WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

COMPARATIVE STUDIES OF DIGITAL VOTING SYSTEM FOR IMPROVED SECURITY OF AUTHENTICATION WITH MULTILEVEL ENVIRONMENTS

Mr. Sachin M. Vaidya[1], Prof. Rahul Patil [2]

Final year Student of Master of Computer Engineering, Bharati Vidhyapeeth College of engineering, Navi Mumbai – 410210, Maharashtra, sachin.m.vaidya@gmail.com[1]

Assistant Professor of Master of Computer Engineering, Bharati Vidhyapeeth College of engineering, Navi Mumbai – 410210, Maharashtra, Rahhul.patil@gmail.com[2]

ABSTRACT

In this paper we are analysis the comparative studies of digital voting system which support the voter authentication in the various election system and decrease the causes of the wrong authentication and reflection in the political environment.

We are also reviewing the different Authentication areas which are affected in the digital voting with the success /failure environment. Also observed the multilevel factor impact for develop in the digital voting system with respective security for future enhancement

Now day authentications are new challenges of the voters and make to right for voting. Digital voting has great potential to decrease election costs and increase voter authentication and performance. It eliminates the need to paper print ballot Papers or open polling stations voters can vote from wherever there is an Internet connection. Despite these benefits, online voting solutions are viewed with a great deal of caution because they introduce new threats. A single vulnerability can lead to large-scale manipulations of votes. Electronic voting systems must be legitimate, accurate, safe, and convenient when used for elections. Nonetheless, adoption may be limited by potential problems associated with digital voting systems.

1. INTRODUCTION

Digital voting mainly is used because of their end-to-end verification should be improve due to duplication authentication. This technology is a beautiful replacement for traditional electronic voting solutions with distributed, non-repudiation, and security protection characteristics. The main goal of this analysis was to examine the current status of digital voting system with multilevel authentication for the implementation the system with review of the Indian society and their user performance for adapted the better system. Digital voting systems and any related difficulties to predict for future developments. This study provides a conceptual description of the electronic voting application and an introduction to the fundamental structure and characteristics of the digital voting. On the other hand, the most often mentioned issues and challenges in digital voting system with privacy protection and transaction speed performance. Digital voting system, the security and authentication improve the voter with respective the election valuable result

2. TRADITIONAL VOTING SYSTEM

Most traditional election systems are far from ideal. They tend to rely on a number of trusted parties who have the ability to conspire to change the outcome of the election or reveal the way particular voters voted. These systems generally work because most of the trusted parties are either trustworthy or have little trust in each other, and thus no conspiracy takes place.

Traditional Voting System.

The voting systems used for national elections in the United States are generally designed to satisfy all of the core properties to some degree. However, there is no official set of criteria which voting systems throughout the U.S. are required to satisfy. In most systems there are opportunities for votes to be changed, lost, or incorrectly recorded during the counting process. Although inaccurate tallies may be the result of fraud, all documented inaccuracies in computerized vote tallying have been the result of problems with or misuse of the voting equipment or software. For example, a 1984 Carroll County, Maryland school board election was incorrectly tallied by a computerized tallying system after an election administrator accidently installed the wrong utility program for reading ballot cards. The use of absentee ballots gives national elections the mobility property, allowing voters to cast their votes from almost anywhere they want. However, absentee ballot systems tend to reduce privacy further and increase the opportunity for ballots to be changed or lost. Despite these procedural shortcomings, it would be difficult for a national election to be thrown because of the large number of precincts and the diversity of voting systems used. In addition, vote buying is probably rare because it is nearly impossible for a voter to prove how he or she voted after leaving the polling booth. (However, vote buying can occur easily when absentee ballots are used.)

The systems used for national elections are usually also used for local elections in the United States. However, when used for local elections these systems are more likely to be abused because a relatively small number of precincts contribute to the final vote tally. With over 10,000 election officials participating in U.S. national elections, widespread fraud or negligence is not likely to go undetected. Large professional, social, and special interest organizations tend to hold their elections through mail-in balloting. These systems allow voters to cast their votes from virtually any location; however, they often sacrifice accuracy and privacy. This method usually works because organizations that use this system tend not to hold highly controversial elections. In addition, they often hire a disinterested party to run their elections.

Many states also use mail-in balloting for some elections, especially in small precincts. Generally voters are asked to submit their ballots in double envelopes to protect their privacy. Probably the largest organization to use mail-in balloting to date is the Teamsters. In 1988 the Teamsters sent mail ballots to 1.5 million members. According to Teamsters election officers, the only problems encountered were a few attempts to vote multiple times or intimidate voters. Nonetheless, many people are still skeptical about the security of mail-in balloting. The California and Kansas Supreme Courts have both ruled on cases involving mail-in balloting. In both cases the courts refused to strike down laws allowing mail-in balloting, despite the Kansas court acknowledging that ``vote by mail increases the potential for compromise of secrecy and opportunity for fraud".

Most traditional election systems can be verified only by party representatives or trusted third parties. It is generally not possible for voters to verify that individual votes were counted correctly. In addition, while the verification process can often detect procedural problems and large discrepancies between the final tally and the number of voters who visited the polls, it usually cannot correct inaccuracies.

The traditional voting system has cost a lot of money and resources and the process of applying modern technologies has created the voting system easy and inexpensive method.

3. DIGITAL VOTING SYSTEM

Digital voting is often seen as a tool for making the electoral process more efficient and for increasing trust in its management. Properly implemented, e-voting solutions can increase the security of the ballot, speed up the processing of results and make voting easier. However, the challenges are considerable. If not carefully planned and designed, e-voting can undermine the confidence in the whole electoral process. This policy paper outlines contextual factors that can influence the success of e-voting solutions and highlights the importance of taking these fully into account before choosing to introduce new voting technologies.

As the world we witness the transformation of technology on how to conduct normal election in a traditional way. Digitalization allow the people to convert to the technologies and to improve the cost and time complexity.

E-voting and I-voting is something wonderful to be enable to use computers to cast and count vote securely, to be enable to vote over the internet with all the convinces the technology brings perhaps we could reduce cost and increase participation. At the same time e-voting raise one of the most

difficult challenges in the field of computer security and is a motivating problem for advances of all kind of cryptography, system construction and usability. E-voting and I-voting is a core security problem because of its usual requirements. We need two things in securing e voting and I-voting systems above all and one of them is integrity and by integrity means the outcome of the election match the voters intend, and the election votes are counted as cast, Secondly Ballot Secrecy which means no body can figure out how you voted. The design of the voting framework must adopt the protocol that will protects the integrity, generality, equality, freedom, secrecy and fairness of the election process to become feasible .

The reason why these are more complicated than other problems that we routinely solve are banking online, making purchases in electronic commerce.

We also have this requirement for ballot secrecy, that the secret ballot is one of the most important technological advances in the history of election technology. The secret ballot is the thing that protects you for been coercive to voting a certain way and to protect you from selling your ballot, the secret ballot says no one can figure out how you voted and even if you try to prove it to them how you voted. This is what we want to protect people of been coercive and prevent them from selling their ballot.

The reason e-voting and I-voting has been a difficult problem, it's largely of these two properties integrity and ballot secrecy. Things we do to increase integrity as we do in e-commerce, to send people a receipt or a bank statement or to do accounting where money goes in / out and is total. These things are very much difficult or impossible to implement when we want to maintain a secret ballot and a strong framework at the same time, we want to

preserve integrity so we need very different mechanism's to achieve e-voting and I-voting system that provides these critical properties and these does not stop people and countries from building electronic voting or internet voting systems.

With the R&D projects primarily focused on technological aspects. Several voting election schemes have been proposed in the last twenty years but overall the chosen technical solutions for internet voting seem rather similar. All of the protocols use cryptography and, so far, none of the protocols has managed to satisfy all of the properties which should make e-voting as secure as traditional voting systems

4. ADVATAGE OF DIGITAL VOTING SYSTEM

In the digital voting system multiple benefit as compare to tradition system

- Faster vote count and tabulation.
- More accurate results as human error is excluded.
- Efficient handling of complicated electoral systems formulae that require laborious counting procedures.
- Improved presentation of complicated ballot papers.
- Increased convenience for voters.
- Potentially increased participation and turnout, particularly with the use of Internet voting.
- More attuned to the needs of an increasingly mobile society.
- Prevention of fraud in polling stations and during the transmission and tabulation of results by reducing human intervention.
- Increased accessibility, for example by audio ballot papers for blind voters, with Internet voting as well for housebound voters and voters from abroad. • Possibility of multilingual user interfaces that can serve a multilingual electorate better than paper ballots.
- Reduction of spoilt ballot papers as voting systems can warn voters about any invalid votes (although consideration should be given to ensuring that voters are able to cast a blank vote should they so choose).
- Potential long-term cost savings through savings in poll worker time, and reduced costs for the production and distribution of ballot papers.
- Cost savings by using Internet voting: global reach with very little logistical overhead. No shipment costs, no delays in sending out material and receiving it back.
- Compared to postal voting, Internet voting can reduce the incidence of vote-selling and family voting by allowing multiple voting where only the last vote counts and prevent manipulation with mail-in deadlines through direct control of voting times.

5. DISADVATAGE OF DIGITAL VOTING SYSTEM

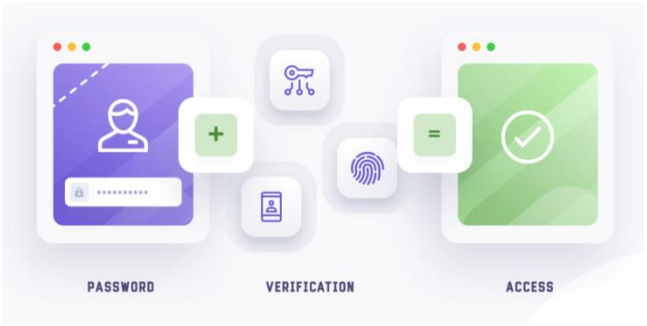
- Lack of transparency.
- Limited openness and understanding of the system for non-experts.
- Lack of agreed standards for e-voting systems.
- System certification required, but no widely agreed standards for certification.
- Potential violation of the secrecy of the vote, especially in systems that perform both voter authentication and vote casting.
- Risk of manipulation by insiders with privileged access to the system or by hackers from outside.
- Possibility of fraud through large-scale manipulation by a small group of insiders.

- Increased costs for both purchasing and maintaining e-voting systems.
- Increased infrastructure and environmental requirements, for example, with regard to power supply, communication technology, temperature, humidity.
- Increased security requirements for protecting the voting system during and between elections including during transport, storage and maintenance.
- Reduced level of control by the election administration because of high vendor- and/or technology dependence.
- Limited recount possibilities.
- Need for additional voter education campaigns.
- Possible conflict with the existing legal framework.
- Possible lack of public trust in e-voting-based elections as a result of the weaknesses above

6. DIGITAL VOTING SYSTEMS WITH OR WITHOUT VOTER AUTHENTICATION

Some e-voting systems are only used for casting the vote and voter authentication remains manual; others contain an additional module for authenticating voters based on an electronic poll book or electoral register. All Internet voting systems, and some voting machines in polling stations, contain an authentication module. A voting system that performs both functions—voter identification and the casting of the ballot—is inherently open to criticism and potentially to malpractice. Even when the two functions are kept rigidly separate, there may be a possibility for inside operators to cross-check the two data sets. This possibility requires the establishment of specific technical and procedural security measures to guarantee that these two sets of information cannot be linked under any circumstances. The secrecy of the vote relies on these measures and it is important that they can be clearly communicated and demonstrated to interested stakeholders.

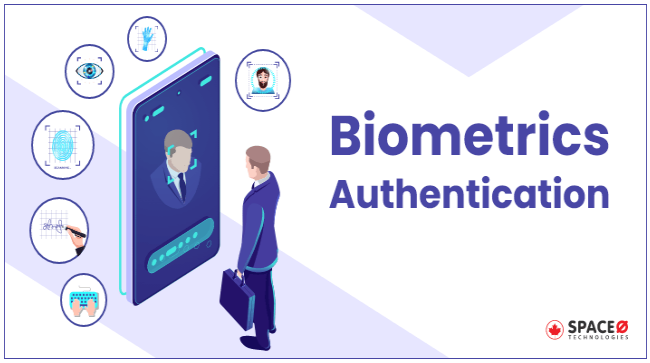
7. DIGITAL VOTING SYSTEM WITH AUTHENTICATION



8. MULTI-FACTOR AUTHENTICATION (MFA)

As the name suggests, Multi-Factor Authentication involves at least two different kinds of authentication factors to elevate security levels. Unlike Two-Factor Authentication that is limited to two factors only, MFA use cases can involve three or more of them. This kind of authentication is now considered to be a key component of any modern Identity and Access Management (IAM) protocol. The typical Multi-Factor Authentication scenario involves the use of a password, after which the user is sent a verification code to the personal Smartphone. The latter can be replaced by biometric techniques like fingerprint scans or voice authentication. Vendors opting for MFA need to look out for false positives and network outages, which can become big problems while scaling up fast

1) BIOMETRIC AUTHENTICATION



Biometric authentication

Biometric authentication is gaining popularity due to the ease of use and customer satisfaction benefits. The user simply doesn't have to remember or reset anything when it comes to this type of authentication. Common biometric devices include fingerprint scanners and facial recognition modules, both of which are commonly available on smart phones and tablets today.

What goes on under the hood with this authentication type?

A sample of the fingerprint or iris/face scan is stored in a dedicated database to compare it with the user's input on-demand. However, smart phones aside, biometric authentication requires an initial investment in endpoint hardware. More importantly, vendors need to make it sensitive enough to minimize false-positives, while keeping it user-friendly and minimizing friction-related churn.

2) TOKEN BASED AUTHENTICATION

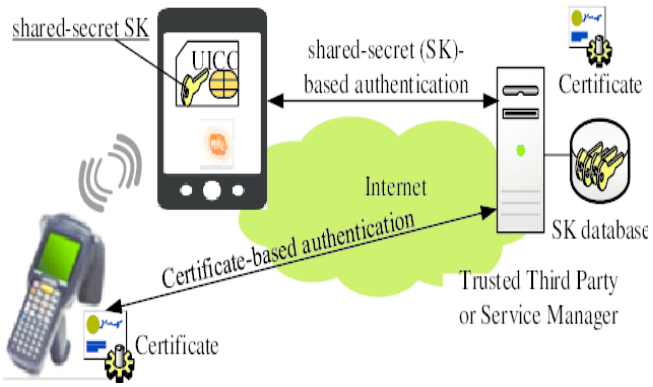
Token-Based Authentication is a commonly used methodology where the user is issued a unique token upon being verified. With this unique token, the user can then access the relevant service. This privilege is active till the token expires. The user doesn't have to use passwords or other credentials during this period. JSON Web Token is a commonly used Token-Based Authentication standard today.

Token Based Authentication

Tokens are being used extensively in multiple scenarios today since they are stateless entities, with all authentication-related information baked into them. There is also the option to separate token generation from token verification, which gives vendors added flexibility. Token-Based Authentication allows full control over the token payloads for fine-grained access control at all times.

3) CERTIFICATE BASED AUTHENTICATION

Certificate-Based Authentication is a protocol that promotes the use of digital certificates to get the job done. These certificates can be used to identify and verify the user or end-device, before granting access permissions. This authentication methodology, which also works seamlessly with Internet of Things (IoT) devices, is commonly used with passwords and usernames.



Certificate Based Authentication

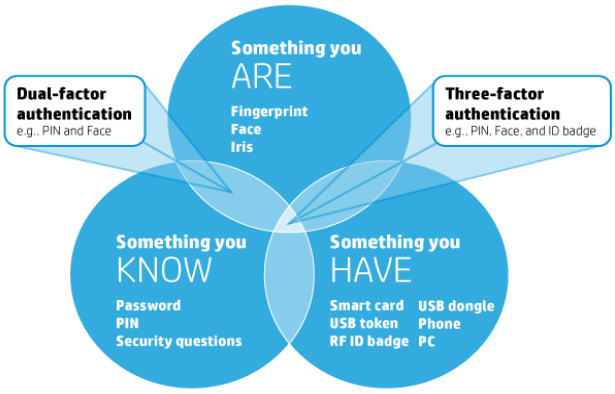
One of the biggest advantages of Certificate-Based Authentication is it's ease of use from the admin's side. No hardware is required, with all digital certificates being stored locally on the relevant device. Issuing, renewing, modifying, and revoking them also becomes very easy. Users also like this kind of authentication, as it requires no further action once the digital certificate has been issued.

4) PASSWORD BASED AUTHENTICATION

We can't wrap up this list without mentioning the proven and tested Password Authentication, which is still being used by thousands of organizations worldwide. But it's pretty clear that this methodology is getting outdated. Just like Biometric Authentication, vendors need to enforce complex password implementation, while also making sure that there is minimal friction for the end-user.

The way Password Authentication works is pretty straightforward, as shown in the diagram above. Firstly, the user inputs his name and password, which are sent via the internet to the Directory Server (DS). If the name binds with the Distinguished Name (DN) and there is a password match, the server decides to authenticate the request and lets the user access the resource for a predefined amount of time.

Password Based Authentication



Multilevel Authentication For Voting System

9. CONCLUSION AND FUTURE WORK

Digital voting has been used in varying forms since 1970s basic benefits traditional systems such as increased efficiency and reduced errors. With the extraordinary growth in the use of multilevel authentication technologies, a number of initiatives have been made to explore the feasibility of using authentication to aid an effective solution of digital voting. This paper has presented the comparative studies of the traditional voting system and digital voting system. Also observe the increase the performance of the authentication for perfection in the voter rights which is impacted the person selected in the respective position.

Digital voting with multilevel authentication leverages benefits such as cryptographic foundations and transparency to achieve an effective solution of digital voting. The proposed approach has been implemented with multilevel and in depth evaluation of approach highlights its effectiveness with respect to achieving fundamental requirements for an digital voting system.

In continuation of this work, we are focused at improving the technology to 'Multilevel authentication /composite authentication problem which will translate as 'authentication for digital voting systems.

We are also improve the multilevel authentication application with help of the technologies and proceed for improving security

REFERENCES

[1] Bohli, J. M., Muller-Quade, J. and Rohrich, S. (2007). Bingo voting: Secure and coercion- free voting using a trusted random number generator, in Proceedings of the 1st International Conference on E-voting and Identity, ser. VOTE-ID'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 111-124.

[2] Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008) Scantegrity: End-to-end voter-veri_able optical- scan voting, IEEE Security Privacy, vol. 6, no. 3, pp. 40-46, May 2008.

[3] Chaum, D. (2004) Secret-ballot receipts: True voter-verifiable elections, IEEE Security Privacy, vol. 2, no. 1, pp. 38{47, Jan 2004.

[4] Chaum, D. (1981) Untraceable electronic mail, return addresses, and digital pseudonym', Commun. ACM, vol. 24, no. 2, pp. 84{90, Feb. 1981.

[5] Chaum, D., Ryan, P. Y. A. and Schneider, P. Y. A. (2005). A practical voter-verifiable election scheme, in Proceedings of the 10th European Conference on Research in Computer Security, ser. ESORICS'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 118- 139.

[6] Dalia, K., Ben, R. , Peter Y. A, and Feng, H. (2012) A fair and robust voting system by broadcast, 5th International Conference on E-voting, 2012. Hao, F., Kreeger, M. N., Randell, B., Clarke, D., Shahandashti, S. F. and Lee, P. H.-J. (2014). Every vote counts: Ensuring integrity in large-scale electronic voting, in 2014 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 14). San Diego, CA: USENIX Association, 2014.

[7] Hao, F., Ryan, P. Y. A., and Zielinski, P. (2010) Anonymous voting by two-round public discussion, IET Information Security, vol. 4, no. 2, pp. 62-67, June 2010.

[8] Gobel, J., Keeler, H. P., Krzesinski, A.E. and Taylor, P.G. (2015). Bitcoin Blockchain Dynamics: the Selfish-Mine Strategy in the Presence of Propagation Delay, May 2015.

[9] Kadam, M., Jha, P. Jaiswal, S. (2015) Double Spending Prevention in Bitcoins Network, International Journal of Computer Engineering and Applications, August 2015.

[10] McCorry, P., Shahandashti, S. F. and Hao. F. (2017) A smart contract for boardroom voting with maximum voter privacy in the proceedings of FC 2017.

[11] Ryan, P. Y. A, (2008) Prêt à Voter with Paillier Encryption, in the Mathematical and Computer Modelling, in Vol. 48, issue 9-10,1646-1662, 2008.

[12] Shahandashti, F. S. and Hao, F. (2016) DRE-ip: A Verifiable E-Voting Scheme without Tallying Authorities, the 21st European Symposium on Research in Computer Security (ESORICS), 2016.

[13] Shahandashti S. F. and Hao, F. (2016). DRE-ip: A Verifiable E-Voting Scheme Without Tallying Authorities. Cham: Springer International Publishing, 2016, pp. 223-240.

[14] Sandler, D., Derr, K. and Wallach, D. S. (2008) Votebox: A tamper-evident, verifiable electronic voting system, in Proceedings of the 17th Conference on Security Symposium, ser. SS'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 349{364.

[15] Malwade Nikita, Patil Chetan, Chavan Suruchi, Prof. Raut S. Y, Secure Online Voting System Proposed By Biometrics And Steganography, Vol. 3, Issue 5, May 2017.

[16] Ankit Anand, Pallavi Divya, An Efficient Online Voting System, Vol.2, Issue.4, July-Aug. 2019, pp- 2631-2634.

[17] Alaguvel.R, Gnanavel.G, Jagadhambal.K, Biometrics Using Electronic Voting System with Embedded Security, Vol. 2, Issue. 3, March 2018.

[18] Firas I. Hazzaa, Seifedine Kadry, Oussama Kassem Zein, Web-Based Voting System Using Fingerprint: Design and Implementation, Vol. 2, Issue.4, Dec 2019.

[19] Alexander. Stakeholders: Who is your system for? IEEE: Computing and Control Engineering, 14(1):22{26, April 2003}.

[20] K. P. Kaliyamurthie, R. Udayakumar, D. Parameswari and S. N. Mugunthan, "Highly Secured Online Voting System over Network," in Indian Journal of Science and Technology | Print ISSN: 0974-6846 | Online ISSN: 0974-5645.

[21] Almyta Systems, Point of Sale Systems. http://systems.almyta.com/Point_of_Sale_,Software.a sp. Accessed on 20th October 2008.

[22] Swaminathan B, and Dinesh J C D, "Highly secure online voting system with multi security using biometric and steganography," in International Journal of Advanced Scientific Research and Technology, vol 2(2), 195– 203.

[23] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti Margaret MacAlpine J. Alex Halderman, November 3–7, 2014, "Security Analysis of the Estonian Internet Voting System," in CCS"14, Scottsdale, Arizona, USA. ACM 978-1-4503-2957-6/14/11.

[24] M A Imran, M S U Miah, H Rahman, May 2015, "Face Recognition using Eigenfaces," in International Journal of Computer Applications (0975 – 8887) Volume 118 – No. 5.

[25] Anand A, and Divya P, "An efficient online voting system," in International Journal of Modern Engineering Research, vol 2(4), 2631–2634.

[26] Electronic copy