JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Review on Block Chain based Security Technique for Electronics Voting

[1]Surabhi Shrivastava, [2]Prof. Shital Gupta
[1]Research Scholar, [2]Assistant Professor
[1&2]Department of Computer Science Engineering,
[1&2]School of Research & Technology, People's University, Bhopal, India

Abstract : Election is a way to choose the representatives through a fairness, integrity, and democratic rules. During the election, the voting system allows authorized voters to cast their vote for candidates. In essence, the voting system can directly influence several aspects that are political science, social science, and economics. Thus, the concept of the voting system must respond and rigorously considered before the election is held. The voting system begins evolving from paper voting, then E-voting and the latest will be I-voting. Concisely, E-voting is simply an electronic system, while I-voting is nothing but remote E-voting (internet accessible). Block chain technology provides a decentralized architecture that distributes digital information synchronously among the P2P network without a central database. This paper provides review on block chain based security technique for electronics voting.

IndexTerms **- Block Chain, E-Voting, I-Voting P2P, Election, Security.**

I. INTRODUCTION

The Electronic voting (also known as e-voting) is voting that uses electronic means to either aid or take care of casting and counting votes. Depending on the particular implementation, e-voting may use standalone electronic voting machines (also called EVM) or computers connected to the Internet. It may encompass a range of Internet services, from basic transmission of tabulated results to full-function online voting through common connectable household devices. The degree of automation may be limited to marking a paper ballot, or may be a comprehensive system of vote input, vote recording, data encryption and transmission to servers, and consolidation and tabulation of election results.

A worthy e-voting system must perform most of these tasks while complying with a set of standards established by regulatory bodies, and must also be capable to deal successfully with strong requirements associated with security, accuracy, integrity, swiftness, privacy, audit ability, accessibility, cost-effectiveness, scalability and ecological sustainability.

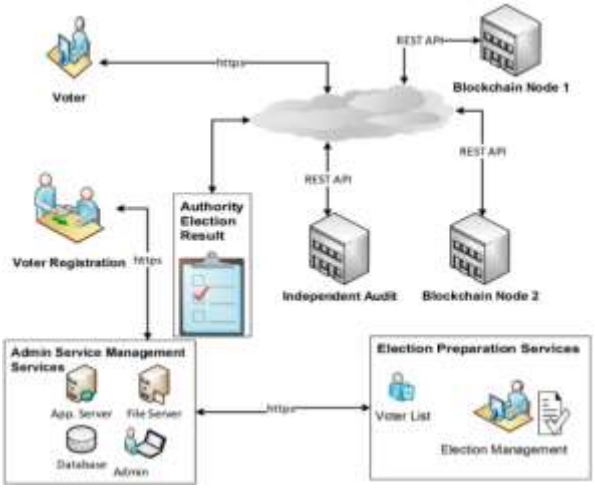

Figure 1: Voting System

Electronic voting technology can include punched cards, optical scan voting systems and specialized voting kiosks (including self-contained direct-recording electronic voting systems, or DRE). It can also involve transmission of ballots and votes via telephones, private computer networks, or the Internet.

In general, two main types of e-voting can be identified:

E-voting which is physically supervised by representatives of governmental or independent electoral authorities (e.g. electronic voting machines located at polling stations);

Remote e-voting via the Internet (also called i-voting) where the voter submits his or her vote electronically to the election authorities, from any location.

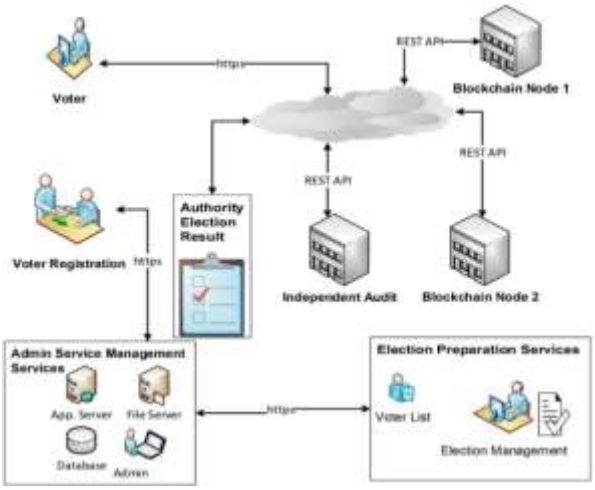

Figure 2: Voting System

Electronic voting technology intends to speed the counting of ballots, reduce the cost of paying staff to count votes manually and can provide improved accessibility for disabled voters. Also in the long term, expenses are expected to decrease. Voters save time and cost by being able to vote independently from their location. This may increase overall voter turnout. The citizen groups benefiting most from electronic elections are the ones living abroad, citizens living in rural areas far away from polling stations and the disabled with mobility impairments.

A smart city refers to an intelligent environment obtained by deploying all available resources and recent technologies in a coordinated and smart manner. Intelligent sensors (Internet of Things (IoT) devices) along with 5G technology working mutually are steadily becoming more pervasive and accomplish users' desires more effectively. Among a variety of IoT use cases, e-voting is a considerable application of IoT that relegates it to the next phase in the growth of technologies related to smart cities. In conventional applications, all the devices are often assumed to be cooperative and trusted. However, in practice, devices may be disrupted by the intruders to behave maliciously with the aim of degradation of the network services. Therefore, the privacy and security flaws in the e-voting systems in particular lead to a huge problem where intruders may perform a number of frauds for rigging the polls.

II. LITERATURE SURVEY

G. Rathee et al.,[1] introduced a secure and transparent e-voting mechanism through IoT devices using Blockchain technology with the aim of detecting and resolving the various threats caused by an intruder at various levels. Further, in order to validate the proposed mechanism, it is analyzed against various security parameters such as message alteration, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attack and authentication delay.

M. Doost et al.,[2] shows e-voting scheme with the help of some cryptographic concepts like bit-commitment and blind signatures. The vital property of their scheme was that it did not use any kind of anonymous channel which is a common and of course hard to implement tool in many e-voting protocols. In this work, we address some security issues in the mentioned scheme and propose an improved version that has the edge on the prior one in terms of preserving privacy of voters and efficiency when it comes to large scale elections.

M. A. Cheema et al.,[3] shows the concepts of personal and public blockchain. The personal blockchain is used for the purposes of voter registration and voting. The public blockchain is used to maintain the integrity of the personal data of the voters by storing the root hash derived from the Merkle hash tree and revealing the results of the voting stations as soon as the voting process is completed. The proposed blockchain-based e-voting system offers transparency, treasury, and confidence and prevents intrusion into the information exchange network.

S. Kashyap et al.,[4] shows a liquid democracy voting protocol is proposed and implemented on a block chain based distributed ledger which is capable of fighting attacks of integrity and non-repudiation while ensuring authenticity of the votes. This system would be transparent thus ensuring people about the legitimacy of their delegation of votes and direct votes. This is a big step up from the current existing system of EVM's that do not guarantee this level of security.

D. Pramulia et al.,[5] proposed a blockchain based e-voting system with Ethereum and metamask. We show that the proposed e-voting system fulfills six basic principles of an election system, namely secret ballot, one-man one-vote, voter eligibility, transparency, votes accurately, recorded and counted, and reliability. Furthermore, the performance evaluation of the e-voting system shows that the slow gas price option gives the lowest gas price per second result, i.e. the best trade-off.

S. T. Alvi et al.,[6] shows many ways of manipulating or modifying digital technology and hindering voting. There should be fairness, independence and impartiality in the voting method. By analyzing the aforementioned problems, this research work combines the digitalisation with the blockchain technology to provide a voting mechanism. The main goals of our voting mechanism are to provide integrity, anonymity, privacy, and security of voters. With the use of markle tree and fingerprint hash, the data integrity and anonymity, privacy, security of the voters has been achieved in our proposed digital voting systems.

Y. Abuidris et al.,[7] provides highlight some of the risks and opportunities of the e-voting systems based blockchain. As well, we believe that this study can bring a valuable contribution as it illustrates some of the risks and opportunities of e-voting systems

based-blockchain. That to offer users and developers a broad view of the potential risks and opportunities associated with the adoption of blockchain in the e-voting system.

A. Pandey et al.,[8] proposed e-voting systems make use of a central database to store data, resulting in the servers used to store these databases being a single point of failure. These systems have also been found to be vulnerable to DoS attacks, leading to concerns over their reliability. Blockchains have been used to build secure and scalable distributed systems which have shown several benefits over centralized systems. They have seen uses in sectors ranging from finance and healthcare to food and energy. In this work, we present VoteChain, a blockchain based voting system to help bring transparency and security to polls. We report on our implementation of VoteChain, as well as the results obtained in testing the system in a real-world poll which prove that such a system can be used in practice for large-scale elections.

E. Bellini et al.,[9] This article aims at introducing a new configurable and multipurpose electronic voting service based on the blockchain infrastructure. The objective is to design architecture to automatically translate service configuration defined by the end user into a cloud-based deployable bundle, automating business logic definition, blockchain configuration, and cloud service provider selection. The article presents the preliminary results of the system and a SOA-based services definition implemented with smart contracts.

A. Alam et al.,[10] proposed an Electric voting (E-voting) model that ensures security, privacy and transparency. Our approach uses blockchain method, a distributed ledger technology where data are shared and distributed into a network. Blockchain system offers transparency, decentralization, irreversibility and reduces the involvement of intermediaries which is crucial for an election process. An optimized algorithm is proposed for blockchain based e-voting system. An internet of things (IOT) based system is designed to exchange data from e-voting devices to the nodes. Moreover, we proposed several possible techniques and improvements for voting scenarios.

F. Sheer Hardwick et al.,[11] propose a potential new e-voting protocol that utilises the blockchain as a transparent ballot box. The protocol has been designed to adhere to fundamental e-voting properties as well as offer a degree of decentralisation and allow for the voter to change/update their vote (within the permissible voting period). This work highlights the pros and cons of using blockchain for such a proposal from a practical point view in both development/deployment and usage contexts. Concluding the work is a potential roadmap for blockchain technology to be able to support complex applications.

A. Singh et al.,[12] presents the blockchain technology in digital e-voting system to solve the security issues and fulfill the system requirements. It offers new opportunities to deploy a secure e-voting system in any organization or country. The solution is far better as compared to other solution because, it is a decentralized system; contain the results in the form of bit-coins, having different locations. We will also analyze the security of our proposed voting system, which shows our protocol is more secure as compared to other solutions.

III. CHALLENGES

An electronic voting system is a voting system in which the election data is recorded, stored and processed primarily as digital information. E-voting is referred as “electronic voting” and defined as any voting process where an electronic means is used for votes casting and results counting. E-voting is an election system that allows a voter to record their ballots in a electrically secured method. A number of electronic voting systems are used in large applications like optical scanners which read manually marked ballots to entirely electronic touch screen voting systems. Specialized voting systems like DRE (direct recording electronic) voting systems, RFID, national IDs, the Internet, computer networks, and cellular systems are also used in voting processes.

A. Securities of the E-voting systems

The main goal of a secure e-voting is to ensure the privacy of the voters and accuracy of the votes. A secure e-voting system are satisfies the following requirements, Eligibility: only votes of legitimate voters shall be taken into account; Unreusability: each voter is allowed to cast one vote; Anonymity: votes are set secret; Accuracy: cast ballot cannot be altered. Therefore, it must not be possible to delete ballots nor to add ballots, once the election has been closed; Fairness: partial tabulation is impossible; Vote and go: once a voter has casted their vote, no further action prior to the end of the election; Public verifiability: anyone should be able to readily check the validity of the whole voting process.

B. Issues of Present Voting System

There have been several studies on using computer technologies to improve elections these studies caution against the risks of moving too quickly to adopt electronic voting system, because of the software engineering challenges, insider threats, network vulnerabilities, and the challenges of auditing. Accuracy: It is not possible for a vote to be altered eliminated the invalid vote cannot be counted from the finally tally. Democracy: It permits only eligible voters to vote and, it ensures that eligible voters vote only once. Privacy: Neither authority nor anyone else can link any ballot to the voter verifiability: Independently verification of that all votes have been counted correctly. Resistance: No electoral entity (any server participating in the election) or group of entities, running the election can work in a conspiracy to introduce votes or to prevent voters from voting. Availability: The system works properly as long as the poll stands and any voter can have access to it from the beginning to the end of the poll. Resume Ability: The system allows any voter to interrupt the voting process to resume it or restart it while the poll stands

The existing elections were done in traditional way, using ballot, ink and tallying the votes later. But the proposed system prevents the election from being accurate. Problems encountered during the usual elections are as follows:

- It requires human participation, in tallying the votes that makes the elections time consuming and prone to human error.
- The voter finds the event boring resulting to a small number of voters.
- Deceitful election mechanism.
- Constant spending funds for the elections staff are provided

The essential requirements for elections to be conducted freely and fairly are:

Timeliness- The need to record information and to have the results available quickly.

Accessibility- The need to have a system that is accessible to all and easy to use.

Secrecy- The need to ensure secrecy of what takes place.

Deliberation- The need for voting to be undertaken seriously, after due deliberation.

Accuracy- The ability to ensure that each individual's vote is recorded and counted accurately.

Security- The need to guard against manipulation and interference with information once recorded.

Authentication- The need to ensure that individuals cannot be impersonated.

Verifiability- The need to verify what has taken place through the use of traceable information Trails.

IV. ONLINE E-VOTING PROCESS

When the voter enters the voting place, he must have same kind of valid identity, which has been stored in database verification, authorized person choose to online e-voting system. Two conditions are verified to allow polling section.

Condition1: When a poll worker confirms that the voter is registered, login the website, type voter ID no and password correct means go to next state, answer to polling question ,this answer correct means go to next state finger print matched to database , matched means this person valid to next condition otherwise automatically closed web site.

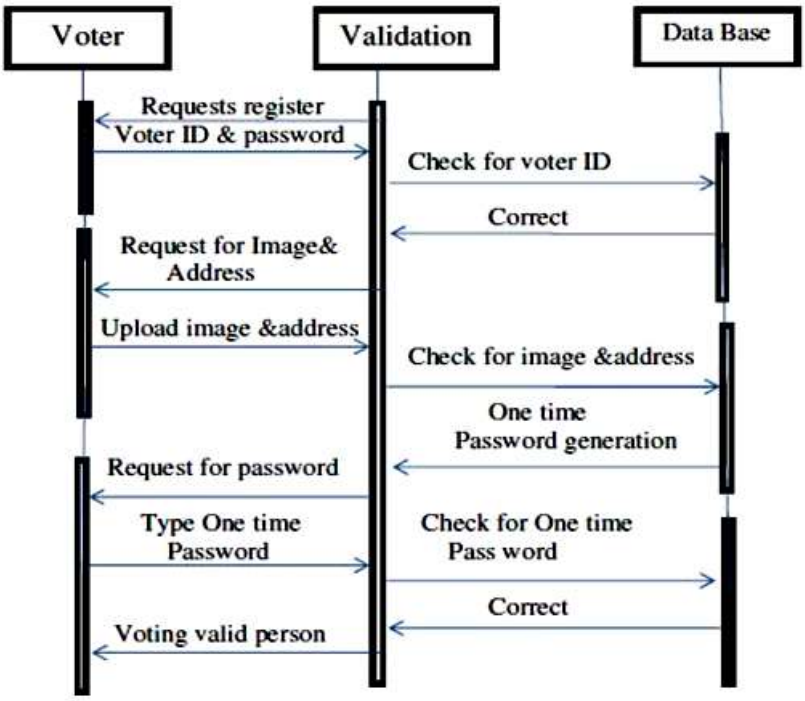

Figure 3: Authentication Sequence Diagram

Condition2: Randomly generated to one time password will be automatically sending through SMS to the authorized person's mobile device using GSM. Then authorized person type to password, if password correct means open the polling window then entered**.**

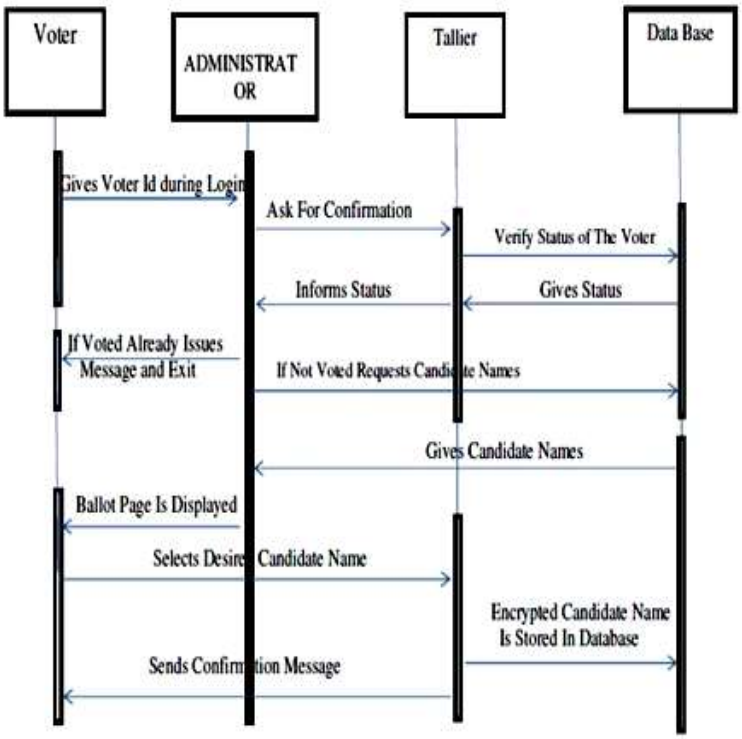

Figure 4: Polling Sequence Diagram

V. CONCLUSION

Electronic voting systems have many advantages over the traditional way of voting. Some of these advantages are lesser cost, faster tabulation of results, improved accessibility, greater accuracy, and lower risk of human and mechanical errors. It is very difficult to design ideal e-voting system which can allow security and privacy on the high level with no compromise. Future enhancements focused to design a system which can be easy to use and will provide security and privacy of votes on acceptable level by concentrating the authentication and processing section. In case of online e-voting some authentication parameters like facial reorganization, In case of offline e-voting some authentication parameters like, Finger Vein and iris matching detection can be done.

REFERENCES

[1]. G. Rathee, R. Iqbal, O. Waqar and A. K. Bashir, "On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities," in IEEE Access, vol. 9, pp. 34165-34176, 2021, doi: 10.1109/ACCESS.2021.3061411.

[2]. M. Doost, A. Kavousi, J. Mohajeri and M. Salmasizadeh, "Analysis and Improvement of an E-voting System Based on Blockchain," 2020 28th Iranian Conference on Electrical Engineering (ICEE), 2020, pp. 1-4, doi: 10.1109/ICEE50131.2020.9260875.

[3]. M. A. Cheema, N. Ashraf, A. Aftab, H. K. Qureshi, M. Kazim and A. T. Azar, "Machine Learning with Blockchain for Secure E-voting System," 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), 2020, pp. 177-182, doi: 10.1109/SMART-TECH49988.2020.00050.

[4]. S. Kashyap and A. Jeyasekar, "A Competent and Accurate BlockChain based E-Voting System on Liquid Democracy," 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2020, pp. 202-203, doi: 10.1109/BRAINS49436.2020.9223308.

[5]. D. Pramulia and B. Anggorojati, "Implementation and evaluation of blockchain based e-voting system with Ethereum and Metamask," 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), 2020, pp. 18-23, doi: 10.1109/ICIMCIS51567.2020.9354310.

[6]. S. T. Alvi, M. N. Uddin and L. Islam, "Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), 2020, pp. 228-233, doi: 10.1109/ICSSIT48917.2020.9214250.

[7]. Y. Abuidris, A. Hassan, A. Hadabi and I. Elfadul, "Risks and Opportunities of Blockchain Based on E-Voting Systems," 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, 2019, pp. 365-368, doi: 10.1109/ICCWAMTIP47768.2019.9067529.

[8]. A. Pandey, M. Bhasi and K. Chandrasekaran, "VoteChain: A Blockchain Based E-Voting System," 2019 Global Conference for Advancement in Technology (GCAT), 2019, pp. 1-4, doi: 10.1109/GCAT47503.2019.8978295.

[9]. E. Bellini, P. Ceravolo and E. Damiani, "Blockchain-Based E-Vote-as-a-Service," 2019 IEEE 12th International Conference on Cloud Computing (CLOUD), 2019, pp. 484-486, doi: 10.1109/CLOUD.2019.00085.

[10]. A. Alam, S. M. Zia Ur Rashid, M. Abdus Salam and A. Islam, "Towards Blockchain-Based E-voting System," 2018 International Conference on Innovations in Science, Engineering and Technology (ICISET), 2018, pp. 351-354, doi: 10.1109/ICISET.2018.8745613.

[11]. F. Sheer Hardwick, A. Gioulis, R. Naeem Akram and K. Markantonakis, "E-Voting With Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing

and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1561-1567, doi: 10.1109/Cybermatics_2018.2018.00262.

[12]. A. Singh and K. Chatterjee, "SecEVS : Secure Electronic Voting System Using Blockchain Technology," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), 2018, pp. 863-867, doi: 10.1109/GUCON.2018.8675008.