Proceedings of the Second International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2020)
IEEE Xplore Part Number: CFP20K58-ART; ISBN: 978-1-7281-4167-1

Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology

Roopak T M
Department of Computer Science and Engineering
Siddaganga Institute of Technology
Tumkur,India.
rakshith178@gmail.com

Dr. R Sumathi
Department of Computer Science and Engineering
Siddaganga Institute of Technology Tumkur,India.
rsumathi@sit.ac.in

Abstract— The e-voting system is one of the frameworks which decreases the percentage of abstention and to ensure the security against tampering of the votes, Blockchain is a distributed and decentralized ledger that is used to record the transactions in an efficient and verifiable manner. Blockchain plays an important role in the e-voting system which ensures the security of votes by preventing modification of data stored in blocks using the cryptographic technique. Aadhar integration to the e-voting system overcomes the duplication or tampering of votes. The proposed scheme provides the secured e-voting system by using biometric details and VID(Virtual ID) of voters obtained from the Aadhar database to cast the Vote and also using the digital signature as the key for the encryption of the votes inside the block.

Keywords—e-voting, VID(Aadhar), Digital signature, Fingerprint processing, Blockchain & Hashing.

I. INTRODUCTION

Voting is a necessary part of a country to choose the right candidate, so generally, this election and voting system are started using a paper ballot system. While casting the vote by any individual it is necessary to keep the process secret. Electronic fair or e-throwing a polling form has a noteworthy activity. Since it's first Use as punched-card casting ballot shapes in the 1960s, e-throwing a polling form structures have achieved excellent way with its adaption using the Internet developments. These parameters join the anonymity of the voter, dependability of the vote and non-renouncement among others.

In this paper, the usage of Blockchain to empower e-throwing a polling form application with the ability to ensure voter lack of clarity, vote uprightness and end-to check is examined. E-polling form is defenseless against the advanced attack and deception vulnerabilities inborn in current programming, similarly as the basic manner by which the Internet is sifted through. This paper acknowledges e-throwing a polling form can use from head Blockchain features, for instance, self-cryptographic endorsement structure among trades (through hashes) and open availability of scattered records. The Blockchain development can expect key employment in the space of web throwing a polling form keeping up decentralized and openly spread record of trades over all of the center points. This makes Blockchain advancement incredibly compelling to deal with the peril of utilizing a fair token more than once and the undertaking to affect the straightforwardness of the result. For affirmation, the person's fingerprint will be checked at the client-side and facilitated offset at the servers with the data removed from the aadhar database.

This paper mainly focusing on using VID of the Aadhar which allows the service providers to make verification. The fingerprint data of voter is retrieved from aadhar database to verify the voter by comparing fingerprint data in the local device and it is converted to the digital signature to ensure integrity.

The flow of this paper is arranged in the following way, Section II focuses on some literature survey and existing system and Section III describes the working of the proposed system and security measures taken against vulnerability, and tampering of blocks. Section IV is mainly focused on explaining the properties of the blockchain e-voting system using VID and Section V concludes the research work.

RELATED WORK

[1] Nowadays technology with digitization is increasing in the world and also helping in the saving of human lives the electronic system has its uses in the different methods. In terms of security and its advantages without using the internet. In general, the system still uses the traditional method in which there are many manual error-scan occurred that might be the database and system also. Here "Blockchain" technology is one solution can be given to the project. Blockchain itself can be used as a decentralized system to ensure security.

[2] Verification of the data from end to end in the machines which are used to vote. And provides the integrity of the data verified by keeping the voters to auditing in the info which is published by the machine, instead of thinking that the system is correct. The practical capability of the machine had been demonstrated within real-time elections booths.

[3] In this they are using the voting system in advance method, In this, every client has to get in the different identity authority numbers and can vote to their choice. This is how it means there will be a highly secured secret key that will be given to the user and very user will into the website by that key and vote is done. The main important thing, here is his/her vote will be addressed to the proper leader hopefully. The voting will be done online, which saves time and vote also. And also it can give a result in an early time.

[4] This Survey is to check and determine how to minimize fake and illegal voting. To enhance the security with the authentication process can be implemented. Here, aadhar data is used for the biometric, and "BLOCKCHAIN" with unique hashtag function

[5] The author in this paper proposed the method for electronic voting using the EVM machine which is integrated with the aadhar verifications based on the Blockchain technology, this may help the election commissioners to reduce the risk of the manipulation of the vote, but it will increase the percentage of the abstention.

II. PROPOSED SYSTEM

The proposed framework is an electronic voting system using virtual ID which is provided by the UIDAI which is unique. Aadhar database helps to get the demographic details including the fingerprint details of the voters/voter. The fingerprint is converted to the digital signature which can be used to ensure the security of the vote in the block while doing the encryption as shown in Fig. 1 [8].

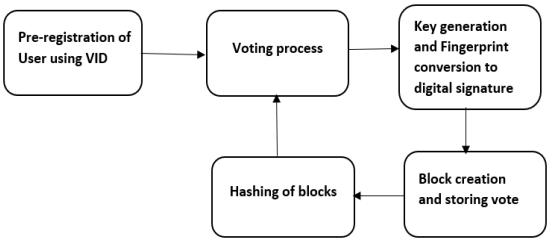

Fig. 1: E-voting system based on VID of aadhar.

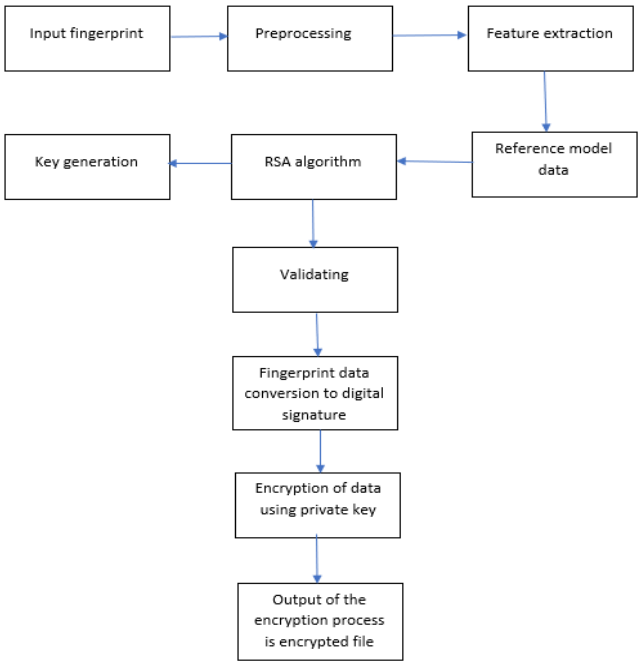

Fig. 2(a): Flow of fingerprint processing.

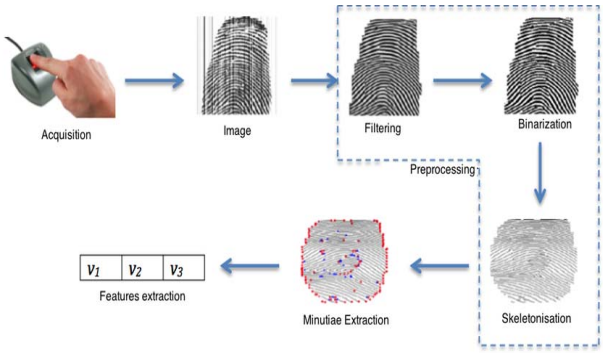

Fig. 2(b): Fingerprint extraction process.

As explained in the above Fig. 2, it shows the process of how the fingerprint is processed from the initial step until the conversion of it to a digital signature.

A. PRE-REGISTRATION OF USER

User registration is the necessary part of the electronic voting system since this system is web-based the registration has to be done earlier.

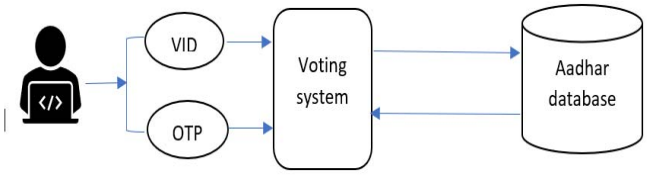

Fig. 3: User registration.

According to the figure (Fig.3), The User must have to register with the Virtual ID which is obtained from the UIDAI which is a temporary ID to get login into the voting system. VID is a regenerative number i.e, valid for a minimum of one day or till the user re-generate it. VID is

used for the authentication of the user and also to e-Know-Your-Customer services.
As shown in Fig.3, the Voting system or election commission officer can retrieve the demographic details of the Voter from the Aadhar database including fingerprint details.

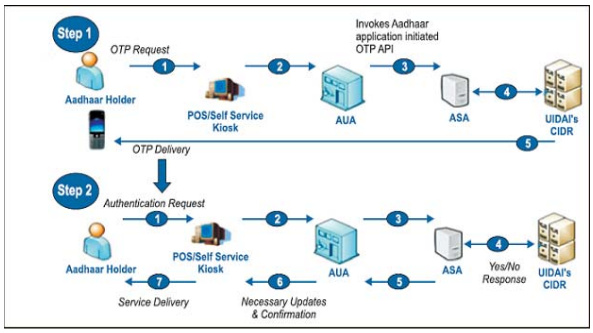

Fig. 4: OTP service and authentication services by UIDAI.

The CIDR(central identities data repositry) is used by UIDAI to maintain the records of the Aadhar and it allows the user to get the OTP for the secure transaction as shown in Fig. 4. About Aadhaar Auth API[14]. Aadhaar validation is the procedure wherein Aadhaar Number, alongside different properties, including biometrics, are submitted online to the CIDR for its check based on data or information or archives accessible with it.

B. VOTING PROCESS

After the registration, By verifying the details retrieved from the Aadhar database, the election commission officials decide whether Voter is eligible to cast vote or not. Based on the decision of Election commission user has to caste the vote through the online using web. Before the vote is submitted, the voter has to scan his/her finger on the PC or mobile devices.
Then the vote is submitted and stored in the block in encrypted format using the private key as shown in Fig.5 [9].
The Asymmetric encryption is used for cryptographic operations like encryption and decryption, where the voter uses the election commission's public key for the encryption process then the election commission members use their private key to decrypt and retrieve the vote to verify the votes [15].

This framework has a strategy to execute activities on encoded information by utilizing Hash work with the assistance of private key (VID which can be recovered). By utilizing public key election official can de-encode information utilizing square chain hash work calculation. On the other end, all the voter details and the voting count will be updated to the election commission but the data will be in the format of cipher-text and it should be decrypted for that election commission

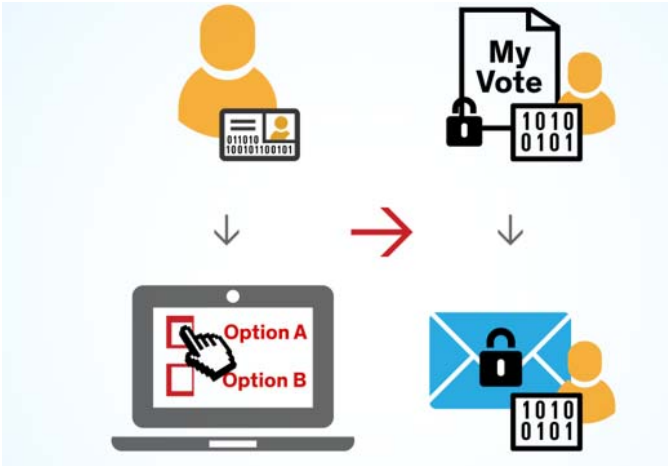

Fig. 5: Voting process.

C. KEY GENERATION

Blockchain uses some cryptographic techniques to perform encryption & decryption to ensure security [10]. To perform the encryption and decryption there are different many types of cryptographic encryption algorithms. Based on the type of algorithms the private key and public keys are used to ensure integrity. In this proposed system private key is used to sign the document (Vote) digitally. The election commissions use the public key to verify the signature made by the voter while voting.
According to Fig. 6 & Fig. 7, The key pair is generated when the fingerprint provided by the voter is matched with the fingerprint stored in the aadhar database. Then the fingerprint is converted to the digital signature.

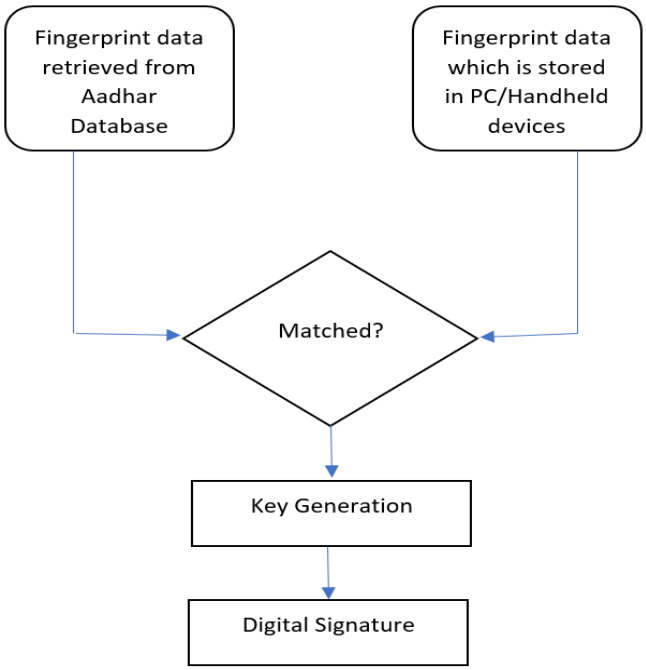

Fig. 6: Fingerprint processing and key generation.

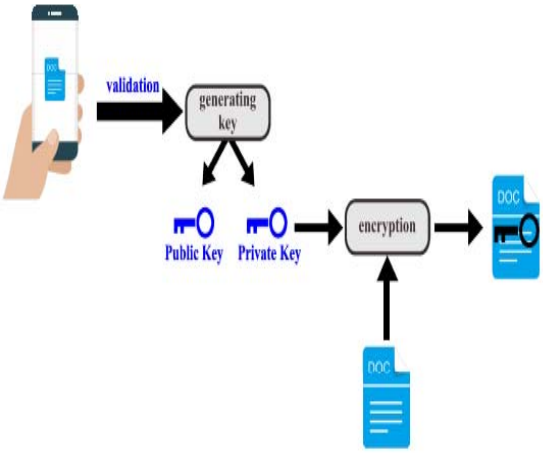

Fig. 7: Key pair generation[11].

As explained in the Fig. 6 in this project, mainly concentrating on how data of the voter can be kept secure and a voter can vote from anywhere, according to this, here comparing 2 datasets of same data, one is fingerprint stored in adhar database and other is when user gives fingerprint data from his/her device.

D. HASHING OF BLOCKS IN BLOCKCHAIN

The blockchain is an appropriated record it is partially open to everyone in the chain[11]. This blockchain has a fascinating property, when data is recorded inside a block-chain it ends up being hard to change. Each square contains three segments,

1. Data,
2. Hash of the square
3. Hash of the past square.

Data: It contains the popularity of based information.

Hash: it allows us to balance the hash with a finger impression, it is continually excellent. At the point when a square is made its hash code has been resolved, if any changes is detected inside the square may make a hash code change. The hash is useful when you have to recognize changes to a square. In case the one of a kind finger impression of square changes, it never again is a comparative square.

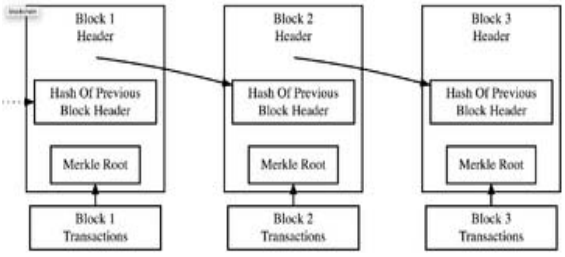

Fig. 8: Hash Function.

As explained [11] in Fig. 8, initially once the voter casts their vote the new block will be created and using pairs of the keys and digital signature the hash is generated and continually the new blocks are created using the Hash of the previous block using some hashing algorithm.

Hash can be generated using the private and public keys as shown in Fig. 9. This Hash ensures the integrity of the blocks which includes votes and voter information.

SHA-256 is one of the hashing algorithms to ensure integrity, it provides the fixed length of 256bit of message hash output irrespective of the length of the input[12] & [13].

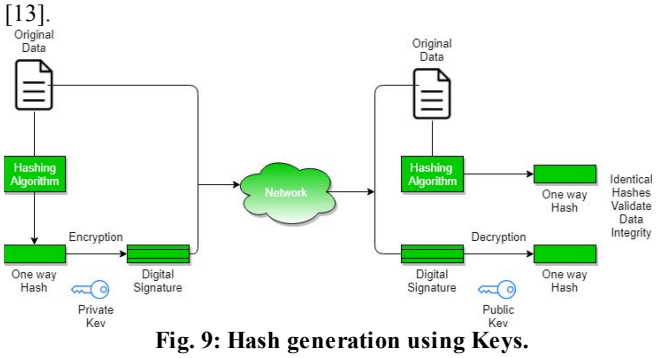

Fig. 9: Hash generation using Keys.

III. PROPERTIES OF BLOCKCHAIN E-VOTING SYSTEM USING VID

A. AUTHENTICATION

This proposed system uses the fingerprint data to ensure the security, and also only the registered voters can cast their votes so that anyone can easily prove that the voter can cast their particular vote by observing the digital signature.

B. AVAILABILITY

This proposed framework can be implemented anywhere across different countries based on their identities. Voters can check their voting eligibility anytime. This framework can be integrated into any of the handheld devices with fingerprint module.

C. PUBLICLY VERIFIABLE

Since the blockchain is one of the distributed and decentralized technology which makes other persons in the election process to verify the votes if they intended and authorized.

D. INTEGRITY

The votes that are collecting by the e-voting system should be accurate and tamper proof and it should not be duplicated.

Hashing helps in ensuring the integrity in blockchain. In parallel the digital signature do not allow modification.

E. SHA ALGORITHM

It is a secure Hash Algorithm, which is under the family of cryptography where it helps in data security [12], It works basically on hash function. There are few modules used in this, they are bitwise operators, modular adition and comaparision function.

V. CONCLUSION

Voting is one of the process which allows the citizens to identify themselves in the society and also it is one of the rights to choose right and humble leader for the society. There are many voting system which are not secure, so the blockchain is used to ensure security by integrating the aadhar verification using VID to it, the digital signature which is converted from fingerprint data, plays a important role here in ensuring security.

In encryption and loosening up, the choices of key-length impact the file size of encoded record what's more the durable of encryption process. Since the VID is temporary ID of the aadhar it eliminates the use of UID number and it allows us to authenticate and verify the user demographic details.

V. REFERENCES

[1]. Rifa Hanifatunnisa, et al, "Blockchain Based EVoting Recording System Design", School of Electrical Engineering and Informatics 2017.
[2]. Vanessa Teague, Steve Schneider, Peter Y.A. Ryan, "End to End Verifiability in voting system from theory to practice" June-2015.
[3]. R.Murali Prasad, et al, "AADHAR based Electronic Voting Machine using Arduino", International Journal of Computer Applications, vol. 145, no. 12, July 2016.
[4]. Desna Sebastian, et al, "Aadhar Based ElectronicVoting System and Providing Authentication", International Journal of Science and Engineering Research (IJ0SER), no. 3, March 2015.
[5]. Navya A et al, "Electronic voting machine based on Blockchain technology and Aadhar verification". 2018 International Journal of Advance Research, Ideas and Innovations in Technology
[6] Ansif Arooj and Mohsin Riazz "Electronic Voting With Biometric Verification Offline and Hybrid EVMs Solution"2016.
[7] Budi Rahardjo and Rifa Hanifatunnisa "Blockchain Based E-Voting Recording System Design"2017.
[8] Erika Rahmawati, et al, "Digital Signature On File Using Biometric Fingerprint With Fingerprint Sensor On Smartphone". 2017 International Electronics Symposium on Engineering Technology and Applications (IES-ETA).
[9]https://hackernoon.com/how-blockchain-will-make-electronic-voting-more-secure-fba15d752bee.
[10] Sivaganesan, D. (2019). Block Chain Enabled Internet of Things. *Journal of Information Technology,* 1(01), 1-8.
[11]https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm
[12] Devika K N, et al, "Parameterizable FPGA Implementation of SHA-256 using Blockchain Concept". 2019 International Conference on Communication and Signal Processing.
[13] Lukman Adewale Ajao, et al, "Crypto Hash Algorithm-Based Blockchain Technology for Managing Decentralized Ledger Database in Oil and Gas Industry" 2019.
[14]https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf
[15]https://www.tutorialspoint.com/cryptography/public_key_encryption.htm