Biometric Secure Electronic Voting System

Ms. Yashaswini H K
Assistant Professor, Department of EEE, Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id- yashaswinisachin@gmail.com

Abstract

System of Voting is the base of Indian democracy in which voters cast their vote to choose their leaders to show their presence for the way that they will be supervised. There is worldwide improvement in computer, communication technologies and the internal infrastructures for online voting. On-line casting votes are a software system with the help which a voter can cast their votes through registering himself on the website available for voting. The main functional properties of an electronic voting system, the e-Voting system must feed for various essential non-functional requirements. Most important are the requirements for security, correctness, consistency, robustness and coherence. The proposed system provides security and voter verifies the accuracy of their cast vote by retaining the hardcopy of cast vote. The proposed system solves the problem of security and transparency.

Keywords: *Biometric, Electronic voting machine, voting system, voting analysis, Security.*

I. INTRODUCTION

In a manual, paper-based election, the electors cast their votes to select their candidates, where they simply deposit their designated ballots in sealed boxes distributed across the electoral circuits around a given country. By the end of the election period, all these boxes are officially opened and votes counted manually in the presence of certified representatives of all the candidates until the numbers are compiled. This process warrants transparency at vote casting time as well as at counting time[1]. However, counting errors frequently occur, and in some situations, voters find ways to vote more than once, introducing anomalies in the results of the final count, which may, in rare cases, entail a full replay of the election process! Moreover, in certain nations, intentionally implemented electoral vote manipulations have taken place in order to skew the outcome of the elections in favor of those candidates. Here, with a well scrutinized electoral procedure, all such mishaps can be prevented, but mistakes can still occur when the electoral votes are too big. Very frequently, in many countries, foreign monitoring bodies are required to track elections[2].

Naturally, this calls for a completely integrated, computerized online election process. In addition to solving widely found electoral pitfalls, electoral voting counts are conducted in real time such that the results are automatically out by the end of the Election Day. With different features depending on the demand and requirements of various countries around the world, the election process can be easily improved. Online voting or e-Voting is no longer a North American or Western phenomenon due to worldwide developments in computer and telecommunication technology and the underlying infrastructures. This high tech form of casting a ballot has spread well beyond the United States, spreading all over the globe. E-Voting can now be found from the developed countries of Europe to the developing countries of Asia and South America, along with its advantages and mishaps. The introduction of electronic voting has been the biggest change to the Irish electoral system since the establishment of the state over 80 years ago. E-Voting may soon become a global reality or a global nightmare[3].

In addition to reliable e-Voting technologies, there is a dire need for international standards to regulate the technology, the reliability and accuracy of the software, the processes and algorithms implemented within the technology, and the verification of all involved hardware, software and protocols. Ultimately, such standards would enable elections to continue in every part of the world without the need for monitoring bodies. Certain factors play out big in a given voting process in any particular country. The rules and regulations which regulate any voting process are largely determined by culture itself and the underlying social factors/values. There are patterns that electoral votes may be misappropriated in several ways in countries where election results are decided by the voting counts that are counted by directly depositing specially crafted voting cards into the voting boxes; some voters appear to try to vote more than the number of times allowable for a given candidate by law; other voters may try to vote[4]. Another concern that may paradise the legitimacy of an election process is counterfeit/malice. Automating an election process will greatly reduce many of the variables that would hamper the healthy development of an election process, thus relying on state-of-the-art computer technology and ICT technologies. Nevertheless, relying solely on available information technology would only guarantee the authentication/validation of the identity of a given voter, but it will also not have the power to block any attempted manipulation of the voting system, i.e. certain voters who simply try to vote on behalf of others[5].

Current applications, including banking applications, protecting high-security facilities, tracking passengers through border posts, among many others, are witnessing rising levels of biometric technologies and devices being used. Biometrics is better characterized as observable physiological and / or biological features that can be used to verify an individual's identity. They include fingerprints, scanning of the retinal and iris, geometry of the hand, speech patterns, facial recognition, recognition of gait, DNA and other techniques. In any field where it is necessary to verify an individual's true identity, they are of interest. Initially, these techniques were employed primarily in specialist high security applications; however, we are now seeing their uses and proposed uses in a much broader range of public facing situations. Essentially, two characteristic characteristics are accompanied by a biometric system: recognition and authentication[6]. The former involves identifying an individual in a database from all biometric measurements gathered. "The question this process is trying to answer is: "Who is this? A one-compared-to-many match, therefore, involves it. Verification requires authenticating the stated identity of an individual from its previously recorded pattern. Is that that he pretends to be? "is the question this method is trying to address. This includes a one-to-one match. Five stages that the device needs to go through are involved in verifying a person's identity against a given biometric measure. Input information is read from the person at the beginning via the reading sensors. The data collected is then sent to some central database hosting a biometric system via a network. The framework, using structured and/or custom matching techniques, will then perform identity matching[7].

The use of biometric technologies can be as easy as using a single biometric technology. However, if not adequately taken care of and administered, a single biometric measure is often subject to security breaches. Naturally, this requires authentication codes, fingerprints, and signatures, all of which can be spoofed when added to an area that is not properly attended. With the proper implementation of combined simple biometric controls, this is greatly alleviated and system security improved[8]. The use of combined weak biometrics results in systems that, in terms of the safety standards achieved, are less complicated and more stable. There are strong single biometric measures involving retinal and iris scans that are very difficult, if not impossible, to breach, but typically lead to more complex systems which, because of the amount of data processing involved, in turn slow down the underlying biometric matching mechanism. For these factors, among others, the type of biometrics mentioned in this work is of the former type that includes the weak forms of combined biometrics. In the following pages, this will be expanded upon.

Besides the main functional properties of a voting system, as described in the previous section, the e-Voting system must cater for several essential non-functional requirements. Of utmost importance are the requirements for correctness, robustness, coherence, consistency, and security. On the server side, a global database is maintained for all registered voters and candidates. Also, the server runs in real-time and provides backend statistics for the entire

Election process. Two more specifications are required on the client side. A local database on the client side is necessary to host the data pertaining to the local voting center in order to lower the traffic rate on the network links. In the sense that the data stored in its tables which differ over the election period, this DB is a very dynamic one. Just a tiny fraction of the global Database on the server side is the size of the local DB at any voting center. The use of a local DB increases the voting process's efficiency. This method, however, introduces a problem of synchronization, which will be discussed in this section later[9].

The transparency of the voting process is the second criterion. In essence, an elector casts his or her vote on a monitor at an electronic voting station. The elector does not have an understanding of how to interpret and/or count his or her vote. In a paper-based election, the elector fills out the ballot and the voter himself drops it into a sealed box. In the presence of the candidates or their members, votes are counted. The elector is confident that his/her cast ballot is in the correct box with his/her choice of vote. One of the problems that an e-Voting system faces is to ensure that no voter is able to mimic another voter and that no voter is able to vote more than once. People use an identifier followed by an authentication method in the suggested framework. The identification is achieved via a card reader that reads a voter's official ID card and pulls the voting record from the local DB or loads the record from the central DB if it is not located in the local DB. A biometric profile of the elector is included in the voter record. We are using a fingerprint authentication method in this report[10].

II. CONCLUSION & DISCUSSION

Based on the design of proposed system & requirements, a prototype of the system is designed for E-voting System has been developed using various electronics equipment. The proposed system has several advantages that have been gained. The advantages of the proposed system are as follows:

1. It gives confidence in the voting system, only the authorized voter is allowed to gain access to voting.

2. The system is user friendly, in the sense that the user can easily understand the system although the user is a first time user. This is because the design is simple, attractive and don't have too many graphical items.

3. Most important are the requirements for security, correctness, consistency, robustness and coherence.

III. REFERENCES

[1] M. M. Sanjai, R. Umamaheswari, and M. S. Muthuraj, “Advanced Technology in Secured Online Voting System,” Int. Res. J. Eng. Technol., no. April, 2018, doi: 10.13140/RG.2.2.36179.48161.

[2] F. A. Haziemeh, M. K. Khazaaleh, and K. M. Al-Talafha, “New applied E-voting system,” J. Theor. Appl. Inf. Technol., vol. 25, no. 2, pp. 88–97, 2011.

[3] ส. ไทรทับทิม, “No Titleการนำสาหร่ายที่ผลิตน้ำมันไบโอดีเซลมาบำบัดน้ำเสียของโรงงานอุตสาหกรรมรีไซเคิล,” 2554, [Online]. Available: http://library1.nida.ac.th/termpaper6/sd/2554/19755.pdf.

[4] P. S. Herrnson, R. G. Niemi, M. J. Hanmer, B. B. Bederson, F. G. Conrad, and M. W. Traugott, “The Study of Electronic Voting,” Voting Technol. Not-So-Simple Act Cast. a Ballot., pp. 1–17, 2007.

[5] M. Amritkar, R. Dudhe, K. Sawant, S. Phutane, and P. Dadhich, “Secure Online Voting System.,” Int. J. Adv. Res., vol. 4, no. 11, pp. 1648–1653, 2016, doi: 10.21474/ijar01/2257.

[6] M. Prandini, L. Sartori, and A. Oostveen, “Why electronic voting ?,” no. October, 2014, doi: 10.13140/2.1.4173.0561.

[7] M. Khasawneh, M. Malkawi, O. Al-Jarrah, L. Barakat, T. S. Hayajneh, and M. S. Ebaid, “A biometric-secure e-voting system for election processes,” Proceeding 5th Int. Symp. Mechatronics its Appl. ISMA 2008, no. June, 2008, doi: 10.1109/ISMA.2008.4648818.

[8] D. B. Venkata Raghav and S. K. Bandi, “Digitalized Electronic Voting System,” Int. J. Reconfigurable Embed. Syst., vol. 5, no. 3, p. 148, 2016, doi: 10.11591/ijres.v5.i3.pp148-152.

[9] M. Faisal, M. D. Hossain, and M. R. B. Bhuiyen, “Design and Implementation of Electronic Voting System (EVS),” IOSR J. Electr. Electron. Eng., vol. 9, no. 5, pp. 56–63, 2014, doi: 10.9790/1676-09515663.

[10] P. A. M.N., S. S. Gandhi, N. R. Kaniampal, and P. S. Naral, “Online Voting System Using Biometric Verification,” Ijarcce, vol. 6, no. 4, pp. 276–281, 2017, doi: 10.17148/ijarcce.2017.6452.