# Implementing Digital Signature based Secured Card System for Online Transactions

Shreenath Acharya
Dept of ISE
St. Joseph Engineering College
Mangalore, India

Sunaina Kotekar
Dept of ISE
St. Joseph Engineering College
Mangalore, India

Seema S Joshi
Dept of ISE
St. Joseph Engineering College
Mangalore, India

Shradda Shetty
Dept of ISE
St. Joseph Engineering College
Mangalore, India

Supreetha Lobo
Dept of ISE
St. Joseph Engineering College
Mangalore, India

## ABSTRACT

The RSA and other allied cryptographic mechanisms are widely used to provide security to the data during any online web based transactions. It has been proved that the Zhang proposed RSA cryptosystem could be easily cracked by an intruder. So, the security of the information in the network is becoming an important aspect in any web based communications. A new mechanism based on RSA to further enhance security is to make use of digital signatures to ensure the receiver that the message was created by a known sender, and that it was not altered in transit. In this paper digital signature mechanism based on the proposed scheme by Lin & Lei is implemented to describe the improved security given to the information while they are in transit during web based online transactions. It provides the security between two servers in IIS, which can be further improved and deployed in various technologies.

## Keywords

Digital signature, RSA, vulnerable network, data integrity, secure transaction.

## 1. INTRODUCTION

### 1.1Problem definition

The Internet is a worldwide collection of networks that links together millions of computers by various means, such as modems, routers, and servers. With the vastly growing number of computer networks connected to the Internet, network security has become a major concern for organizations throughout the world. It provides connections to businesses, the government, educational institutions and individuals. Hence the integrity and security of data transfer through the vulnerable network are very important issues in case of huge online transactions. So, in order to provide an efficient and secure transaction through the vulnerable network, improved version of digital signature scheme with fault tolerance based on the RSA cryptosystem is used.

Digital signature is the mathematical scheme for demonstrating the authenticity of a digital message or document. Digital signatures are one of the most important techniques of modern cryptography, and have many applications in information security systems. Digital signature is easily verified as authentication by anyone using the corresponding public key.

This "self-authenticating" property is quite suitable for some uses, such as broadcast of announcements and public key certificate. But it is unsuitable for many other applications. This property of self-authentication makes signatures those are somewhat commercially or personality sensitive, for instance, much more valuable to the industrial spy or extortionist. Thus, self-authentication is too much authentication for many applications. A well-established network security and a well implemented security policy can provide a highly secure solution so that only authorized people gain access to the system, that communications on the network are kept private from outsiders, and that data being communicated is kept safe. This paper addresses the key concepts of network security, common network vulnerabilities, network security threats and attacks, security measures and tools, and the development of a network security policy and proper violation response plan.

## 2. LITERATURE SURVEY

R. Rivest et. al[1] have proposed RSA as a public key cryptosystems based technique to keep the confidentiality of the data that transfers over the network. According to them, a legal user can use the receiver's public key to encrypt a message and the specific receiver can use his/her secret key to decrypt the encrypted message. They also conveyed that a user can sign a message with his/her secret key and any receiver can verify the signature by using the user's public key. The RSA technique was found to be useful in keeping the confidentiality of the transferred message, verifying the integrity of the received message, and to prove the senders' identity.

Zhang [2] has pointed out the vulnerabilities in the RSA to detect and correct errors. He proposed a new idea of digital signature scheme with fault tolerance based on RSA cryptosystem in which message to be sent is in the form of m*n matrix. He added each row and column checksums to the matrix along with the calculations of the hash value to be included in the matrix. Afterwards, the newly formed (m+1)*(n+1) matrix is converted into cipher text and sent through the network. This scheme efficiently keeps the confidentiality of the transferred message. Furthermore, it is able to detect and correct the error occurring in the computation processes or data transmission process.

Iuon-Chang Lei et. al [3] have pointed out the vulnerability of Zhang's scheme, i.e. a malicious user can generate a different message by permuting the rows or columns in the original

message matrix *X* with the same signature. They proposed a new improved version of Zhang's scheme in which an m*n message matrix is multiplied with two m*n prime matrices and then for the resulting matrix hash value is calculated which is a digital signature. Afterwards, the original matrix is appended at the end with the checksum calculated for each row and column. The hash value is appended to the last position of the matrix. The resulting (m+1)*(n+1) matrix is converted into cipher text and sent to the intended user. They showed that a malicious user cannot forge a valid message with the same signature by permuting the rows and columns in the matrix.

S. Ornar et. al [4] have proposed a student card system using a smart card technology which described how they can be used in an educational institution. They depicted the application of the smart card as a multipurpose means like student identification and security by not carrying cash. They also discussed about the type of cards as contact and contactless which could be used in applications as per the need.

Tzer-Shyong Chen et. al [5] have shown the utilization of Elliptic Curve Cryptosystem to overcome the flaws in RSA based and ElGamal based public key cryptosystems. They revealed that the encryption-decryption of RSA key is too large and the signature authentication mechanism of ElGamal is too long making them unsuitable for certain systems. Their approach integrated the short secret key characteristic of elliptic cryptography with (t, n) threshold method to create a scheme with simultaneous signaturing ie, group signature.

Hui-Feng Hwang et al. [6] proposed a fair blind signature based mechanism for untraceable electronic cash systems. They stated that only with the help of a judge or government, the signer can derive a link between a signature and the instance of signing protocol. They described that this scheme could be used in smart cards or mobile units making it suitable for electronic transactions.

Hyung-Kyu Yang et. al[7] have proposed an efficient dual signature scheme of undeniable signatures. They described that only the nominee can verify the signer's signature and only he can prove to the third party that issued signature is valid or not. They further stated that signature verification can only be done with the cooperation of signer unlike nominative signature schemes. They constructed protocols that implement this scheme using smart card.

Mei Hong et. al[8] have proposed a multi-service system model which allows the users to use a smart card to access different services with a single password. They achieved the service confidentiality through a set of protection mechanisms to guarantee the user's anonymity to all the service systems and ensured a high unlinkability between different services. They utilized the indirect password authentication scheme, mutual authentication protocols, and key agreement scheme to ensure communication confidentiality, efficiency and better performance of the transactions.

Hamed Taher doost et. al [9] have proposed a study of security principals of smart cards and to assess the security aspects towards the acceptance of this technology. They described by their survey conducted on university students and conveyed that most of the students have found it to be secure and have considered security as an important aspect to prove the confidentiality and authenticity of the user information in transit.

Taher Elgamal [10] proposed a public key cryptosystem and a signature scheme based on the difficulty of computing discrete algorithms over finite fields. He described through experiments that GF(p) is better for implementing any cryptographic system. His estimates specified that public file size is larger than the RSA scheme, but the difference is at most a factor of two and the size of the cipher text is double than that of the RSA system.

Smart Card Alliance[11] have proposed in their paper that privacy and security are the primary design goals of any personal ID system and they must be factored in to the specification of ID system policies, processes, architectures and technologies. They revealed the capacity of smart cards as a means to provide authenticated and authorized information access, implementing a personal firewall for the individual and releasing the information only when the card is presented.

Chung Kei Wong et.al[12] have proposed a tree chaining based signing/verification scheme for multiple packets. They have shown after comparison with the other digital signature schemes like RSA, DSA, ElGamal and Rabin that their proposed eFFS scheme is the fastest in signing, as fast as RSA in verification and also allows adjustable and incremental verification by receivers at different security levels.

Uma Somaniet. al[13] have proposed a scheme to ensure confidentiality, integrity and availability of the data used in cloud computing which is a modern computing technique through web based services. They described their implementation of digital signature based RSA Encryption Algorithm wherein the user data is message digested using hashing and encrypted with the private key to produce the signature which will be encrypted using RSA through receivers' public key to produce the cipher text. At the receivers' end the reverse process is performed to retrieve the original plain text thereby ensuring the data security.

## 3. SYSTEM ARCHITECTURE AND WORKING METHODOLOGY

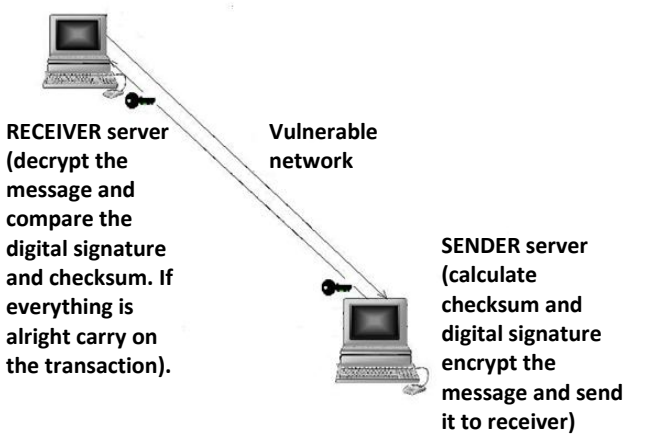



**Fig1:Architectural Diagram of Secure Student Card Software System**

A web application was created to help the college to maintain the complete transaction information about the students in a large database. It was mainly developed to make the job of an accountant easier i.e. they don't have to receive the cash by hand.

Whenever the payment (college, revaluation, dues or hostel fees) has to be done the bar code reader reads the bar code on the card and the money will be directly transferred from the student account to the college account. Performing transactions online is not secure. In order to provide full security and integrity, an Improved Digital Signature Scheme with Fault Tolerance in RSA which is an improved version of Zhang's Scheme has been implemented. The security part for the text box is explained in the following session.

In this paper few of the text boxes which have to be sent with security is converted to m*n message matrix, the transpose of the matrix is created of the size n*m and then the matrix is encrypted using the sender's private key. Later the checksum and hash value is also calculated accordingly as shown in the calculation part and those are encrypted. Encrypted hash value is called as digital signature.

For the key distribution a large hash file where the p, q, and public key will be stored is used. This large hash file will be stored in both the sender and the receiver side. Actually one part of the message is used to calculate hash value and according to that the public key in the large hash file is chosen. And the part of the message is sent to the receiver so that it can get the value of p. q, public key from the large hash file stored in the receiver side and can calculate the private key from that. This is successfully implemented in the IIS server.

The transaction information was encrypted and digital signature was calculated in the college server and used to send to the bank server through URL. In the bank side the information was decrypted and the checksum, hash value was calculated for the decrypted message. The hash value was compared with the received hash value to check the identity of the sender. And the calculated checksum was compared with the received checksum to find the message integrity. If there was no problem found in the digital signature and checksum the transaction was carried out in the bank side automatically after checking for the sufficient amount in the student account. If there was any problem found in the digital signature or checksum the transaction would be cancelled, thinking that some hacker had tried to change the data.

## 4. PROPOSED SCHEME

Improved version of Zhang's digital signature scheme [3] with fault tolerance is based on the RSA cryptography. In the RSA cryptography, each user provides a public key ($e$, $N$) and a secret key $d$, where $N$ is the product of two large prime numbers $p$ and $q$ such that $N = p \times q$, and the public key $e$ and secret key $d$ must satisfy the equation $d = e^{-1} \bmod (p-1)(q-1)$.

Let $(e_S, N_S)$ and $(e_R, N_R)$ be the public keys of sender and receiver, $d_S$ and $d_R$ are their secret keys. Assume $N_S \neq N_R$ and the length of $N_S$ and $N_R$ are the same for simplification.

If n number of text boxes in the particular page are to be encrypted and m is the maximum string size out of those m text box contents. Then data in text boxes can be converted to n*m matrix format, which is actual data to be sent in a safe way.

An improved algorithm is as shown. Here the original message matrix is not directly encrypted. But the transpose of the message matrix is taken and then encrypted. As observed in the result part though anyone tries to decrypt the message it is not the clear message line by line.

**Step 1:** The message has to be sent is in the form of n*m matrix as follows. Where m is the maximum horizontal length and n is the maximum vertical length of message matrix.

$$X = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1m} \\ x_{21} & x_{22} & \dots & x_{2m} \\ . & . & . & . \\ : & : & \ddots & : \\ x_{n1} & x_{n2} & \dots & x_{nm} \end{pmatrix}$$

Where $xij, 1 \le i \le n, 1 \le j \le m$, is a message block which has the same length as $N_S$ and $N_R$.

**Step 2:** Now we take the transpose of the original matrix:

$$T = \begin{pmatrix} t_{11} & t_{12} & \dots & t_{1n} \\ t_{21} & t_{22} & \dots & t_{2n} \\ . & . & . & . \\ : & : & \ddots & : \\ t_{m1} & t_{m2} & \dots & t_{mn} \end{pmatrix} = \begin{pmatrix} x_{11} & x_{21} & \dots & x_{n1} \\ x_{12} & x_{22} & \dots & x_{n2} \\ . & . & . & . \\ : & : & \ddots & : \\ x_{1m} & x_{2m} & \dots & x_{nm} \end{pmatrix}$$

**Step 3:** The sender creates two prime number matrixes $P$ and $Q$ as follows:

$$P = \begin{pmatrix} p_1 & p_2 & \dots & p_n \\ p_1 & p_2 & \dots & p_n \\ . & . & . & . \\ : & : & \ddots & : \\ p_1 & p_2 & \dots & p_n \end{pmatrix} \quad Q = \begin{pmatrix} q_1 q_1 & \dots & q_1 \\ q_2 q_2 & \dots & q_2 \\ . & . & . & . \\ : & : & \ddots & : \\ q_m q_m & \dots & q_m \end{pmatrix}$$

Where matrix $P$ and Matrix $Q$ have same dimensions as matrix T.

**Step 4:** Now the sender computes the new message matrix T, which is the entry-wise product of matrix T, $P$ and $Q$:

$$T = \begin{pmatrix} t_{11} t_{12} & \dots & t_{1n} \\ t_{21} t_{22} & \dots & t_{2n} \\ . & . & . & . \\ : & : & \ddots & : \\ t_{m1} t_{m2} & \dots & t_{mn} \end{pmatrix} \bullet \begin{pmatrix} p_1 & p_2 & \dots & p_n \\ p_1 & p_2 & \dots & p_n \\ . & . & . & . \\ : & : & \ddots & : \\ p_1 & p_2 & \dots & p_n \end{pmatrix} \bullet \begin{pmatrix} q_1 q_1 & \dots & q_1 \\ q_2 q_2 & \dots & q_2 \\ . & . & . & . \\ : & : & \ddots & : \\ q_m q_m & \dots & q_m \end{pmatrix}$$

$$= \begin{pmatrix} t_{11}*p_1*q_1 & t_{12}*p_2*q_1 \ldots & t_{1n}*p_n*q_1 \\ t_{21}*p_1*q_2 & t_{22}*p_2*q_2 \ldots & t_{2n}*p_n*q_2 \\ \vdots & \vdots & \vdots \\ t_{m1}*p_1*q_m & t_{m2}*p_2*q_m \ldots & t_{mn}*p_n*q_m \end{pmatrix}$$

$$= \begin{pmatrix} t_{11}t_{12} & \ldots & t_{1n} \\ t_{21}t_{22} & \ldots & t_{2n} \\ \vdots & \ddots & \vdots \\ t_{m1}t_{m2} & \ldots & t_{mn} \end{pmatrix}$$

**Step 5:** For the message matrix, the sender now constructs an (n+1)*(m+1) matrix $X_h$ as follows:

$$T_h = \begin{pmatrix} t_{11}t_{12} & \ldots & t_{1n} & T_1 \\ t_{21}t_{22} & \ldots & t_{2n} & T_2 \\ \vdots & \ddots & \vdots & \vdots \\ t_{m1}t_{m2} & \ldots & t_{mn} & T_m \\ T_1\ T_2 & \ldots & T_n & h \end{pmatrix}$$

Where,

$T_i = \prod_{j=1}^{n} t_{ij} * p_j \bmod N_S$, for $i<i<m$,

$T_j = \prod_{i=1}^{m} t_{ij} * q_i \bmod N_S$, for $i<j<n$,

$h = \prod_{j=1}^{n} (\prod_{i=1}^{m} t_{ij} \bmod N_S) \bmod N_S$

**Step 6:** The sender computes an (n+1)*(m+1) ciphered matrix as follows:

$$C_h = \begin{pmatrix} c_{11}c_{12} & \ldots & c_{1n} & C_1 \\ c_{21}c_{22} & \ldots & c_{2n} & C_2 \\ \vdots & \ddots & \vdots & \vdots \\ c_{m1}c_{m2} & \ldots & c_{mn} & C_m \\ C_1\ C_2 & \ldots & C_n & h_c \end{pmatrix}$$

Where,

$C_{ij} = t_{ij}^{eA} \bmod N_R$

$C_i = T_i^{eA} \bmod N_R$

$C_j = T_j^{eA} \bmod N_R$

$h_c = h^{dB} \bmod N_S$

Note that $T_i$ and $T_j$ are the checksums and $C_i$ and $\tilde{\tilde{C}}_j$ are the ciphered checksums.

**Step 7:** The receiver uses his/her secret key $d_A$ to decrypt $C_h$ and obtains decrypted message as follows:

$$X_h = \begin{pmatrix} t`_{11}t`_{12} & \ldots & t`_{1n} & T`_1 \\ t`_{21}t`_{22} & \ldots & t`_{2n} & T`_2 \\ \vdots & \ddots & \vdots & \vdots \\ t`_{m1}t`_{m2} & \ldots & t`_{mn} & T`_m \\ T`_1\ T`_2 & \ldots & T`_n & h` \end{pmatrix}$$

**Step 8:** Now the receiver verify the checksum to check the following:

$T`_i = \prod_{j=1}^{n} t`_{ij} * p_j \bmod N_S$

$T`_i = \prod_{i=1}^{m} t`_{ij} * q_j \bmod N_S$

$h` = \prod_{j=1}^{n} (\prod_{i=1}^{m} t`_{ij} \bmod N_S) \bmod N_S$

If the verifications are positive, then the receiver believes that the message was not altered during the transmission.

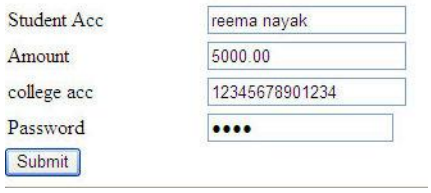
**Step 9:**The receiver takes the transpose of the matrix which will result in message as follows:

$$X_h = \begin{pmatrix} x`_{11} & x`_{12} & \ldots & x`_{1m} \\ x`_{21} & x`_{22} & \ldots & x`_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ x`_{n1} & x`_{n2} & \ldots & x`_{nm} \end{pmatrix} = \begin{pmatrix} t`_{11} & t`_{21} & \ldots & t`_{m1} \\ t`_{12} & t`_{22} & \ldots & t`_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ t`_{1n} & t`_{2n} & \ldots & t`_{mn} \end{pmatrix}$$

## 5. RESULTS

The above method was practically experimented by encrypting the confidential text box as shown below.

This shows some set of the text box which was sent with security measures.




Initially, the number of text box and length of the longest string in the text box is found out. In our example, the number of text box is 4 and length of longest string is 14. So we have created a matrix of size 4 rows and 14 columns shown as below.

```
Original text
r e e m a n a y a k * * *
5 0 0 0 . 0 0 * * * * * * *
1 2 3 4 5 6 7 8 9 0 1 2 3 4
s o n y * * * * * * * * * *
```

The 4*14 matrix obtained above is inverted ie, converted to a 14*4 matrix as shown below.

```
r 5 1 s
e 0 2 o
e 0 3 n
m 0 4 y
a . 5 *
0 6 *
n 0 7 *
a * 8 *
y * 9 *
a * 0 *
k * 1 *
* * 2 *
* * 3 *
* * 4 *
```

The character matrix is converted to integer matrix so that it will be easy for our further manipulation.

```
after changes
114 53 49 115
101 48 50 111
101 48 51 110
109 48 52 121
97 46 53 42
32 48 54 42
110 48 55 42
97 42 56 42
121 42 57 42
97 42 48 42
107 42 49 42
42 42 50 42
42 42 51 42
42 42 52 42
```

The generated prime matrix to be multiplied with the information matrix is as below.

```
Prime Matrix1
2 3 5 7
2 3 5 7
2 3 5 7
2 3 5 7
2 3 5 7
2 3 5 7
2 3 5 7
2 3 5 7
2 3 5 7
2 3 5 7
2 3 5 7
2 3 5 7
2 3 5 7
2 3 5 7
```

This is the second prime matrix generated to be multiplied with the information matrix.

```
Prime matrix2
2 2 2 2
3 3 3 3
5 5 5 5
7 7 7 7
11 11 11 11
13 13 13 13
17 17 17 17
19 19 19 19
23 23 23 23
29 29 29 29
31 31 31 31
37 37 37 37
41 41 41 41
43 43 43 43
```

The resultant multiplication matrix after multiplication of the information matrix, first prime matrix and second prime matrix looks like following matrix.

```
after matrix multiplication
456 318 490 1610
606 432 750 2331
1010 720 1275 3850
1526 1008 1820 5929
2134 1518 2915 3234
832 1872 3510 3822
3740 2448 4675 4998
3686 2394 5320 5586
5566 2898 6555 6762
5626 3654 6960 8526
6634 3906 7595 9114
3108 4662 9250 10878
3444 5166 10455 12054
3612 5418 11180 12642
```

For the above matrix at the end of row and column checksum is appended. The hash value is calculated and appended at the last row last column.

```
after checksum hash
456 318 490 1610 18
606 432 750 2331 20
1010 720 1275 3850 18
1526 1008 1820 5929 17
2134 1518 2915 3234 0
832 1872 3510 3822 13
3740 2448 4675 4998 9
3686 2394 5320 5586 3
5566 2898 6555 6762 23
5626 3654 6960 8526 29
6634 3906 7595 9114 21
3108 4662 9250 10878 28
3444 5166 10455 12054 0
3612 5418 11180 12642 5
2 27 30 13 17
```

The original information matrix is encrypted which shown in 4 columns and 14 rows in the below matrix. The checksum and hash value from the above matrix is encrypted and appended to encrypted matrix. This is 5th column, 15th row and last entry in the below matrix.

```
encripted matrix to be sent
108 144 43 123 86
186 146 84 15 41
186 146 51 206 86
99 146 52 127 153
193 210 144 87 0
128 146 7 87 208
206 146 217 87 185
193 87 62 87 126
127 87 73 87 56
193 87 146 87 74
113 87 43 87 200
87 87 84 87 46
87 87 51 87 0
87 87 52 87 164
59 105 140 208 29
```

**At the receiver side:**

The encrypted matrix is received and it is decrypted using key.

```
decripted matrix
114 53 49 115 18
101 48 50 111 20
101 48 51 110 18
109 48 52 121 17
97 46 53 42 0
32 48 54 42 13
110 48 55 42 9
97 42 56 42 3
121 42 57 42 23
97 42 48 42 29
107 42 49 42 21
42 42 50 42 28
42 42 51 42 0
42 42 52 42 5
2 27 30 13 17
```

Here digital signature is calculated and compared with the received digital signature.

If the signature matches, then the checksum is calculated and compared with received checksum. If this is fine then we can say there is no alteration in the sent data. The received information matrix looks like below matrix.

```
decripted message
r 5 1 s
e 0 2 o
e 0 3 n
m 0 4 y
a . 5 *
0 6 *
n 0 7 *
a * 8 *
y * 9 *
a * 0 *
k * 1 *
* * 2 *
* * 3 *
* * 4 *
```

The above matrix is then inverted so that it is readable to the receiver.

```
Original text
r e e m a n a y a k * * *
5 0 0 0 . 0 0 * * * * * * *
1 2 3 4 5 6 7 8 9 0 1 2 3 4
s o n y * * * * * * * * * *
```

## 5. CONCLUSION

The implemented algorithm tries to solve the security aspects of the vulnerable network and provides an efficient data transmission. As observed clearly, the improved version of the Zhang's scheme which was proposed for the large file encryption can also be used to provide network security in case of large online transaction. It is very important to encrypt the information on web pages which contains confidential information such as transaction details. So the proposed scheme can be successfully implemented for this purpose.

The proposed scheme further provides extra security by making use of transpose matrix. If an intruder looks into the message he will find it difficult to understand or calculate checksum/ hash value thus it will confuse the intruder. Hence this is a very good solution for eavesdropping problem. During the transaction, after receiving the information at the receiver side if there is any miss match in hash or checksum value could be immediately stopped**.**

## 6. REFERENCES

[1] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.

[2] C.N. Zhang, "Integrated Approach for Fault Tolerance and Digital Signature in RSA" IEEE Proceedings-Computers & Digital Techniques, vol. 146, no. 3, pp. 151-159, 1999.

[3] Iuon-Chang Lin and Hsing-Lei Wang, "An Improved Digital Signature Scheme with Fault Tolerance in RSA", Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. IEEE, 2010.

[4] S. Ornar and H. Djuhari, "Multi-Purpose Student Card System using Smart card technology", IEEE 2004.

[5] Tzer-Shyong Chen, Tsung-Chih Hsiao, and Tzer-Long Chen, "An Efficient Threshold Group Signature Scheme", IEEE 2004.

[6] Hue-Feng Huang and Chin-Chen Chang, "An Untraceable Electronic Cash System Using Fair Blind Signatures", IEEE International Conference on e-Business Engineering-ICEBE'06, 2006.

[7] Hyung-Kyu Yang and Young-HwaAn, "The Efficient Signature in the smart card system", IEEE 1998.

[8] Meri Hong and Hui Guo, "Design of Multi Service Card Systems for High Security and Performance", International Journal of Security and its Applications", Vol. 3, No.1, January 2009.

[9] Hamed Taher doost, Shamsul Sahibuddin, and Neda Jalaliyoon, "Smart Card Security, technology and Adoption",International Journal Security(IJS), Volume(5), Issue(2), 2011.

[10] Taher Elgamal, "A Public Key CryptoSystem and a Scheme based on Discrete Algorithms", Springer Verlag, 1998

[11] "Privacy and Secure identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology", Smart Card Alliance White Paper, 2003.

[12] Chung Kei Wong and Simon S. Lam, "Digital Signatures for Flows and Multicasts", IEEE/ACM Transactions On Networking, Vol. 7, No. 4, August 1999.

[13] Uma Somani, KanikaLakhani, and Manish Mundra, Implementing Digital Signature with RSA Encryption to Enhance the Data Security of Cloud in Cloud Computing", 1st International Conference on Parallel, Distributed and Grid Computing (PGDC), IEEE, 2010.