E-Voting using Finger Print Recognition and Digital Signature

Rahimullah Niazai[1] Kumari Archana[2]
[1]M. Tech Student [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Alakh Prakash Goyal Shimla University, Shimla, India

Abstract— Using the decade old election system to collect votes from the citizens is no longer considered efficient due to the various recurring errors. So time has arrived that the paper based primordial voting system which has already proven itself an inefficient and slow procedure is changed immediately. The system that is being followed currently, from data collection procedure to counting of the votes is a manual process. Here we are proposing an automated electronic voting system. For the voter registration and authentication processes which are performed on the system, the voter is expected to have his or her fingerprints captured and the minutiae extracted that is stored on the database. This is done to prevent the occurrence of multiple registrations or identity. Thus, during the authentication period, voters are expected to undergo a matching verification of their fingerprint samples against the values stored in the database which is identified through the use of a unique voter identification number assigned during registration. The election commission authority is authorized to access the details but they aren't authorized for modifying or changing the details. Modification of the voters' information requires the fingerprint of the particular voter. This paper provides a secure approach for online voting system using the concept of encryption trough RSA and digital signature. So the system will help to minimize the corruption done by others, and hopefully corruption may be diminished at some point of time. In this system Voter will select his/her preferable candidate by providing his or her opinion on a touch screen where all candidates' voting sign is displayed. Four layered network system will be used here for sending the votes from client to the main database there are three application server, and a client. Among them one application server will work as dispatcher. The encrypted votes will be sent from the client to the dispatcher through an application server and this layer will send those votes to main database through another application server. They will be counted there automatically which will take lesser time than the manual system. So the result will be faster, more accurate and reliable.

Keywords: Fingerprint Recognition, Digital Signature, RSA Algorithm and Web Server

I. INTRODUCTION

Election process is a central administrative work in every country. It has variety of process implemented and all are human work. Now days voting process is converted in electronically and implemented in various computerized work. This reduces normal paper work and increase time. E-voting is a computerized voting system implemented in both on-line process and offline process. Each voter registers his details with unique ID and stored in database. Normally all computers connected with LAN or internet. Whenever voting process implements, voter details are retrieved and verified. This process implemented in several stages. Major stages are voter details collection, voter details matching with high security, voting tabulation with central administration. Voter identification is the crucial factor in E-voting system. This process is implemented in two stages. One is data security and another one is human identity. Data security is implemented in RSA algorithms and Digital Signature and human identity is implemented in Fingerprints Recognition. Data security focuses voter details with unique ID. These details are encrypted and stored securely. Simply it is converted in digital format because voter details matching process is simple one when accessing digital data. Counting process is automated and secured in this system. Human identity is also important factor in E-voting system because some security violations detected in this system such as human malpractices. Biometric security features are implemented in this system such as iris recognition, retina based recognition[2][6].

II. SECURITY METHODS IN E-VOTING

Security is the major factor of e-voting process. The main focus of this E-Voting system is security and privacy and it can be time-consuming and very hard for election committee administrators. Finally it is difficult to handle voters. User privacy achieves greater security in e-voting. It brings the clarity of this voting system. This system satisfies the factors such as Requirement: each voter has only one voting account and allowed to one time, Privacy: voter's votes are private and secure one and no alternative process. It is useful for voting calculations. Voter simply put their votes and no other actions implemented. Any public sectors can verify this voting process in effective manner. Researchers improve the security in this system by implementing security algorithms and achieve greater results. Researchers improve normal voting system to reduce paper works and automate computerized implementation. But accuracy and scalability is the important factors in e-voting system. Security attacks are also the major issues in this voting system. Security is implemented in hardware, software and data. Hardware security is physical system properties such as computer connected in LAN, and operating system performance. Software security is the e-voting system application security, this leads to prevent unauthorized access in this system. Data security is the user data privacy that data is stored in an encrypted and sign form and no one access without permission. All these security system achieves greater results in e-voting system. Security policies are also implemented in e-voting system. That is, each voter has a unique id implementation and some essential details are included in this system. Then each voter has only one vote and no other way to put vote in alternative methods. These policies bring greater security and most of security violations are reduces in this system[3][8].

A. Fingerprint Security Method in E-Voting

A fingerprint scanner is a type of technology that identifies and authenticates the fingerprints of an individual in order to grant or deny access to a computer system or a physical facility. [5]

A fingerprint scanner typically works by first recording fingerprint scans of all authorized individuals for a particular system or facility. These scans are saved within a database. The user requiring access puts their finger on a hardware scanner, which scans and copies the input from the individual and looks for any similarity within the already-stored scans. If there is a positive match, the individual is granted access[9].

Fingerprint scanners most commonly use an individual's thumbprint as identification.

B. RSA Algorithm

In 1978, Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman introduced a cryptographic algorithm, which was essentially to replace the less secure National Bureau of Standards (NBS) algorithm. Most importantly, RSA implements a public-key cryptosystem, as well as digital signatures. RSA is motivated by the published works of Diffie and Hellman from several years before, who described the idea of such an algorithm, but never truly developed it. Introduced at the time when the era of electronic email was expected to soon arise, RSA implemented two important ideas:

Public-key encryption. This idea omits the need for a \courier" to deliver keys to recipients over another secure channel before transmitting the originally intended message. In RSA, encryption keys are public, while the decryption keys are not, so only the person with the correct decryption key can decipher an encrypted message. Everyone has their own encryption and decryption keys. The keys must be made in such a way that the decryption key may not be easily deduced from the public encryption key.

Digital signatures. The receiver may need to verify that a transmitted message actually originated from the sender (signature), and didn't just come from there (authentication). This is done using the sender's decryption key, and the signature can later be verified by anyone, using the corresponding public encryption key. Signatures therefore cannot be forged. Also, no signer can later deny having signed the message. This is not only useful for electronic mail, but for other electronic transactions and transmissions, such as fund transfers. The security of the RSA algorithm has so far been validated, since no known attempts to break it have yet been successful, mostly due to the difficulty of factoring large numbers n = pq, where p and q are large prime numbers[11][13][4].

C. The math of the method

So far, we expect to make E and D easy to compute through simple arithmetic. We must now represent the message numerically, so that we can perform these arithmetic algorithms on it. Now let's represent M by an integer between 0 and n - 1. If the message is too long, sparse it up and encrypt separately. Lete; d; n be positive integers, with (e; n) as the encryption key, (d; n) the decryption key, n = pq. Now, we encrypt the message by raising it to the eth power modulo n to obtain C, the ciphertext. Wethen decrypt C by raising it to the dth power modulo n to obtain M again. Formally, we obtain these encryption and decryption algorithms for E and D:

$$C \equiv E(M) \equiv M\ e \pmod{n} \quad (5)$$

$$M \equiv D(C) \equiv C d \pmod{n} :$$

Note that we are preserving the same information size, since M and C are integers between 0 and n - 1, and because of the modular congruence. Also note the simplicity of the fact that the encryption/decryption keys are both just pairs of integers, (e; n) and (d; n). These are different for every user, and should generally be subscripted, but we'll consider just the general case here. Now comes the question of creating the encryption key itself. First, choosing two \random" large primes p and q, we multiply and produce n = pq. Although n is public, it will not reveal p and q since it is essentially impossible to factor them form n, and therefore will assure that d is practically impossible to derive from e. Now we want to obtain the appropriate e and d. We pick d to be a random large integer, which must be coprime to (p - 1) · (q - 1), meaning the following equation has to be satisfied:

$$\gcd(d; (p - 1) \cdot (q - 1)) = 1 \quad (6)$$

"gcd" means greatest common divisor.

The reason we want d to be coprime to (p - 1) · (q - 1) is peculiar. I will not show the "direct motivation" behind it; rather, it will become clear why that statement is important when l show towards the end of this section that it guarantees (1) and (2). We will want to compute e from d, p, and q, where e is the multiplicative inverse of d. That means we need to satisfy

$$e \cdot d = 1 \pmod{\varphi(n)} : (7)$$

Here, we introduce the Euler totient function φ(n), whose output is the number of positive integers less than n which are coprime to n. For primes p, this clearly becomes φ(p) = p - 1 . For n, we obtain, by elementary properties of the totient function, that

$$\begin{aligned} \varphi(n) &= \varphi(p) \cdot \varphi(q) \\ &= (p - 1) \cdot (q - 1) \quad (8) \\ &= n - (p + q) + 1 \end{aligned}$$

From this equation, we can substitute φ(n) into equation (7) and obtain

$$e \cdot d \equiv 1 \pmod{\varphi(n)}$$

which is equivalent to

$$e \cdot d = k \cdot \varphi(n) + 1$$

for some integer k.

By the laws of modular arithmetic, the multiplicative inverse of a modulo m exists if and only if a and m are coprime. Indeed, since d and φ(n) are coprime, d has a multiplicative inverse e in the ring of integers modulo φ(n).

So far, we can safely assured the following:

$D(E(M)) \equiv (E(M))d \equiv (M\ e)d \pmod{n} = M\ e{\cdot}d \pmod{n}$

$E(D(M)) \equiv (D(M))e \equiv (M\ d)e \pmod{n} = M\ e{\cdot}d \pmod{n}$

Also, since e · d = k · φ(n) + 1, we can substitute into the above equations and obtain

$$M^{e \cdot d} \equiv M^{k \cdot \varphi(n)+1} \pmod{n} :$$

Clearly, we want that to equal M. To prove this, will need an important identity due to Euler and Fermat: for any integer M coprime to n, we have

$$M^{\varphi(n)} \equiv 1 \pmod{n} : (9)$$

Since we previously specified that $0 \leq M < n$, we know that M would not be coprime to n if and only if M was

either p or q, of the integers in that interval. Therefore, the chances of M happening to be p or q are on the same order of magnitude as 2=n. This means that M is almost definitely relatively prime to n, therefore equation (9) holds and, using it, we evaluate:

$M^{e \cdot d} \equiv M\, k \cdot \varphi(n)+1 \equiv (M\, \varphi(n))kM \equiv 1kM \pmod{n} = M$:

It turns out this works for all M, and in fact we see that (1) and (2) hold for all M; $0 \leq M < n$. Therefore E and D are inverse permutations[1][12][7].

D. How secure is RSA?

The RSA algorithm is indeed among the strongest, but can it withstand anything? Certainly nothing can withstand the test of time. In fact, no encryption technique is even perfectly secure from an attack by a realistic cryptanalyst. Methods such as brute-force are simple but lengthy and may crack a message, but not likely an entire encryption scheme. We must also consider a probabilistic approach, meaning there's always a chance someone may get the "one key out of a million". So far, we don't know how to prove whether an encryption scheme is unbreakable. If we cannot prove it, we will at least see if someone can break the code. This is how the NBS standard and RSA were essentially certified. Despite years of attempts, no one has been known to crack either algorithm. Such a resistance to attack makes RSA secure in practice.

In section 8, we will see why breaking RSA is at least as hard as factoring n. Factoring large numbers is not provably hard, but no algorithms exists today to factor a 200-digit number in a reasonable amount of time. Fermat and Legendre have both contributed to this field by developing factoring algorithms, though factoring is still an age-old math problem. This is precisely what has partially \certified" RSA as secure.

To show that RSA is secure, we will consider how a cryptanalyst may try to obtain the decryption key from the public encryption key, and not how an intruder may attempt to "steal" the decryption key. This should be taken care of as one would protect their money, through physical security methods. The authors of RSA provide an example: the encryption device (which could be, say, a set of integrated chips within a computer), would be separate from the rest of the system. It would generate encryption and decryption keys, but would not print out the decryption key, even for its owner. It would, in fact, erase the decryption key if it sensed an attempted intrusion[11][12][15].

E. Digital Signatures

Digital signatures are implemented in e-voting system and uses hash functions to convert data into signatures. Signatures are help to identify data when transferring electronically in this system. Digital signatures are not analogous to physical hand written signatures as they provide unique identity of who signed a message in elections, impressions are used to sign the contents of voting process to ensure that this system is not changed[15][17].

F. Advantages of Digital Signature

In this section, we will learn about the different reasons that call for the use of digital signature. There are several reasons to implement digital signatures to communications [16].

G. Authentication

Digital signatures help to authenticate the sources of messages. For example, if a bank's branch office sends a message to central office, requesting for change in balance of an account. If the central office could not authenticate that message is sent from an authorized source, acting of such request could be a grave mistake.

H. Integrity

Once the message is signed, any change in the message would invalidate the signature.

I. Non-repudiation

By this property, any entity that has signed some information cannot at a later time deny having signed it.

III. PARTTAKERS

The participants are voter, voting client, voting server, voting authority. The system will be comprised of the following phases.

1) Registration
2) Authentication
3) Voting
4) Counting

A. Registration Phase:

An authorized person of an organization will go to each office of the election and after verifying the valid identity of the employee the authorized person will register him/her finger for voting.

B. Authentication Phase:

When voter login using fingerprint scanner, the voting system will check authentication of the voter.

C. Voting Phase:

In this phase first request for ballet is done. Voter will get ballet and public encryption key. The vote will encrypt using this key. Again that encrypted vote is digitally sign using voter private key. Encrypted vote and digital signature is sent to voting server. Voting server first check digital signature and then store that encrypted vote.

D. Counting Phase:

In this phase all the encrypted votes are decrypted and then counting is done. The authorized person will enter the private decryption key for decryption. The counting is done and the result will be declared.

IV. SYSTEM DESIGN

We are designing this system for an election both security user authentication and data security. In a user authentication we used fingerprint because fingerprint is more secure then USER NAME and PASSWORD in this phase we store the voter finger image in a database during the registration. And one other main concern is that to provide security to casted vote, when it is being transferred from voter to voting server for storage purposes. We are focusing to provide security from intruders both passive as well as active. The passive intruder can access the casted vote of a voter and create challenge to secrecy and privacy characteristics of voting

system. The active intruder may tamper the casted vote and encounter problem for integrity of casted vote. So to tackle this security concern, we are using the concept of cryptography and taking advantages of digital signature. To provide security from passive intruders, we are encrypting the casted vote on client system, and then will send that to voting server with the help of internet, on server side decryption of that vote is done before counting. We require two keys for this purpose one for encryption on voter system, which should be publicly known and second key for decryption of encrypted vote before counting on voting server, this key must be private. So for this purpose we need a pair of symmetric keys. A pair of asymmetric keys. To provide security from active intruder who can alter or tamper the casted vote when vote is transferring from voter to voting server, we are using digital signature. When a voter cast his/her vote after that he/she will digitally sign on that by using his/her own private digital signature, and send this to voting server, on voting server side that signature is checked by digital signature verifier of that voter which is publicly known. For this purpose each voter should have a private digital signature and a public digital signature verifier, for this we are using a pair of asymmetric keys for each registered voter.

As figure 2 consist of voting sever, voting client, voter and voting authority. A registered voter connects to voting server by using his login identification. Voting client and voting server communicate by internet.

When a voter wishes to cast the vote he needs to request for ballet to the server. The server sends the ballet with public encryption key. Voter encrypts casted vote using this key, then voter digitally sign on encrypted vote by using his private key. And send both to the server. On server side, voting server verifies digital signature of voter by applying decryption on voter signature using public signature verifier of voter. If signature is valid vote is store for counting otherwise vote is discarded.

A. On Client Side

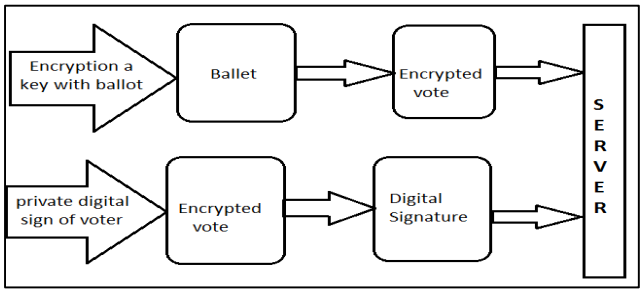

Fig. 1: Voting client side computing

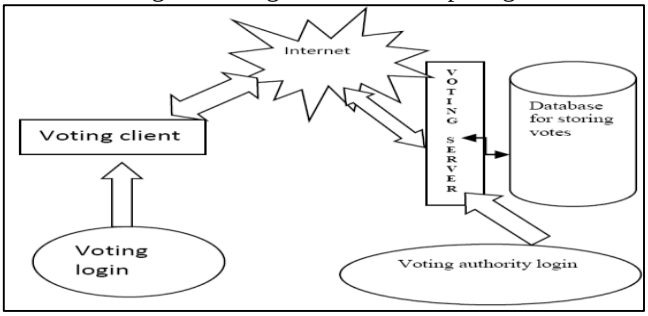

Fig. 2: shows computation on client side.

V. RESULTS AND IMPLEMENTATION

The authorized voting authority will visit to each office of company and do registration of voter by manually verifying the identification of employee. During registration voter generate a pair of asymmetric keys in which one is private and other is public voter keep his private key secrete and other public key goes to server along with other registration details of voter.

For security purpose voter can login by using fingerprint scanner. When a voter request for ballet, server send ballet along with public encryption key. Voter cast his vote and encrypts it using public encryption key. We have internally assigned an Id with each candidate competing for election when voter cast his vote that Id is encrypted by public encryption key provided with ballet. After that, voter signs digitally on that vote using own private digital signature. And send both these to server. If the casted vote is access by passive intruder, he cannot know to whom voter has voted because vote is in encrypted form. If active intruder altered the vote and send it to voting server, server easily knows about alteration of vote because vote digitally signed, active intruder alter vote signature also altered and server when verifies signature, server came to know that vote altered and server inform voter about it. After election is over, on the day of counting authorize voting officer, decrypt the encrypted vote to normal vote by using private decryption of voting system and counting is done and result is declared.

VI. CONCLUSION

We tried our level best to introduce a new voting system that will be accurate, transparent, and faster and will ensure a single vote for a single person. Our proposed system has covered all of these issues successfully. Moreover this system will provide boundary less voting. A better database maintenance, automated registration system, RSA encryption, Digital signature for sing the document and the process of casting vote using finger print will further help us to fulfill our purpose

Online E-voting system is a prototype developed by using spring boot. As the need for voting system has started to increase and some organizations or countries has started to look for the solutions, this can be the starting point to improve and deploy in the real world scenarios. In this project I have tried to explain the importance of RSA cryptosystem, its unique properties and its application areas especially in e-voting. We need to keep in mind that voting is not the only process during the whole voting processes. There might be some other security concerns that need to be considered when such an application is built for practical reasons. Lastly, RSA Cryptosystem efficiency can be improved as suggested in this papers.

REFERENCES

[1] Ali Fawzi Najm Al-Shammari.. Sergio Tessaris" Vote Verification through Open Standard: A Roadmap",. 978-1- 4577-0953-1/(2011)IEEE .
[2] Amir Omidi. Saeed Moradi "Modeling and Quantitative Evaluation of an Internet Voting System Based on

Dependable Web Services",. 978-1-4673-0479-5/12/© (2012) IEEE.
[3] Amir Omidi and Mohammad Abdollahi Azgomi. "An Architecture for E-Voting Systems Based on Dependable Web Services" . 978-1-4244-5700-7/10 © (2009)IEEE .
[4] Haijun Pan, Edwin Hou and Nirwan Ansari" Ensuring Voters and Candidates‟ Confidentiality in E-voting Systems" . 978-1-61284-680-4/11/$26.00 ©2011 IEEE.
[5] Jain, R. Bolle, S. Pankanti Eds, "BIOMETRIC – Personal Identification in Networked Society", . Kluwer Academic Publishers, Boston/ Dordrecht/ London, 1999.
[6] KashifHussainMemon, Dileep Kumar and Syed Muhammad Usman,Next Generation A Secure E-Voting System Based On Biometric Fingerprint Method 2011 . International Conference On Information And Intelligent ComputingIPCSIT Vol.18 (2011).
[7] George Saleem S TevaramaniAnd K B RajaPerformance Comparison Of Face Recognition Using Transform Domain Techniques . World Of Computer Science And Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 3, 82-89, 2012.
[8] Pallavi V Chavan, Dr. Mohammad Atique, and Dr. Anjali R Mahajan,"An Intelligent System for Secured Authentication using Hierarchical Visual Cryptography-Review", .published in 2011.
[9] Sanjay Kumar, Manpreet Singh, "Design A Secure Electonic Voting System Using Fingerprint Technique", . published in July 2013.
[10] Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman Attacking the Washington, D.C. Internet Voting System In Proc. 16th Conference on Financial Cryptography &Data Security, (Feb. 2012).
[11] Shankar, K., and P. Eswaran. ―A secure visual secret share (VSS) creation scheme in visual cryptography using elliptic curve cryptography with optimization technique.‖ . Australian Journal of Basic & Applied Science 9.36 (2015): 150-163.
[12] Shankar, K., and P. Eswaran. ―RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography. China Communications 14.2 (2017): 118-130.
[13] Sumit Jagtap, Smitesh Vichare, AlpaVaidya, Mangesh Jogdand, Prof. Shivani Sthapak, "VC Technology in Internet Voting System", . published in 4, April 2016.
[14] V. C. Ossai, e. A. Enhancing E-voting systems by Leveraging Biometric Key Generation(Bkg)‖, pp. 180-190,. in American journal of Engineering research (AJER)Vol. 2, Issue-10, p (2013).
[15] David A. Wagner, et al. California Secretary of State's Top-to- Bottom Review (TTBR) of Electronic Voting Systems. July 2007.
[16] Eliza Newlin Carney. Voting Without a Net in South Carolina. National Journal, June 21, 2010. http://www.nationaljournal.com/njonline/rg_20100621_7815.php.
[17] Andrew W. Appel. How I Bought Used Voting Machines on the Internet. Feb 7, 2007. http://www.cs.princeton.edu/~appel/avc/.

