major objective of this paper is to design a practical electronic payment protocol which is the safest and most secured mode of transaction. This technique may reduce fake transactions which are above 20% at the global level.

Keywords: E-Learning Material, Security, Mobile Transaction, Data Cube Technique, Credit/Debit Card

INTRODUCTION:

The rapid growth of mobile system services has changed the economical, cultural and social activities. In most of the countries, people are using these services for sale and purchase. Day-by-day, companies are hosting the web pages on the server which is connected through the autonomous mobile systems. The arrangement of the mobile systems is according to the distributed computer system, in which customers or consumers can access the server and this connectivity is having the high class of bandwidth like 2G, 3G. Mobile Commerce popularity known as M-Commerce is a new way to do business transactions electronically. Mobile transaction is a very important part of M-Commerce and therefore a much secured electronic transactions are required. A Secure Mobile Payment Transaction (SMPT) is a system which ensures the security of financial transactions on the Mobile Internet. Mobile money (M-money) or digital cash (e-cash) is merely an electronic representation of funds. M-money is observed with a net result of funds transferred from one party to another. The primary function of e-cash or M-money is to facilitate secure transaction on the network. M-money is a necessary innovation in the financial markets. This may become popular in the era of globalization and very fast economic activities and secure transactions.

The Electronic payment system has two major components:

1. Mobile Module (Client module)
2. Server module.

The connectivity between these two modules is defined as interface module and generally known as user interface module for client. The objective of this module is to send the request from Mobile to server. This module will store all transaction information in the form of data[1] cubes. The user interface module and the server module communicate with each other using WAP or TCP/IP protocol. Let us now describe some of the important references related to security of the electronic payment system.

The connectivity between these two modules is defined as interface module and generally known as user interface module for client. The objective of this module is to send the request from Mobile to server. This module will store all transaction information in the form of data cubes. The user interface module and the server module communicate with each other using WAP or TCP/IP protocol. Let us now describe some of the important references related to security of the electronic payment system.
In the present work, transactional information is saved in the form of Online Analytical Processing (OLAP) Data Cubes for secure and reliable Electronic Payment System (EPS). The flow of credit card number from customer computer system to the server must be secured for which a cryptography algorithm is used. The algorithm is called as Rivest, Schmidt and Adelman (RSA) algorithm, which is a type of Public-key Cryptosystem, for Mobile payment which can provide confidentiality and security. It uses a pair of related keys one for encryption and other for decryption. One key, which is called the private key, is kept secret and other one is known as public key.

A case study of Credit Card System is demonstrated after designing the model through design of data cubes. The whole study is based upon the concept of the prime numbers which are generated automatically through the above approach.

**METHODOLOGY**

Let us first describe the Mobile client/Server architecture model in which Client or Customer’s Mobile system is connected through network with the Server. The numbers of customers are connected through the network called as the Internet and the architecture is based on the distributed computing system. The Mobile client and server can communicate with each other using WAP protocol. The connectivity between the Mobile client and server computer systems is shown in Figure 1. After getting the connectivity with server computer system, Mobile is able to fetch any kind of information which are available in the form of web pages i.e. client is able to access the E-learning materials. For this Online Analytical Processing (OLAP) is done i.e. OLAP system serves as a tool for storing data and for retrieving information from all users in this system. For accessing the information from server, customer has to supply his credit/debit card number along with MPIN on the internet only if the services are paid. The searching and sorting of the databases available on the computer systems are faster if one uses the Data Cubes methodology[2]. Various steps for OLAP are described below:

![Global Access](image1.png)

**Figure 1. Mobile-Client Server**

![Cube design with details](image2.png)

**Figure 2. Cube design with details**

**Step 2.1:**

The first step is to store the customer information in the form of data cubes. When the user enters his/her credit/debit card number or account information on the web page then this information first is stored in the form of OLAP data cubes.
as represented below in Figure 2. Online Analytical Processing (OLAP) products are developed to store these transactional data for easy retrieving. It helps for the system analysts to do decision support on historic transactional data. They expose a multidimensional view of the data logically with numeric attributes like sales, amount and revenue forming the measures or cells of the multidimensional cube. In table 1, the credit/debit card of the customer consists of three major attributes namely "CREDICARD_NO", "CUST_NAME", and "BANK_NAME" which are taken along x, y and z axes, respectively for credit card number, customer name and bank name.

<table>
<thead>
<tr>
<th>Bank name</th>
<th>XXX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank IFC code</td>
<td>XXX</td>
</tr>
<tr>
<td>ACC NO</td>
<td>XXXX</td>
</tr>
<tr>
<td>CREDICARD NO</td>
<td>XXXXX</td>
</tr>
<tr>
<td>MIP</td>
<td>XXX (Encrypted)</td>
</tr>
</tbody>
</table>

Table 1 Customer details

Step 2.2:
On the basis of step 1, let us create N records of the customers and these customers desire to access E-learning materials or want to purchase the product. This information as per the designed data cubes for the attributes are given in Table 1. The table is normalized and primary key is the CREDICARD_NO while the secondary key is the CUST_NAME as represented in the table. This information is designed with the help of data cubes which is shown in Figure 3.

Step 2.3:
Now we want to secure the supplied credit card numbers through an innovation algorithm known as MJL- RSA algorithm. For this purpose, a constant ‘bit strength’ is used, which is the size of the MJL- RSA modulus in bits. The algorithm is based upon the computation of the encryption and decryption keys which are relatively primes and used to secure the credit card numbers. The sub steps are given below:

2.3.1. The Signer Choose sufficiently large distinct primes \(p_1, p_2, \ldots, p_r\) at random.

2.3.2. Compute \(\prod\limits_{i=1}^{i=r} P_i = P_1 \cdot P_2 \cdot \ldots \cdot P_r = N\) and

\[
J_e(N) = \prod_{j=1}^{N^k}(1 - \frac{1}{p_j^k}) = \left(\frac{p_j^k - 1}{p_j^k - 1}\right) - \ldots - \left(\frac{p_j^k - 1}{p_j^k - 1}\right) = \prod_{j=1}^{r}(p_j^k - 1)
\]

2.3.3. Choose a random integer \(E < J_e(N)\) such that \(gcd(E, J_e(N)) = 1\).

2.3.4. Compute the integer \(D\) Which is the inverse of \(E\) i.e., \(ED \equiv 1 \pmod{J_e(N)}\).

2.3.5. for \(1 \leq i \leq r\), compute \(D_i = D \pmod{P_i}\)

Public Key = \((p_1, p_2, \ldots, p_r, D_1, D_2, \ldots, D_r))

2.3.6. Compute \(D\) such that \(ED \equiv 1 \pmod{J_e(N)}\) i.e., compute \(D \equiv E-1 \pmod{J_e(N)}\)

i.e. find a unique value \(d\) such that 960 divides \(7D - 1\)

Simple testing with \(D = 1, 2, 3 \ldots J_e(N)\)

compute \(D\) such that \(ED \equiv 1 \pmod{J_e(N)}\)

i.e. compute \(D \equiv E-1 \pmod{J_e(N)}\) \(D \equiv 7-1 \pmod{960}\)

i.e. find a unique value \(d\) such that 960 divides \(7D - 1\)

Simple testing with \(D = 1, 2, 3 \ldots J_e(N)\)

Proc. of SPIE Vol. 5334 53342J-3
After step 2.3.5, we have two keys, encryption and decryption keys $E$ and $D$, respectively. Now, the credit card number of the customer is treated as the plain text defined as $P$ and initially this credit card number is encrypted as shown in Figure 2. The plain text is converted into the cipher text represented as $C$ and it is given by

$$C = M^k \mod N$$

(1)

The file to encrypt is processed as a group of strings each containing the specified number of characters and each character in such a string is converted to its ASCII code. After performing the encryption we get the value of $C$, which is used as an input for the decryption process.

2.3.7. After step 2.3.6, the cipher text $C$ is to be decrypted so that one could get again the Plain Text $P$ which shows that the credit card number is successfully reached at the server computer system for secure transaction. The plain text i.e. original credit card number is obtained by

$$M = C^e \mod N$$

(2)

The process of above shows decryption. The above steps are based upon the concept of the prime numbers. The computations involved for the above steps are for prime numbers which become very large for small values of the prime numbers as shown in the next section i.e. experimental study and discussion.

**Experimental Study and Discussion**

<table>
<thead>
<tr>
<th>CREDITCARD_NO</th>
<th>CREDITCARD_NAME</th>
<th>BANK_NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>6220218920900013</td>
<td>YYYYYYYY</td>
<td>SB, Tampi</td>
</tr>
<tr>
<td>6220218920900053</td>
<td>XXXXXXXXXX</td>
<td>ICICI, Hyderabad</td>
</tr>
</tbody>
</table>

Let us start the experimental study by considering the credit card number and we have to perform the above 2.3.7 steps. Suppose the credit card number of the customer is 6220218920900013 as shown in the Table 2 after applying the above steps 2.3.1 to 2.3.5. For the step 2.3.6 and for the security of the credit card number[3] over the Internet, let us compute the encryption and decryption as computed below: Assume the two small prime values for demonstration of the result

i.e. $p = 3, q = 11$, therefore, $N = p^q = 3^3 \times 11 = 33, k = 2$

$E(N) = (p^q - 1)(q^p - 1) = (9 - 1)(121 - 1) = 960$

Now let us compute the encryption and decryption keys $E$ and $D$, respectively.

Choose $E = 7$

Check gcd($E$, $p^q - 1$) = gcd ($7$, $120$) = 1

Check gcd ($E$, $q^p - 1$) = gcd ($7$, $8$) = 1

This gives $D = 823$ range increases

The complete encryption and decryption technique in which original credit card number is supplied by the customer or consumer or client on the Mobile communication and whether it is reached safely at the server computer machine for which two keys i.e. public and private keys are used. The credit card number (6220218920900013) supplied by the customer is used as a value of $P$ for each digit and then after performing encryption and decryption similar digits are obtained at receiver's end i.e. Server-end which shows that credit card number reached safely.
GRAPHICAL PERFORMANCE ANALYSIS BETWEEN RSA AND MJ₁-RSA

4.1. Key Generation Time Performance

<table>
<thead>
<tr>
<th>Bits</th>
<th>RSA</th>
<th>MJ₁-RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>512</td>
<td>78</td>
<td>78</td>
</tr>
<tr>
<td>1024</td>
<td>391</td>
<td>222</td>
</tr>
</tbody>
</table>

4.2. Encryption Time Performance

<table>
<thead>
<tr>
<th>Bits</th>
<th>RSA</th>
<th>MJ₁-RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>512</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>1024</td>
<td>475</td>
<td>192</td>
</tr>
</tbody>
</table>

4.3. Decryption Time Performance

<table>
<thead>
<tr>
<th>Bits</th>
<th>RSA</th>
<th>MJ₁-RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>512</td>
<td>47</td>
<td>48</td>
</tr>
<tr>
<td>1024</td>
<td>305</td>
<td>183</td>
</tr>
</tbody>
</table>

4.4. Comparison between RSA and MJ₁-RSA

CONCLUSION

From the above analysis, it is concluded that Data Cube designing method is one of the most powerful tools for storing the large database of any organization and it gives simplicity for searching and storing the database in mobile computing. In the present work, the number of credit card numbers of the customers are stored in the data cubes and then transmitted over the mobile network. The Mobile Client and Server Computer Systems exchange the private and public keys for security of the credit card numbers supplied for the mobile payment over internet. In our secured M-payment system communication between the Mobile and the server are communicating with each other using MJ₁-RSA algorithm and code as described above, which uses two different keys, public and private keys, to encrypt and decrypt the data. Since both keys are different so it is more secure as compared to other conventional cryptographically algorithms.

REFERENCES


Proc. of SPIE Vol. 8334 83342J-6
Fair-Exchange Protocols for E-Commerce Based on MJ₂-RSA Mono and dual signature Schemes

Abstract: This paper presents the design of our proposed protocols using MJ₂-RSA cryptosystem and signature scheme for invoking communication between Customer, Trader, Multi Level Trader and Bank for registration and generation of secret key, publication of public keys and distribution of private keys with ZTTP.

Key Words: Key-Generation, protocols, MJ₂-RSA cryptosystem, signature scheme.

1 INTRODUCTION

Fair-exchange is an important property that must be ensured in all electronic commerce environments where the merchants and the customers are reluctant to trust each other. This property guarantees that none of the transacting parties suffers because of the fraudulent behavior of the other party in the transaction. In this paper, we propose the design of our MJ₂-RSA protocol for registration phase of Customer, Trader, ML-Trader, and Bank to overcome the problem of fair-exchange for digital products. The protocol is based on our novel cryptographic technique. We show how to use our MJ₂-RSA VRES software components to develop such a protocol. Applications such as e-commerce payment protocols, electronic contract signing, and certified e-mail delivery require fair exchange to be assured. A fair-exchange protocol allows two parties to exchange items in a fair way so that either each party gets the other’s item, or neither party does. We describe a novel method of constructing very efficient fair-exchange protocols by distributing the computation of MJ₂-RSA signatures and MJ₂-RSA dual-signatures. Today, the vast majority of fair-exchange protocols require the use of zero-knowledge proofs, which is the most computationally intensive part of the exchange protocol. Using the intrinsic features of our dual-signature model, we construct protocols that require no zero-knowledge proofs in the exchange protocol.

In fair-exchange protocols with an on-line ZTTP, a ZTTP is directly involved in every exchange, and must be available for the entire duration of the exchange. The protocol itself is relatively simple MDS computationally efficient. However, maintaining a ZTTP that needs to be online constantly can be expensive. Moreover, the ZTTP can become a bottleneck, and pose scalability problems. In our proposed system, the ZTTP is involved in the protocol only if one of the parties behaves unfairly or aborts the protocol prematurely; otherwise, the ZTTP is never involved in the protocol. To clarify fairness primitive is used in an exchange protocol, we present an example of a basic optimistic fair-exchange protocol.

3 REGISTRATIONS WITH ZTTP

The registration protocol needs basic information of different parties such as customer, Trader, ML-Trader and Bank. The registration phase is to be performed only once, after which it supports any number of exchanges. We assume that the registration protocol is performed via confidential and authenticated channels which can be generated to different parties for submitting their details to ZTTP and the ZTTP will verify and generates the Symmetric key in our proposed protocol using Diffie-Hellman key Exchange algorithm. Using this symmetric key both parties exchange information using private key algorithm (RC4). The key is used to encrypt the public and private keys.

4 KEY GENERATION PHASE

In Key Generation Phase our proposed protocol MJ₂-RSA algorithm will starts with the symmetric key distribution. In our proposed
protocol, we are generating the single public key, (Mono) private key for Trader, Customer and single public key, dual private keys for ML-Trader and Banker to gain the hierarchy authentication

Let KG denote the key generation algorithm for the mono-signature, dual-signature scheme. The algorithm KG, on input of some security parameters, first selects multiple -primes \( P_1, P_2, P_3, \ldots, P_t \) such that their product is \( N \). The Public key is obtained by selecting a random integer \( E, 1 < E < j_2(N) \), such that \( \gcd(E, j_2(N)) = 1 \).

4.1 Key Generation Monotype for Customer, Trader

The Private key is generated by finding the unique integer \( D, 1 < D < j_2(N) \), such that \( ED = 1 \) (mod \( j_2(N) \)). \( E \) is the public key and \( D \) is the private key.Mono key for Customer or Trader are \( \text{keys}(E, D, N) \).

4.2 MJ-RSA Based Mono-signature Scheme for Customer / Trader

MJ-RSA based Mono-signature (Signature) scheme that allows two signers to compute a signature efficiently. Each associated signer will have signature computation based on the equation \( \text{Sig} = H(MD)^D \) (mod \( N \)). In our fair-exchange protocol, we employ an MJ-RSA based signature scheme.

signature generation for Customer, Trader

The signer create their respective signatures, \( \text{Sig}_1 = H(MD)^D \) (mod \( N \)), using their respective private keys \( D \). These are multiplied modulo \( N \).

The signature is considered valid if and only if \( \text{Sig}_1 \equiv H(M) \) (mod \( N \)).

The signature \( \text{Sig}_1 \) is verified using the public key \( E \).

5. REGISTRATION PROCESS OF CUSTOMER WITH ZTTP

1. Customer Request for Connection establishment to ZTTP Server
2. ZTTP Server establishes the Connection
3. ZTTP Server Creates the Session for Customer for future Communication
5. ZTTP Generates the Prime number set-P
6. ZTTP Select the Largest Prime(\( P_t \)) and finds its primitive root \( (Y) \) and sends the Customer
7. Customer Stores the \( P_t \) and \( Y \)
8. ZTTP generates the random number \( g \) and calculates the \( G = Y^g \) mod \( P_t \)
9. Sends \( G \) value to the Customer
10. Customer generates the random number \( h \) and calculates the \( H^h \) mod \( P_t \)
11. ZTTP Server Generates the SyKey = \( G^h \) mod \( P_t \)
12. Customer Generates the SyKey = \( H^h \) mod \( P_t \)
13. Customer sends ask and requesting for public and private keys
14. Server generates the public and private keys using MJ-RSA
15. Server encrypts the public and private keys using RC4 Symmetric algorithm and key as symmetric key (SyKey)
16. Customer decrypts the public and private keys using RC4 Symmetric algorithm and key as symmetric key (SyKey) and Stores it
17. Customer sends response to the ZTTP Server
18. ZTTP server publishes the Customer Public Key
19. Server closes the Session of Customer.

6. DUAL KEY GENERATION FOR ML-TRADER, BANK

The Private key is generated by finding the unique integer \( D, 1 < D < j_2(N) \), such that \( ED = 1 \) (mod \( j_2(N) \)). The corresponding (primary signer's) partial private key is generated by finding the unique integer \( D_1 \), such that \( ED = 1 \) (mod \( j_2(N) \)). Next, the (co-signer's) partial private key \( D_2 \) is computed as \( D_2 = D / D_1 \).

6.1 Our MJ-RSA based dual-signature Scheme for ML-Trader / Bank

MJ-RSA based dual-signature scheme that allows two signers to compute a dual-signature efficiently. The core idea behind his scheme is to multiplicatively split the private key \( d \) into two partial keys \( D_1 \) and \( D_2 \) each associated with a different signer. That is, \( D = D_1D_2 \) (mod \( j_2(N) \)).

The dual-signature computation is then based on the equation \( H(M) = H(M) \) (mod \( N \)). In our fair-exchange protocol, we employ an MJ-RSA based dual-signature scheme that also splits \( D \) into two partial keys, but the splitting is done additively instead of multiplicatively.

6.2 Dual-signature generation for ML-Trader, Bank

The primary signer and co-signer create their respective partial signatures, \( \text{Sig}_1 = H(M)^{D_1} \) mod \( N = 1,2 \)
\( \text{Sig}_2 = H(M)^{D_2} \) mod \( N \) for signer
\( \text{Sig}_3 = H(M)^{D_2} \) mod \( N \) for co-signer
using their respective partial private keys \( D_1 \) and \( D_2 \). These are multiplied modulo \( N \) to form the dual-signature \( \text{Sig} \). That is, \( \text{Sig} = H(M)^{D_1D_2} \) mod \( N \).
The partial signature $a_1$ is considered valid if and only if
\[ \text{Sign}^E \mod N = H(M). \]
The dual-signature Sign is verified using the public key $E$.

7. REGISTRATION PROCESS OF ML-TRADER WITH ZTTP

1. ML-Trader Request for Connection establishment to ZTTP Server.
2. ZTTP Server establishes the Connection.
3. ZTTP Server Creates the Session for ML-Trader for future Communication.
4. ML-Trader Request for Symmetric key for that sends information.
5. ZTTP Generates the Prime number set = $P$.
6. ZTTP Selects the Largest Prime($P_i$) and finds its Primitive root($Y$) and sends the ML-Trader.
7. ML-Trader Stores the $P_i$ and $Y$.
8. ZTTP generates the random number $g$ and calculates $G = Y^g \mod P$.
9. Sends $G$ value to the ML-Trader.
10. ML-Trader generates the random number $h$ and calculates $H = Y^h \mod P$.
11. ZTTP Server Generates the SyKey = $G^h \mod P$.
12. ML-Trader Generates the SyKey = $H^g \mod P$.
13. ML-Trader sends $ack$ and requesting for public and private keys.
14. Server generates the public and two private keys($Co-Singer$ & $Ve-Singer$) using $M_{12}$ RSA.
15. Server encrypts the public and two private keys($Co-Singer$ & $Ve-Singer$) using RC4 Symmetric algorithm and key as symmetric key ($SyKey$).
16. ML-Trader decrypts the public and two private keys($Co-Singer$ & $Ve-Singer$) using RC4 Symmetric algorithm and key as Symmetric key ($SyKey$) and Stores it.
17. ML-Trader sends response to the ZTTP Server.
18. ZTTP server publishes the ML-Trader Public Key.
19. Server closes the Session of ML-Trader.

8. CONCLUSION

The protocols provide strong fairness. At the end of each exchange, a party obtains his counterpart's item(s) if and only if the other party obtains his item(s). If fairness is not achieved during a normal exchange process, a ZTTP can be invoked for assistance. In this paper we propose fair exchange system by encrypting the exchanged signature so that the receiver could verify its correctness, while both its originator and an agreed ZTTP could decrypt the signature; in the case when the ZTTP is involved, the signature's confidentiality is preserved from the ZTTP.

9. REFERENCES