A Review on 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: The main challenge in electronic voting (EV) systems is the security issue which has gained an interest of researchers in the last twenty years. EV system is one of the most significant internet related activities. Nowadays many countries moved to electronic voting instead of a traditional on for many reason. Electronic voting has been studied for over the last 20 years. Until now many Electronic voting schemes have been proposed, However there is no a complete solution in both theoretical and practical area. So the researchers try to maintain the cryptographic primitives to build e-voting schemes with high efficiency to achieve these requirements. In this paper, we present a new cryptographic verifiable voting system. The digital signature represents one of the most important applications of cryptographic protocol In order to implement the cryptographic protocol in the field EV systems, it is important to secure the communication channel to the legal users. Therefore, the main target of this paper is to design a scheme which is more effective and achieving higher security properties based on finger print recognition, RSA and digital signature technology. In this system, the improper behavior of the voter will be detected and invalid or double votes will not be taken into account. In addition, the voter has the ability to prove that his vote is in correct form without disclosing any other information about his vote and his decision.

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

I. INTRODUCTION

In the next few years, various applications and services will increasingly depend on computer networks and the collected amount of data also will be incredibly large. Thus cryptography technologies will be applied in most areas of computing such as EVs and cryptographic protocols will become more important. The cryptographic verifiable electronic voting system is a web based system. The web-based scheme is accessed by the voter through the web browser. The cryptographic voting system is an open-audit system, universally verifiable, with several features included in the scheme for verification and control purposes. The cryptographic voting scheme implements cryptographic techniques using standard algorithms to maintain ballot secrecy while providing a mathematical proof that the election tally was correctly computed. In the voting system, the votes are encrypted with a hybrid system using the standard algorithms RSA. When the application is initialized, it does not access the Internet until the vote is completely encrypted, digitally signed and ready to be cast and for user identification we are used in this system finger print recognition till complete the both of security issues user authentication and data security.

In this paper, we present a new cryptographic voting scheme based on the Public Key Infrastructure (PKI), RSA Public Key Technology and Digital Signature based on RSA cryptosystem. We first summarize cryptographic primitives used in our proposed scheme. Finally, we discuss the security of our proposed scheme. The proposed cryptographic voting scheme in this paper satisfies the following properties which have been proposed in [3] [8].

• **Voter privacy:** while it must be ensured that the eligible voters can cast a ballot, it must be impossible to connect the voter identity with the content of his/her cast vote.

• **Voter verifiability:**

We used for user identification in this system finger print recognition of acquiring details of any person in the election.

• **Voter privacy:** while it must be ensured that the eligible voters can cast a ballot, it in which **e**ach eligible voter can verify that his vote was really counted.

• **Democracy:** each eligible voter has the right to cast his vote and is not allowed for anyone to vote for others.

• **Robustness:** the system must be secure and non-infiltrated by adversaries preventing any harmful behavior of voters, by authorities or strangers.

• **Receipt-freeness:** No one must know the content of the voter's vote. This property prevents vote selling or buying.

• **Correctness:** An election scheme is said to be correct if the ballots are counted correctly.

• **Fairness:** No participant can gain any knowledge, except his vote, about the (partial) tally before the counting stage.

• **Coercion-resistance:** An election scheme is said to be coercion resistance if the voter cannot cooperate with a coercer to prove to him that she voted in a certain way.by their voters that were inserted in final tally and must be counted correctly. There are two types of verifiability that are Universal Verifiability in which anyone can check that the published final tally is really the sum of the votes and Individual Verifiability [2] [5] [18].

Significance of Study

The main purposes of EVS include:

- Provision of improved voting services to the voters through fast, timely and convenient voting.
- Reduction of the costs incurred by the Kenyan Electoral Commission during voting time in paying the very many clerks employed for the sake of the success of the manual system.
- Check to ensure that the members who are registered are the only ones to vote. Cases of “Dead People” voting are also minimized.
- Online voting system (EVS) will require being very precise or cost cutting to produce an effective election management system.
- Therefore crucial points that this (EVS) emphasizes on are listed below.
    - Require less number of staff during the election.

- This system is a lot easier to independently moderate the elections and subsequently reinforce its transparency and fairness.
- Less capital, less effort, and less labor intensive, as the primary cost and effort will focus primarily on creating, managing, and running a secure online portal.
- Increased number of voters as individual will find it easier and more convenient to vote, especially those abroad [9].

II. LITERATURE SURVEY

Jena Catherine Bel.D et.al, [23] "A Secure Approach for E-Voting Using Encryption and Digital Signature" This paper provide a secure approach for online voting system using the concept of encryption and digital signature. We have implemented the concept of AES and RSA algorithm and provide security from all type of attacks, when vote is travelling from voting client to voting server from our experimentation. These attacks include security threat from passive as well as active intruder. We can use this system also for taking opinions of employee on certain issue. In future for authentication of voters instead of username if we can use thumb impression of voters or capture photo of his/her face and compare it with photos stored in our database, it will be more secure. This system save money, time requirement in traditional voting system. Also it is eco-friendly and avoid wastage of paper.

Ashwini S H et.al, [24] "A Real Time E-Voting System" designs an Internet Voting system using combined Digital Signature Algorithm and Multiple Data Encryption Standard Algorithm which provides security, privacy and transparency. It could be concluded that the system is able to provide security from all types of attacks, when vote is travelling from voting client to server. Attacks could be security threats from passive as well as active intruder. This system can also be used to take opinion of people on certain issue. This system saves money and time requirement when compared to traditional voting system. It is also eco-friendly and avoids wastage of paper. Future work will focus on integrating this system with biometric authentication of the citizens who will be casting their votes. For authentication of voter USERNAME could be replaced with thumb impression of voter or capture photo of his/her face and compare it with photo stored in our database, it will be more secure.

R.Suganya et.al, [25] "A Survey on Security Methodologies in E-Voting System". This paper focuses a survey for security methodologies in E-voting system and mainly focuses various security algorithms like RSA and MD5 algorithms. 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 finger print recognition, iris recognition, and retina based recognition.

Jambhulakar, Chakole et.al, [26] "a novel security for the online voting system by using multiple encryption schemes". Provide security for casting vote when it is submitted from voting poll to voting server. Multiple encryptions to pass up DOS attack. Security provide obedient as well as an active intruder. This system is to take a decision on certain issues. This paper uses cryptography concepts to take Advantages of the digital signature. Encrypting the send forth vote to client server then send to voting server with the help of the net. After sending encrypted vote then server side decrypts the vote before counting. On server side decryption of that votes is done before counting. We need two keys, for this reasons one for encryption on voter system, which should be freely known and the second key for decryption of encrypted vote before counting on the voting server this key should be confidential. So for this reasons we require a couples of asymmetric keys. To give safety from active interloper who can change or fiddle the casted vote when the vote is transferring from voter to voting server, we are using a digital signature.

Achal Kamdi et.al, [27] "A Novel Approach for Online Voting System Using Visual Cryptography and Face Detection". In this paper, we compared all the existing systems for E-Voting system, have discussed the methods used in each of the mechanism and the drawback of the same. To overcome the drawback in the existing systems we have proposed one advanced mechanism which will use the joint approach of Face Detection and visual cryptography, to provide more suitable online voting system, through which the voting system will be more efficient, user friendly and will have higher security.

III. 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 Rivest, Adi Shamir, and Leonard Adleman 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. Digital signatures Algorithm

Digital signatures allow us to check the author, date and time of signatures, authenticate the message contents. It also includes authentication function for additional capabilities [19] [2].

D. Authentication

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

E. Integrity

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

F. Non-repudiation

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

IV. PURPOSED 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 [21] [16].

A. Purposed System Data Flow Diagram

Data flow diagram for proposed system.

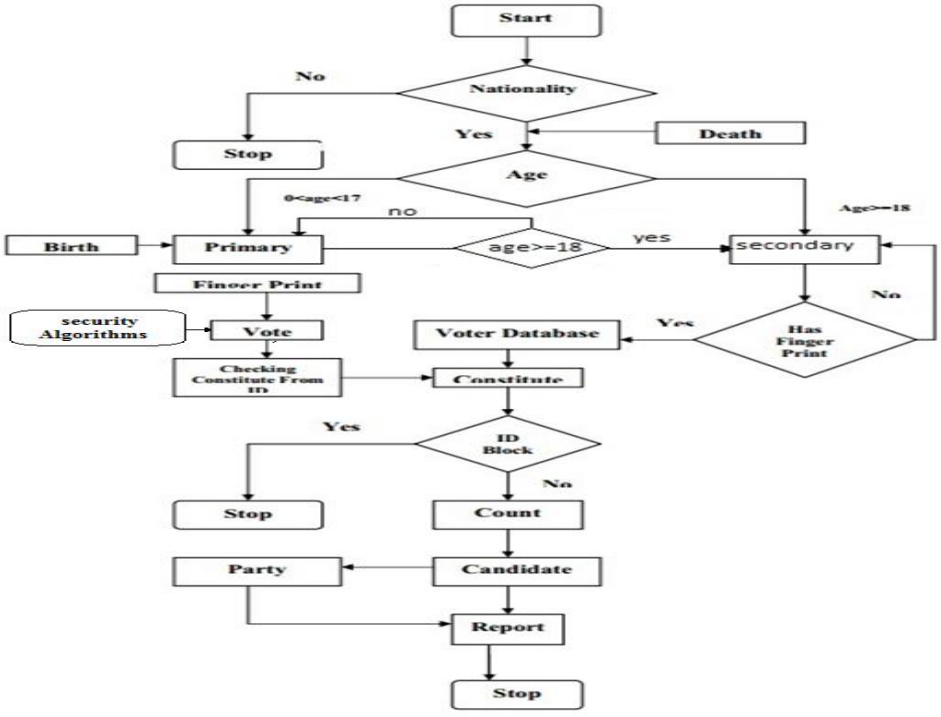

Figure 1: Flow Chart

Description of data flow diagrams

According to the dataflow diagram we see 6 processes are here with several inputs and outputs for different purposes. Process 1 is for population management system. It has three inputs one is for new born baby that come from the organization 'X' another one is for the information about the people who has already passed away that comes from the organization 'Y'. The election commission authority provides another input for the population management system about the general people. Process 2 that is general voter list has one input from the process 1 that is about the people who are living voters of the country and who are registered with both their finger print and details. These voters are sorted according to their area. Process 3 that is voting area management deals with the voter under each area or seat. The responsibility of this process doesn't limited to only accepting the voters under that area from process 2 but also check the validity of the vote given by each participant. Process 4 supervises the voting procedure that is keeping track of votes for each candidate. It also provides result to the process 6 whish's responsibility is to show result for each candidate as well as each party attending the polling session. Process 5 engages with getting the encrypted packets containing the vote and the finger print and subsequently processing them that is checking the validity, counting vote for candidate, counting overcome seat for each party, sending them to process 4 as well as to process 6. Process 6 as said before keep busy itself to publish the result for each candidate as well as each party, in the security algorithms we used RSA for Data Encryption and Digital Signature for Sign the documents.

V. CONCLUSION & FUTURE WORK

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 research work, we 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 concern 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. The system presented here uses the finger print scanning technology to authenticate the elector's identity. Though it is considered to be secure, it still has many flaws which are yet to be exploited. In the future iris scanning technology can be used to authorize a person's identity which is considered to be more secure.

REFERENCES

[1] Ali Fawzi Najm Al-Shammari. Sergio Tessaris" Vote Verification through Open Standard: A Roadmap",. 978-1- 4577-0953-1/11IEEE . (2011).

[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/© IEEE. (2012).

[3] "Cryptographic Algorithms for Protection of Computer Data During Transmission and Dormant Storage," Federal Register 38, No. 93 (May15, 1973).

[4] Al-Jarrah, K. M. A Biometric-Secure e-Voting System for Election Process. Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08). Amman, Jordan.(2008).

[5] Altun A.A, K. H. "Genetic algorithm based feature selection level fusion using fingerprint and iris biometrics", International Journal Pattern Recognition Artificial Intelligence. (IJPRAI), 22(3): 585-600, November 2008.

[6] Aman Kumar, D. J. "Distinction between Secret key and Public key Cryptography with existing Glitches" IJEIM-0067,vol.1, 2012.

[7] Amir Omidi and Mohammad Abdollahi Azgomi. (2009). "An Architecture for E-Voting Systems Based on Dependable Web Services" . 978-1-4244-5700-7/10 © IEEE .

[8] Cetinkaya, O. Analysis of Security Requirements for Cryptographic. Proc. 3rd Int. Conf. on Availability, Reliability and Security (ARES 2008), Technical University of Catalonia,Barcelona, March 4–7, pp. 1451–1456. IEEE Computer Society.

[9] Chou, J. C. On the Efficient Implementation of Pairing-Based Protocols. Cryptology ePrint Archive, http://eprint.iacr.org/.(2011).

[10] Costello, C. a. Fixed Argument Pairings. Proc. 1st. Int. Conf. on Cryptology and Information Security in Latin America, Puebla, Mexico, August 8–11, pp. 92–108.Springer, Berlin/Heidelberg.(2010).

[11] Elminaam, D. K. "Evaluation of the Performance of Symmetric Encryption Algorithms", International Journal of Network Security Vol.10, No.3, PP.216–222, May 2010.

[12] Fouque, P.-A. a. Indifferentiable Hashing to Barreto–Naehrig Curves. Proc. 2nd Int. Conf. on Cryptology and Information Security in Latin America, Santiago, Chile, October 7–10, pp. 1–17. Springer, Berlin/Heidelberg.(2012).

[13] Galbraith, S. L. Endomorphisms for faster elliptic curve cryptography on a large class of curves. J. Cryptol., 24, 446–469.(2011).

[14] 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.

[15] Jain. R. Bolle, S. Pankanti Eds, "BIOMETRIC – Personal Identification in Networked Society", . Kluwer Academic Publishers, Boston/ Dordrecht/ London, 1999.

[16] Kashif Hussain Memon, 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).

[17] Kharchineh, B. a. A New ElectronicVoting Protocol Using a New Blind Signature Scheme. Proc. 2nd Int Conf. on Future Networks (ICFN 10), Sanya, Hainan, China, January 22–24, pp. 190–194. IEEE Computer Society.(2010).

[18] Lee, C. C. A New Proxy Electronic Voting Scheme Based on Proxy Signatures. In Park, J., Leung, V., Wang, C.L. and Shon, T. (eds), Future Information Technology, Application, and Service. Springer,Netherlands.(2012).

[19] Li, C. a. Security enhancement of Chang–Lee anonymous E-voting scheme. Int. J. Smart Home,anonymous E-voting scheme. Int. J. Smart Home,(2012).
[20] McGaley, M. "Irish Citizens for Trustworthy Voting." 6 July 2004. http://evoting.cs.may.ie/.
[21] Achal Kamdi, Mamta Kamble, Vijaya Tayade: A Novel Approach for Online Voting System Using Visual Cryptography and Face Detection. International journal of Advances in Electronics and Computer Science, ISSN: 2393-2835. http://www.iraj.in, April 2017.
[22] Srivatsan Sridharan: "Implementation of Authenticated and Secure Online Voting System", 4th ICCCNT 2013 July 4 - 6, 2013.
[23] Jena Catherine Bel.D, Savithra.K, Divya.M. A Secure Approach for E-voting using encryption and Digital Signature. International journal of engineering Development and Research, ISSN: 2321-9939, IJEDRCP1502004, NC#N 2015. (www.ijedr.org).
[24] Ashwini S H, Punitha C P, Bhavana R, Shashidhar V. A Real Time E-voting System. International journal of, ITSI Transactions on Electrical and Electronics Engineering (ITSI-TEEE) ISSN (PRINT): 2320-8945, 2016.
[25] R.Suganya, R.Anandha Jothi, Dr.V.Palanisamy: A Survey on Security Methodology in E-voting System. International journal of Pure and Applied Mathematics, ISSN: 1311-8080 (PRINT) ISSN: 1341-3395. http://www.ijpam.eu, on 29 April 2018.
[26] Achal Kamdi, Mamta Kamble, Rajeev verma: A Novel Approach for Online Voting System Using Visual Cryptography and Face Detection. International journal of Advances in Electronics and Computer Science, ISSN: 2393-2835. http://www.iraj.in, April 2017.
[27] Srivatsan Sridharan: "Implementation of Authenticated and Secure Online Voting System", 4th ICCCNT 2013 July 4 - 6, 2013.