An Analytical study of E-voting System

Neha Saini, Himani Verma, Mr. Pankaj Sharma

Department of Information Technology, ABES Engineering College Ghaziabad, AKTU Lucknow

Abstract- **Voting is a fundamental decision making instrument in any consensus-based society and thus, plays a critical role in formation of real democratic environment which not only require a secure but a fair voting system. Thus, this proposed system deals with design, build and test an E-Voting System that facilitates a voter, candidates and administrator to participate in an online voting. The proposed system will speed up the counting of ballots and also reduce the cost & human effort during election as well as post election activities. In our traditional voting system, the administrative staff generally do verification using traditional methods of biometric enabled devices but in this proposed system, the security of the system can be enhanced using Blind multi signature scheme or Threshold blind signatures. Nowadays, every person has a unique Aadhar card number which can also be used to improve the authentication of the voting system. This can be done by formal registration through administrators and by entering One time password and Aadhar Card. Not only this it will also ensure privacy, authentication, fairness, transparency, integrity and incoercibility.**

***Keywords*—Cryptography, E-voting, Verifiability, Denial of service (DOS)**

I. INTRODUCTION

As the modern communications and Internet, today are almost accessible electronically, the computer technology users, brings the increasing need for electronic services and their security. Usages of new technology in the voting process improve the elections in natural. This new technology refers to electronic voting systems where the election data is recorded, stored and processed primarily as digital information.

Nowadays, the application of Information and Communications Technology (ICT) is introduced at several domains of fields. Its multidimensional benefits are becoming more visible from time to time. The economical benefit gained from the technology is the most significant one. Furthermore, it helps to increase the qualities of the work, reduces the complexities of tasks, keeps the security of data in most favourable condition, makes data transfer more easy, and others. ICT role is wide, starting from low level systems to high level business and governmental applications. The business applications are used by business people to manage the business process; e-commerce can be taken as one example that shows the application of ICT to the business community. Similarly, ICT can play its role for governmental applications. Election is one of the tasks of the government that can be benefited from ICT.

II. ELECTRONIC VOTING SYSTEMS

Electronic voting (also known as 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 include punched cards, optical scan voting systems and specialized voting kiosks (including self-contained direct-recording electronic voting systems, or DRE). It can also involve transmission of ballots and votes via telephones, private computer networks, or the Internet. It can speed the counting of ballots . Today e-voting processes use various cryptographic algorithms to propose a secure protocol. Generally an e-voting system consists of five main phases as depicted in Fig 2.1. In the Registration phase each voter must register to provide his/her identification data for the participation in election process. The Setup phase generates the keys used in encryption and signature scheme in order to encrypt and sign votes. In the Authentication phase the administrator verifies a registered citizen to become an eligible voter by comparing his/her details with the information given at the time of registration. The Voting phase manages the casting of the vote in a secure manner so that no early results can be obtained which could influence the remaining voters; this is done by encrypting and signing the votes. Counting phase is responsible for the last and final stage of the election process in which invalid votes are checked and removed, valid votes are counted and finally the election result is generated.

A. **Securities of the E-voting systems** The main goal of a secure e-voting is to ensure the privacy of the voters and accuracy of the votes. A secure e-voting system satisfies the following requirements, Eligibility: only votes of legitimate voters shall be taken into account; Unreusability: each voter is allowed to cast one vote; Anonymity: votes are set secret; Accuracy: cast ballot cannot be altered. Therefore, it must not be possible to delete ballots nor to add ballots, once the election has been closed; Fairness: partial tabulation is impossible; Vote and go: once a voter has casted their vote, no further action prior to the end of the election; Public verifiability: anyone should be able to readily check the validity of the whole voting process.

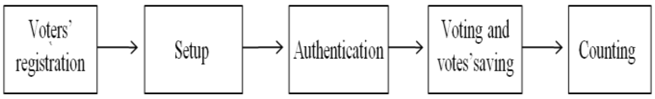


Fig. 2.1 Phases of an e-voting system

B. **Issues of Present Voting System** There have been several studies on using computer technologies to improve elections these studies caution against the risks of moving too quickly to adopt electronic voting system, because of the software engineering challenges, insider threats, network vulnerabilities, and the challenges of auditing. Accuracy: It is not possible for a vote to be altered or be eliminated the invalid vote cannot be counted from the finally tally .Democracy: It permits only eligible voters to vote and, it ensures that eligible voters vote only once. Privacy: Neither authority nor anyone else can link any ballot to the voter

Verifiability: Independently verification of that all votes have been counted correctly. Resistance: No electoral entity (any server participating in the election) or group of entities, running the election can work in a conspiracy to introduce votes or to prevent voters from voting. Availability: The system works properly as long as the poll stands and any voter can have access to it from the beginning to the end of the poll. Resume Ability: The system allows any voter to interrupt the voting process to resume it or restart it while the poll stands . The existing elections were done in traditional way, using ballot, ink and tallying the votes later. But the proposed system prevents the election from being inaccurate. Problems encountered during the usual elections are as follows:

- It requires human participation, in tallying the votes that makes the elections time consuming and prone to human error.
- The voter finds the event boring resulting to a small number of voters.
- Deceitful election mechanism.
- Constant spending funds for the elections staff are provided.

So, the proposed electronic voting system has to be addressed with these problems.

C. Proposed system of online e-voting

The process of voter registration before the election process is always done by Administrator as follows the before . Registration phase begins by storing the Voter information such as Unique AADHAR CARD NUMBER and GSM one time password which will authenticate the user and eligibility to vote as well. This not only improve voting phase but also authentication phase. The proposed system uses a set of cryptographic primitives and fingerprint recognition mechanism to provide strong security requirements of a voting system. This will use Identity based mediated RSA algorithm (IB-mRSA) as the encryption tool 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 and blind signature scheme through RSA provides the required anonymity to the voter.

III. MOTIVATION

Today voting processes are the most important element of democracy as the society way to make decisions. Such processes have been influenced by information technologies until becoming be named electronic voting. This topic has been an active research area, on which, cryptographic primitives are used in order to propose secure protocols. 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. 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.

IV. PROJECT OBJECTIVE

The objectives of “Electronic Voting System” are as follows

- To decrease the computing time and storage requirements.
- To ensure voter authentication through Fingerprint recognition.
- To increase Robustness by using Threshold decryption scheme.
- To develop a general prototype system that provides security and trusted electronic voting.

V. VOTING STYLES

In an election, the voting style defines the different way by which the user can cast a vote. There are numerous different types of voting styles:

[1] 1-out-of-2 voting (yes/no voting): Voter’s answer is a “yes” or “no”. Vote is a one bit: 1 for “yes” and 0 for “no”.

[2] 1-out-of-L voting: Voter has L possibilities and he chooses one of them.

[3] K-out-of-L voting: Voter selects K different elements from a set of L possibilities. The order of the selected elements is not important.

[4] K-out-of-L ordered voting: Voter puts into order K different elements from a set of L possibilities.

Write-in voting: Voter formulates his own answer and writes it down. Vote is a string of letters with specified maximum length, representing the name of an individual or a party.

VI. SCOPE OF THE PROJECT

1. Proposal of an Improved and Biometric-Secure Electronic Voting System.
2. Feasibility study for technical and operational analysis of system’s implementation.
3. Design of protocol & division into modules

Setup module: This phase generates the keys and signature and also divides the decryption key among administrators.

Authentication module: In this phase a fingerprint recognition mechanism based on minutiae matching is used to authenticate a registered citizen to become an eligible voter.

Voting module: An option is selected by the voter, which is encrypted with the public key generated in the Set-up phase, and then blindly signed with the private key of the identity selected by the voter. 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.

Counting module: 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. 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.

4. Integration of the Modules.
5. Deployment of the system on Apache Tomcat web server.
6. Performance analysis of the system.

VII. RELATED PREVIOUS WORK

Many different voting protocols and systems have been proposed before [1, 2, 3, 4, and 5] 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 No practical, easily administered, and allows many ballot formats. It does however have some disadvantages, denying it the candidacy for a real world election.

- If a voter registers, but abstains from the voting phase, the administrator can add a vote on the voter's behalf without fear of detection.
- The scheme demands 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 [5] Cramer et al. (1997), Homomorphic ElGamal 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 [4] 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 elections, and seems to be the first election scheme that fits right into a real world election scenario.

Gallegos et al. (2009) in [3] 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 [2], 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).

VII. LITERATURE SURVEY

1.1 ELECTRONIC VOTING AND ITS REQUIREMENTS

Over the last decade, the growth of the World Wide Web has changed the ways of interaction between us. The term 'online' is being applied in more and more areas, and adapting to the online platform seems to be the natural way to go. Today online services are used during shopping, ticket bookings for traveling, bill payments, and work from home, etc. Most people seem to appreciate the ease of use, availability and flexibility offered by these services. Commercial service providers have been the first to adapt to this new technology, but now many governments are also starting to use this platform as a tool for their public services. Many of these services are easily implemented by existing technology, but there still is one important governmental service missing from the online platform. Large scale democratic elections are still being conducted in the same manner as they always have. Voters show up at an election facility, prove their identity and deliver their voting intention in the secrecy of a voting booth. Migrating elections to the online platform seems like a clear next step.

At first look, implementing electronic elections may not seem like a difficult task. A common conception is that if one can do secure financial transactions over the Internet, then one must be able to use the same technology for securely transferring voting intentions.

As it turns out, the concept of online voting introduces so many potential problems, that some people think remote electronic voting never will reach the level of security required for democratic elections.

Electronic voting promises the possibility of a convenient, efficient and secure facility for recording and tallying votes. It can be used for a variety of elections, from small committees, university elections or on-line communities through to full-scale national elections.

1.2 Challenges of Online Electronic Voting [23]

As mentioned in the introduction above, requirements for voting schemes are often assumed similar to those of financial transactions schemes. They do share some of the same challenges, but remote electronic voting has a lot more issues attached. The most obvious problems are related to the use of a public network. These are problems shared by any service offered on a public network.

DOS (Denial of Service) attacks can be launched against any participant in a voting scheme.

Administrators may be cut off from the public, or single voters denied the opportunity to register their ballots. It does not seem possible to prevent DOS attacks with current technology. When doing online electronic voting we have to allow the election process to last for a longer period of time, i.e. 1-2 weeks. If DOS attacks are launched during this period, there would be time to counter the attacks, and carry on with the election. Countering DOS attacks with this method only works if the voters register their votes as early as possible. If a majority of the voters wait until the end of the voting phase, it is not hard to see the damage that could be done by a last day DOS attack. As long as the Internet technology is as vulnerable as it is, we need to have as a backup the opportunity for voters to cast their vote in a traditional voting booth.

Fake servers can impersonate the real administrators. Digital certificates are required for authenticating all participants.

Malicious software, like virus or worms, can infect the voting process. They can alter or invalidate ballots, and the voters may not be able to detect it. It is important for any voting scheme to have procedures for verifying the software in use, so that once malicious software is introduced, it can be detected and removed.

Underlying technology, like hardware and network protocols, will always be beyond the control of the election administrators. The security of the scheme must not depend on this technology.

Digital certificates are a means of providing confidentiality and proof of identity. Today, digital certificates are mostly used in commercial applications like online banking and e- stores. In electronic elections, the use of digital certificates is required for all users, including the voters. A PKI (Public Key Infrastructure) must be in place before large scale electronic elections can be conducted. Nationwide implementations of PKI's are being worked at today, but there will still be a few years before they are ready for electronic voting.

Some challenges are not related to the technology applied, but to aspects of societies. Many governments want to control the use of cryptography for national security reasons. Most electronic voting schemes depend on this technology, and acts and regulations may be an obstacle for their implementations.

The term Digital Divide is an expression used to illustrate the consequences of computers entering the society. In an electronic voting scenario, computer illiterates, or anyone without access to computers, are clearly disadvantaged. Even if the voters still have the opportunity to vote in traditional voting booths, there still is a difference in convenience for the voters. This is clearly not fair, and it is not hard to see that differing convenience for different population groups has an effect on the outcome of the election.

The complexity of e-voting schemes can be a problem. Very few will be able to understand how they work, and this can cause lack of trust in the system. When implementing electronic voting, it is important to inform and educate the voters, giving them an opportunity to learn how the schemes work.

1.3 Need of e-voting

Given all the problems and challenges associated to remote electronic voting, the thing is, the systems in use today are far from perfect. There is a need of more accuracy. It could lead to increased voter turnout; it could give elections new potential (by providing ballots in multiple languages, accommodating lengthy ballots, facilitate early and absentee voting, etc.) thus enhancing democratic process. It could also open a new market, thus supporting the commerce and the employment. Voters need more convenience. Although it is not at all clear that voting from anywhere will increase voter turnout, mobility seems to be increasingly important in today's society. In order to adapt to this change, there is a need of more flexible voting system. Voting from anywhere may also make it easier for the disabled, the elderly and the foreign residents to participate in elections. Once implemented, an electronic voting system may also dramatically decrease the costs of conducting elections. This will make it possible to keep more frequent polls, or even to implement direct democracy, where citizens are allowed to participate in all major decisions.

It seems clear that remote electronic voting could offer many advantages compared to traditional voting systems. There is a risk that no such system can ever match the security of traditional elections, but looking into finding one certainly seems worthwhile.

1.4 Requirements for e-voting

Through the research done on electronic voting, necessary and desirable properties have been singled out. This list of properties is generally agreed upon by those working on this subject, and most voting schemes are evaluated in terms of these properties.

Basic security requirements

- Completeness: All valid votes are counted correctly. [3]
- Soundness: Invalid votes should not be counted.
- Privacy: All votes must be kept secret ie the fact that a particular voted in a particular way is not revealed to anyone.
- Unreusability: No voter can vote twice.
- Eligibility: only legitimate voters can vote.
- Fairness: Nothing must affect the voting. I.e., no intermediate election results can be known to anyone.

▪ Verifiability: No one can falsify the results of the voting.

Extended security requirements

▪ Robustness: No reasonably sized coalition of voters or authorities can disrupt the election.
▪ Atomic verifiability: Individual voters can verify that their vote has been properly counted.
▪ Universal verifiability: Anyone can verify the tally.
▪ Receipt-freeness (Coercion-resistance): No voter is able to construct a receipt proving the contents of his vote. There is some ambiguity about this term, as the definition has changed with the development of voting schemes. The early schemes were designed to give atomic verifiability, and receipt-freeness then meant that voters could verify that their votes had been counted, without revealing the contents of the vote. The term incoercibility then had the same meaning as our current definition of receipt-freeness. As the focus shifted from atomic to universal verifiability, the old definition of receipt-freeness no longer applied, and the term receipt-freeness replaced incoercibility.
▪ Declarability: It is possible to check if a particular voter has voted. This is necessary when participation in the voting process is mandatory.
▪ Reviseability: Voters can change their vote. This is the only property dealing with a coercer looking over the voters shoulder. If this property is implemented, the coercer has no way of knowing if the voter later will change the coerced vote. Reviseability seems to be the only means for preventing coercion when the voting location is not controlled by the election administrators.

Practicality requirements

▪ Flexibility: Allow many ballot formats.
▪ Efficiency: The election can be administered with a reasonable amount of resources.
▪ Mobility: Voters can vote from anywhere
▪ Convenience: Also known as the walk-away property. Vote casting consists of one round of communication with the authorities.

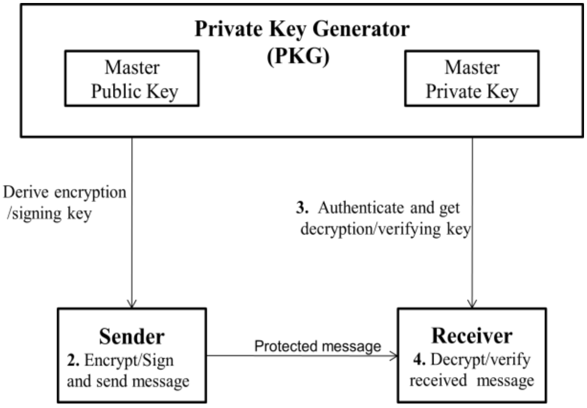
Many different voting protocols and systems have been proposed before [1, 2, 3, 4, and 5] based on different cryptographic primitives they used and the requirements they fulfilled. Fujioka et al.[1] brought new ideas into the design of electronic voting schemes, by combining the techniques of blind signatures and anonymous channels. In Cramer et al.[5], Homomorphic ElGamal 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. Baudron et al. [16] 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. Gallegos et al. in [9] propose the first protocol based on threshold from bilinear pairings. It considers a responsibility distributed model, in which the votes are decrypted with t of n users. In 2010 Gallegos, Gomez and Duchen [8] 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.

A brief introduction to the cryptographic primitives necessary to develop the proposed approach is given in the following sections.

2 . IDENTITY-BASED CRYPTOGRAPHY [6,7,8,9]

In 1984 Shamir [6] 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. An example scenario to understand the concept is that Alice wants to send a secure message to Bob. She does not want to get his public key from a key server; she does not want to verify some trusted third party's signature on his public-key certificate; and she does not even want to store Bob's public key on her own computer. She just wants to send him a secure message.

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

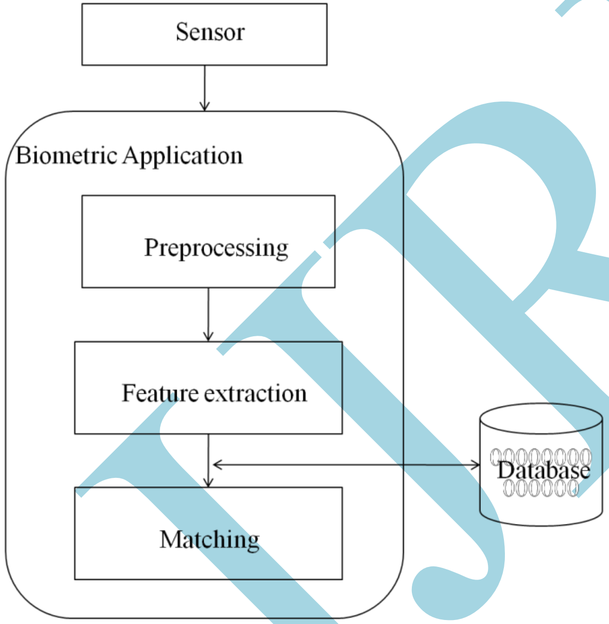

Private Key Generator (PKG)
Master Public Key
Master Private Key
1. Derive encryption /signing key
3. Authenticate and get decryption/verifying key
Sender
2. Encrypt/Sign and send message
Protected message
Receiver
4. Decrypt/verify received message

Identity-Based Cryptography

uses the master private key to generate the private key for identity ID. Fig. depicts the complete scenario. In the following section Identity based public key encryption schemes are described and one of them is used in the proposed system.

3. BIOMETRIC SYSTEMS [10, 11]

Biometrics is the science that tries to fetch human biological features with an automated machine either for verification or for identification. The identification involves identifying a person from all biometric measurements collected in a database. The question that this process seeks to answer is: “who is this?” It, therefore, involves a one- compared- to - many match . Verification involves authenticating a person’s claimed identity from his/her previously enrolled pattern. “Is this who he claims to be?” is the question that this process seeks to answer. This involves a one-to-one match. Biometric systems try to exchange knowledge with an individual feature, e.g. finger print. Recording of the feature should be comfortable and fast. The most commonly use biometric feature is the finger print. Verifying the identity of a person against a given biometric measure involves five phases the system needs to go through. At the beginning, input data is read from the person through the reading sensors. Collected data is, then, sent across a network to some central database hosting a biometric system. The system will, then, perform identity matching using standardized and/or custom matching techniques.



Data flow in a typical biometric identification process

4. Blind signature

It is a cryptographic protocol that can be used to authenticate a voter without disclosing the content of his ballot. Blind signatures are the electronic equivalent of signing carbon-paper-lined envelopes. Writing a signature on the envelope leaves a carbon copy of the signature on a slip of paper within the envelope. When the envelope is opened, the slip will show the carbon image of the signature. The Blind Signature protocol can described as follows:

Step 1. a voter V blinds his vote v using a random string r, and the public key KA of authority A as, BV = blind (v, r, KA), then signs BV using his private key KV-1as,SignV(BV, KV-1) and sends it to authority A.

Step 2. A verifies the validity of V (by verifying the signature with V’s public key KV), then signs BV with his private key KA-1 as, signA(BV, K A-1), and sends it to V.

Step 3. V verifies signature of A and then unblinds (removes r) to obtain signA(v, KA-1) which is the blindly signed vote v. Such a protocol was proposed in [12] using RSA cryptosystem [13].

VIII. PROPOSED VOTING SYSTEM

In real elections, an electronic voting protocol must offer the same benefits as a conventional protocol does; in addition it should reduce costs and increase processing speed. In order to accomplish these features, the proposed protocol is divided into four stages: voting set-up, authentication, voting and counting.

1. Voting Set-up

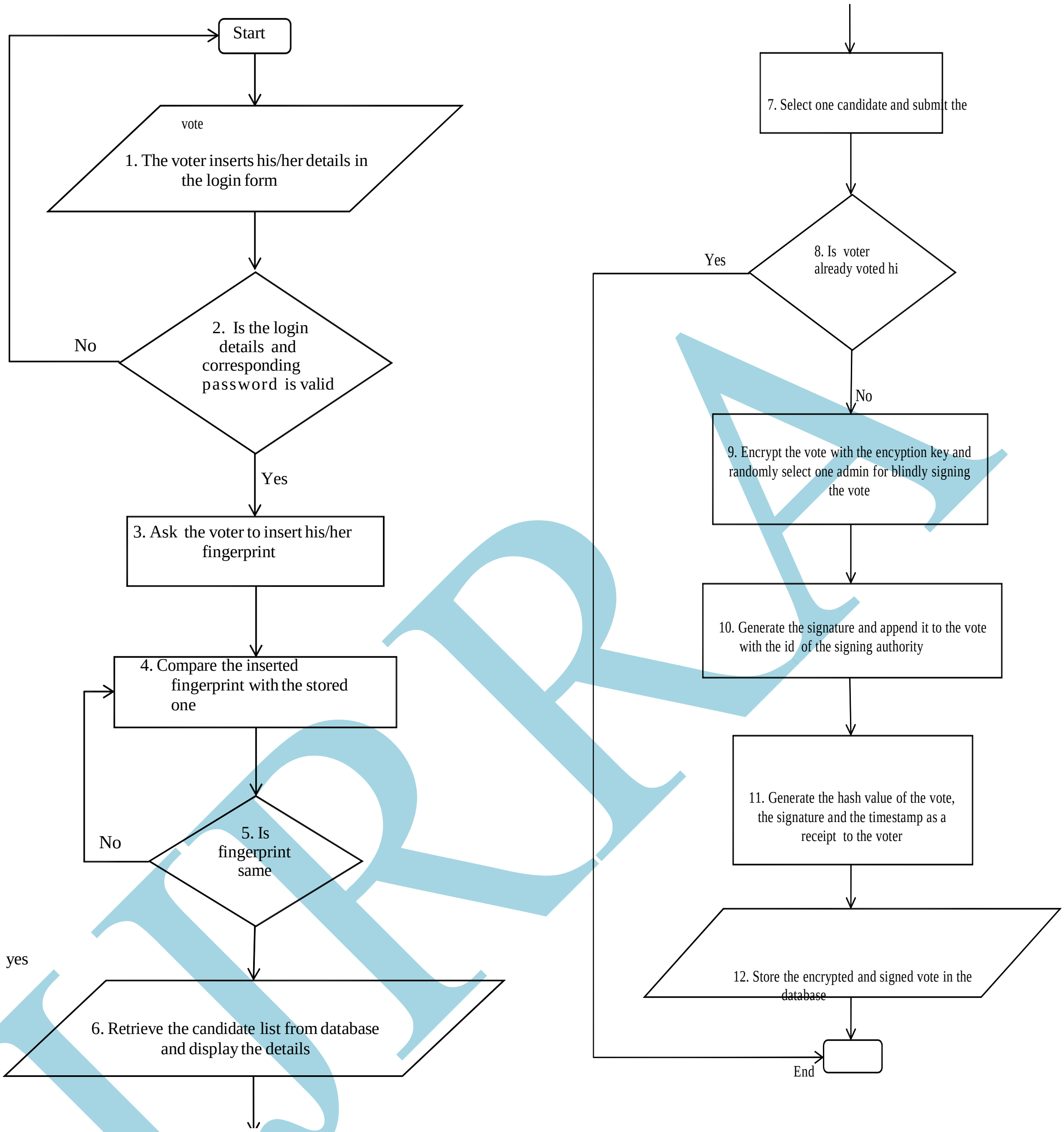
It involves different authorities, in order to generate two key pairs. One of them will be used by the administrators of ballot in the voting phase to sign it blindly. The other one will be used by the voters and the counters to encrypt votes during the voting phase and to decrypt them during the counting phase. The cryptosystem also considers Threshold Decryption in which key shares of decryption key are also generated and divided among administrators.

2. 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.

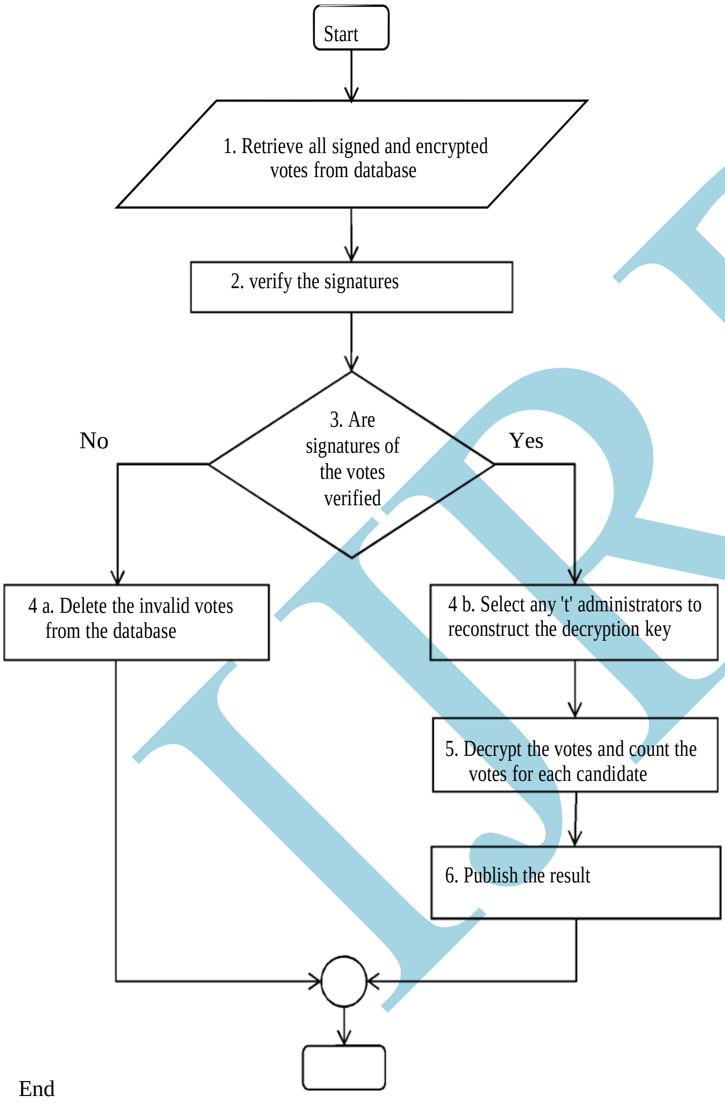
3. Voting

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 .


Start
vote
1. The voter inserts his/her details in the login form
No
2. Is the login details and corresponding password is valid
Yes
3. Ask the voter to insert his/her fingerprint
4. Compare the inserted fingerprint with the stored one
No
5. Is fingerprint same
yes
6. Retrieve the candidate list from database and display the details
7. Select one candidate and submit the
Yes
8. Is voter already voted hi
No
9. Encrypt the vote with the encryption key and randomly select one admin for blindly signing the vote
10. Generate the signature and append it to the vote with the id of the signing authority
11. Generate the hash value of the vote, the signature and the timestamp as a receipt to the voter
12. Store the encrypted and signed vote in the database
End

4. Counting

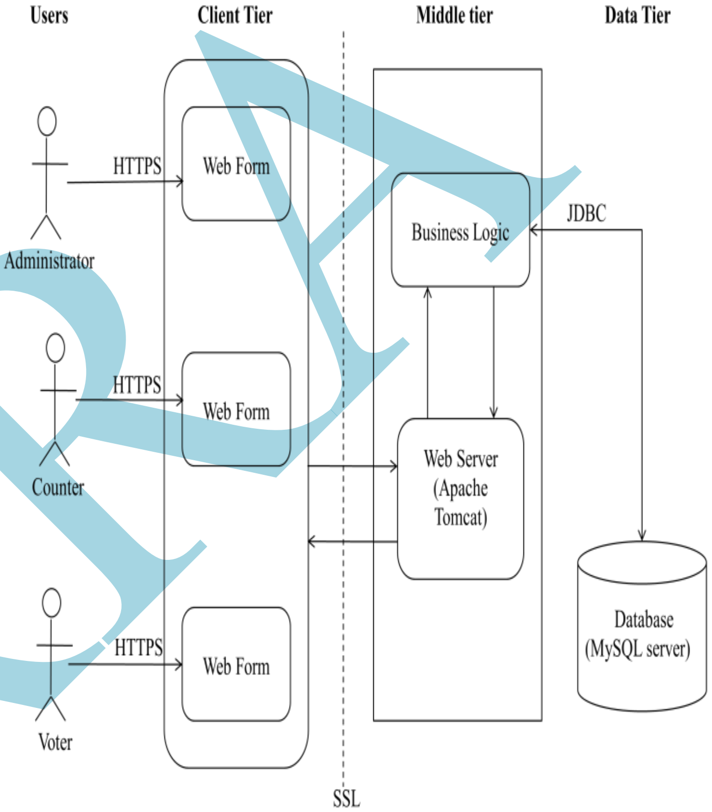
Before votes are counted and the tally is published, the signatures of the votes have to be verified with the verification algorithm of the blind signature, based on RSA algorithm. Then, in order to decrypt the votes using the decryption algorithm, it is necessary to collect valid decryption shares from 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 .


Start
1. Retrieve all signed and encrypted votes from database
2. verify the signatures
3. Are signatures of the votes verified
No
Yes
4 a. Delete the invalid votes from the database
4 b. Select any 't' administrators to reconstruct the decryption key
5. Decrypt the votes and count the votes for each candidate
6. Publish the result
End

COUNTING FLOWCHART

IX. ARCHITECTURE OF THE SYSTEM

The architecture chosen for the system is three tier. The first layer runs on the client side (web browser), the second layer at the middle layer (web server) and the third layer will be the database system. The system will run using java web technology. This architecture provides greater application scalability, high flexibility, high efficiency, lower maintenance, and reusability of components. Since each tier runs on a separate machine, it improves systems performance. The system uses dynamic web technology, i.e., adding and retrieving data to and from the database whenever requested is possible. It needs server side functions that implement the functional requirements and the database system that stores data.



There are numerous vulnerabilities associated with the various e-voting systems [14-15]. With punch card systems, incompletely punched holes in the form of dimples or hanging chads make the card unreadable. This is known as an under-vote. Similarly, if the voter inadvertently punches too many holes for a given office, this over-vote will also make the card unreadable. By performing a manual recount, it is possible to determine the voter’s intent for at least some of these uncounted ballots. However, the manual recount process can be difficult and contentious.

X . E-VOTING SYSTSEM VULNERABILITIES

For optical scan systems, an under-vote may be caused when the voter’s marks are illegible and an over-vote may be caused when the voter makes too many marks or if the paper gets smudged in the wrong place. The percentage of under-votes and over-votes, which is known as the error rate, can be high.

The high-rate of under-votes and over-votes in paper-based systems is one of the main reasons behind the great interest in DREs. By eliminating the need for the voter to mark a paper or punch a card, DREs significantly reduce the error rate. However, by eliminating the voter's ability to verify the ballot, they introduce a new type of vulnerability: the inability to verify that one's vote has been correctly recorded. This vulnerability is leading a growing number of voters to lose faith in the efficiency of voting.

Given that voters cannot themselves verify that DREs correctly record their votes, another way to maintain faith in these systems would be if some trusted authority could assure voters that their votes were counted. However, this is problematic too because putting trust in a single authority is risky in fear that it might be corrupted.

Current electronic voting systems are not sufficient to satisfy trustworthy elections as they do not provide any proofs or confirming evidences of their honesty. This lack of trustworthiness is the main reason why e-voting is not widely spread even though e-voting is expected to be more efficient than the current plain paper voting. Many experts believe that the only way to assure voters that their intended votes are casted is to use paper receipts [16]. If the paper receipt is in plain text or barcoded, this gives a high rate of bribe and coercion. By using visual cryptography, the chance of bribe and coercion decreases since the voter cannot prove to a potential coercer how he voted.

Internet-based voting systems are vulnerable to attack at three major points [17]; the server, the client, and the communications infrastructure. Penetration attacks target the client or server directly whereas denial of service attacks target and interrupt the communications link between the two. Penetration attacks involve the use of a delivery mechanism to transport a malicious payload to the target host in the form of a Trojan horse or remote control program. Once executed, it can spy on ballots, prevent voters from casting ballots, or, even worse, modify the ballot according to its instructions. Remote control software may compromise the secrecy and integrity of the ballot by those monitoring the host's activity.

Remote voting systems will also have to contend with an attack known as spoofing-luring unwitting voters to connect to an imposter site instead of the actual election server. While technologies such as secure socket layer (SSL) and digital certificates are capable of distinguishing legitimate servers from malicious ones, it is infeasible to assume that all voters will have these protections functioning properly on their home or work computers, and, in any event, they cannot fully defend against all such attacks. Successful spoofing can result in the undetected loss of a vote should the user send his ballot to a fake voting site. Even worse, the imposter site can act as a "man-in-the-middle" between a voter and the real site, and change the vote. In short, this type of attack poses the same risk as a Trojan horse infiltration, and is much easier to carry out.

In principle, poll site voting is much less susceptible than remote voting to the previously mentioned attacks. The software on voting machines would be controlled and supervised by elections officials, and would be configured so as to prevent communication with any Internet host except the proper election servers. However, opportunities for attack and insider fraud would still exist.

An e-voting system can be divided into three main categories namely hardware, software, and human factors. The security-relevant elements for hardware are the mechanical, electromechanical, and electrical parts. The security-relevant elements for software are the operating system, drivers, compilers, programs, databases, rules used in the program, procedures and sequences (order of voting events, voting protocols, encryption techniques). The security- relevant elements for human factors are usability, rules, strategies (e.g. information flow, security management), politics, and other diverse aspects such as transparency, acceptance, and trust. All parts of the system have to be considered as equally important in terms of security risks [20].

XI. COMPARISON WITH PREVIOUS PROTOCOLS

In order to compare the proposed protocol with previous work, Table 9.1 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 protocol considers. C.A and T.A mean Certification and Trust Authority respectively.

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-Hellma n
Gallegos [9]	2	1	1	Bilinear Diffie-Hellma n
Proposed protocol	2	0	0	Prime factorization (RSA/OAEP)

From the comparison details shown in table 9.1 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.

IB-mRSA versus Boneh/Franklin IBE [21]

As identity based encryption (IB-mRSA) is used for encrypting the votes in the voting phase but the most general implementation of identity based encryption is based on bilinear pairings (Boneh/Franklin IBE). In [9], a detailed comparison of the IB-mRSA and Boneh/Franklin IBE [22] is given by authors. The key points of this comparison are:

- IB-mRSA is much easier to deploy.
- IB-mRSA is fully compatible with standard RSA.
- IB-mRSA is fully compatible with current PKI-s.
- IB-mRSA is noticeably faster than BF-IBE in both key generation and message encryption, see table 9.2 for details.
- BF-IBE does not prevent the type of an attack where by an adversary compromises a previous or current key.
- A compromise of a SEM alone does not result in a compromise of any users' secret keys, but a compromise of a PKG results in a total system breakdown.

If BF-IBE is used to provide fine-grained revocation, frequent key generation and secure key distribution are expensive procedures. Although a PKG is not required to be on-line all of the time, in practice, it must be constantly available since users do not all request their current private keys at the same time. Therefore, as the revocation interval in BF-IBE gets smaller, the on-line presence of a PKG becomes more necessary.

	BF-IBE	IB-mRSA
Private Key Generation	3ms	< 1ms
Encryption Time	40ms	7ms
Decryption Time	40ms	35ms

Table 9.2 Performance comparison of BF-IBE(on PIII 1GHz)
and IB-mRSA (on PIII 800MHz) with 1024-bit security [9]

XII. CONCLUSION

A voting system is perceived as trusted if it attracts voters and if it leads to confidence regarding the integrity of the published results and the secrecy of the vote. It appears that security features are only one premise underlying a system's acceptance among the electorate. The challenge is to exploit these features at establishing the required trust among the public. There are three gaps that must be comprehended prior to developing (security) requirements for e-voting systems. These gaps are the technological gap —that is, between hardware and software, the sociotechnical gap —that is, between social and computer policies, and the social gap — that is, between social policies and human behaviour. Changing technology is not enough; voter education is needed. Transparency in the voting process increases voter confidence. Software used should be open to public inspection. Viruses or spyware which are targeted specifically at an upcoming online election pose a real threat to voters .

The proposed system will be having several advantages as follows:

i) It gives confidence in voting system, only the legitimate voter is allowed to gain access to voting .

ii) The system is user friendly, in the sense that the user can easily understand the system although the user is a first time user. This is because the design is simple, attractive and do not have too many graphicalitems.

It accomplishes all major security requirements of an electronic voting system: privacy, eligibility, uniqueness, transparency, accuracy, and robustness.

This system can be used for voting since it overcome all the drawbacks of ordinary voting machine also provide additional security. Thus it will help in conducting the fair and secured voting

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]. 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.

[3]. 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.

[4]. 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.

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

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

[7]. 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.

[8]. 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.

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

[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]. 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.

[12]. Chaum D. Blind signature system. In: Advances in cryptology –CRY TO '83. lenum ress; 1984. p. 153.

[13]. Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public keycryptosystems. Communications of the ACM 1978;21:120–6.

[14]. Jefferson D, Rubin AD, Simons B, Wagner D. A securityanalysis of the secureelectronicregistrationand votingexperiment(SERVE). Technical Report available online at http://servesecurityreport.org/; 2004.

[15]. Baoyuan Kang. Cryptanalysis on an e-voting scheme over computer network. International conference on computer science and software engineering. Vol. 3; 2008. p. 826-29.

[16]. Y Lee, S Park, M Mambo, S Kim. Towards Trustworthy e-Voting using Paper receipts. In Computer Standards & interfaces, Elsevier, Volume 32, Issues 5–6, Pages 305-311, October 2010.

[17]. OO Okediran, SO Olabiyisi .A Survey of Remote Internet Voting Vulnerabilities. In World of Computer Science and Information Technology Journal (WCSIT) Vol.1, Issue 7, pages 297-301, 2011.

[18]. Barbara Ondrisek. E-Voting System Security Optimization. In proceedings of the 42nd Hawaii International Conference on System Sciences, 2009.

[19]. Sampigethaya, K. and Poovendran, R. A framework and taxonomy for comparison of electronic voting schemes. Elsevier Computers & Security, Vol. 25, No. 2; 2006. p. 137-53

[20]. Mitrou L, Gritzalis D. Revisiting legal and regulatory requirements for secure e-voting. Proceedings of the IFI PTC 11 17th International Conference on Information Security; 2002. p. 469 – 80.

[21]. Neal R. Wagner, 2003 University of Texas, San Antonio. [online] Available at :http://www.cs.utsa.edu/~wagner/lawsbookcolor/laws.pdf [accessed 07 June 2011]

[22]. 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.

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