Quantitative Analysis of Non Repudiable Protocol for Remote Voting

Saira Yousuf, Malik Sikandar Hayat Khayal, *Member IACSIT*, Imran Sohail, and Aihab Khan

***Abstract*—With the phenomenal growth of internet and electronic transactions, security services, such as non repudiation, become crucial to many applications, e.g. electronic voting, electronic commerce, digital contract signing, and so on. The basic purpose of this research paper in to provide the quantitative analysis of a proposed non repudiable scheme in the published research paper named "Non Repudiation for Remote Voting". Non-repudiation provides the proof of the casted vote and ensures the authenticity of voter using digital signatures. In remote voting system the use of digital signature scheme is relatively low due to the complexity and insecurity of existing digital signatures algorithms, therefore, for authentication, usually keys, tokens or IDs are used. The proposed scheme has introduced the simplified way of digital signature generation using simple built in functions. Also, the complexity of RSA key generation for the signatures has also been reduced. The quantitative analysis has been done by calculating the time and complexity level of different signature generation functions, which concluded that the approach of digital signatures functions is quite simple as compare to other lengthy techniques of digital signatures, as their execution time and complexity is less as compare to existing signature generation techniques.**

***Index Terms*—Authenticity, digital signature, non repudiation, remote voting.**

I. Introduction

The purpose of this research paper is to provide the quantitative analysis of the proposed non-repudiable protocol in the research paper named "Non Repudiation for remote voting system"[1], which provided a mechanism for the authentication of voter and non repudiability of casted vote using digital signatures. In remote voting systems, issues such as confidentiality, integrity, accuracy and fairness, etc have been studied extensively; most interest in non-repudiation has only come in recent years but, for non repudiability the use of digital signatures is still relatively low and in most of the cases, the vote casting has been done without the use of digital signature scheme due to the complexity level and insecurity of existing digital signature algorithms. Also, the key generation and distribution process of RSA and DSA is another complex procedure, therefore, for authentication, usually keys, tokens or IDs are used. The complexity level, time and memory consumption of existing digital signature algorithms is also very high.

As remote voting enters the stage of real world implementations, the proposed digital signature scheme gives a recipient reason to believe that the vote was created by a valid voter, and that it was not altered in transit. Digital signature is the ways of authenticating the voter and unlike the normal signature it is difficult to forge and therefore it is a much safer to transact. Keeping this thing in view, the proposed scheme simplified the signature and key generation using simple built in functions. A single pair of RSA key is being generated for the system to produce signature rather than generating separate key for each voter which made vote cast easy for voter.

In electronic data exchange, the proposed digital signatures scheme can be used for software distribution, financial transactions, Domain Name System Security Extensions, online banking and in cases where it is important to detect forgery or tampering**.** The objectives of the proposed technique are the enhancement of security, simplification of the practical implementation, and the quantitative and comparative analysis of the proposed technique with the existing techniques w. r. t simplicity and efficiency.

Section 1 provides the brief introduction of the paper. Section 2 includes the related work being done so far and the comparison of proposed technique with the existing techniques. Section 3 gives the description of the proposed technique. Section 4 gives the obtained results with the help of tables and graphs. Section 5 gives conclusion and future work. Section 6 gives references.

II. Related Work

Eric L. Lazarus et al. [2] delivered a quantitative security analysis of internet voting vs. two other voting systems. The main purpose of this research paper is to deliver a report on preliminary results of a quantitative security analysis comparing three different voting systems: Hand Counted Paper Ballots (HCPB), Remote Poll-site voting with Ballot on Demand and Internet Voting. The paper chose HCPB to establish a security baseline, since it is a simple and well understood RPVBoD is a new proposal for overseas military voting where paper ballot are printed just before the voter votes, the ballot are marked by the voters and the paper ballots are returned the voters local jurisdiction to be counted. In internet voting the voted ballots are returned electronically. The paper analyzes the effect of attacks over these three voting systems. The paper concludes that the internet voting is much less secure then

Manuscript received February 15, 2012; revised March 26, 2012.

Saira Yousuf and Imran Sohail are with the Department of Software Engineering Fatima Jinnah Women University, The Mall, Rawalpindi, Pakistan (e-mail: saira_bse@yahoo.com, Imran.sohail@fjwu.edu.pk).

Malik Sikandar Hayat Khayal is with the Head Of Academic (SE), APCOM, Khadim Hussain Road, Lalkurt, Rawalpindi, Pakistan (e-mail: m.sikandarhayat@yahoo.com).

Aihab Khan is with the Department of Computer Science IQRA University, 5 Khayaban e Johar H-9, Islamabad, Pakistan (e-mail: aihabkhan@yahoo.com).

other voting systems including a realistic alternatives system for overseas voting.

Damian *et al.* [3] delivered a new secured protocol for medium scale e voting, based on Cetinkaya's Dyna Vote solution. The main features of this protocol are to improve security requirements and assure non repudiation of voter that is necessary in specific voting scenario. The protocol is divided into three phases: Obtaining Id's from authorities to communicate with other instances, obtaining the voting ballot and sending vote and counting votes and publishing results. In the proposed system, the solution for the safe medium scale e voting protocol is described. It consists of new mechanism that ensures uncoercibility and non repudiation of voting.

Bo Meng *et al.* [4] proposed a fair non repudiation protocol for electronic commerce and mailing. The proposed protocol uses hash value of cipher text and plain text message instead of plain text itself in non repudiation token, which solves transmitting large amount of data problem and improves confidentiality of msg. The purpose of non repudiation service in this paper is to generate, collect and maintain the evidence on the events and actions and to protect the parties involved in a transaction against the other party denying that a particular event took place. This paper uses tokens and the involvement of trusted third party for the non repudiation of origin and receipt.

Hao Wang *et al.* [5] proposed A Non-repudiable Protocol for Secure Messaging, which means that if the e mail is successfully sent, the sender cannot deny of sending the mail and the recipient cannot deny of receiving it.. The protocol uses an efficient RSA based convertible signature. This paper fixes convertible signature with non interactive zero knowledge proof method which is the signature scheme to elaborate an efficient non repudiable e mail protocol.

Jithra Adikari [6] proposed an efficient non repudiation protocol for techno information environment. This paper maps the traditional non repudiation mechanism in techno information environment. The evaluation methodology for efficiency of non repudiation mechanism has been improved during this work. The protocol uses the blind factors and the efficiency graphs for the non repudiability in techno environment. The paper focuses on strength of blind factors, forge ability, alterability and verifiability of the technique used. In the protocol, the ENRP is compared with the other existing non repudiation mechanisms and it is capable of delivering efficient non repudiation in techno environment.

Figure 1 shows the proposed model for the non repudiability of vote and the authenticity of voter presented in the published research paper.

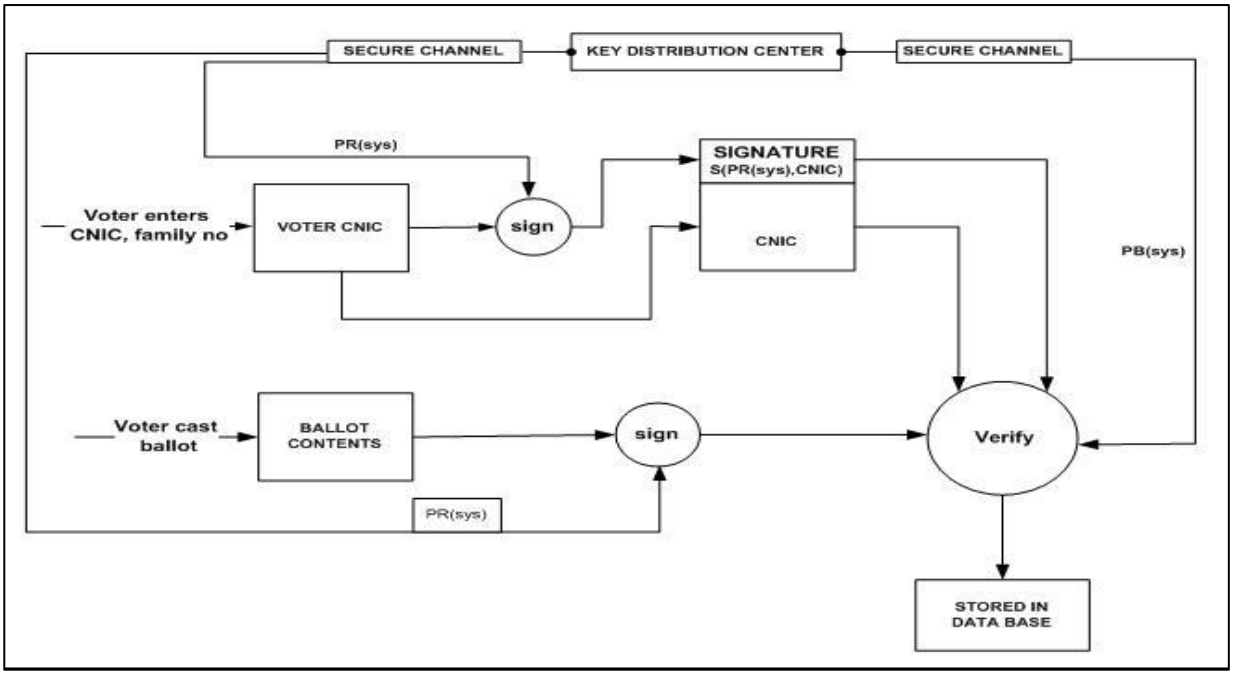

Fig. 1. Proposed model of non repudiation for remote voting

The TTP once distributes the key pairs to the system for signature and verification. The voter enters his login information to login to the system. Using private key, he generates signature and the system verifies the received signature to ensure authenticity of voter. The voter after casting ballot, re generate signature on ballot contents. After verification of signature, the signature and ballot contents are stored in database as a proof of casted vote which could not be reputed.

Comparative Analysis of Existing Techniques with Proposed Technique

Voter non repudiation oriented scheme for medium scale e -voting protocol proposed by Damian *et al.* [3] used tokens and IDs for the verification and authentication. In the first phase, the voter has to obtain [ID]SKCA from authorities to communicate with other instances in one voting session. Each voter get the certificate from TTP to sign a message using blind factor that will guarantee non repudiation. Voter has to receive confirming token IDvcfr (voter confirm key) from the organization holding the election before it start and to prepare request to obtain the ballot, and his private key. In case of denial of casted vote, If the voter is taken in to account by the authorities, the voter send the blind factor and signed components, that validate and proves that

particular voter has voted. The authorities check the voter's and counter's signatures and if message is correct they save the blind factor which would be used in counting phase.

On contrary, the proposed approach used digital signatures without generation of blind factors and certificate for authentication. The approach needs to involve TTP once before the election start. TTP needs to distribute a single pair of key for the system to generate and verify signature for authentication and non repudiability. Therefore each voter does not need to prepare request for his own private key, as the signature would be generated and verified by system itself. The voter does not need to blind or un blind the signature and contents. For the proof of casted vote the proposed technique saves the ballot against the generated signature, which could be shown in case of denial and vote cast could be challenged.

A non repudiable protocol for secure messaging proposed by Hao Wang *et al.* [5] used an RSA based convertible signature. This paper fixed convertible signature with non interactive zero knowledge proof method which is the signature scheme to elaborate non repudiability in e mail protocol. The RSA algorithm used prime modulo generation and modular exponentiation for RSA key generation, which comprises of complex multiple steps.

On contrary, the proposed approach used four simple steps for public and private key generation. The public and private key pair is generated using openssl genrsa -des3 -out privkey.pem 2048. Once done with this, the openssl genrsa is used for RSA key. The keys are stored in separate files and can be fetched when required.

Efficient non-repudiation for techno information environment proposed by Jithra Adikari [6] used the blind factors and the efficiency graphs for the non repudiability in techno environment. The paper focused on strength of blind factors, forge ability, alterability and verifiability of the technique used. The approach focused on the theoretical aspects of the protocol.

The proposed approach has the practical approach for the authenticity and verifiability. The graphs are used to show the comparative analysis of existing and proposed models.

A fair non repudiation protocol for electronic commerce and mailing proposed by Bo Meng *et al.* [4], proposed a protocol that used hash value of cipher text and plain text message instead of plain text itself in non repudiation token, which solves transmitting large amount of data problem and improves confidentiality of msg.

The proposed approach used the built in hash function in signature functions for the digest of signature.

III. Proposed Work

The proposed work provides the quantitative analysis of the proposed non repudiable technique in remote voting system. After casting the vote, the voter cannot deny having casted the vote. To achieve non repudiability, digital signatures are used to ensure the origin of casted vote and authenticity of voter.

A. Proposed Mathematical Model

Figure 02 shows the proposed mathematical model for the non repudiation of vote and the authenticity of voter in remote voting system. The voter enters CNIC and family number to login to the system. Using private key, he generate signature on CNIC. The system verifies the received signature to ensure authenticity of voter. The voter after casting ballot, re generate signature on ballot contents. After verification of signature, the signature and ballot contents are stored in database as a proof of casted vote which could not be reputed. Complex digital signature algorithms e. g RSA and DSA have been used for signature generation which required much execution time and memory space. Here it is proved that how the developed mechanism ensures authenticity and origin of vote using secure but efficient digital signature scheme and occupy less memory and time.

1) Identified real problem

a) To what extent digital signature scheme is efficient?

b) How execution time is affected by length of contents and signature?

c) To what extent the proposed technique is better than the existing techniques?

Suppose the available data is:

Length of vote contents=13

Number of signatures to be analyzed=4

The hash function to digest.

2) Formulated mathematical model

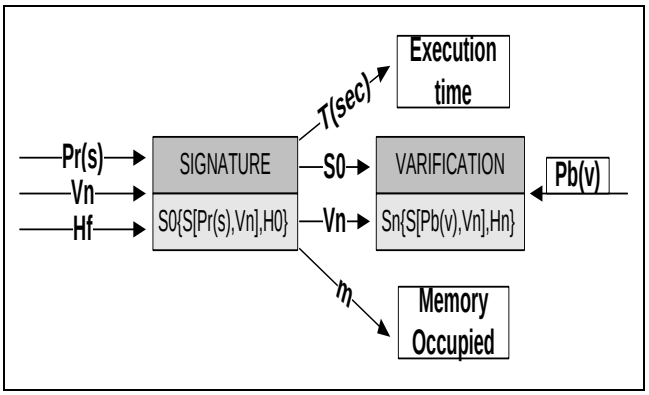

Fig. 2. Mathematical model for signature generation and verification

List of Factors

Vn: Length of vote contents
T: Execution time of signature
m: Memory occupied by signature
H: Hash produced
Hf: Hash function
Pr(s):Private Key of system for signature
Pb(v):Public key of system for verification
S0: Signature produced

3) Obtained mathematical solution

In order to generate signature signature '*S*' over the vote contents 'Vn' of length 'n', the systems private and public keys (*Pr*(*s*) , *Pb*(*s*)) are generated for the signature generation and verification.

Vn is the length of vote contents. The signature generated over Vn using the private key Pr(s), comes out to be

S0=S [*Pr*(*s*), *Vn*]

S0 is the signature generated by the voter, *H0* is the hash produced on signature to digest it i.e

H0=H (*Hf*, *S0*)

The overall signature becomes

S0={*S* [*Pr*(*s*), *Vn*], *H0*}

On receiver side the signature S is being verified using the public key *Pb*(*v*)

Sn=*S* [*Pr*(*s*), *Vn*]

Hn=*H* (*Hf*, *Sn*)

Sn={*S* [*Pb*(*v*), *Vn*], *Hn*}

If(*S0*= = *Sn*)

{

Signature Verified}

Otherwise voter not authentic.

4) Comparison with reality

The signature generation technique is secure because the signature is encrypted using private key and the hash produced used in it is irreversible. The private and the public keys are distributed through the secure channel once to the system; therefore it is difficult for the attacker to decrypt it.

The RSA and DSA signature scheme take large amount of memory (1024 bits) and so execution time too. The proposed signature scheme occupies 128 bits with execution time 0.00345 sec that ensures efficiency of the algorithm used.

The analysis of the proposed system gives the following results.

IV. Results and Analysis

A. Analysis of Signature Generation Time

As part of the research, the comparative analysis of signature generation time and efficiency is being done. For each signature, numbers of trials were made and the signature generation time is being observed. From most of the trials and test cases, it is being observed that the signature with hash function MD4 takes less time and is most efficient as shown in table 1and figure 03.

Trials	Length of Contents	OPEN_SSL SHA1	OPEN_SSL MD 2	OPEN_SSL MD4	OPEN_SSL MD5
1	37	5.974044	2.098898	1.234444	4.098988
2	37	5.8623373	2.338838	1.322232	4.234555
3	37	5.7666377	2.992238	1.995656	4.339833
4	37	6.0988333	3.009993	1.654333	4.123333

Table 1: Comparison of signature generation time

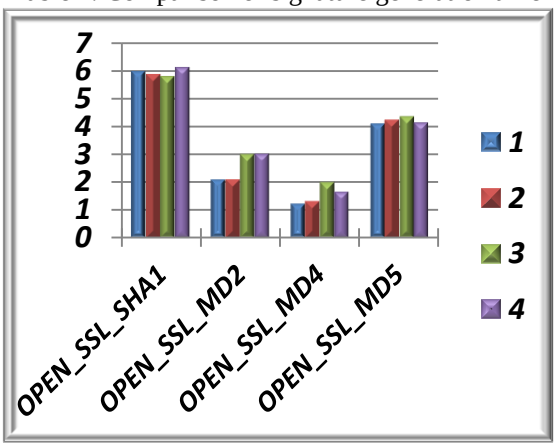

Fig. 3. Comparison of signature generation time

B. Mean Time

The mean time and standard deviation for the number of trials of each signature is being calculated

B7 =AVERAGE(B2:B5)

	A	B	C	D	E
1	Trial	OPEN_SSL_SHA1	OPEN_SSL_MD2	OPEN_SSL_MD4	OPEN_SSL_MD5
2	1	5.974044	2.098898	1.234444	4.098988
3	2	5.8623373	2.098898	1.322232	4.234555
4	3	5.7666377	2.992238	1.995656	4.339833
5	4	6.0988333	3.009993	1.654333	4.123333
6					
7	Mean	5.925463075	2.55000675	1.55166625	4.19917725
8	Std Dev	0.143326788	0.520945946	0.346860871	0.110793895
9	Sqrt(n)	2	2	2	2
10	Std Error	0.071663394	0.260472973	0.173430435	0.055396947

Fig. 4. Comparison of mean time

Figure 04 and 05 shows that the mean time for signature generation with hash MD4 is also very low, which ensures the efficiency of the digital functions used.

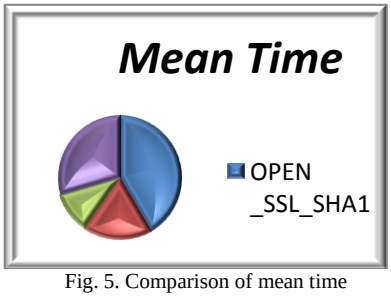

Fig. 5. Comparison of mean time

C. Standard Deviation and Standard Error

The standard deviation is a measure of the amount of variation in the data set. To measure the reliability of the calculated mean; the standard error is being calculated. The standard error is calculated by dividing the standard deviation by the square root of sample size, as shown in figure 06.

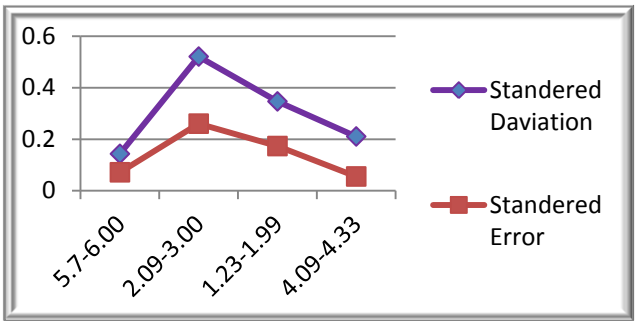

Fig. 6. Comparison of reliability measure of mean and STD deviation

As all the observations are close to the mean value, the standard deviation is small. If most of the observations differ greatly from the mean, then the standard deviation would be large.

D. Complexity Analysis of Digital Signature Algorithm Vs Openssl_Sign Function

1) Digital signature algorithm (DSA) Gary Locke at al.[7]

In DSA, Digital signature is computed using a set of domain parameters, a private key x, a per- message secret number k, date to be signed, and a hash function. A digital signature is verified using the same domain parameters, a public key y that is associated with the private key x used to generate the signature, data to be verified, and the same hash function that was used for the signature generation. The DSA is defined as follows:

Key Generation

Given a set of parameters, the second phase computes private and public keys for a single user. The keys are generated using RSA algorithm. Choose x by some random method, where $0 < x < q$. The key generation includes.

1. Choose two large prime numbers p and q of size.
2. Compute product, $n=pq$.
3. Compute $\phi(n)=(p-1)(q-1)$.
4. Choose an integer e between 1 and $\phi(n)$.
5. Calculate $y = g^x \bmod p$.

Public key is (p, q, g, y). Private Key is x.

Signature Generation

Let H be the hashing function and m the message:

- Generate a random per-message value k where $0 < k < q$.
- Calculate $r = (g^k \bmod p) \bmod q$.
- In the unlikely case that $r = 0$, start again with a different random k.
- Calculate $s = (k^{-1}(H(m) + x\, r)) \bmod q$.
- In the unlikely case that $s = 0$, start again with a different random k.
- The signature is (r, s).

Verification

- Reject the signature if $0 < r < q$ or $0 < s < q$ is not satisfied.
- Calculate $w = s^{-1} \bmod q$.
- Calculate $u1 = H(m)\, w \bmod q$.
- Calculate $u2 = r\, w \bmod q$.
- Calculate $v = ((g^{u1}\, y^{u2}) \bmod p) \bmod q$.
- The signature is valid if $v = r$.

Complexity of Key Generation: *Amar kumar Mohapatra at al. [8]*

Complexity for step 1:

1. For selecting the prime numbers p and q, the complexity for prime number p is O(s.(log.p)3. ln(p)) and for q is O(s.(log.q)3. ln(q)).

Complexity for step 2:

2. As step 2 involves computation of n, which is the product of p and q, so the complexity of step 2 is O(log2p.log2q).

Complexity for step 3:

3. By modular exponentiation, the complexity of step 3 is O((log2(p-1).(q-1))3.)(p-1). (q-1)-1)).

Complexity for step 4:

4. The complexity for gcd(e, ϕ (n))=1 is O((log2(p-1).(q-1))3.)(p-1). (q-1)+1)).

2) Openssl_sign function

Using this built in function does not require going through all those steps for signature generation and verification as described in DSA. The signature is generated using following parameters:

Openssl_sign($data, $binary_signature, $private_key, OPENSSL_ALGO_SHA1).

$data is the plain text on which the signature would be generated.

$binary_ signature is the variable in which the signature would be stored.

$ private_key is the generated private key.

OPENSSL_ALGO_SHA1 is the built in hash function, used for digest.

Before signature generation, a public and private key pair is generated as described:

To generate a RSA public and private key pair

A RSA key can be used both for encryption and for signing [9].

Generating a RSA key for the OPENSSL_SIGN is quite easy. The key generation comprises of four simple steps:

- ❖ Generate public and private key pair using openssl genrsa.
- ❖ Store the public and private key in separate files, using .txt extension.
- ❖ Fetch the private key from the txt file for signature generation using OPENSSL_Get_Private Key function.
- ❖ Fetch the public key from the text file using OPENSSL_Get_Publickey, for signature verification.

To generate signature, openssl genrsa -des3 -out privkey.pem 2048 is used. With this variant, one will be prompted for a protecting password. If someone don't want the key to be protected by a password, remove the flag '-des3' from the command line above.

The number 2048 is the size of the key, in bits. Today, 2048 or higher is recommended for RSA keys, as fewer amount of bits is consider insecure.

V. Conclusion

From the above complexity analysis of the DSA *vs* openssl_sign function, it is concluded that the built in functions for key and signature generation have reduced the complexity of implementation and simplified the key and signature generation over head. The complete RSA and DSA algorithms have been embedded behind these built in functions; so one does not need to develop the code for the

lengthy algorithm. Therefore, using these built in functions is quite an easy and smart approach for signature generation.

REFERANCES

[1] http://www.journalofcomputing.org/volume-3-issue-5-may-2011 http://www.scribd.com/doc/56905905/Non-Repudiation-for-Remote-Voting-System

[2] Eric L. Lazarus, David L. Dill, and Bruce Schneier, "Quantitative Security Analysis if Internet Voting vs. Two Other Voting Systems," A position paper for the "Workshop on UOCAVA Remote Voting Systems," pp. 1-5, August 06-07-2010.

[3] Damian Rusinek and Bogdan Ksiezopolski, "Voter Non Repudiation Oriented Scheme for the Medium Scale E voting Protocol," *Proceedings of the International Multi conference on Computer Science and Information Technology*, pp. 325-330, 2007.

[4] Bo Meng, Jianying Zhou, and D. Gollman, "A Fair Non Repudiation Protocol," IEEE Symposium on Security and Privacy, pp 68-73, 2007.

[5] Hao Wang, Yuyi Ou, Jie Ling, Xiaotao He, Lu Liang, Xiang Xu, "A Non-repudiable Protocol for Secure Messaging," *IFIP International Conference on Network and Parallel Computing Workshops*, pp. 490-494, 2007.

[6] Jithra Adikari, "Efficient Non Repudiation for Techno Information Environment," *First International Conference on Industrial and Information System*, pp. 454-458, 2008.

[7] Gary Locky, Patrik Galagher, "Digital Signature Standered," FIPS Pub 186-3, issued June 2009.

[8] Amar kumar Mohapatra, Neha Gupta, and Dr. Nupur Prakash, "Step-Wise Calculation of Performance Analysis of Safer with RSA Algorithm."

[9] http://www.openssl.org/docs/HOWTO/keys.txt, accessed July 2011.

BIBLIOGRAPHY

Saira Yousuf is the graduate student of Department of Software Engineering, Fatima Jinnah Women University the Mall, Rawalpindi, Pakistan, E-mail: saira_bse@yahoo.com. She has been awarded the first price for the thesis project "*Non Repudiation for Remote Voting*" in the software competition at COMSATS Abbotabad for EMCOT 2011. She also has a publication of the research paper named "*Non Repudiation for Remote Voting*" in US Journal of Computing [1].

Dr. M. Sikandar Hayat Khiyal born at Khushab, Pakistan. He is Professor and Head of Academic (ES), Army Public College of Management and Sciences (APCOMS), Khadim Hussain Road, Lalkurti, Rawalpindi, Pakistan. He Served in Pakistan Atomic Energy Commission for 25 years and involved in different research and development program of the PAEC. He developed software of underground flow and advanced fluid dynamic techniques. He was also involved at teaching in Computer Training Centre, PAEC and International Islamic University. His area of interest is Numerical Analysis of Algorithm, Theory of Automata and Theory of Computation. He has more than hundred research publications published in National and International Journals and Conference proceedings. He has supervised three PhD and more than one hundred and thirty research projects at graduate and postgraduate level. He is member of SIAM, ACM, Informing Science Institute, IACSIT. He is associate editor of IJCTE and Co editor of the journals JATIT and International Journal of Reviews in Computing. He is reviewer of the journals, IJCSIT, JIISIT, IJCEE and CEE of Elsevier.E-mail: m.sikandarhayat@yahoo.com.

Imran Sohail is the Assistant Professor and Web Administrator in Fatima Jinnah Women University the Mall, Rawalpindi, Pakistan, E-mail: Imran.sohail@fjwu.edu.pk, Imran.sohail@aresreklam.com. He did M.S in Internet Systems from BTH Sweden and worked as a web developer in Ericson Stockholm, Sweden. He is an associated author of publications: Network Security and DDoS (ISBN 978-3-8383-7009-5), Search Engine Optimization Techniques Practiced in Organization and Effectiveness of Intrusion Prevention System (IOS) in Fast Networks. He has vast experience of programming and has developed number of web applications including the web application of FJWU i.e**. www.fjwu.edu.pk.**

Aihab Khan is faculty member in Iqra university, Islamabad, Pakistan. His research interests are in the fields of data mining, data ware housing and information security. E-mail: aihabkhan@yahoo.com.