International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Secure Online E-voting Protocol Based on Voters Authentication

V. Sahaya Sakila, Debin Jose, Abhijith K P, Adith R Babu

Abstract: ***Although there are many e-voting systems present by analysis it is found that they all are vulnerable to privacy risk and weakness of unreliable protocols and denial of service attacks. Here is the need to implement the public key encryption e-voting system. The primary objective of this system is to make ensure reliability, privacy and security of the protocol and voting is convenience to users. As a result of the specification requirements, the system was summarized into three parts: access control process which limit access to a system or to any other resource. Secondly, voting process was done by encrypting voter's electronic ballot before submitting to the server. Finally, the final result was sorted through deciphering the received encrypted information. The System is more efficient than other E-Voting systems, since voters can vote from their devices without extra cost and effort, and encryption ensures the security. A pseudo random number is generated using the OTP principle, is used by the voter for authentication purpose while casting the vote. These techniques provide a secure platform, thus exceeding vulnerabilities of the traditional voting system.***

Keywords: Pseudo algorithm (false name), time based One Time Password algorithm (TOTP), Security algorithm (RSA).

I. INTRODUCTION

India is the largest democracy in the world and it is maintained so through the voting process which take place in every 5 years. It is one of the most firstly amended Fundamental rights giving every citizen of India above the age of 18 to participate in the electoral voting process. An estimated Rs.60000Cr. was spent on the 2019 lok sabha election. Considering how far the internet has progressed and the impact it has on our daily lives, there should be provision for people to vote online without compromising on security. Through online voting or E- voting, the entire voting procedure can be completed at a fraction of this cost and at break neck speeds. The election model code which comes to effect after election is declared greatly hampers the smooth functioning of the government. So, if the time taken for carrying out the electoral procedure is reduced, it will greatly improve efficiency of the government.

Revised Manuscript Received on November 30, 2019.
* Correspondence Author
Debin Jose*, pursuing his Bachelor degree in computer science and engineering from the prestigious SRM institute of science and technology.
Abhijith K P, pursuing his Bachelor degree in computer science and engineering from the prestigious SRM institute of science and technology.
Adith R Babu, pursuing his Bachelor degree in computer science and engineering from the prestigious SRM institute of science and technology.
V. Sahaya Sakila, assistant professor at the computer science and engineering department of SRM institute of science and technology.

I. RELATED WORKS

As of now considering the security parameters the most efficient way to excute the E-voting can be done through AADHAR CARD as the data directly enters to the database mentioned by election commission of India.
But its dis advantages is that the illegal voting can be done through the expired voters [1].
Secure Authentication for Online Voting System In this mentioned paper a system using digital biometrics and steganography is used to secure the identity of the voters[2].
Through online voting or E- voting, the entire voting procedure can be completed at a fraction of this cost and at break neck speeds. The election model code which comes to effect after election is declared greatly hampers the smooth functioning of the government. So, if the time taken for carrying out the electoral procedure is reduced, it will greatly improve efficiency of the government[3][4].
Application For Online Voting System in this paper they discribed voter can easly enters to their vote from anywhere with the help of android device [5][6].Using this method the security is being compromised as anyone can add the device and get the data from database. Voting through internet is not secure as any person and the candidate hack the device and could unauotherislly acess the data related to the people voted and candidate who recived that vote.[7][8]This unauthorized users could manipulate the voters data and will be able to create to fake votes effecting the exsistence of the system itself. This is a serious issue as this can question the entire democracy of our nation.[9][10]
The Patchwork of Internet Voting in Canada In this paper hacking is also a major drawback, as regular voting is highly decentralised in most countries. It makes it hard to manipulate on a large scale (especially from outsiders. i.e. not the government itself). If there is confirmed fraud on an online system (for example, more votes than citizens) [8]. All votes are invalid and should be redone. In regular voting only the affected district should be redone [11][12].
The existing electoral method, election is conducted on the date fixed by the Election commissioner of India. In this type Election commission of India has settle the booth for voting. The voters can use their own unique password and ID proof(AADHAR, Driving License). In the account the voter can easly verifies their details and check to their voting status. Voter can moves to Election Commission website. In this website contains all the informations of candidate name, candidate party name and logo of that party. voter can select their favourite candidate and party. Then he/she can click the OK button for the submission of their vote to their favourite candidate. But this system exists more disadvantages like chance of widespread booth capture, multiple voting or voter impersonation, vote rigging, ballot-box stuffing, influencing voters through intimidation or bribery, Illegal intervention in the voting process.

II. PROPOSED SYSTEM

The system we propose uses a three layer approach that indicates the voters who are eligible for voting. Secondly, the voting process was done by encrypting voter's electronic ballot before submitting to the server. Finally, the final result was sorted through deciphering the received encrypted information. The System is more efficient than other online voting systems because voters who can vote without extra cost and effort, and encryption ensures the security. Mainly this system has features are it does not depend or require manual control and fully is automated and voting details will be stored in encrypted format.

A) EIGamal Algorithm

ElGamal cryptosystem is very well known . We assume that the cyclic group (G,q,g) is defined and there are n users in the system. Each i-th user has its own public key yi and secret key xi. The distributed ElGamal cryptosystem consists of the following algorithms. *Key Generation:* A common public key

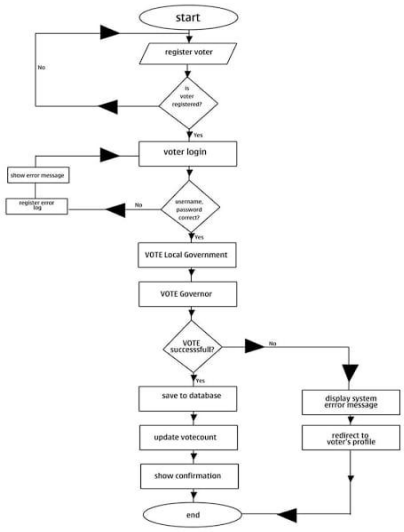
$PK = \pi^{n}_{i=1} y_i = g^{x_1 + \ldots + x_n}$

is used in the distributed ElGamal cryptosystem. *Encryption:* To encrypt a plaintext message m∈G:

i. Randomly choose an integer r from Z∗ q;
ii. Computes c1 =gr;
iii. Computes c2 =gm·PKr.

The encrypted message is E(m)=(c1,c2).

B) Flow chart



III. SYSTEM ARCHITECTURE

A) Voter Authentication:
B) Encrypt Vote
C) Administrative Login
D) Result declaration

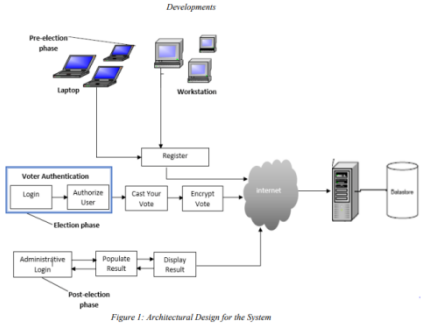


Figure 1: Architectural Design for the System

A. Voter registration phase

In this phases the voter can enter their details like their name, address ,age, sex, contact number ,etc..
In this module following below steps are mentioned:

I. First step is that election commission can logging their systems and start registration process.
II. Main authority can take the detais of registered voters .That means their Name, Age, Sex, Address, Number etc..
III. And the next procedure is Authority Asks voters to submit their own id proof .That means their AADHAR, Driving Licence, etc…
IV. Authority operates voters can enter password.

B. Date and time of Election phase

In this phase, the Authority conform a date for voting, With that particular time period the voters can vote. That vote will be going to Election Commission Database. Authority plan the time period according to Indian Standard time Zone which is nearly +5.30 offset from GMT. The voters who are not in their area can also vote according to this time period. They can easly mention their vote for their candidate.

C. Election Day phase

On that day of Election, Authority responsible for that particular area they arrange the location for mobile boothing. That particular time Election Commission open that website for voting. Then that particular time zone the voters can enter their vote for their preferred candidate at that particular area.

D. Vote Submission phase

In this phase the voters can login their account. That means the voters can use their own unique password and ID proof (AADHAR, Driving License). In the account the voter can easly verifies their details and check to their voting status. Voter can moves to Election Commission website. In this website contains all the informations of candidate name, candidate party name and logo of that party. voter can select their favourite candidate and party. Then he/she can click the OK button for the submission of their vote to their favourite candidate.

E. Cross check/Verification of votes phase

In Verification phasen, votes are verified by Election Commission of India through election database.

F. Result Declaration phase

Finally the verification process is done. After that count the number of votes that the candidate get by voters .And finally announced the result.

IV. IMPLEMENTATION

A. Adding Voter Information

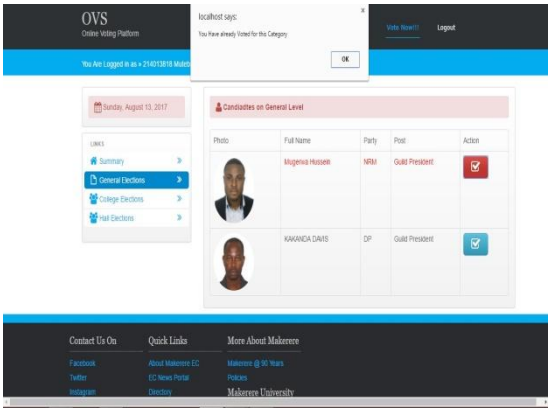
Voters can add their details according to their unique id number(registration number).In this registration number is helped to Identify the booth and party of that candidate.After completion of this process the Authority will give a Use name and password ,that can be used for the voters to login the website of Election Commission at the time of election day.

B. Adding Candidate Information

In this phase adding the candidate informations like their name,party,and party flag. It will displayed the website of Election Commission. It helps to voters can easly identify their favourite candidate and party

C. Cast vote

This is the last phase of E-voting. Here the voters can enters the website through their username and password , that arte already given by the registration phase. Then the voters can select their favourite candidate and party. This information will be stored in Election Commission database.



V. RESULT ANALYSIS

The world moves to a digital era where every thingis being digitized. Through the digitization, all the process is being domain through the digital system .Since technology has deeply been integrated through our lives .The future of voting is through digital mediums .Digital mediums are more accessible than the traditional voting systems. This give a good advantage that makes sure online voting will be in our near future.

VI. CONCLUSION

E voting is a very beneficial and innovative idea, through this medium, non- residential Indians and people who are unable to cast their votes in their respective Booths will be able to take part in the election process. This will ensure continuous governance and reduce the time period for a stop gap government E voting is the future of our voting process and let's hope to embrace and implement it effectively.

REFERENCES

1. Himanshu Agarwal, G.N.Pandey “Online Voting System for India Based on AADHAAR ID” Indian Institute of Information Technology.
2. Smitha B. Khairnar, P. Sanyasi Naidu, Reena Kharat “Secure Authentication for Online Voting System” Pimpri Chinchwad College of Engineering, Pune.
3. Himanshu Vinod Purandre, Akash Ramswaroop Saini, Freddy Donald Pereira “Application For Online Voting System Using Android Device “ St.John College of engineering and Management,Palghar.
4. Hayam, Ketal “The Patchwork of Internet Voting in Canada”.
5. B. Rashidi, C. Fung, and E. Bertino, ‘‘Android resource usage risk assessment using hidden Markov model and online learning,’’ Comput. Secure., vol. 65, pp. 90–107, Mar. 2017.
6. M. Gregory. (2016). Electronic Voting May be Faster but Carries Security Risks. [Online].
7. J. Lavelle and D. Kozaki. (2016). Electronic Voting has Advantages but Remains Vulnerable to Security, Software Problems. [Online]. Available: http://www.abc.net.au/news/2016-07-11/electronic-voting-hassupport-but-security-fears-remain/7587366
8. S.J.BramsandP.C.Fishburn,‘‘Goingfromtheorytopractice:Themixed success of approval voting,’’ in Handbook on Approval Voting (Studies in Choice and Welfare). Springer-Verlag, 2005, pp. 19–37
9. T. ElGamal, ‘‘A public key cryptosystem and a signature scheme based on discrete logarithms,’’ IEEE
10. K. E. Lauter, ‘‘Practical applications of homomorphic encryption,’’ in Proc. ACM Workshop Cloud Comput. Secure., 2012, pp. 57–58.
11. X. Yang et al., ‘‘A verifiable ranked choice Internet voting system,’’ in Proc. Int. Conf. Web Inf. Syst. Eng. (WISE), 2017, pp. 490–501.
12. M. Hirt and K. Sako, ‘‘Efficient receipt-free voting based on homomorphic encryption,’’ in Advances in Cryptology—EUROCRYPT. Bruges, Belgium: Springer, 2000, pp. 539–556. [Online]. Available: http://www.springer.com/us/book/9783540675174Trans. Inf. Theory, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.
13. X. Yi and E. Okamoto, ‘‘Practical remote end-to-end voting scheme,’’ in Electronic Government and the Information Systems Perspective. Toulouse, France: Springer, 2011, pp. 386–400. [Online]. Available: http://www.springer.com/us/book/9783642229602
14. B.Adida,‘‘Helios:Web-basedopen-auditvoting,’’inProc.USENIXSecur. Symp., vol. 17. 2008, pp. 335–348.

AUTHERS PROFILE

Debin Jose is currently pursuing his Bachelor degree in computer science and engineering from the prestigious SRM institute of science and technology. His current interests lie in the domains of machine learning and data science. He is a meritorious student who has excellent academic achievements to his credit.

Abhijith K P is currently pursuing his Bachelor degree in computer science and engineering from the prestigious SRM institute of science and technology. His current interest’s lies in the domains of Algorithms and machine learning and is looking out for a prospective career in his domain.

Adith R Babu is currently pursuing his Bachelor degree in computer science and engineering from the prestigious SRM institute of science and technology. He is interested in the domain of machine learning and also intrigued in the domain of mathematics and neural networks.

V. Sahaya Sakila is currently an assistant professor at the computer science and engineering department of SRM institute of science and technology. She has achieved M.E in computer science and engineering.She has a research interest in Networking and Cyber Security