A Block-chain Based Network Security Mechanism for voting system

Kowsalya P
Assistant Professor, Department of Electronics and Communication Engineering, Info Institute of Engineering, India

Amutha A
Head of the Department, Department of Electronics and Communication Engineering, Info Institute of Engineering, India
Email: amuthaphdsalem@gmail.com

Kowsalya K
Student, Department of Electronics and Communication Engineering, Info Institute of Engineering, India

Roshini B
Student, Department of Electronics and Communication Engineering, Info Institute of Engineering, India

Kousalya V
Student, Department of Electronics and Communication Engineering, Info Institute of Engineering, India

Kowsika M
Student, Department of Electronics and Communication Engineering, Info Institute of Engineering, India

Abstract

With the stable progress in the technological world, concern for safety also enlarge day by day. Protection like keys can be simulated quite easily. This paper aims to avoid theft and crime at bank locker. A smart security system with the use of Raspberry-Pi microcontroller, piezo-Electric, PIRSENSOR, Camera Module and a buzzer is proposed. The security system be based on a "secret knocking pattern" which can be install to a 'safe' or any other similar object which wants protection. The lock unlocks only when a certain secret knocking pattern is implemented and a mail alert is sent by detecting their face if anyone tries to sneak into contents by knocking differently. This concept eliminate the fear of duplication as there is no physical unlock object to start with. Thus, the smart 'Knock Based Security System' is added protection in our everyday lives. Raspberry-pi board which act as a microcontroller unit. The piezo sensor takes the knocking input as well as facial recognized input and then passes it to the pi board where the input pattern and face detection is compared with the original Secret pattern. Using IOT, mail will be sent to the required person. Now-days technology advances many countries have now opted for electronic voting system. Any voting system must follow principles of transparency and impartiality in order to achieve fairness; the electronic voting process must also be protected against cyber-attacks or denial–of-service attacks (DDOS) because such attacks may affect the processing time in voting procedures and even hinder the fairness in voting. It establishes a network security mechanism for voting systems based on block chain technology. The block chain mechanism employs a distributed architecture that can prevent shutdown resulting from malicious cyber-attacks; additionally, any user in the block chain can authenticate data integrity, which satisfies requirements of transparency and impartiality in voting systems. It denotes bilinear pairing to establish network security in voting systems, which call for anonymity, authenticity, integrity, and non-repudiation. When authenticating voting integrity, the user's anonymity must be ensured to prevent identity revelation, and the data must be protected against malicious tampering such security measures also fulfil block chain requirements. The proposed voting system relies on the basis of block chains to create a trust worthy voting system. In current block chain technology, smart contracts allow the establishment of voter-related regulations to prevent controversies during voting processes. A additionally, in order to establish both a secret ballot and an open ballot system, the study also implements a bilinear pairing security mechanism to ensure the overall security of a voting procedures.

Keyword: *Block chain; Bilinear pairing; Digital Recording Electronic (DRE); Electronic Voting Machine (EVM**);** Network Security; Voting Mechanism.*

1. INTRODUCTION

Our democracy voting is one of the fundamental political rights of citizens. Voting is the most important element of the electoral system. In recent days, they make the claimed benefits of voting system such as controversies, cyber-attack or abused will be ensure. These behaviours must be sufficiently transparent for voters and who can accept the election result.

Figure 1 Vote Mark

According to that technology, Electronic voting system was introduced. Electronic voting system is often hardware system that introduced to polling stations. These machines include interactive an touch screen display interfere through were the voters can cast their ballots question arise in recent days whether there is a way to observe voting results accurately and test which will be difficult without paper backup and some systems might have fail safe login not all but few and this leads to the ideas of e-voting.

Figure 2 Voter Identity Cards

Whenever officials of the given party had a separate time with machines there arises possibilities of tampering or fraud. Hence in order to achieve the fairness of all their demands. The performance results, pairing, security, identity features of bilinear pairing for new security mechanisms. The aims of this experiment are prove our e-voting system.

2. EXISTING SYSTEM

Digital voting is use of voting machine or an internet browser to cast votes. These are sometimes referred to as e-voting when voting using machine in a polling station and e-voting when using a web browser. It can also involve transmission of ballots and votes via telephones, private computer networks or the interrupt.

A direct recording electronic system is essentially a computer. Voters view ballots on a screen and make choices using an input device such as a bank of buttons or a touch screen. Some DRE systems also employ a card swipe or cartridge system that must be activated before a ballot can be cast. The controversy surrounding the electronic voting machine is tampering. This creates the issue with the election commission in recent year, EVM provide with a button for each voter's choice which is connected by a cable to an electronic ballot box.

This EVM consist of two units namely control units, ballots units and both the units are connected by a five meter cable. When a voter presses a button against the candidates he/she wishes to vote for, the machine locks itself. This EVM can be operated only with a new ballot numbers. These ways to, EVM ensure that one person gets to vote only once millions of and here, tampering place. EVM's means doing away with paper ballots and in turns. This saves true being art. It makes entire process of voting simpler and once by clicking on the button your vote is registered. These machines don't require electricity and run on batteries. And most importantly, this work exist is slower in vote counting process, delivering results must be in hours but as against manual counting of votes, which could take days.

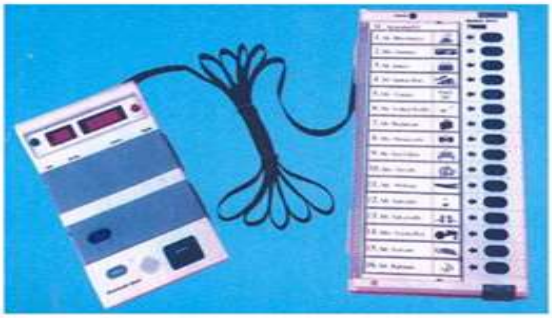

Figure 4 Control Units and Ballot Unit

3. PROPOSED WORD

System Model

The behavior of e-voting must be sufficiently transparent to voters and candidates who can achieve the election result. According to this our proposed system illustrates. All identity authentication units focus on authenticating the voter's identity.

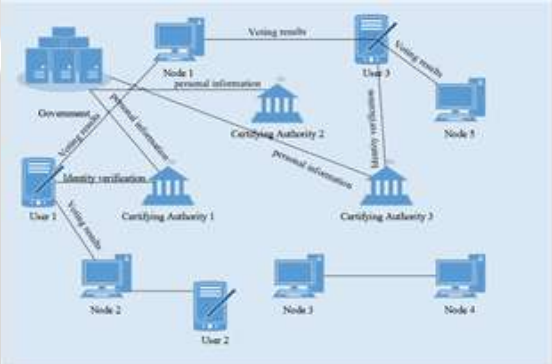

Figure 5: System Illustration

Once when a voter is successfully authenticated and completes thus voting, the voting result on the node is placed on the system. So that the node may authenticate success of the voting outcome while other users can authenticate the power and integrity of every piece of data on the node and this achieves the transparency of election fairness.

VOTER AUTHENTICATION

Voter authentication is the process of recognizing user's identity. This paper present the online voting system with authentication which seeks to make use of the uniqueness of the minutiae of human figure print to enhance further level of trust and confidential of the voters in the system.

Figure 6: Voters Authority

In order to achieve uniqueness of e-voting system proposed and developed a new secured e-voting system using notations like, user1 identification wishes to conduct voting. First, they must undergo identity authentication with certifying Authority 1 ID, which has already obtained the user's identity information from the government. When ID uses ID public key to encrypt personal information, and then transmit it to ID for authentication. ID creates ID's ballot information M, anonymous ID, public key and private key PR. Figure shows the flowchart of voters authentication.

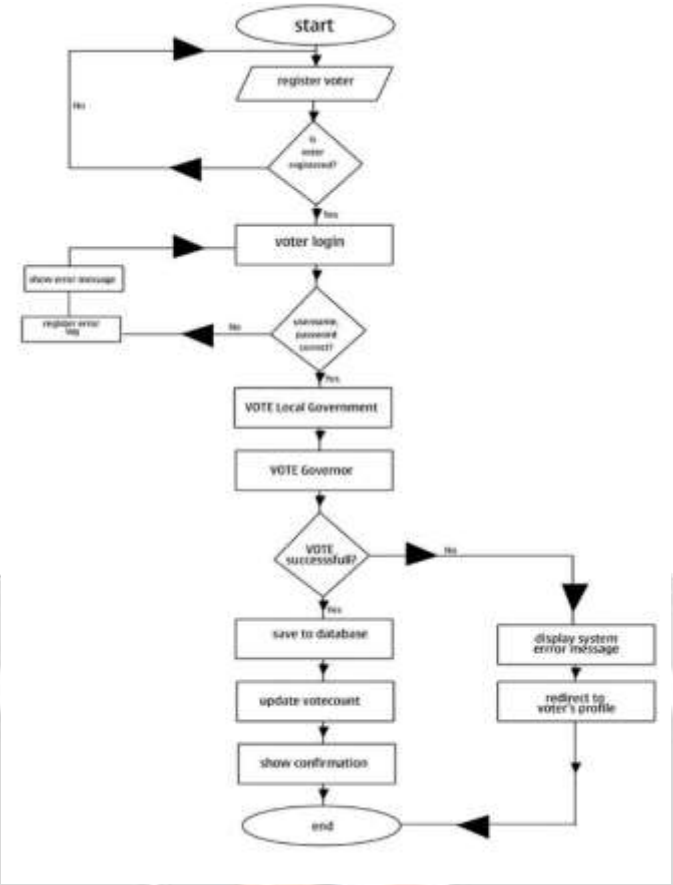

Figure 7: Flow Chart of Voter's Authentication

DATA TRANSMISSION AND AUTHENTICATION

In order to achieve the data transmission and authentication without any fraudulent, tampering or corruption, E-voting system must satisfy the requirements correctness eligibility, un-reusability, inscrutability, fairness, voter verifiability, and vote and exist, accuracy, privacy, democracy, resistance, Accessibility, restart ability. When identification (ID) successfully completes authentication, ID uses the public key to encrypt information such as voting result and transmit it to the node. The node then authentication whether PK was indeed sent by ID; if yes, then the deciphered text shall reveal ID as a legitimate user. The process started, when another user wishes to authenticate ID's voting results, they must first authenticate whether the public key was indeed issued by, in which, and T are public information. If the computed values are identical, this signifies that ID is a legitimate user.

Node MCU

Node MCU is a Wi-Fi System on a chip produced by espresso if System. It is based ESP8266-12E Wi-Fi module. It is a highly integrated chip designed to provide full internet connectivity in a small package. It can be programmed directly through USB port using LUA programming or Arduino IDE. By simple programming we can establish a Wi-Fi connection and define input/output pins according to your needs exactly like arduino, turning into a web server. Node MCU is the Wi-Fi equivalent of Ethernet module. It combines the features of Wi-Fi access point and station microcontroller.

ESP8266

Node MCU is than open source IOT platform. It includes firmware which runs on the ESP8266 Wi-FiSoC from Espressif system, and hardware which is based on the ESP-12 module. The firmware uses the Lua scripting language. The ESP8266 is a low-cost Wi-Fi microchip with full TCP/IP stack and microcontroller capability produced by manufacturer Espressif Systems in shanghais china.

Figure 8: Node MCU

LCD DISPLAY

Liquid crystal display is a flat panel display that uses the light modulating properties of liquid crystal. Liquid crystals do not emit light directly, instead uses a backlight or reflector to produce letters or monochrome. It's called "liquid crystal display" because these compounds have crystalline arrangement of molecule and still they flow like a liquid .In LCD flat panel display two glass plates, each containing a light polarized at right angle to the other, sandwich a liquid crystal material. Rows of horizontal transparent conductors are built into one glass page and columns of vertical conductors are put into the other plate.

Figure 9: LCD display

4. SIMULATION RESULTS

Simulation results showing the model for a block-chain based e-voting system. The proposed model is capable of handling electronic ballots with multiple scopes. This caters for the integrity of an election process in terms of functional and non-functional requirements. This function requirement is embedded in the design of proposed system warrant well. Secured identification and authentication process for the voter. As a result this given the most important requirements for correctness, robustness, coherence, consistency and security. This simulation result verifies the robustness, coherence, consistency and security.

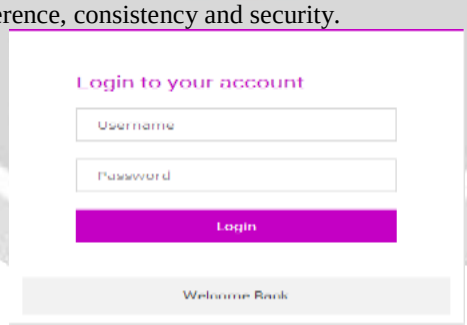

Figure 10 Blockchain Secure Voting System

Figure 11 Simulation Results for Counting Votes

5. CONCLUSION

The block chain, that allows only addition of data and not modification of data. This is effectively allows all users are conduct data authentication. The bilinear pair for low encryption/decryption which reduces the data storage in the corresponding nodes. Thus the anonymous voting system has achieved.

REFERENCES

[1] Peter Y.A Ryan, Steve Schneider, and Vanessa Teague, "End-to-end verifiability in voting systems, from theory to practice", IEEE Security and Privacy2015; vol.13(3): pp. 59-62.

[2] Xiang Yang Chao Liang, Miao Zhao, Hong WeiWang, Hao Ding, Yong Liu, Yang Li, and JulianZhan, "Collaborative filtering-based recommendation of online social voting," IEEE Transactions on Computational Social System 2017;Vol.4(1):pp. 1-13.

[3] Bengi Aygun, and Alexander M. Wyglinski, "A voting-based distributed cooperative spectrum sensing strategy for connected vehicles," IEEE Transactions on Computational Social System 2016;Vol.66(6), pp.109.

[4] Saber Salehkaleybar, Arsalan Sharif-Nassab, and S.Jamaloddin Golestani, "Distributed voting/ranking with optimal number of states per node, "IEEE Transaction on signal and Information Processing over Networks 2015; vol.1(4), pp. 259-267.

[5] Qiang Liu, Hailin Zhang, "Weighted voting system with unreliable links," IEEE Transactions on Reliability 2017; vol.66(2), pp. 339-350.

Authors Biography (Mandatory)

Kowsalya P, is a Assistant Professor, Department of ECE in Info Institute of Technology/ Anna University. She completed her BE in ECE department at Anna University of Technology. She completed her M.E in VLSI design department at Info Institute of Engineering. Her are of interest is electronic devices, communication systems,VLSI Design.

Authors Biography (Mandatory)

Dr.Amutha A, is a Professor and Head of the department, Department of ECE in Info Institute of Engineering/ Anna University. She completed her BE in department ECE at P.S.N.A college of Engineering and Technology. She completed her M.E in Applied Electronics at K.S.Rangasamy College of Technology. Her research interests are nanoscience, image processing,networks.