

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

E- Voting System with Biometric Authentication

Aher Ruchita¹, Wagh Asmita², Bankar Rupali³, Prof. Pokharkar S.T.⁴

UG Student, Department of Computer Engineering, Shri Chhatrapati Shivaji College of Engineering,
Ahmednagar, India^{1,2,3}

Assistant Professor, Department of Computer Engineering, Shri Chhatrapati Shivaji College of Engineering,
Ahmednagar, India⁴

ABSTRACT: Voting schemes have evolved from counting hands in early days to systems that include paper, punch card, mechanical lever and optical-scan machines. Electronic voting systems provide some characteristic different from the traditional voting technique, and also it provides improved features of voting system over traditional voting system such as accuracy, convenience, flexibility, privacy, verifiability and mobility. But it suffers from various drawbacks such as Time consuming, Consumes large volume of pare work, No direct role for the higher officials, damage of machines due to lack of attention, Mass update does not allows users to update and edit many item simultaneously. These drawbacks are overcome by Online Voting System. Online Voting System is a voting system by which any Voter can use his/her voting rights from anywhere in the country. We provide a detailed description of the functional and performance characteristics of online voting system. Voter can cast their votes from anywhere in the country without visiting to voting booths, in highly secured way. That makes voting a fearless of violence and that increases the percentage of voting.

KEYWORDS: Voter ID, Finger Print Module.

I. INTRODUCTION

India is a constitutional democracy with a parliamentary system of government, and at the heart of the system is a commitment to hold regular, free and fair elections. These elections determine the composition of the government, the membership of the two houses of parliament, the state and union territory legislative assemblies, and the Presidency and vice-presidency. Elections are conducted according to the constitutional provisions, supplemented by laws made by Parliament.

The aim of the project is to create and manage polling and election details. This is a system which enables all citizens to cast their vote online. Increasing the voting percentage across the country is the major goal of this project. People have to visit the booth to cast their vote in the present system across the country. This system is online and hence even people who live out of their home town can also vote. Database of all the eligible citizens and candidates are maintained by the system.

Online voting system gathers its own significance since the NRI voting Rights bill have been passed by the parliament on Feb 11 in year 2011. The new law will allow an Indian citizen residing abroad to enroll in voters list and exercise his franchise even if he or she remained away from place of residence in India for more than six months owing to employment, education or otherwise. In the present case the person should be present within the constituency on the day of polling for exercising his right to vote. Thus our project, online voting should enhance the opportunities of voters outside the country to vote for their nation on implementation. The Online voting system is implemented using .NET platform using MySQL as a back end.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

Main aim of The Online voting system is to develop an online application for citizens who are above 18 years of age through online using this system citizens of an India can vote through online without visiting polling booth. A centralized data based is maintained by election commission of India where citizen information is maintained where citizen is using online voting system his/her information is authenticated with present data in database. If user is not in the list he cannot use online voting system.

II. LITERATURE SURVEY

Xuechao Yang et al. [1] describe advanced security methods are necessary to introduce effective online voting (e-voting) in the whole world. Elections conducted on paper consume a lot of resources and contribute to the destruction of forests, which leads to climate deterioration. Recent online voting experiences in countries such as the United States, India and Brazil demonstrated that further research is needed to improve security guarantees for future elections, to ensure the confidentiality of votes and enable the verification of their integrity and validity. In this paper, we propose a ranked choice online voting system, which addresses these challenges. It eliminates all hardwired restrictions on the possible assignments of points to different candidates according to the voter's personal preferences. In order to protect the confidentiality of the votes, each cast ballot is encrypted using the exponential ElGamal cryptosystem before submission. Furthermore, during voting the system ensures that proofs are generated and stored for each element in the cast ballot. These proofs can then be used to verify the correctness and the eligibility of each ballot before counting without decrypting and accessing the content of the ballot. This validates the votes in the counting process and at the same time maintains confidentiality. The security and performance analyses included in this paper demonstrate that our method has achieved significant improvements in comparison with the previous systems. The outcomes of our experiments also show that our proposed protocols are feasible for practical implementations.

X. Yang et al. [2] describe advanced security methods are necessary to introduce effective online voting (e-voting) in the whole world. Elections conducted on paper consume a lot of resources and contribute to the destruction of forests, which leads to climate deterioration. Recent online voting experiences in countries such as the United States, India and Brazil demonstrated that further research is needed to improve security guarantees for future elections, to ensure the confidentiality of votes and enable the verification of their integrity and validity. In this paper, we propose a ranked choice online voting system, which addresses these challenges. It eliminates all hardwired restrictions on the possible assignments of points to different candidates according to the voter's personal preferences. In order to protect the confidentiality of the votes, each cast ballot is encrypted using the exponential El Gamal cryptosystem before submission. Furthermore, during voting the system ensures that proofs are generated and stored for each element in the cast ballot. These proofs can then be used to verify the correctness and the eligibility of each ballot before counting without decrypting and accessing the content of the ballot. This validates the votes in the counting process and at the same time maintains confidentiality. The security and performance analyses included in this paper demonstrate that our method has achieved significant improvements in comparison with the previous systems. The outcomes of our experiments also show that our proposed protocols are feasible for practical implementations.

A. Ara et al. [3] describe due to advancements in the development of wireless medical sensing devices and wireless communication technologies, the wireless body area network (WBAN) has become an eminent part of e-healthcare systems. WBAN uses medical sensors to continuously monitor and collect the physiological parameters of a patient's health and send them to a remote medical server through a portable digital assistance (PDA)/mobile. Due to limitations in communication, such as power, storage, and the computational capabilities of sensors, data aggregation techniques are used to reduce the communication overhead in real-time data transmission in WBAN. However, since the WBAN transmits sensitive health data, data security and data privacy are a major concern. In this paper, we propose a secure privacy-preserving data aggregation (SPPDA) scheme based on bilinear pairing for remote health monitoring systems to improve data aggregation efficiency and data privacy. Our proposed SPPDA scheme utilizes the homomorphic property of the bilinear ElGamal cryptosystem to perform privacy-preserving secure computation and combines it with the aggregate signature scheme, enabling data authenticity/integrity in the WBAN. The proposed

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

SPPDA scheme is proved to be semantically secure under the decisional bilinear Hellman assumption. Security analysis demonstrates that our proposed scheme preserves data confidentiality, data authenticity, and data privacy; it also resists passive eavesdropping and replay attacks. A performance evaluation based on simulation results and a comparison of computational cost with related schemes show that data aggregation and batch verification at the PDA significantly reduce communication and transmission overhead and support efficient computation at the remote server.

Z. Li et al. [4] describe identity-based proxy re-encryption (IBPRE) is a powerful cryptographic tool for various applications, such as access control system, secure data sharing, and secure e-mail forwarding. Most of the existing efficient IBPRE schemes are based on the Hellman assumption, and they only focus on the single-hop construction. Based on the work of Chandran et al. lattice-based proxy re-encryption (PRE) scheme (PKC'14) and Yamada's lattice-based identity-based encryption (IBE) scheme (EUROCRYPT'16), in this paper, we first show the possibility of assembling lattice-based IBE into lattice-based PRE. Then, we present the construction of a new efficient single-hop homomorphic IBPRE from learning with errors (LWEs) via key homomorphic computation. Furthermore, using branching program (BP), we obtain an efficient multi-hop IBPRE scheme. To the best of our knowledge, our scheme is the first multi-homomorphic IBPRE scheme via BP. Our scheme supports homomorphic evaluation and is proved secure under the decisional LWE assumption.

O.Hasan et al. [5] Reputation systems make the users of a distributed application accountable for their behavior. Their reputation of a user is computed as an aggregate of the feedback provided by other users in the system. Truthful feedback is clearly a prerequisite for computing a reputation score that accurately represents the behavior of a user. However, it has been observed that users often hesitate in providing truthful feedback, mainly due to the fear of retaliation. We present a decentralized privacy preserving reputation protocol that enables users to provide feedback in a private and thus uninhibited manner. The protocol has linear message complexity, which is an improvement over comparable decentralized reputation protocols. Moreover, the protocol allows users to quantify and maximize the probability that their privacy will be preserved.

III. PROPOSED SYSTEM

Working of this Biometric Voting System for Election is a little bit complex for beginners. First of all, user needs to enroll finger or voters (in this code max limit of the voter is 25) with the help of push buttons/keys. To do this user need to press ENROLL key and then LCD asks for entering location/ID where finger will be a store. So now user needs to enter ID (Location) by using UP/DOWN keys. After selecting Location/ID user needs to press an OK key (DEL key). Now LCD will ask for placing finger over the finger print module. Now user needs to put his finger over finger print module. Then LCD will ask to remove the finger from finger print module and again ask for placing the finger. Now user needs to put his finger again over finger print module. Now finger print module takes an image and converts it into templates and stores it by selected ID in to the finger print modules memory. Now voter will be registered and he/she can vote. By same method all the voter can be registered into the system.

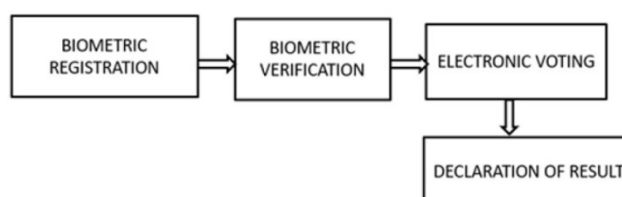


Fig 1: System Architecture

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

IV. RESULT



Fig 2: Home Page

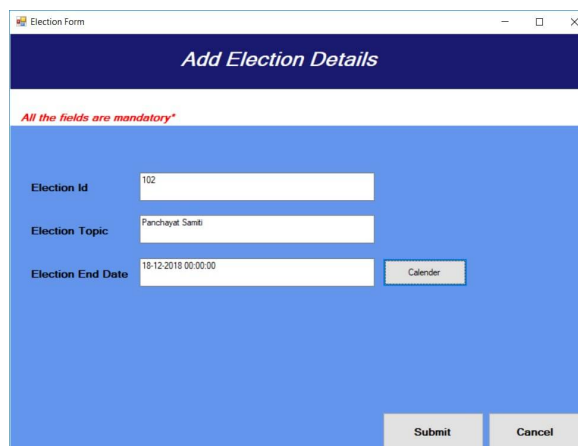
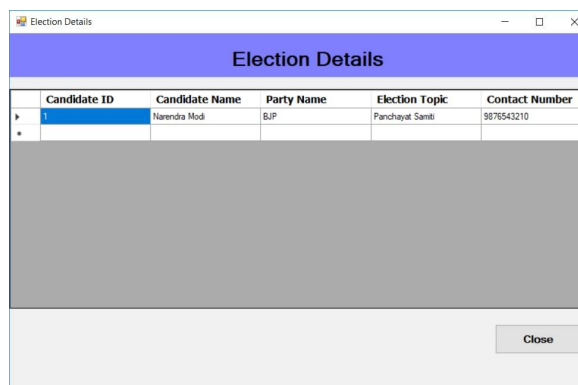


Fig 3: Add Election Details



Election Details				
Candidate ID	Candidate Name	Party Name	Election Topic	Contact Number
1	Narendra Modi	BJP	Panchayat Samiti	9876543210

Fig 4: Election Details

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

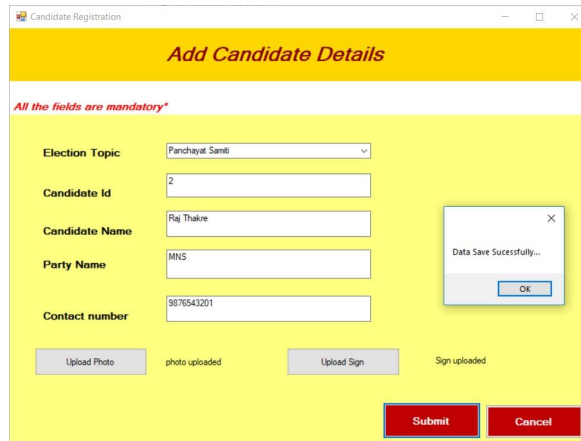


Fig 5: Add Candidate Details

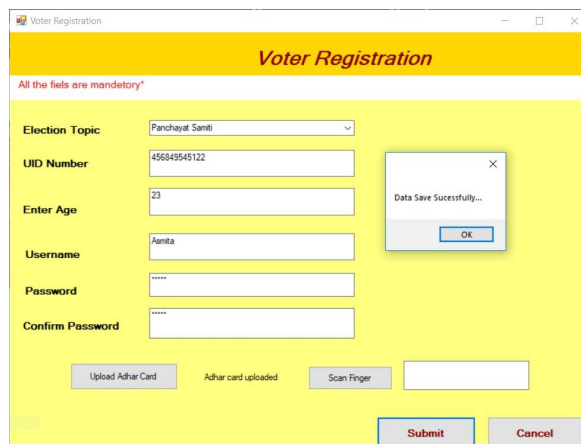


Fig 6: Voter Registration

V. CONCLUSION

This Online Voting system will manage the Voters information by which voter can login and use his voting rights. The system will incorporate all features of voting system. Its provide the tools for maintaining voters vote to every party and it count total no. of votes of every party. There is a database which is maintained by the election commission of India in which all the names of voter with complete information is stored. In this user who is above 18 years register his/her information on the database and when he/she want to vote he/she has to login by his id and password and can vote to any party only single time. Voting detail store in database and the result is displayed by calculation. By online voting system percentage of voting is increases. It decreases the cost and time of voting process. It is very easy to use and it is vary less time consuming. It is very easy to debug.

The Online Voting System (OVS) platform can be made more secure by using the following methods Password Changing Fingerprinting Cornea Detection The password used by the user to vote is provided by the administrator. In the future the user can be given the privilege of changing the password. So it helps to increase the security of the system. The other two methods that can be used are cornea detection and fingerprinting. But here the problem is that it decreases the scope of the platform because these systems need some electronic components to

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

implement. So it will avoid the user's privilege to cast the votes at their fingertips. But it can guarantee that fake voting will be impossible.

REFERENCES

- [1] Ahmed Ben Ayed, "A Conceptual Secure Block Chain-Based Electronic Voting System", IEEE International Journal of network Its Applications (IJNSA), 03 May 2017.
- [2] RifaHanifatunnisa, Budi Rahardjo, "Blockchain Based E-Voting Recording System Design", IEEE 2017.
- [3] Kejiao Li, HuiLi, HanxuHou, Kedan Li, Yongle Chen, "Proof of Vote: A High Performance Consensus Protocol Based on Vote Mechanism Consortium Blockchain", IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems, 2017.
- [4] Ali KaanKo, EmreYavuz, Umut Can abuk, GkhanDalkilic, "Towards Secure E-Voting Using EthereumBlockchain", IEEE, 2018.
- [5] Freya Sheer Hardwick, ApostolosGioulis, Raja NaeemAkram, Konstantinos Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy", IEEE, 03 July 2018.
- [6] Supriya Thakur Aras, Vrushali Kulkarni, "Blockchain and Its Applications A Detailed Survey", International Journal of Computer Applications (0975 8887) Volume 180 No.3, December 2017.
- [7] D. A. Lopez Garcia, A flexible e-voting scheme for debate tools, Computers Security, vol.56, pp. 5062, 2016.
- [8] J. Dreier, P. Lafourcade, and Y. Lakhnech, Denying privacy for weighted votes, single and multi-voter coercion, in European Symposium on Research in Computer Security, ESORICS 2012. Springer, 2012, pp. 451468.
- [9] A. O. Santin, R. G. Costa, and C. A. Maziero, A three ballot-based secure electronic voting system, IEEE Security Privacy, vol. 6, no. 3, pp. 1421, 2008.
- [10] A. A. Philip, S. A. Simon, and A. Oluremi, A receipt-free multi-authority e-voting system, Int. J. Computer Applications, vol. 30, pp. 1523, 2011.
- [11] M. Hirt and K. Sako, Efficient receipt-free voting based on homomorphic encryption, in Advances in Cryptology, EUROCRYPT 2000. Springer, 2000, pp. 539556.