

Performance Improvement using Pseudorandom One Time Password (OTP) in Online Voting System

Preeti Ahlawat¹, Rainu Nandal^{1*}

¹*University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak, India (124001)*

Abstract: In today's world of growing advanced mobile technologies, the traditional voting method can be changed to a newer and effective approach termed as mobile voting. The Mobile voting system provides a convenient, easy and efficient way to vote eliminating the shortcomings of traditional approach. In this paper we propose to build an E-Voting system which is basically an online voting system through which people can cast their vote through their smart phones or by using an e-voting website. To achieve the required security we are using OTP (one time password) approach, which is most commonly on the web to tell the difference between a human using a web service and an automated bot thus making the website more secure against spam-bot attacks. If the results of the matching algorithm are three point match then checks whether this person own voter ID after that it will check with AADHAAR ID. If he has the right to vote then a voting form is presented to him, and the third level of authentication is carried out by using One Time Password (OTP) principle. The OTP principle emphasizes that each time the user tries to log on, the algorithm produces pseudorandom output thus improving the security. The result shows that the proposed algorithm capable of finding over 90% of the faces in database and allows their voter to vote in approximately 58 seconds. choices regarding exact issues, pieces of rule, citizen initiatives, constitutional amendments, recalls and/or to select their government and political representatives. [19] Nowadays Technology is being used more and more as a tool to contribution voters to cast their votes. To allow the use of this right, almost all voting systems around the world contain the following steps:

Voter identification and authentication, voting and recording of votes cast, vote counting, publication of election results. [16]

Voter identification is required during of the electoral process:

1. first for voter registration in direction to establish the right to vote and then, at voting time, to allow a citizen to use their right to vote by authenticating if the person satisfies all the requirement needed to vote (authentication). [14]
2. Security is important of the e-voting process. Therefore the necessity of designing a secure e-voting system is very important. Generally, mechanisms that ensure the security and privacy of an election can be time consuming, expensive for election administrators, and inconvenient for voters.[12]

Keywords: mobile; voting; digital voting; one time password (OTP), Pseudo-random number

I. Introduction

The aim of this research is to project an appropriate application for real time online electronic voting systems for polling commission.[17]The voting is to permit voters to use their right to prompt their 3. There are different stages of e-voting security. Therefore serious actions must be occupied to keep it out of public domain. Also, security must be practical to hide votes from publicity. [9] 4. There is no capacity or measurement for acceptable security level, because the level depends on type of the information. An acceptable security level is a constant cooperation-between usability and power of security method.[7]

II. Literature Review

In [1], the author Kohno T., Stubblefield A., Rubin A. and Wallach D. S, (2004), describes the security features of the electronic voting system and e-voting system is better than manual voting system. Also, the author shows that voters, without any insider privileges can cast unlimited votes without being detected by any mechanisms within the voting terminal software.

In [2], the author CiprianStănică- Ezeanu (2008) reviewed e-voting procedure by describing its advantages and disadvantages. His work was majorly on the security measures such as firewalls or SSL communications which are necessary but not sufficient to guarantee the specific security requirements of e-voting. Also, the author describes the additional layer of

specialize dsecurity technology to address the specific risks posed by electronic voting and guarantee critical security requirements such as voters' privacy, vote integrity and voter-verifiability. The author equally suggested the use of Biometrics and smartcard for authenticating users. One major issue the author stressed out is the difference between biometric and "classic" authentication like smart cards. The e-voting system proposed in [2] does not interact in any way with the biometric characteristics of the actual users, but still authenticates the user with the help of the user's authentication certificate on the smart card. In [3], **Manish K, Suresh K.T, Hanumanthappa. M, Evangelin G.D (2005)** the author specified mainly on securing the voting system, by comparing the insecurities that exist in the manual voting system to that of the electronic voting system.

Authors **Rossler T.G (2011)** in [4] suggested the use of Remote Internet Voting, with a view to enhance voter convenience, increase voter confidence and voter turnout. In the survey, authors suggested remote poll-site electronic voting as the best step forward as it provides better voter convenience, but at the same time, does not compromise security.

In [5], the author **Avi Rubin (2001)** review the security measures needed for remote online voting system by focusing on two cases where voters cast their ballots over the Internet – the 2000 Arizona Democratic Primary and the University of Virginia Student Council Elections. The author claims that a secure voting system must thoroughly satisfy four major requirements: authentication, availability, confidentiality and integrity.

III. Problem Statement

Making the electronic voting system has an obligation of security and of acquiring user confidence , usually user can access to the electronic voting system and voting on the text without security system, that any user can access to the electronic voting system through the ID number for another user and he/she can vote more than one time at the same text, The users could know the result of voting during the process of voting which make the system dicey and mistrust, The user can dominate the result of voting by the access that he or she has of the result before the end of election day.[8]

IV. System Model

Electric Election systems are capable to mark the voting system more controlled, secure and speedy. E-Election system helps public to elect their representatives more securely and express their preferences for how they want to be governed. [6]

Election development has very strong media coverage mainly, if something goes wrong [10]. This system will increase the level of security and make the trust and confidence in voters.

The origin of Maoist violence and presented that public need a more secure method of casting their vote. [16] To make the voting system trust well-meaning is very hard just because it needs high security requirements: privacy and integrity. Confidentiality means all voters developconfident about the privacy of votes and prevent export of votes. Integrity means declaration of perfect results of elections and the correct including of votes. Integrity is easy to become through a public show of hands, but this dissipates confidentiality and confidentiality comes from the secret ballots, but this fails the integrity. The full E-Election system provides people to vote in a secure way without any fear. The online voting system also providing the security to the voter's by storing the vote in a secure digital form, if the voter votes beside spiteful applicant. This system also guarantees not to leak the vote in obverse of anyone.

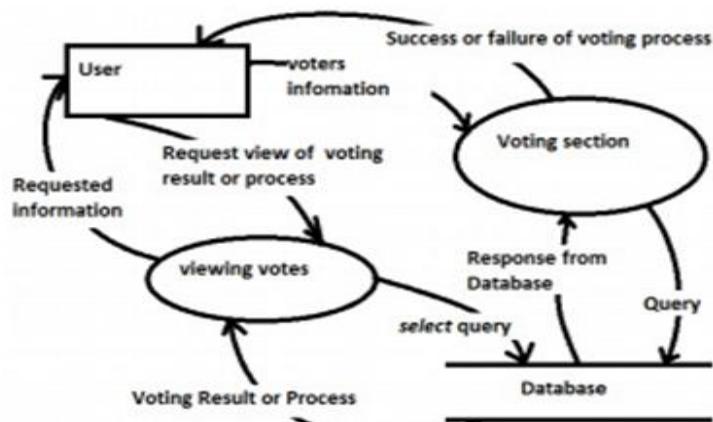


Figure 1: Diagram of analyzing voters section

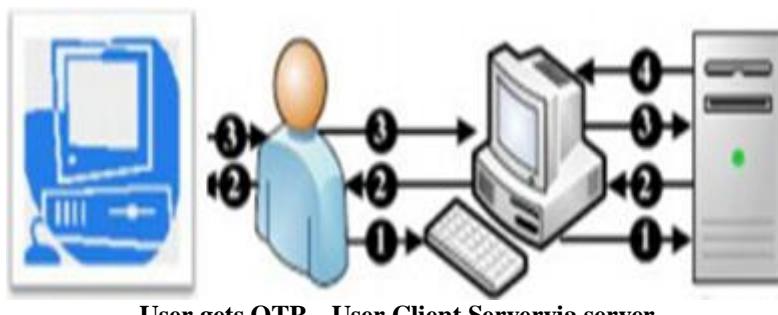
V. Proposed Implementation

The Online Voting should:

- Be able to display all registered voters in the database to the SYSTEM ADMIN(s) as per their access rights and privileges.
- Have a user-friendly interface and user guides understandable by people of average computer skills.
- Be robust enough so that users do not corrupt it in the event of voting.
- Be able to handle multiple users at the same time and with the same efficiency, this will cater for the large and ever growing population of voters.

OTP

The Main Security implementation of our project is the concept of One Time Password i.e. every time a new password is generated and sent to the user on his mobile phone. One Time Password is a Random 6 Digit Number that changes every time, whenever user logs on to the system and performs some transaction.



The Concept has been implemented in such a way that it adds high level of security to our banking Application.

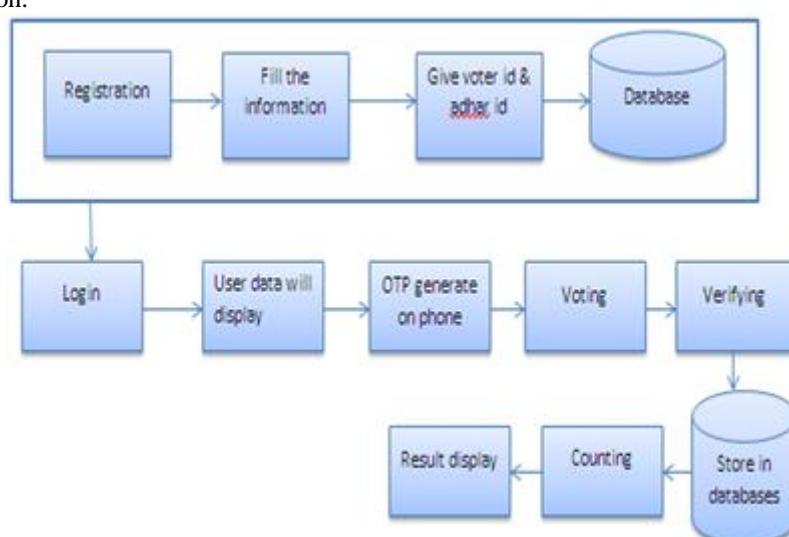


Figure 2: proposed Flow chart

The Flow chart of the mobile voting shows the sequential flow of how the data passes from one activity to another. It starts from Registration, Login and Forgot password .The Fig 2 shows the initial screen when the application starts. It has the login form, registration and forgot password and then continues

Registration: - This option is used when the user is first registering through the application. It will take them to a registration screen.

Login: This option allows us to log us in for voting.

Result Activity: The task of voter registration is strictly preserved for the system administrator. Therefore if you are logged in as a mere user/voter, you don't have this privilege, therefore, the registration page link is disabled for you.

OTP Activity: The task of OTP (one time password) is to send a mobile phone on the registered mobile after logging in the account, so that we can cast vote only after we are authorized to do so by the OTP sends us a random message on our mobile an random number and then we can insert the number to vote.

Voting Activity: - After voting, a voter is allowed to check the results by visiting the results page.

VI. Result

The proposed Online Voting System with OTP scheme is described in this section. In this proposed method we will commence the work with database creation. In order to create the database we collect the voter detail from different voters as shown in the figures.

The screenshot shows a 'New Voter Registration' form. It has two sections: 'Voter Registration' and 'User Login'. The 'Voter Registration' section contains fields for Admin Login (Admin ID: PA123456, Voter ID: PA654321), User Login (First Name: PREETI, Last Name: AHLAWAT, Father Name: Praveen, Contact No: 8663017180, Age: 22, Address: [empty], PIN Code: 121001, Email: preet6123@gmail.com), and User Details (User Name: PREETI, Password: [redacted]). Validation messages are displayed next to some fields: 'Alpha or Numeric value Allowed Only' for Admin ID and Voter ID, 'Maximum 30 Character allowed' for First Name and Last Name, 'Maximum 30 Character allowed' for Father Name, '10 digit allowed only' for Contact No, 'Above 18+ allow only' for Age, and 'Maximum 50 Character allowed' for Address. Below the form, a note states: 'jpg;png;gif;jif Format Mandatory'.

Figure 1: Voter registration form

The screenshot shows a 'HOME PAGE' with a 'MENU' on the left containing 'Voter Registration', 'Admin Login', and 'User Login'. On the right, there is a 'LOGIN' section with 'ADMIN LOGIN' fields for 'LOGIN:' (admin) and 'Password:' (*****). A 'login' button is at the bottom.

Figure 2: Admin Login form

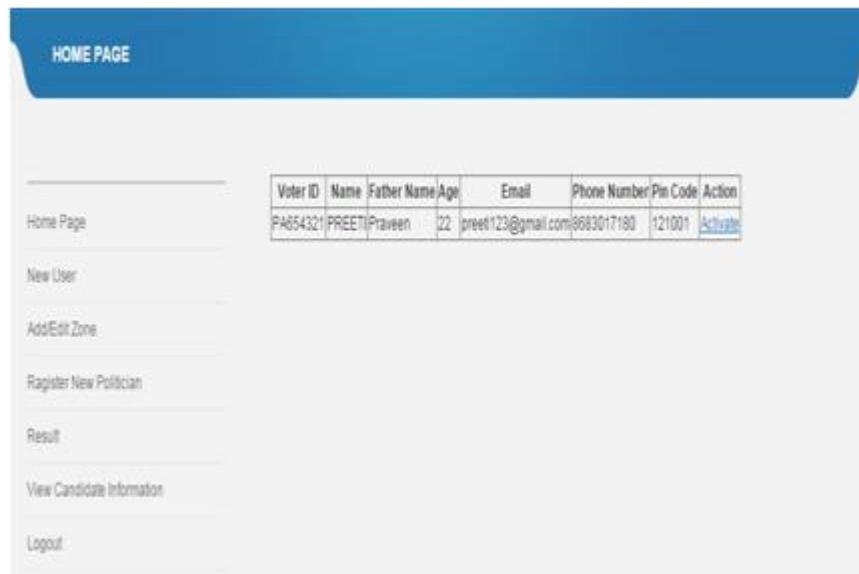


Figure 3: Activate to voter by Admin permission

The screenshot shows a 'HOME PAGE' header. To the right is a 'New Politician Registration' form. The form fields include: Politician ID (pol510), Name (ushma), Contact No. (7867772343), Address (ashok), Party Name (BJP), Political Sign (image of the Indian flag), and Zone (Delhi). There is also a 'Remember Me' checkbox and a 'Submit' button at the bottom.

Figure 4: New Politician form

The screenshot shows a 'HOME PAGE' header. On the left is a 'MENU' section with links: Voter Registration, Admin Login, and User Login. On the right is a 'LOGIN' section with fields: ADHAR ID (PA123456), VOTER ID (PA654321), and Password (*****). Below these fields are two buttons: 'login' and 'Button'.

Figure 5: New voter login form with authorized voter id, AADHAAR id and password

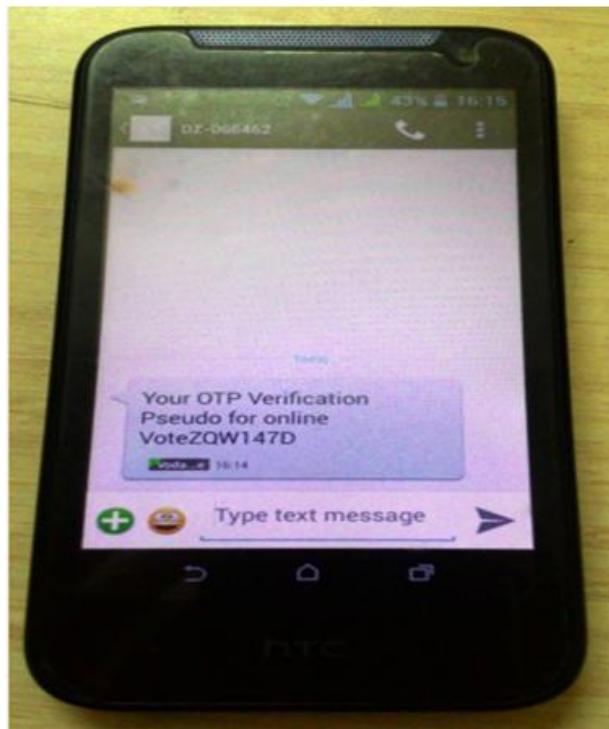


Figure 6: Access OTP on registered mobile for vote

HOME PAGE

MENU

Voter Registration Admin Login User Login

Enter OTP Here:

Validate one time password

Validate OTP Reganerate OTP

Figure 7: Now validate OTP

HOME PAGE

WELCOME PREETI

Thanks! Your Vote Submitted Successfully

SelectZone: Delhi

Select Party: BJP

MODI

Vote now

Home Page Voter now Update Account View Candidate Information View Election Result Change Password Logout

Figure 8: voter get successfully vote



Figure 9: Final result

VII. Conclusion

Genuine voter

In Present time, OTP (one time password) applications are increased. Security is an important issue for handling such services. Current system provide security card based facility to authenticate user but this is not secure enough and may not be available on any time or situation. To overcome such type of issues we propose online e-Voting authentication system using OTP with aadhaar id and pseudorandom number generator that identification is too complex which is improving the security for brute force attack.

The practicable future scope of the project includes the improvement in the security level of the system. In annexation to that it would be interesting to meet some other confidential primitives to improve the security level of online voting system.

References

- [1]. Kohno T., Stubblefield A., Rubin A. and Wallach D. S. (2004), "Analysis of an Electronic Voting System", In Proceedings of IEEE Symposium on Security and Privacy 2004, pp. 1-23
- [2]. CiprianStănică-Ezeanu (2008), "e-Voting Security", Buletinul Universității Petrol – Gaze din Ploiești, Vol. LX (2), pp 93-97
- [3]. Manish K, Suresh K.T, Hanumanthappa. M Evangelin G.D (2005), "Secure Mobile Based Voting System", Retrieved online at http://www.iceg.net/2008/books/2/35_324_350.pdf on November 17th 2012.
- [4]. Rossler T.G (2011),"E-voting: A survey and Introduction",Availableat<http://wiki.agoraciudadana.org/images/5/56/An%2BIntroduction%2Bto%2BElectronic%2BVoting%2BSchemes.pdf> Retrieved on 15th June 2012.
- [5]. Avi Rubin (2001),"Security Considerations for Remote Electronic Voting over the Internet", AT&T Labs – Research Florham Park, NJ. Available at <http://avirubin.com/evoting.security.html>, (date accessed 7th July, 2012).
- [6]. Dr. Aree Ali Mohammed, Ramyar Abdolrahman Timour, "Efficient E-Voting Android Based System", Volume 3, Issue 11, November 2013, ISSN: 2277,128X
- [7]. JaideepMukute, HemantNagpure, HarshalKuthe, NehaMohadikar, ChaitaliDevade, "Online Banking AuthenticationSystem Using QR-Code and Mobile OTP",Vol.3, Issue 2, March-April 2013, ISSN: 2248-9622.
- [8]. Kim, K and Hong, D (2007), "Electronic Voting System using Mobile Terminal. World Academy of Science, Engineering and Technology, Vol .3(2), pp.33-37
- [9]. J A. Chefranov, "One-Time Password Authentication with Infinite Hash Chains. Novel Algorithms and Techniques", In Telecommunications, Automation and Industrial Electronics, 2008, pp. 283-286
- [10]. Noha E. El-Sayad, Rabab Farouk Abdel-Kader, Mahmoud Ibraheem Marie" Face Recognition as an Authentication Technique in Electronic Voting" -(IJACSA).
- [11]. SKINNER, C. "75% of young adults want to vote by sms in the election. 89% expect text voting to be introduced soon". PC ADVISOR. February18,2010.
- [12]. Mohamed HamdyEldefrawy, Khaled Alghathbar, Muhammad Khurram Khan, "OTP- Based Two-Factor Authentication Using Mobile Phones",Eighth International Conference On Information Technology: New Generations, 2011.
- [13]. W. Smith, "New cryptographic election protocol with best-known theoretical properties," in Proc. Of Workshop on Frontiers in Electronic Elections, 2005.
- [14]. S. G. Weber, R. Araujo, and J. Buchmann, "On coercion-resistant electronic elections with lineework," in The Second International Conference on Availability, Reliability and Security (ARES2007), april 2007, pp. 908–916.
- [15]. R. Araujo, S. Foulle, and J. Traore, "A practical and secure coercionresistant scheme for remote elections," Frontiers of Electronic Voting, vol. 7311, 2007.
- [16]. Chun-Ta Li, Min-Shiang Hwang, Yan-Chi Lai "A Verifiable Electronic Voting Scheme Over the Internet", 2009 Sixth International Conference on Information Technology: New Generations
- [17]. G.O. Ofori-Dwumfuo and E. Paatey , "The Design of an Electronic Voting System", Research Journal of Information Technology 3(2): 91-98, 2011 ISSN: 2041-3114

- [18]. Tai-Pang Wu, , Sai-Kit, Yeung,JiayaJia, Chi- Keung Tang, AndGe' RardMedioni Closed-Form Solution To Tensor Voting:TheoryAndApplicationsTransactions On Pattern Analysis And Machine Intelligence, Vol. 34, No. 8, August 2012
- [19]. 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
- [20]. Jossy P. George Saleem S TevaramaniAnd K B RajaPerformance Comparison Of Face Recognition
- [21]. Using Transform Domain Techniques World Of Computer Science And Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 3, 82-89, 2012