Anjali S *et al*, International Journal of Computer Science and Mobile Applications,
Vol.6 Issue. 2, February- 2018, pg. 100-107 **ISSN: 2321-8363**
Impact Factor: 5.515

A Security Enhanced Voter Identity Verification System based on Blockchain

[1]Anjali S, [2]Abhishek Nambiar C,
[3]Meenakshi Omprakash, [4]Parvathy TR, [5]Paul Louis
[1]Assistant Professor, Department of Computer Science & Engineering Government Model Engineering College, Thrikkakara, Kochi, India, anjalisivakumar@gmail.com
[2,3,4,5]U.G Student, Department of Computer Science & Engineering Government Model Engineering College, Thrikkakara Kochi, India

Abstract
In today's world where electoral fraud and election manipulation is increasing, it becomes necessary to find measures to decrease the amount of cheating. One solution for this is to recognize the person with the help of various security measures including OTP, graphical password etc. All voters must register on the proposed system. The user must then use this account to input his/her fingerprint. This feature is optional because it is not feasible for every household to have a fingerprint scanner. The details of every registered voter will be saved in the database using Block Chain and thus the particular person can be identified easily later. Upon verification using OTP (via text message, email), fingerprint and graphical password, the voter can cast his/her digital vote. The votes will be evaluated on a particular date. Until then, the user has the option of changing his or her vote. The use of ID cards is therefore avoided. It helps in recording the number of votes cast, number of voters appeared etc. and decreases the manual labor involved.

Keywords—Blockchain, Graphical Password Authentication, OTP, Electronic voting machine.

1. Introduction

A blockchain can be defined as a list of records that grows continuous. Each record is a block, which is linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data. A blockchain can serve as "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way." For use as a distributed ledger a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Here, the concept of blockchain is used to evaluate votes, thus making the voting system more secure and simple. Many electronic voting systems has been built and implemented in the past two decades. David Shaum developed the first ever electronic voting system based on Blind Signature Theorem[11].

2. Related Work

A. Microcontroller Based Smart Electronic Voting System

For the purpose of a voting system, an electronic voting machine EVM is introduced which replaced conventional methods of voting i-e manual voting. Proposed machine is faster, efficient, and reliable and error free as compared to manual voting system which is slower, poses full day fatigue on people and chances of error are greater. Its main feature is its ease to operate[9] .Voter polls a vote very easily and final results are displayed in no time by just pressing a result button, after the elections have been conducted.

B. A Secure e-Government's e-Voting system

It proposes a reliable cost effective secure electronic voting system that can be used in cost effectively way in many development countries like Egypt[11]. The important obstacle in any e-voting system across the world is the security issue. Election's results may be modified when delivered to the Higher Elections Committee, unauthorized voter may vote instead of the eligible voter, a vote may not be calculated; also the voter has to ensure that nobody has the possibility to know his ballot data. The proposed Voting Model System overcomes these obstacles.

C. Development of a Credible and Integrated Electronic Voting Machine Based on Contactless IC Card, Biometric Fingerprint Credentials and POS Printer

In recent times there has been a decline in the confidence of common people over electronic voting machines (EVMs)[14]. To elucidate the system in brief, multiple layered verification process would be carried out on a potential voter by the means of fingerprint recognition and a Near Field Communication (NFC) smart card entry in order to authenticate his or her identity. Subsequently, the person would cast the vote by pressing a button corresponding to a particular candidate which would be recorded in the system providing the vote caster a visual confirmation. The final vote would then be printed out spontaneously onto a ballot box using a POS (Point of Sales) printer for an added level of validation.

D. Identity Verification System Using Data Hiding and Fingerprint Recognition

This technique proposes an identity verification system using data hiding and fingerprint recognition [2]. At user's home, the client's account information is encrypted and embedded into the fingerprint image via data hiding method secretly. Then the fingerprint image with embedded data is transferred to the bank over Internet. At bank side, the client's account information is extracted. It is used to retrieve the client's registered fingerprint from central database, which is then matched with extracted fingerprint via fingerprint recognition method to verify user's identity. This system is more reliable and secure than transferring password alone. The data are embedded with quantization watermark in the JPEG 2000 coding pipeline.

3. Challenges and Applications

- Consensus mechanisms: In a distributed database such as a blockchain, effort must be expended in ensuring that the nodes in the network reach consensus. Depending on the consensus mechanism used, this might involve significant back-and-forth communication and/or dealing with forks and their consequent rollbacks.
- Redundancy: This isn't about the performance of an individual node, but the total amount of computation that a blockchain requires. Whereas centralized databases process transactions once (or twice),in a blockchain, they must be processed independently by every node in the network.
- Not many people are aware and are experts in block chaining.

Blockchain technology has a large potential to transform business operating models in the long term. Blockchain distributed ledger technology is more a foundational technology- with the potential to create new foundations for global economic and social systems- than a disruptive technology, which typically "attack a traditional business model with a lower-cost solution and overtake incumbent firms quickly." Even so, there are a few operational products maturing from proof of concept [1]. The use of blockchains promises to bring significant efficiencies to global supply chains, financial transactions, asset ledgers and decentralized social

networking. Blockchain technology can be integrated into multiple areas. This means specific blockchain applications may be a disruptive innovation, because substantially lower-cost solutions can be instantiated, which can disrupt existing business models. Blockchain protocols facilitate businesses to use new methods of processing digital transactions. Examples include a payment system and digital currency, facilitating crowd sales or implementing prediction markets and generic governance tools.

TABLE 1: Comparison Table

Name of work	Advantages	Disadvantages
Micro-Controller Based Smart Electronic Voting Machine System	• Supports various languages by reprogramming the device. • Persons with disabilities can access the device as it can provide necessary accessibility using headphones and other adaptive technology. • Electronic voting reduces the possibility of fraud on large scale. Because its code is not accessible and cannot be changed once it is burnt.	• As costly to make as the earlier inefficient methods of electronic voting like direct-recording electronic (DRE) voting systems. • Keeps count of the votes on the hardware itself and is not uploaded to the internet. • Does not allow for changing the vote once cast.
A Secure e-Government's e-Voting System	• Each system contains an ID card reader and a fingerprint reader for user verification. • The architecture of the system is decentralized. • Results are encrypted and hashed to secure from attacks.	• Needs a phase of auditing to ensure that errors haven't crept in. • Vote once cast cannot be changed. • Require the physical transport of the voting machine.
Development of a Credible and Integrated Electronic Voting Machine Based on Contactless IC Cards, Biometric Fingerprint Credentials and POS Printer	• Uses NFC smart card and fingerprint recognition for voter ID verification. • Thermal "point-of-sale" (POS) printer would print the vote and dispense it into a ballot box for further assurance of the voter and also to eliminate any discrepancy arising during counting.	• Included fingerprint reader can only store 256 fingerprints. • Uses POS printer to print the votes. Thus, the votes are not digital. • There is no encryption used in the system to protect it from outside attacks.
Identity Verification System Using Data Hiding and Fingerprint Recognition	• Firstly, biometric recognition is used to enhance the reliability of the system. • Secondly, watermark data is embedded into the fingerprint image secretly. It is more difficult for hostile party to realize the very existence of the secret message.	• QIM (Quantization Index Modulation) based data hiding algorithm is hard to implement. • Watermark Extracting Algorithm is also complex.

4. Proposed System

The proposed security enhanced voter identity verification system based on Ethereum DApp provides the most security and is immune to vote manipulation or vote fraud [5]. A vote once cast is recorded and has a hash value associated with it. This hash value can be used in future to determine whether any of the votes have been altered. This totally eliminates the occurrence of vote fraud. Additionally, there is a specific time window spanning up to days decided by the administrator of the website, during which the registered users are able to

change the vote cast previously. The use of ID cards is therefore avoided. Fig. 2 shows the overall system architecture. Upon verification using OTP, fingerprint and graphical password, the voter can cast his/her digital vote, thereby increasing the security. The database will store information like the users name, age, sex, mail-id etc. This module has to be highly scalable keeping in mind the number of users that will access the website. This system uses a hybrid model consisting of server side scripts and decentralized storage of user data and votes.

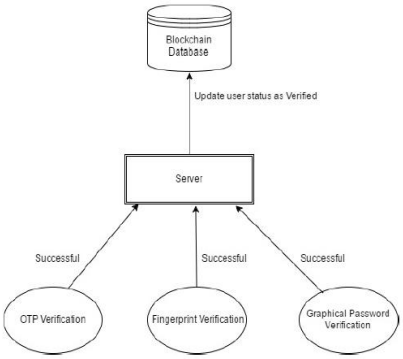

Figure 1: Security Module

Server side modules are used to send OTP via email and SMS. Decentralized storage in blockchain is used to store each user's details and voting information. Smartcontracts allow the performance of credible transactions without third parties. These transactions are traceable and irreversible. Hence data entered into the blockchain cannot be edited and is secure. The system also allows the users to change their profile information and re cast their vote while the election is active. The system also provides an admin panel that is used to start elections, specify candidates for an election and also view/edit user information. The system can be mainly divided in to two modules, Security module and a Voting Module. In the security module (Fig.1)- OTP Verification that uses two methods (phone number and email id) as well as Graphical password verification has been included. Furthermore, fingerprint verification can also be incorporated in those situations where scanners can be bought in a bulk amount. (e.g. within an organization).The voting module includes the voting website and the backend database which is used to store the users' information. The database is maintained in blockchain using smart contracts written in solidity programming language. The code for the backend is run in Remix IDE which is then connected to a test environment run in the terminal of a Linux based OS using the code testrpc. Testrpc gives us 10 ETH accounts of which we use one in Remix to interact with our test environment.

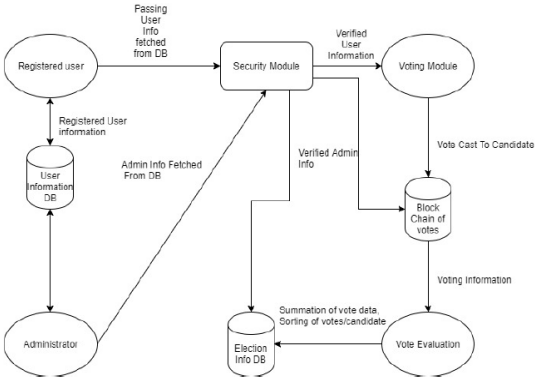

Figure 2: System Architecture

5. Algorithms

Level 1 and 2 of security phase includes sending OTP via SMS and Email ID

Algorithm for OTP generation

1. random_number = intval(rand(0,9) . rand(1,9) . rand(0,9) . rand(0,9) . rand(0,9) . Rand(0,9));
2. Send random_number to both registered email id and password.
3. if(email id OR mobile number does not exit)
   logout user with a message saying invalid mobile number/ email id.
   else
   prompt user to enter the recieved OTP
   if(entered OTP ==random_number)
   forward user to level 3 security

In the Security Phase Level 3 we make a 3X3 grid for showing 9 images of which one will be the user uploaded image he/she chose as her graphical password during the registration. Unsplash provides free images which can be used as random images in our 3X3 grid. We use 7 random unsplash images. Other websites can be used as well but unsplash provided to be the most reliable.

Algorithm for Graphical Password

1. Retrieve the image hash of the current user's graphical password
2. Store this in 0^{th} position of the array.
3. Store random images in rest of the 7 positions as follows using the usplash placeholders.
   For (i=1;i<=7;i++)
   img_loc[i++]='https://source.unsplash.com/random?sig=i';
4. Shuffle all the image locations and display it in a 3X3 grid
   numbers= range(0,8);
   shuffle(numbers);
   i=0;
   foreach(numbers as number)
   num[i]=number; i++;
5. Next find the user's pic from the shuffled array
   For (i=0;i<=8;i++)
   {If (img_loc[num[i]]==img_loc[0])
   correct=i;}

where correct is the variable used to store the location of the user's image URL.

6. if(selected pic ID == correct)
   forward user to the voting page.
   Else logout the user

The below algorithm is used to always fetch the latest profile information related to each user ignoring the past edits he/she has made.

Algorithm for getting latest user profile after edits.

1. Get the email id of the user just logged in.
2. Use the email id to get the block associated with his profile information.
3. j= returnLatest(email);
4. return to client the user information contained in user[j].

The below algorithm will always fetch the latest information related to the inputted email.

Algorithm for returnLatest

Input: User email id
Output: Latest information related to the email id inputted.

```
1.  Let l=0;
2.  while (sha3(user[i].email)==”inputed email”)
     {        if(user[i].timestamp>l){
l=user[i].timestamp;blockRequired=i;
                        }return i;}
```

The election ID will the product of all the candidates IDs participating in it. This is bound to be unique as the candidate Id's are prime numbers. The below algorithm shows the same.

Algorithm for vote summation

Input: election id of the particular election which is to be evaluated.
Output: the total number of votes for each candidate

```
1.  Fetch election id from the election info structure upon
    the date of election end.
2. n=new int[1..no of factors]; sum=new int[1..n]
3. n [ ] =factorize (election id)
Enter into array n all the elections ID's as subsequent array values.
4. for i=1 to end of block in blockchain
      for j=1 to sizeof (n )
            if(n[j]==candidate id)    sum[n[j]]=sum++;
5. return sum[ ]
```

All the candidate Id positions will be filled in the sum[] array with the respective no of votes each candidate procured. This data can then be sorted to get the candidate who won the particular election.

6. Findings

The system will generate an input that contains the voter identification numberfollowed by the complete name of the voter as well as the hash of the previousvote.This way each input will be unique and ensure that the encrypted output willbe unique as well. The encrypted information will be recorded in the block header of each vote cast. The information related to each vote will be encrypted using SHA-256. After a block is created, and depending on the candidate selected,theinformationis recorded in the corresponding blockchain. Each block gets linked to the previously caste vote.In a distributed database such as a blockchain, effort mustbe expended in ensuring that nodes in the network reach consensus.

7. Conclusion

With the help of blockchain, each vote is validated cryptographically as an independent node and is stored, thus making the system completely immune to all malicious tampering attacks. The same mechanism is also applies to the voter information as the voter details too are stored as blocks inside the blockchain database. The 3 step voter authentication process further enhances the security and is immune against all the electoral fraud and election manipulation. The authentication of the correct user is verified by this system. Further on authentication, the voters can caste his/her votes. Upon the deadline, the total number of votes cast and the winning status of each candidate will be provided. The proposed system helps in recording the number of votes cast, number of voters appeared etc and decreases the manual labor involved. As a result, this system can be seen as an apt replacement for the existing voting system.

References

[1] Madise, Ü. Madise and T. Martens, 2006,"E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world*.", Electronic voting, 2nd International Workshop*, Bregenz,Austria August 2-4.

[2] Guorong Xuan, Dan Jiang, Hongfei Ji,Yun Q. Shi, Dekun Zou, Liansheng Liu, Heisheng Liu , 2005 ,"Identity Verification System Using Data Hiding and Fingerprint Recognition",*IEEE 7th Workshop on Multimedia Signal Processing*, .

[3] C. Meter and A. Schneider and M. Mauve, 2017,"Tor is not enough: Coercion in Remote Electronic Voting Systems. *arXiv preprint*.

[4] https://medium.com/@mvmurthy/full-stack-hello-world-voting-ethereum-dapptutorial-part-1-40d2d0d807c2

[5] https://vivekcek.wordpress.com/2017/07/02/developing-an-ethereum-blockchainbased-web-application-for-voting/

[6] http://ethdocs.org/en/latest/introduction/what-is-ethereum.html

[7] https://www.quora.com/How-does-the-OTP-one-time-password-work

[8] D. L. Chaum, ,1981 ,"Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms",*Communication of the ACM*. Vol. 24(2).,pp.84-90.

[9] Sahibzada Muhammad Ali," Micro-Controller Based Smart Electronic voting machine system", *IEEE International Conference on Electro/Information Technology (EIT)*,2014.

[10] T. ElGamal, ,1985,"A public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms",*IEEE Trans. Info. Theory*. Vol. 31., pp. 469-472.

[11] S. Ibrahim and M. Kamat and M. Salleh and S. R. A. Aziz, 2003,"Secure E-Voting with Blind Signature",*Proceeding of the 4th National Conference of Communication Technology*, Johor, Malaysia, January 14-15.

[12] J. Jan and Y. Chen and Y. Lin,2001, "The Design of Protocol for e-Voting on the Internet", *ProceedingsIEEE 35th Annual International Carnahan Conference on Security Technology*, London,England, October 16-19.

[13] Mohammad Hosam Sedky, Essam M. Ramzy Hamed,2015," A Secure e-Government's e-Voting System", *Science and Information Conference*, London, UK.

[14] Syed Mahmud Hasan, Md. Tahmid Rashid, Md. Shadman Sakib Chowdhury and Dr. Md. Khalilur Rhaman, 2016,"Development of a Credible and Integrated Electronic Voting Machine Based on Contactless IC Cards,Biometric Fingerprint Credentials and POS Printer", *IEEEE Canadian Conference on Electrical and Computer Engineering* (*CCECE*)
[15] Justo Carracedo Gallardo and Emilia P. Belleboni 2009,"Use of the New Smart Identity Card to Reinforce Electronic Voting Guarantees",*International Conference for Internet Technology and Secured Transactions . ICITST.*

