Secure Transaction in Online Banking System Using IB-mRSA

S. Renuga Devi
ME Student, Department of CC,
National Engineering College, Kovilpatti
Tamilnadu, India

S. Chidambaram
Asst.Professor, Department of IT
National Engineering College, Kovilpatti
Tamilnadu, India

V. Manimaran
Asst.Professor, Department of IT
National Engineering college, kovilpatti
Tamilnadu, India

Abstract

Now a day's more number of clients using online banking, online banking systems are becoming more desirable targets for attacks. To maintain the clients trust and confidence in the security of their online banking services, financial institutions must identify how attackers compromise accounts and develop methods to protect them. Towards this purpose, presents a modified model to authenticate clients for online banking transactions through utilizing Identity-Based mediated RSA (IB-mRSA) technique in conjunction with the one-time ID concept for the purpose of increasing security, avoiding swallow's sorties and preventing reply attacks. The introduced system exploits a method for splitting private keys between the client and the Certification Authority (CA) server. Generating key splitting into two parties one for SEM (SEcurity Mediator) another key using for client using this key encrypt the message. SEM using key for Decrypt the client requests.

Index terms: **Certification Authority, Asymmetric key, SEM, one time ID**

1.Introduction

Cryptography techniques for secure (confidential) communication of two parties over an insecure (public) channel; verification of the authenticity of the source of a message; verification of the integrity of the messages transmitted via an insecure channel and unique identification of the originator of any message. Cryptanalysis attacks against the cryptographic techniques, and attack models will be presented. For many consumers, electronic banking means 24-hour access to cash through an automated teller machine (ATM) or Direct Deposit of paychecks into checking or savings accounts. But electronic banking involves many different types of transactions. Electronic banking, also known as electronic fund transfer (EFT), uses computer and electronic technology as a substitute for checks and other paper transactions. EFTs are initiated through devices like cards or codes that let you, or those you authorize, access your account. Many financial institutions use ATM or debit cards and Personal Identification Numbers (Pin's) for this purpose**.**

Some use other types of debit cards such as those that require, at the most, your signature or a scan. For example, some use radio frequency identification (RFID) or other forms of "contact less" technology that scan your information without direct contact. The federal Electronic Fund Transfer Act (EFT Act) covers some electronic consumer transactions. Cryptography and data encryption involved in protecting the transactions and information exchanged in Secure Online Banking operations. Both CA certificates and Site Key techniques are used to accomplish this feat. Banking customers must be protected from not only the loss of their sensitive financial and personal data to malicious hackers, but also from diabolical phishing attacks. These types of attacks involve using deception to trick banking customers into revealing sensitive person or financial data on a false website utilized to gather such information. Typically an e-mail is sent out to individuals, telling them that their banking institution needs to verify their account, as it has been frozen due to suspicions of online fraud, until this verification process is completed.

There is online fraud occurring, but it centers in that very email which is soliciting the customer's information. If the individual is so deceived into clicking on the link in the e-mail, he or she will be taken to a disguised web site, which looks like the real site of that bank that is being misrepresented. Here, they will be asked to verify the information to a number of important

questions, such as his or her social security number, credit card numbers, or bank account numbers. Protecting consumers from this requires more than just the use of standard SSL certificates. The customers must have a confident way to know if they are on the correct website for a given institution, or instead on a cleverly disguised fraudulent site. This is accomplished in the next generation SSL certificates. There are two technology issues needed to be resolved: (1) Security: is the primary concern of the Internet-based industries. The lack of security may result in serious damages and (2) Authentication: Encryption may help make the transactions more secure, but there is also a need to guarantee that no one alters the data at either end of the transaction.

1.1 Steps in online Banking System

- When visiting online banking's sign-on page, your browser establishes a secure session with our server.
- The secure session is established using a protocol called Secure Sockets Layer (SSL**)** Encryption. This protocol requires the exchange of what are called public and private keys.
- Keys are random numbers chosen for that session and are only known between your browser and our server. Once keys are exchanged, your browser will use the numbers to scramble (encrypt) the messages sent between your browser and our server.
- Both sides require the keys because they need to descramble (decrypt) messages received. The SSL protocol assures privacy, but also ensures no other website can "impersonate" your financial institution's website, nor alter information sent.
- To learn whether your browser is in secure mode, look for the secured lock symbol at the bottom of your browser window.

2. Identity Based Mediated RSA

Mediated RSA (mRSA) involves a special entity, called a SEM an on-line partially trusted server. To sign or decrypt a message, Alice must first obtain a message-specific token from the SEM. Without this token Alice can not use her private key. To revoke Alice's ability to sign or decrypt, the administrator instructs the SEM to stop issuing tokens for Alice's public key. At that instant, Alice's signature and/or decryption capabilities are revoked. For scalability reasons, a single SEM serves many users. One of the mRSA's advantages is its transparency: The main idea behind mRSA is the splitting of an RSA private key into two parts as in threshold RSA [9]. One part is given to a user while the other is given to a SEM. If the user and the SEM cooperate, they employ their respective half-keys in a way that is functionally equivalent to (and indistinguishable from) standard RSA. The fact that the private key is not held in its entirety by any one party is transparent to the outside, i.e., to the those who use the corresponding public key. Also, knowledge of a half-key cannot be used to derive the entire private key. Therefore, neither the user nor the SEM can decrypt or sign a message without mutual consent.

2.1 Identity Based Encryption

Identity-based encryption and digital signatures are important tools in modern secure communication. In general, identity-based crypto- graphic methods facilitate easy introduction of public key cryptography by al-lowing an entity's public key to be derived from some arbitrary identification value such as an email address or a phone number. Identity-based cryptography greatly reduces the need for, and reliance on, public key certificates. Mediated RSA (mRSA) is a simple and practical method of splitting RSA private keys between the user and the Security Mediator (SEM). Neither the user nor the SEM can cheat one another since each signature or decryption must involve both parties. mRSA allows fast and fine-grained control (revocation) over users' security privileges. However, mRSA still relies on public key certificates to derive public keys. Current identity-based cryptographic methods do not support fine-grained revocation while mediated cryptography (such as mRSA) still relies on public key certificates to derive public keys. In this paper we present IB-mRSA, a variant of mRSA that combines identity-based and mediated cryptography. IB-mRSA is simple, secure and very efficient.

3. Literature Survey

S.Rajalakshmi and S.K.Srivatsa(2007) Identity Based Encryption using mRSA in Electronic

Transaction in proposed system using a PKG (Public Key Generators) algorithm. First exchange a secret key of some kind. Using this secret key and an encryption algorithm, the sender encrypt the message. The receiver using same secret key and corresponding decryption algorithm decrypt the message. This is done by Certification Authority (CA), which distributes the public key of a user in the form of signed certificate.

Satoshi Koga, Kenji Imamoto, and Kouichi Sakurai(2004) proposed system are PKI(Public Key Infrastructure) is the basis of security infrastructure whose services are implemented and provided using public key technique in the paper is Enhancing Security of Security-Mediated PKI by one time ID. the PKI, a certificate is used to bind an entity's identity information with the corresponding public key. The certificate verifier must check not only the expiration date on the certificate but also the revocation information of it.

Kemal Bicakci Nazife Baykal A new alternative called SAOTS (server assisted one-time signatures) where just like proxy signatures generating a public key signature is possible without performing any public key operations at all SAOTS is a more promising approach since the signature is indistinguishable from a standard signature, no storage is necessary for the signer to prove the server_s cheating and the protocol works in less number of rounds (two instead of three). On the other hand, the drawback of SAOTS is the increased bandwidth requirement between the sender and server.

Joris Claessens, Valentin Dem,et.al.,Current technology is evolving fast and is constantly bringing new dimensions to our daily life. Electronic banking systems provide us with easy access to banking services. The interaction between user and bank has been substantially improved by deploying ATMs, phone banking, Internet banking, and more recently, mobile banking. These banking activities may include: retrieving an account balance, money transfers between a user's accounts, from a user's account to someone else's account, retrieving an account history.

Candid Wüeest Symantec Security Response, Dublin)in threats to online banking. The number of malicious applications targeting online banking transactions has increased dramatically. These malicious applications employ two kinds of attack vector – local attacks which occur on the local computer, and remote attacks, which redirect the victim to a remote site. The possibility also exists that both approaches will be combined. Some attacks may be foiled by adopting security measures such as transaction numbers (TAN).

4. Proposed System

4.1 Existing System

A secure website uses a method of encryption to transfer data across the Internet. Website can either be fully or partially secured or completely unsecured. Web pages that are used for general browsing are usually not secured pages which may be used to transmit sensitive information such as credit card details or personal information. In the real time, an organization, company or industry, password is very popular insecurity website, system and others.

- It is a unidirectional proxy re-encryption schemes with chosen-cipher text security in the standard model.
- It is a realistic adversarial model where attackers may choose dishonest users' keys on their own.
- The malicious parties could generate their public keys
- The proxy decrypts it using its copy of her secret key and re-encrypts the plaintext.
- By using the master key security property in that the proxy is unable to collude with delegates in order to expose the delegator's secret.
- A model Unidirectional Secure Proxy Re-Encryption for securing Chosen-cipher text attack.

4.2 Objective in proposed System

- An unidirectional proxy re-encryption schemes with chosen-cipher text security in the standard model.
- Including non-interactive temporary delegations.
- A secure chosen-cipher text from attacks while keeping them efficient and robust.
- Introducing of arbitrary delegates of public keys in the system.

In order to provide effective and secure banking transactions, there are two technology issues needed to be resolved:

(1) Security: is the primary concern of the Internet-based industries. The lack of security may result in serious damages

(2) Authentication: Encryption may help make the transactions more secure, but there is also a need to guarantee that no one alters the data at either end of the transaction

4.3 steps involved in Proposed System

Step 1: The client first sends a message to the CA containing the client's identity (ID). We use e-mail addresses as a unique identifier of clients to the system that will be used to compute the public exponent for each one

Step 2: The CA server checks the client's identity. Only if this identity is valid according to the sorted data, the CA takes care of all key setup. The first four parameters are generated in the same manner as in standard IB-mRSA in which a public key EKi is computed.

Step 3: CA produces a corresponding private key Instead di is effectively split into two parts d^{bank} and d^{sem} in which the bank and a SEM respectively secretly hold.

Step 4: At the first session, the CA generates the list of clients' identity and stores it in encrypted database for security. This shared secret key is required between the CA and SEM for state maintenance. The hash function is a one-way function that maps a variable-length message into a fixed-length value called a hash code.

Step 5: Following the computation of the above values, CA issues to the client the public key certificate, EKi, plus the token (OIDi,j, K_{client}) created for each session.

Step 6: After receiving the token from CA, the client sends a request to the bank by launching a message m that includes the client one-time ID encrypted with the received public key along with K_{client} that is used to verify the client

Step 7: The bank receives the above response, confirms that the content of a response is fresh by checking K_{client}, and then forwards the received message to the SEM for authentication

Step 8: SEM checks that the client is not revoked by comparing both of k^{bank}_{client} and k_{CA}^{client} getting from bank and CA respectively. If so, it signs the requested message with its private key to produce a partial signature

Step 9: If the bank's half signature fails verification (i.e. it signs a different message or includes an incorrect signature counter), the bank abort the protocol and concludes that a hostile attack has occurred. If there is no error, the banking system allows the client to perform its online transactions. In this case, no signature storing is required for the signer to prove the server's cheating

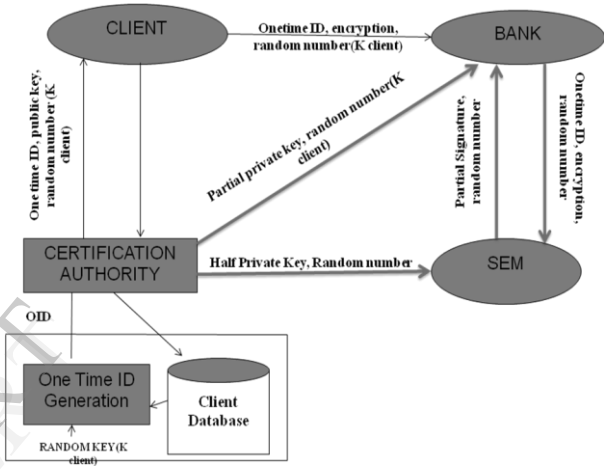

Fig1. The Proposed Online Transaction Security Model

4.4 Modules

There are four modules in the proposed systems

- Certificate Authority Module
- Key Generation (One Time ID)
- Key Splitting Module
- Security Mediator Module (SEM)

4.4.1 Certification Authority

Certification Authority (CA) module is the central of the whole architecture corresponding to a trusted third party that issues certificates.
The CA architecture is transparent to the sender of a message and to the verifier of a signature because the encryption and verification operations remain the same as in classical RSA. The purpose of CA server is to generate client bundle and Security Mediator (SEM) bundle that encapsulate the needed security component for

electronic banking transactions by splitting private keys into two parts, one for the client and the other for the SEM.

4.4.2 Key Generation (one Time ID)

One-time ID Module is a user's extraordinary identity, which has two properties: (i) an attacker cannot specify who is communicating even when he eavesdrops on one-time ID.(ii)one-time ID can be used only once.

4.4.3Key Splitting

Getting private keys split into two half send through the one half of the Bank another send through the mediator (SEM). Using this key for decryption operation

4.4.4 Security Mediator

Security Mediator (SEM) module is an online partially trusted server. The SEM can eliminate the need for certificate revocation list since the private key operations cannot occur after revocation. A SEM can be configured to operate in a state or stateless model. The former involves storing per user state (half-key and certificate) while, in the latter, no per user state is kept; however, some extra processing is incurred for each user request. The trade-off is clear: the former and fast request handling versus the latter and somewhat slower request handling. SEM can cheat one another since each signature or decryption must involve both parties. mRSA allows fast and fine-grained control (revocation) over users' security privileges. However, mRSA still relies on public key certificates to derive public keys.

5. Experimental Results

Banking system connecting database in SQL Server 2005 using for accessing the client's data. Implementation using DOT NET in C# language is intended to be a simple, modern, general-purpose, object-oriented programming language.

To validate the goals and experiment with the proposed model's implementation, we ran a number of tests with different key sizes. First experiment, we measured communication latency by varying the key size, which directly influences message sizes. Table 1. Latency is calculated as round trip delay between clients and the CA.

Key Size(bit)	Message Size(byte)	Average Latency(ms)
512	125	5.13
1024	205	6.72
2048	298	10.9

Table 1 : Average latency in key and message size

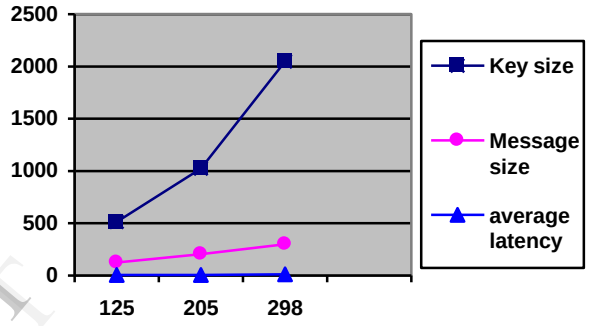

Fig 2: Communication Latency

The second experiment, the IB-mRSA results are obtained by measuring the time starting with sending of client's identity message to the CA and ending with the client encryption and bank decryption process time will be measured as see table 2

Processor	Key length(Bit)		
	512	1024	2048
PI-233 MHZ	25.32	40.1	255.7
pIII-500 MHZ	10.5	14.8	82.5
pIII-700 MHZ	9.5	10.3	55.7
pIII-933MHZ	8.9	7.3	43.9
PIV-1.2 GHz	7.53	9.3	58.7

Table 2 : processor speed and key lengths

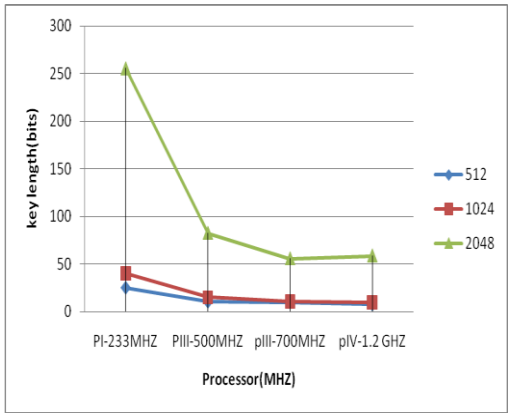

Fig 3: processor speed and key lengtth

6. Conclusion

Banking Transaction over internet has become a common feature in all clients. But how secure this all transactions. A solution to his secure transaction using a new model cryptography technique is IB-RSA and main advantage of this paper using one time-ID for each transaction. In that transaction ID using only once. This model to evaluate the performance metric average latency based on parameter key size and message size. Using IB-mRSA algorithm we achieve low average latency compare to other algorithms.

REFERENCES

[1]. K. Bicakci, N. Baykal, *Improved server assisted signatures*, Computer Networks 47 (2005) 351–366.

[2]. J. Cleens, V. Dem, J. Vandewalle, *On the security of today's online electronic banking systems*, Journal of Computers & Security 21 (3) (2002) 257–269.

[3]. W. Diffie and M. Hellman, *New directions in cryptography*, *IEEE Transactions on Information Theory*, 22 (1976), pp. 644-654.

[4]. D. Ding, G. Tsudik, *Simple identity based cryptography with mediated RSA*, in: The Cryptographers Track RSA Conference, San Francisco, USA, 2003.

[5]. T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory, 31 (1985),pp. 469-472.

[6]. K. Edge, R. Raines, M. Gremial, *The use of attack and protection trees to analyze for an online banking system*, in: Proceedings of the 40th Annual Hawaii International Conference on System Sciences, Hawaii, 3–6 January 2007.

[7]. M. O'Neill, *Low-cost SHA-1 hash function architecture for RFID tags, in: Proc. of IEEE International Symposium on Circuits and System (ISCAS,07)*, USA, 27–30 May 2007, pp. 1839–1842

[8]. R. L. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public key cryptosystems*, *Communication of the ACM*, 21(1978), pp. 120-126.

[9]. S. Rajalakshmi, S. Srivatsa, *Identity based encryption using mRSA in electronic transactions*, Information Technology Journal 6 (3) (2007) 435–440.

[10]. A.Shamir, *A polynomial time algorithm for that breaking the basic Merkle Hellmancryptosystem*, Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, IEEEtransact Computer Society Press 1982,pp. 145-152.

[11]. N. Smart, *The discrete logarithm problem on elliptic curves of trace one*, *Journal of Cryptology*, 12 (1999), pp. 193-196.

[12]. K. Satoshi, K. Imamoto, K. Sakurai, *Enhancing Security of Security-mediated PKI by one-time ID*, in: Proc. the 4th Annual PKI R&D Workshop, USA, April 19–21,

[13]. E. Verheul, *Evidence that XTR is more secure than super singular elliptic curve cryptosystems*, *Advances in Cryptology* EUROCRYPT 2001,Lecture Notes in Computer Science, 2045 (2001), Springer-Verlag, pp. 195-210