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

Blockchain Solutions for Mitigating Security Risks in Digital Elections

Hemant Swami[1], Dr. Swapnil Singha[2]
[1]M.Tech Scholar, [2]Associate Professor
Department of Computer Science and Engineering
Jaipur Institute of Technology- Group of Institutions, Jaipur (Raj)

Abstract: India is a vast democracy country. Voting is available for any Indian citizen that is above 18 years old. As of now, the general percentage of voting among these citizens is always below 100%. The majority of people don't believe the voting system is transparent, and some people can't find time to vote because they don't want to have to wait in a queue. But with technology we have now, like smartphones, there could be an option for online voting which could solve these issues. To safeguard the identity of voters and make voting safer, blocks in a blockchain would be encrypted with "multiple servers verified by the impulse." This model will record the voter's identity from their Aadhar Card ID along with fingerprints and a picture. This information is put on a blockchain that also connects all of the individuals verified data to multiple secure servers. If a hacker tries to change one person's information, it won't match with the rest of the systems. With the proposed model, multiple votes can be made to look like just one vote. This saves time for waiting in voting lines and reduces the potential for fraud.

Index Terms **– Blockchain, Online Voting , Aadhar Card ID.**

I. INTRODUCTION

Every citizen of legal voting age has the right to vote, irrespective of their caste, religion, gender, educational qualification, or financial status. To ensure that not even one person is denied this right for any reason whatsoever, an official list of all eligible voters (who are able to vote) is prepared and called the "Election Roll." The voters list is available before the election to allow people to verify if they're registered and make corrections. On voting day, the voter casts their ballot according to their name in the voter list. This ensures that all registered individuals have voting rights and there's no electoral discrimination. [1]

The government's responsibility is to maintain a current voter list with up-to-date information and deleting those who are deceased. The voter list is updated every five years. On election day, voters mark their vote for a chosen candidate by providing an identity card and showing up to the polls. They vote one at a time, with someone inside the booth marking their finger after they have disclosed who they would like to vote for. Polling officials keep a list of those who have voted while they await a final count. Voting requires money, time, and labor; therefore, it should be primarily online. The opportunity to increase election coverage will be a result of such changes.[1]

Though there are security measures with online voting, blockchain can provide a solution to digital voting's inherent insecurity. Security experts advise against common passwords, but most people have difficult remembering many different passwords. The problem becomes worse when the common password is a personal or pet name. Even though you may be lucky, and the password works for other accounts, it is incredibly easy for hackers to find your common password with dictionaries and work around it. [1]

Data security is an important issue in today's business world. The top cyber security challenge medium and large businesses are now facing is data loss. A report shows that this concern is increasing every day. Data loss is expensive in various ways, and often costs around $200 per record lost. A number of recent breaches have highlighted this issue, such as Equifax's hacking that compromised the information of half the US population. When your data is stolen, it can lead to various problems for a corporation or even a personal user. If your bank account points of interest are taken, it can be equally as detrimental as the person who pried that data from the company's database.

Data security has been an important subject for a while now. It's possible to make all your data compliant with the latest laws thanks to a myriad of apps and technologies. There are various choices for securing your data. For example, online presences such as web identity (ID). It is a social identity that is built up in online groups and sites. It's considered an introduction of oneself. A lot of people on the Internet use fake names to protect their anonymity, or for some other unknown purpose. An online identity controlled by a user's relationship to a specific social society. Some people may even use false identities or misleading facts about themselves on the Internet. [2]

Blockchain helps in the providing the security enhancement in case of the data security , whether journal or in case of voting. Blockchain is a decentralized and distributed ledger that records the online assets. Blockchain is designed in a way so the data can never be modified. It has the potential to disrupt industries like payments, cybersecurity, and healthcare because of its inherent properties. Blockchain technology is a structure that stores transactional records, which is known as the block, in several databases and chains. Typically, this storage is referred to as a 'digital ledger.' The ledger is authorized by the digital signature of the owner and has unique data, making it resistant to tampering. [3]

Blockchain is an immutable ledger, or a Google spreadsheet shared among networked computers. When you record transactional records for purchases in a blockchain, the idea is that these records can't be corrupted or changed. Blockchain is a decentralized financial system that records transactional records and then stores them based on the actual purchases. The fascinating aspect of blockchain, is that it cannot be edited by anyone. Blockchain creates an immutable ledger that records transactions, making it impossible to alter, delete or destroy any record. [3]

II. Literature Survey

Shahzad, B., & Crowcroft, J. (2019) [4] This paper discusses ways in which the electronic voting process can be improved through implementing a block sealing concept. The last two decades have shown that the use of paper-based voting has not been successful. Since there are security and privacy flaws, this paper suggests a framework that would reduce redundancies of data and make for an efficient process by using effective hashing techniques. The concept of block creation ensures security in voting because it makes blockchain adjustable to the need for polling. Patidar, K., & Jain, S. (2019) [5] Majority opinion is that e-voting isn't secure and easy to hack. The blockchain eliminates some of the limitations found in existing voting systems, and resolves challenges such as double spending by using a smart contract-based system. This paper discusses blockchain technology and its application to e-voting. Blockchain has many benefits, such as eliminating voter coercion and increasing transparency. This paper focuses on elections like ones within corporations, board rooms, etc. A smart contract is used with a private blockchain and Ethereum. Truffle framework is also discussed as well as Ganache (Ethereum client) and Meta-mask (Browser Wallet). Zhang, W., Yuan, Y., Hu, Y., Huang, S., Cao, S., Chopra, A., & Huang, S. (2018) [5] As blockchain technologies mature and ecosystems over blockchain evolve, peers on blockchain networks often face situations in which they need to conduct voting for decision-making.

Currently, there is no built-in voting system on any existing blockchain network, so decisions are delegated to a few people who make such decisions offline or are dependent on third party online voting services. By using this system, peers could vote more securely and in a decentralized way without the need for a trusted party or centralized system. M. H. Zaki et. al (2017) [6] Secured with the help of mathematicians, the key-based secret phrase validation strategy proposed here is more secure and efficient than before. This paper is proposing a key-based validation method that allows for the user to use a mix of example numbers and select keys to create a password for their account. This prevents shoulder surfing, animal power assaults, and so on by increasing the complexity of guessing the key from just design to it from design and then from key. Moreover, this plan doesn't overburden the human memory because you're not going through three different levels of guessing with one guess like some other methods.

III. Proposed Work

Algorithm 1 User Identity Validation

1: **Input:** Digital Identity (Aadhar Card/Driving License), Fingerprint, Picture Rotation Pattern
2: **Output:** User's unique digital identity blockchain
3: GenerateUserIdentityBlockchain
4: $idHash \leftarrow$ BLAKE2b-512Hash($DigitalIdentity$)
5: $fingerprintHash \leftarrow$ BLAKE2b-512Hash($Fingerprint$)
6: $rotationPattern \leftarrow$ GenerateRotationPattern($Picture$)
7: $userBlockchain \leftarrow$ Combine($idHash, fingerprintHash, rotationPattern$)
8: Store $userBlockchain$ in multiple servers
9: **return** $userBlockchain$

Algorithm 2 Vote Casting Process

1: **Input:** User's unique digital identity blockchain, Election ID
2: **Output:** Unique instance of the vote cast by the user
3: CastVoteuserBlockchain, electionID
4: $voteBlockchain \leftarrow$ GenerateElectionBlockchain($electionID$)
5: $combinedBlockchain \leftarrow$ Combine($userBlockchain, voteBlockchain$)
6: Store $combinedBlockchain$ in the election database
7: **return** $combinedBlockchain$

Algorithm 3 Generate Rotation Pattern

```
Input: Picture
Output: Rotation pattern string
GenerateRotationPatternPicture
pattern ← ""
for angle in [90, 180, 270, 360] do
    rotatedImage ← Rotate(Picture, angle)
    pattern ← pattern + ImageHash(rotatedImage)
end for
return pattern
```

IV. Implementation and Result Analysis

The implementation work is done in the Visual Studio 2010 and SQL Server Express 2008 is taken as the backend for that.

Fig 3. Implementation Snapshot

2410398_549575_887_891

The blockchain is generated using the using National Identity system like Aadhar Card, Driving License, which is clubbed with the fingerprint and picture rotation based blockchain.

The resultant blockchain which is generated is as follows,

Picture Rotation Blake2b Hash

04c688cf6792239a291e9f00d4cd1ef7c1996171b9601f7fd2daac78302d18b48f46e9e85006429b6be6da3f0cdbc0a8483d1657a4b80d2f7eef311b051d7e70

Fingerprint Blake2bHash

f5676c5f0edee92a4816d146796f4cd172d414bf9051dbfb1538f11e0dfe2117644ba766f08a996e0a28b5064213a8890b61bd57d9447515bd2277dd7fbd3748

Other Parameters Like Aadhar Car, National Identity System and more Blake2B

c764c170dbd662963de7e7d1ad6cf653907d0fd93888f06eca75f2f1c3cdfd456d11dd5aaed967e85210c06f19b2e830f669417617f c867356c5602251b2bacd

Then we will combine the extract of 30 characters from each,

04c688cf6792239a291e9f00d4cd1e_ f5676c5f0edee92a4816d146796f4c_ c764c170dbd662963de7e7d1ad6cf6

Base Paper: M Hamza Zaki Title "Secure Pattern-Key Based Password Authentication Scheme"
Password pattern: bbbb n > z A n a n

Table 1 Result Comparison Table Base Work

Proposed Work OTP	Website/Tool	Result
bbbb n > z A n a n	Password Blue	Entropy 53 bits
bbbb n > z A n a n	Cryptool2	Bit Strength : 62 Entropy 2.37

Table 2 Result Comparison Table Proposed Work

Proposed Work OTP	Website/Tool	Result
04c688cf6792239a291e9f00d4cd1e_ f5676c5f0edee92a4816d146796f4c_ c764c170dbd662963de7e7d1ad6cf6	Password Blue	Entropy 309 bits
04c688cf6792239a291e9f00d4cd1e_ f5676c5f0edee92a4816d146796f4c_ c764c170dbd662963de7e7d1ad6cf6	Cryptool2	Bit strength 177 Entropy 3.9

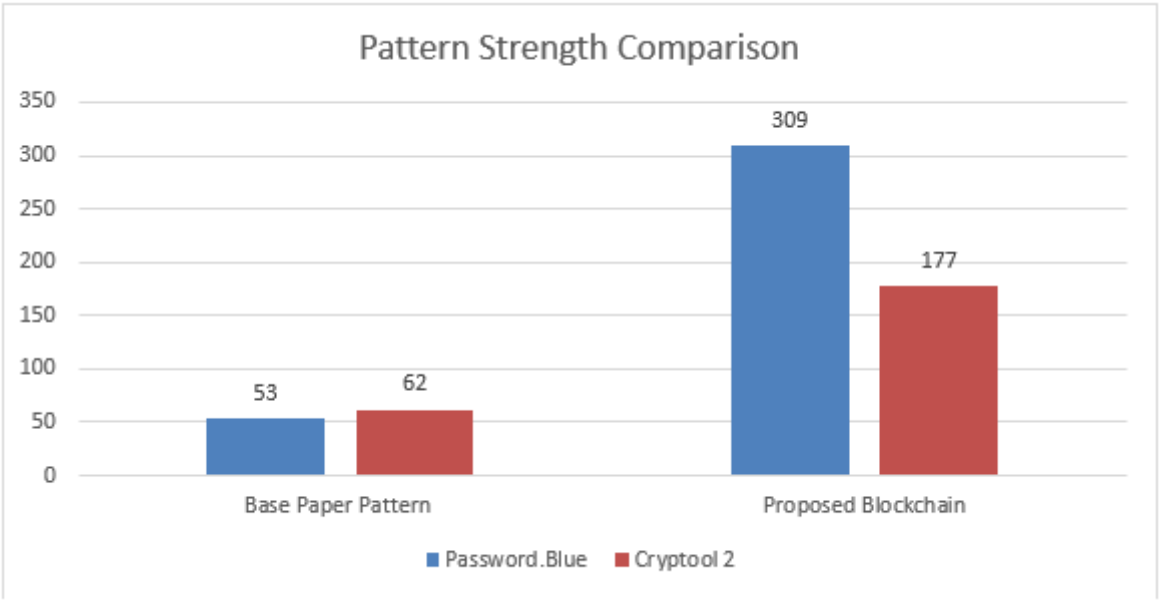

Fig 4. Pattern Strength Results

V. CONCLUSION

The model proposed the user identity or better say the voter identity blockchain creating using National Identity system like Aadhar Card, Driving License, which is clubbed with the fingerprint and picture rotation based blockchain. The blockchain identity of the individual person is also stored on the multiple servers which is verified in the impulse that all servers are checked for the identity verification of the user, so that we can safeguard the user identity for the hackers or being forged. Now, when comes for the casting of the vote the block chain is generated for the election purpose which identifies an election code, and the user identity block chain is clubbed and maintained on multiple servers, when the user has casted the vote , similar check of this blockchain is performed before casting in order to ensure that the multiple votes are not being casted. Using the proposed model, we can not only save time for being in queues for casting vote but also we can also increase the percentage of voting and reduce the cost involved in the elections.

REFERENCES

1. Al-madani, A. M., Gaikwad, A. T., Mahale, V., & Ahmed, Z. A. T. (2020). Decentralized E-voting system based on Smart Contract by using Blockchain Technology. *2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC)*, 176–180.
2. Alvi, S. T., Uddin, M. N., Islam, L., & Ahamed, S. (2020a). A Blockchain based Cost effective Digital Voting System using SideChain and Smart Contracts. *2020 11th International Conference on Electrical and Computer Engineering (ICECE)*, 467–470.
3. Alvi, S. T., Uddin, M. N., Islam, L., & Ahamed, S. (2020b). From conventional voting to blockchain voting: Categorization of different voting mechanisms. *2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI)*, 1–6.
4. Shahzad, B., & Crowcroft, J. (undefined 2019). Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 24477–24488. https://doi.org/10.1109/access.2019.2895670.
5. Patidar, K., & Jain, S. (2019). Decentralized E-voting portal using blockchain. *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1–4.
6. Zhang, W., Yuan, Y., Hu, Y., Huang, S., Cao, S., Chopra, A., & Huang, S. (2018). A privacy-preserving voting protocol on blockchain. *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 401–408.
7. M. H. Zaki, A. Husain, M. S. Umar and M. H. Khan, "Secure pattern-key based password authentication scheme," 2017 International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT), 2017, pp. 171-174
8. Bera, B. *et al.* (2021) "Designing blockchain-based access control protocol in IoT-enabled smart-grid system," *IEEE internet of things journal*, 8(7), pp. 5744–5761. doi: 10.1109/jiot.2020.3030308.
9. Bellini, E., Ceravolo, P., & Damiani, E. (2019). Blockchain-Based E-Vote-as-a-Service. *2019 IEEE 12th International Conference on Cloud Computing (CLOUD)*, 484–486.
10. Febriyanto, E., Triyono, Rahayu, N., Pangaribuan, K., &Sunarya, P. A. (2020). Using blockchain data security management for E-voting systems. *2020 8th International Conference on Cyber and IT Service Management (CITSM)*, 1–4.
11. Gao, S., Zheng, D., Guo, R., Jing, C., & Hu, C. (undefined 2019). An anti-quantum E-voting protocol in blockchain with audit function. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 115304–115316. https://doi.org/10.1109/access.2019.2935895
12. Giraldo, F. D., Milton C., B., &Gamboa, C. E. (2020). Electronic voting using blockchain and smart contracts: Proof of concept. *IEEE Latin America Transactions*, *18*(10), 1743–1751. https://doi.org/10.1109/tla.2020.9387645.
13. Li, H. *et al.* (2021) "A blockchain-based traceable self-tallying E-voting protocol in AI era," *IEEE transactions on network science and engineering*, 8(2), pp. 1019–1032. doi: 10.1109/tnse.2020.3011928.
14. Kashyap, S., & Jeyasekar, A. (2020). 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)*, 202–203.
15. Nelaturu, K. *et al.* (2020) "On public crowdsource-based mechanisms for a decentralized blockchain oracle," *IEEE transactions on engineering management*, 67(4), pp. 1444–1458. doi: 10.1109/tem.2020.2993673.
16. Panja, S., Bag, S., Hao, F., & Roy, B. (2020). A smart contract system for decentralized Borda count voting. *IEEE Transactions on Engineering Management*, *67*(4), 1323–1339. https://doi.org/10.1109/tem.2020.2986371
17. Rathee, G. *et al.* (undefined 2021) "On the design and implementation of a blockchain enabled E-voting application within IoT-oriented smart cities," *IEEE access: practical innovations, open solutions*, 9, pp. 34165–34176. doi: 10.1109/access.2021.3061411.
18. Sun, G. *et al.* (2021) "Voting-based decentralized consensus design for improving the efficiency and security of consortium blockchain," *IEEE internet of things journal*, 8(8), pp. 6257–6272.
19. Tan, Y., Liu, J. and Kato, N. (2021) "Blockchain-based key management for heterogeneous flying ad hoc network," *IEEE transactions on industrial informatics*, 17(11), pp. 7629–7638. doi: 10.1109/tii.2020.3048398.
20. Vairam, T., Sarathambekai, S. and Balaji, R. (2021) "Blockchain based Voting system in Local Network," in *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)*. IEEE, pp. 363–366.
21. Zaghloul, E., Li, T. and Ren, J. (2021) "*d*-BAME: Distributed blockchain-based anonymous mobile electronic voting," *IEEE internet of things journal*, 8(22), pp. 16585–16597. doi: 10.1109/jiot.2021.3074877.