International Journal of Advance Research in Science and Engineering
Vol. No.4, Special Issue (01), Spetember 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

BIOMETRIC-SECURE ELECTRONIC VOTING SYSTEM: A NOVEL APPROACH FOR VOTING

Lakshmi Kumari[1], Dayanand[2], Vinay Kumar[3]

[1,2]Assistant Professor, Dept. of CSE, [3]Software Engineer, NEC Technologies

HMR Institute of Tech. & Mgt.New Delhi New Delhi, (India)

ABSTRACT

Election processes are the most important and critical part in democratic world. With the growth in Information and Communications Technologies, election processes are greatly influenced. This topic has been an active research area, on which, cryptographic primitives are used in order to propose secure protocols. Electronic Voting is a means of voting in which whole election process or a part of it is done through electronic devices. Most of the protocols proposed before are based on public key infrastructure (PKI) which requires large computing time and storage infrastructure to bind the keys to entities involved in election and enable other entities to verify key bindings. In this paper we propose the use of Identity based mediated RSA algorithm to eliminate the use of PKI, minutiae based fingerprint recognition algorithm to verify voters.

Keywords-Biometric Authentication, Electronic Voting, Identity Based Cryptography, Mediated RSA.

I. INTRODUCTION

Nowadays, the application of Information and Communications Technology (ICT) is introduced at several domains of fields. Voting processes are also influenced by information technologies until becoming be named electronic voting. Electronic voting (aka e-voting) is a term Encompassing several different types of voting, embracing both electronic means of casting a vote and electronic means of counting votes. It can speed the counting of ballots and can provide improved accessibility for disabled voters. Biometrics comprises methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In voting system, in particular, biometrics can be used as a form of identity access management and access control.In order to develop an electronic voting protocol the participation of several players such as: the representative of the political parties, a federal authority, officials and voters, are required, who perform four main phases: set-up phase, in which a citizen must be registered as a voter; authentication, where a voter becomes an authenticated voter depending on the authentication mechanisms used; voting phase, where an authenticated voter cast its vote, and counting phase, performed by tallying entities or a special entity, who counts the votes. The protocols proposed until now addressed their security requirements with Public Key Cryptography

PKC, which offers high flexibility through key agreement protocols and authentication mechanisms. However, when PKC is used, it is recommendable a Public Key Infrastructure PKI to bind the use of the public keys to entities and enable other ones to verify public key bindings. As a consequence of that, the components of every

protocol increase notably and a large amount of computing time and storage is required when the number of users increase rapidly. An alternative to the aforementioned is the Identity Based Cryptography IBC, where the key pair is generated unequivocally from data that are of relevance to the usage of the public key. With this kind of cryptography, it is possible to have all the benefits that the PKC does, without the PKI. Nonetheless, relying totally on available information technologies can only warrant the authentication/validation of the identity of a given voter, but, still, would not have the capacity to block any attempted abuse of the voting system, *viz.*, those voters who simply try to vote on behalf of others. Without additional measures, the integrity of a voting process, within the proper context, is far from any acceptable standard/s; the incorporation of *biometrics* would definitely have an added value towards achieving the required levels of election integrity. As the e-voting system involves participation of several entities, the single counting entity can be malicious therefore the authority of decryption of votes can be divided to increase *Robustness* of the overall system by using Threshold Schemes.

We propose an online e-voting protocol that does not improve only voting phase but also authentication phase. The protocol uses Identity based mediated RSA algorithm (IB-*m*RSA) as the encryption mechanism and a minutiae based fingerprint recognition algorithm to verify voters. A threshold decryption algorithm based on Shamir secret scheme is used to provide robustness by distributing the decryption authority among administrators. Blind signature scheme through RSA provides the required anonymity to the voter. The remainder of this document is organized as follows. Section 2 describes the functionality of the main construction blocks we use. In Section 3, the related work is summarized. Section 4 presents the electronic voting protocol we propose. Section 5 shows the evaluation we made of our electronic voting protocol. Finally, Section 6 summarizes our conclusions and draft out further work for this research.

II. MAIN CONSTRUCTION BLOCKS

In this section, we give a brief description of the different cryptographic primitives used as the main construction blocks.

2.1 Identity-Based Cryptography

In 1984 Shamir [3] asked for a public key encryption scheme in which the public key can be an arbitrary string. Shamir's original motivation for identity-based encryption was to simplify certificate management in e-mail systems.

Identity-based public key encryption facilitates easy introduction of public key cryptography by allowing an entity's public key to be derived from an arbitrary identification value, such as name, e-mail address or network address (or telephone number, or physical street address, or whatever). The main practical benefit of identity-based cryptography is in greatly reducing the need for, and reliance on, public key certificates.Identity-based systems allow any party to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the private key generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key (referred to as *master key*). Given the master public key, any party can compute a public key corresponding to the identity *ID* by combining the master public key with the identity value. To obtain a corresponding private key, the party

authorized to use the identity *ID* contacts the PKG, which uses the master private key to generate the private key for identity *ID*.

2.2 Blind Signatures

In 1983, Chaum [6] pioneered the idea of Blind signatures. The idea is for one party to have a document signed by a second party, but without showing the actual document to the second party. This technique can be very useful in electronic voting schemes. A voter can blind his ballot, and present it to the election administrators together with proof of eligibility. If the administrators approve of the eligibility of the voter, they sign the blinded ballot. The voter later unblinds his signed ballot, and delivers it anonymously to the election administrators. The administrators verify that the anonymously delivered ballot has been properly signed, and hence are assured it was delivered by an eligible voter.

2.3 Threshold Cryptography

In order to obtain robustness threshold secret sharing schemes are needed. In electronic elections these schemes are used for removing the requirement that all authorities act honestly, or that no authority is allowed to fail. A *(t, n)* threshold scheme requires a dealer and *n* participants. The dealer knows the secret value *s*, and is responsible for creating and distributing shares of *s.* Each participant is given a unique share of *s*, and *t* participants then have to pool their shares in order to recreate *s*. No set of participants less than t is able to gain any knowledge of *s*. The values of the parameters *(t, n)* are selected so that it is unlikely that as many as *t* participants act dishonestly, or that as many as $n - t$ participants fail.

2.3.1 Shamir Threshold Scheme

In [2], Shamir introduced the first threshold scheme. It is simple and elegant, and is still being used in many applications today. The dealer first selects *n* distinct, non-zero, random elements $x_i \in Z_p$, $1 \le i \le n$. To share a secret *s*, he selects another $t-1$ random elements $a_j \in Z_p$, $1 \le j \le t-1$, and uses the polynomial

$$f(x) = s + \sum_{j=1}^{t-1} a_j x^j \pmod P$$

in creating the *n* shares s_i of *s*, so that $s_i = f(x_i)$. The pair (x_i, s_i) is then given to participant *i*. The values x_i and *P* are public, the values $a_j$are secret, and each S_i is known only to the dealer and participant *i*. From the definition of *f(x)*, one can see that $s = f(0)$. To recreate the secret *s*, a group of *t* participants must pool their shares, and use them to evaluate the polynomial *f(x)* at 0. This is done with the simplified Lagrange interpolation formula. For any set of *t* pairs (x_{i_j}, s_{i_j}), $1 \le j \le t-1$, the secret *s* is computed as

$$s = \sum_{j=1}^{t} s_{i_j} \prod_{k=1, k \ne j}^{t} \frac{x_{i_k}}{x_{i_k} - x_{i_j}} (mod P)$$

III. RELATED WORK

Many different voting protocols and systems have been proposed before [1, 7, 8, 11 and 12] based on different cryptographic primitives they used and the requirements they fulfilled. Fujioka *et al.* (1992) in [1] brought new ideas into the design of electronic voting schemes, by combining the techniques of blind signatures and

anonymous channels. This scheme is practical, easily administered, and allows many ballot formats. It does however demand from all voters to return for a second time when opening their commitments. This is not convenient, and we have to expect a large number of voters not to complete their participation in the election.The voters can easily demonstrate how they have voted by just revealing their bit commitment key. This makes coercion or vote-selling an easy task.

In [12] Cramer *et al.* (1997), HomomorphicElGamal encryption is the basis of the election scheme. It uses multiple administrators, and a fault-tolerant threshold cryptosystem in dividing the trust amongst these administrators. Shares of the private decryption key are computed by the administrators in a joint key generation protocol, assuring privacy since no single participant gains knowledge of the actual key. This scheme is also not coercion resistant since voter can reveal its vote by showing randomness used in ElGamal encryption.

Baudron*et al.*(2001) in [11] propose a voting protocol that guarantees privacy of voters, public verifiability and robustness against a coalition of malicious authorities. Their scheme is based on the Paillier cryptosystem. The scheme is not coercion resistant in its basic description, but it is shown how to achieve this property by the use of randomizers, who re-encrypt ballots and create new proofs, so they no longer are recognized by the voters. Another contribution of this scheme is the design of a global election model. The scheme is adapted to national, regional, and local levels of elections, and seems to be the first election scheme that fits right into a real world election scenario.

Gallegos *et al.* (2009)in [8] propose the first protocol based on threshold identity based encryption from bilinear pairings. It considers a responsibility distributed model, in which the votes are decrypted with *t* of *n* users. Their scheme assumes the existence of trusted third party Private Key Generator (PKG) that runs a *key/common parameter generation algorithm* to generate its master/public key pair and all the necessary common parameters for threshold identity based encryption. The security of (PKG) can be a concern since it knows all users' secrets, and a compromise of (PKG) results in a total system break. Their scheme also uses blind signature scheme based on Public Key Infrastructure (PKI).

In [7],Gallegos, Gomez and Duchen (2010) gave an electronic voting protocol based on identity based cryptography, in order to provide stronger security requirements than protocols based on Public Key Infrastructure and without requiring the entire infrastructure needed by them. They combined identity based cryptography with threshold encryption scheme and blind signature scheme to accomplish all the security requirements of this kind of protocols. Their scheme also assumes the existence of two trusted third party Private Key Generators (PKG).

IV. OUR ELECTRONIC VOTING PROTOCOL

This section describes about the proposed e-voting protocol, and protocol description.

4.1 **Proposed E-Voting Protocol**

Our electronic protocol is divided into four stages: voting set-up, authentication, voting and counting.

I. Voting Set-up: It involves different authorities, in order to generate two key pairs. One of them will be used by the administrators of ballot in the voting phase to sign it blindly. The other one will be used by the voters and the counters to encrypt votes during the voting phase and to decrypt them during the counting phase.

The cryptosystem also considers Threshold Decryption in which key shares of decryption key are also generated and divided among administrators.

II. Authentication: This stage concerns with the authentication of the user, ensuring it is a valid voter. The authentication is done in two steps firstly by verifying the id and password of the voter assigned during registration and secondly a fingerprint recognition mechanism based on minutiae matching is used to verify a registered citizen to become an eligible voter.

The process of fingerprint verification has following steps.

- Gray level Enhancement
- Binarization
- Thinning (skeletonisation)
- Feature extraction
- Matching

Gray level Enhancement

It involves the adjustment of brightness, contrast or color in an image. A common reason for manipulating these attributes is the need to compensate for difficulties in image acquisition. For example, in images where an object of interest is backlit, that object can be underexposed almost to the point of its outer boundary. Convolution technique is used for Gray level Enhancement. It aims to improve the image such that content of image become visually more pleasing and clear.

Binarization

Most minutiae extraction algorithms operate on binary images where there are only two levels of interests: the black pixels that represent ridges and the white pixels that represent valleys.Binarization is the process that converts an image of up to 256 gray levels to a black and white image. The binarization process involves choosing a threshold value, and classifies all pixels with values above this threshold as white, and all other pixels as black.

Thinning

The final image enhancement step typically performed prior to minutiae extraction is thinning. Thinning is a morphological operation that successively erodes away the foreground pixels until they are one pixel wide. The patterns obtained after thinning are called as skeletons. The application of thinning algorithm to a fingerprint image preserves the connectivity of the ridges while forming a skeletonized version of the image.

Feature Extraction

The fingerprint minutiae are found at the feature extraction stage. Operating upon the thinned image, the minutiae are straightforward to detect as a ridge is only one pixel wide. The minutiae points are thus those which have a pixel value of one (ridge ending) as their neighbor or more than two(ridge bifurcations) in their neighborhood i.e. Ridge endings are found at termination points of thin lines and Ridge bifurcations are found at the junctions of three lines.

Matching

It includes one to one matching between the input images. Match point distance movement (a threshold value) is chosen. If distance between minutiae points is less than the threshold value then, points are matched.

III. Voting: First of all, in this stage a candidate must be selected by the voter. Then, if we want to encrypt the selected option, *the encryption algorithm* (the Identity Based Mediated RSA) needs to be run. The identity of any *"n"* entities, which developed voting set-up, is necessary. Finally, in order to ensure the voting phase is valid, a randomly chosen administrator must blindly sign it. A hash value is generated by using the vote, the signature and hash value of a timestamp which is delivered to the voter as a receipt. The voting process discussed above is shown in the flow diagram of Fig. 1.

IV. Counting: Before votes are counted and the tally is published, the signatures of the votes have to be verified with the *verification algorithm* of the blind signature, based on RSA algorithm. Then, in order to decrypt the votes using the *decryption algorithm*, it is necessary to collect valid decryption shares from at least "*t"* parties, to reconstruct the decryption key and finally, the plaintext can be generated. The counting process discussed above is shown in the flow diagram of Fig. 2.

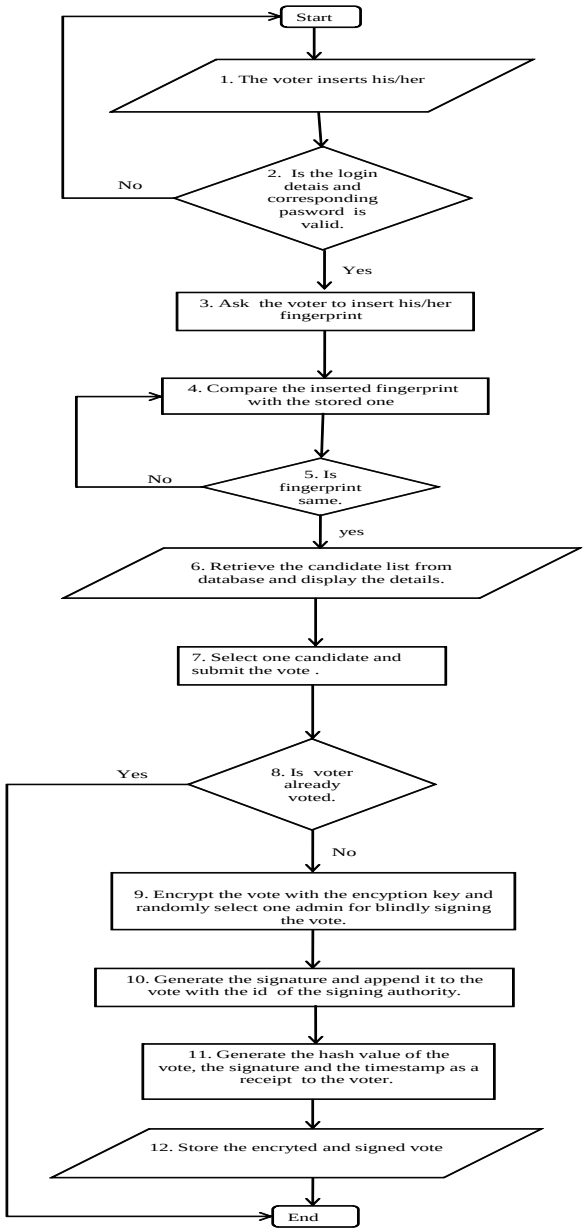

Fig. 1. Voting flowchart

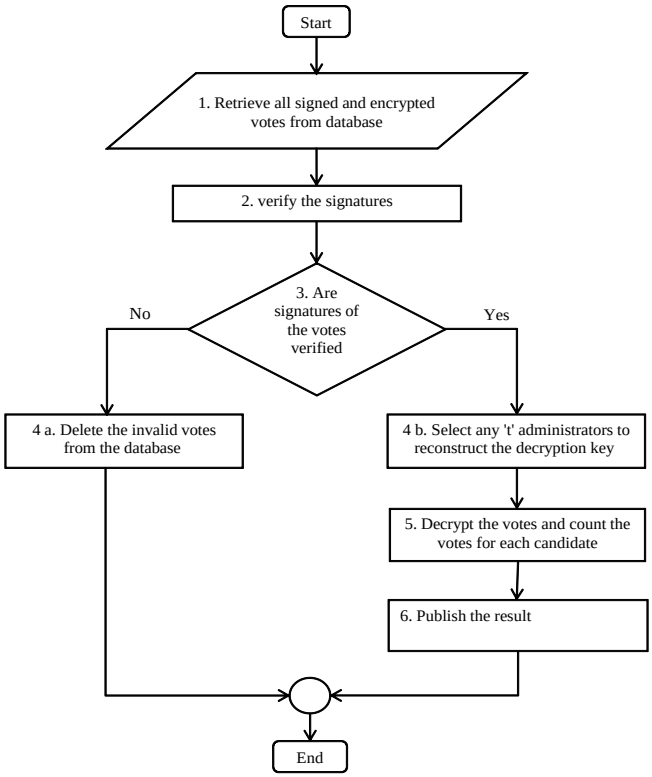

Fig. 2. Counting Flowchart

4.2 Protocol Description

I. Set-Up phase:

1. To generate the key pair (K_{pr},K_{pu}) used by the encryption primitive (m-RSA), Let k (even) be the security parameter.
2. Generate random $k/2$-bit primes p', q'such that $p = 2p'+1$, $q = 2q'+1$ are also prime and calculate $n \leftarrow pq$and$\varphi(n) \leftarrow (p-1)(q-1)$ where n is the modulus.
3. Randomly choose one administrator whose identity (ID_{admin}) is public, to derive the key pair.
4. Generate the hash code of the identity using the one way mapping function $KG\ (\ )$ and calculate $l \leftarrow k-|KG()|-1$.
5. The public exponent (e_{voter}) is constructed as the output of $KG(ID_{admin})$ represented as a binary string of the same length as n, with the least significant bit set, which ensures that it is odd and relatively prime to $\varphi(n)$. i.e. $e_{voter} \leftarrow 0^{l} \| KG(ID_{admin}) \| 1$.
6. The private exponent is calculated as $d_{voter} \leftarrow e_{voter}^{-1} \bmod \varphi(n)$.
7. The public keyK_{pu}consists of (n, e_{voter}) and the private key K_{pr}consists of (n ,d_{voter}).
8. For threshold decryption (t, n_t) scheme, select a polynomial of degree $(t-1)$, $f(x) = s+a_1 x+a_2 x^2+...a_{t-1}x^{t-1}$ for random $a_1...a_{t-1} \in Z^*$ where $s$is the secret to be shared and it contains private key K_{pr}i.e$s = K_{pr}$.
9. For every administrator $admin_i$where $1 \le i \le n_t$ the share of the secret (private key) is calculated as $x_i = f(i) \in Z^*$ and the pair (i, x_i) is given.It is possible to note that when $i = 0$, we can obtain the secret $s = x_0 = f(0)$.

10. Generate the key pairs ($K_{sig}^{(i)}$,$K_{ver}^{(i)}$) used by signature primitive for every*admin*$_i$using blind RSA signature technique and store in database.

II. Authentication phase

1. This phase is divided into two steps, in first step every voter is asked to fill the details (voter name, voter ID) with password in the login page.
2. If the details submitted with associated password are same as in the database then the voter is directed to the fingerprint acquisition page for the next step.
3. The acquired fingerprint is enhanced and matched with the corresponding fingerprint stored in the database.
4. If the voter fingerprint matches then voter is allowed to vote.

III. Voting phase

1. The voter chooses an option, denoted by *v* from the list of legal candidates, then it is encrypted with the K_{pu}as w = E [K_{pu} ,*v*].
2. In order to blindly sign the encrypted vote (w), the voter selects an admin randomly.
3. The voter chooses a random number *r* called the blinding factor and computes the blinded vote as B = w r^emod n_s and sends it to the selected admin for signing where (e, n_s) is the admin public key.
4. The admin signs the blinded vote and computes the blind signature as B′= B^d mod n_s and send it back to the voter.
5. The voter unblinds the signed vote by dividing B′ by *r* mod n_s resulting in the required signature *sig* = B′r^{-1}mod n_s
6. The database stores the vote, the signature of the vote and *id* of the admin who blindly signed the vote.
7. A hash value is generated by using the vote, the signature and the hash value of the timestamp; it is delivered to the voter as receipt H (w || *sig* || (Timestamp)) where H is a cryptographic hash function.

IV. Counting phase

1. Given the encrypted vote (w), the signature (*sig*) and *id* of admin who signed the vote, the Combining Entity (CE) verifies the signatures by checking that: *sig* = w^dmod n_s where(d, n_s) is the admin private key.
2. Then, in order to decrypt the votes, the CE selects a set $U \in \{1,..., n\}$ of *t* decryption shares $K_{pr}^{(i)}$=(i, x_i) ...$K_{pr}^{(t)}$ =(t, x_t) and computes: K_{pr}= $\sum_{i \in U} L_i x_i$where L_i = $\prod_{i \in U i \neq j} \frac{-x_i}{x_j - x_i}$ is the Lagrange interpolation coefficient.
3. Once CE has K_{pr}, it recovers plaintext for each voting: v = D[K_{pr}, w]
4. All the votes are counted and the tally is published in a bulletin. The voter can check that its vote was counted by verifying if its receipt appears on the published tally.

V. EVALUATION OF OUR PROTOCOL

5.1 Security

1. **Privacy:**The identity based encryption proposed in [14] is used as encryption primitive, which is shown secure against adaptive chosen ciphertext attack (CCA-2) under the random oracle assumption. It means that in the random oracle model, there does not exists an attacker *A* who has non-negligible advantage $Succ^{IB}_{n}(t, q_d, q_e)$ in a CCA-2 attack against the IB-RSA in a time *t*, where $q_d(q_e)$ denote the maximum number of decryption (encryption) queries allowed for each public key. The threshold scheme also assures the privacy property such that only the Combining Entity, jointly with *t*decryption shares, is able to decrypt the cast votes during the last stage. In addition to this, the privacy remains even when the votes are stored, because of the use of the hash value of a time stamp.
2. **Eligibility and Uniqueness:**The eligibility of the voters is checked by the system in two steps during the authentication stage. The first step is a password based authentication and in second step fingerprint recognition is used. To ensure that the voter cast its vote only once the voter id is also stored with the vote in the encrypted form, so when the vote is to be stored first voter id of the voter that casted the vote is checked in the database if it exists then vote is discarded.
3. **Incoercibility:**As soon as the voter selects the option it wants, it is encrypted. Then, the administrator, who receive the vote, receive it encrypted, and as mentioned before, there does not exists an algorithm that can break the IB-RSA in a polynomial time, with this, the encryption primitive used become hard to break. The administrator receives the encrypted vote in order to blindly sign, which means that the voter uses a blind parameter to blindly send its encrypted vote. With this, the voter cannot be forced to cast its vote in a particular way, it votes freely.
4. **Transparency:**In the protocol, a bulletin is used to publish the results of the counting phase. Moreover the reliability of our protocol relies in the cryptographic systems used instead on the secrecy of the network, which cannot be guaranteed.
5. **Accuracy:**During the voting phase, the voter receives a hash value as a receipt, which does not bind the voter with its vote. With this receipt, the voter can check if its vote was counted, because the counting entity will publish a bulletin with all the hash values counted. If any voter does not find its hash value in such a bulletin, it can make a complaint with officials.
6. **Robustness:**We assume that $n \geq 2t - 1$, in such way that at least *t* players are honest. In order to decrypt the votes, the CE selects from a set $U \in \{1... n\}$ any *t* decryption shares $K_{pr}^{(i)}=(i, x_i)$ ...$K_{pr}^{(t)}=(t, x_t)$ and computes: $K_{pr}= \sum_{i \in U} L_i x_i$where $L_i = \prod_{i \in U i \neq j} \frac{-x_i}{x_j - x_i}$ is the Lagrange interpolationcoefficient.

5.2 Comparison with Previous Protocols

In order to compare the proposed protocol with previous work, Table. 1 shows a comparison in terms of the total number of keys pairs and required authorities by the related protocols. In it, L is the number of levels that the protocolconsiders. C.A and T.A mean Certification and Trust Authority respectively.

Table. 1. Comparative Table

Protocol	Key Pairs	T.A	C.A	Complexity assumptions
Cramer [17]	1	0	1	Diffie-Hellman
Baudron [16]	1 * L	0	1 * L	Composite Residuosity Class
Gallegos [8]	2	2	0	Bilinear Diffie-Hellman
Gallegos [9]	2	1	1	Bilinear Diffie-Hellman
Our protocol	2	0	0	Prime factorization (RSA/OAEP)

From the comparison details shown in Table 1 it is possible to see that Cramer's protocol requires only one key pair but it also requires a PKI in registration of the voters and later in verification of the vote. This scheme is also coercive as voter can reveal its randomness parameter used in ElGamal encryption. The proposed protocol is satisfying all the basic security requirements of a voting system and also more practical as it does not involve any third party systems.

VI. CONCLUSION

In this paper, a secure electronic voting protocol based on identity based cryptography has been proposed. The encryption algorithm IB-*m*RSA/OAEP is semantically secure against adaptive chosen ciphertext attacks (CCA-2) in the random oracle model which assures that breaking of the protocol would not be easy. It accomplishes all major security requirements of an electronic voting system: privacy, eligibility, uniqueness, transparency, accuracy, incoercibility and robustness. With the incorporation of biometric features in the authentication phase the proposed scheme is capable of denying access to any illegal voter's, preventing multiple votes by the same voter, and blocking any introduced forms of malice that would adversely affect the voting process altogether. Moreover, the proposed voting system caters for the needs of the physically challenged voters that would facilitate voting to a voter's convenience.As a future work we consider the use of multisignature schemes. These schemes allow any subgroup of a group of users to sign a document jointly, such that a verifier is convinced that each member of the subgroup participate in signing. We also consider incorporating threshold blind signatures in our protocol, in which the secret key will be distributed among *n* parties with the help of a trusted dealer or without it by running an interactive protocol among all parties. To sign a message *M* as vote, any subset of more than *t* parties can use their shares of the secret and execute an interactive blind signature generation protocol, which outputs signatures of the voters that can be verified by anybody using the unique fixed public key. It is important to mention that all the signatures have to be made blindly in order to avoid the signer can act as a malicious party in an electronic voting protocol. One issue remains for future work is IB-*m*RSA performance. Using a hash function for public key mapping makes encryption more expensive than RSA since the public exponent is random (and on the average half of the bits are set). It is required to investigate alternative mapping functions that can produce more "efficient" RSA exponents. From biometric point of view Fingerprint recognition can be combined with other (more complex like iris recognition) biometric features to make the authentication more secure and error free.

REFERENCES

[1] A.Fujioka, T. Okamoto, K. Ohta., 1992. A Practical Secret Voting Scheme for Large Scale Elections. Advances in Cryptology - AusCrypt'92, pp. 244-251.

[2] A. Shamir., 1979. How to share a secret.Communications ACM 22, pp. 612-613.

[3] A. Shamir., 1984. Identity-based cryptosystems and signature schemes. Advances in Cryptology-Crypto84, LNCS 196, Springer-Verlag, pp. 47-53.

[4] D. Boneh and M. Franklin, 2001. Identity-Based Encryption from the Weil Pairing. In Proc. Of the 21st Annual International Cryptology Conference on Advances in Cryptology, LNCS 2139, Springer-Verlag, pp. 213-229.

[5] D. Boneh, X. Ding, G. Tsudik, and C.M. Wong., 2001. A method for fast revocation of public key certificates and security capabilities. In 10th USENIX Security Symposium, Washington, D. C.

[6] D. Chaum. 1983. Blind Signatures for untraceable payments.Advances in Cryptology Crypto82, LNCS, Springer-Verlag, pp.199-203.

[7] G. Gallegos-G, R. Gomez-C and G.I. Duchen-S., 2010. Electronic Voting using Identity Based Cryptography.In Proc. of the 4th International Conference on Digital society,IEEE Computer Society, St. Maarten, pp. 31 – 36.

[8] G. Gallegos-G, R. Gomez-C, M. Salinas-R and G.I. Duchen-S., 2009. A New and Secure Electronic Voting Protocol Based on Bilinear Pairings.In Proc. of the 19th International Conference on Electrical, Communications and Computers, IEEE Computer Society, Puebla-Mexico, pp. 240-244.

[9] Goldwasser, S. and Bellare, M., 1996-2008. Lecture Notes on Cryptography. Summer course on cryptography, MIT [online]. Available at : http://cseweb.ucsd.edu/~mihir/papers/gb.pdf [accessed 24 may 2011]

[10] Khasawneh. M, Malkawi. M, Al-Jarrah. O, Barakat. L, Hayajneh. T.S, Ebaid. M.S., 2008. A Biometric-Secure e-Voting System for Election Processes.In Proc. of the 5th International Symposium on Mechatronics and its Applications, IEEE Computer Society, Amman- Jordan ,pp. 1 – 8.

[11] O. Baudron, P. Fouque, D. Pointcheval, G. Poupard and J. Stern., 2001. Practical multi-candidate election system.In Proc. Of the 20th Symposium on Principles of Distributed Computing, ACM, pp. 274-283.

[12] R. Cramer, R. Gennaro, and B. Schoenmakers., 1997. A Secure and Optimally Efficient Multi-Authority Election Scheme. Advances in Cryptology EURO CRYPT'97,LNCS 1233,Springer Verlag, pp. 103-118.

[13] Sonja Hof., 2004. E-Voting and Biometric Systems?.In Proceedings Electronic Voting in Europe Technology, Law, Politics and Society. LNI P-47, pp. 63-72.

[14] Xuhua Ding and Gene Tsudik., 2003. Simple Identity Based Cryptography with Mediated RSA.LNCS 2612 Springer-Verlag,pp.192–209