Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 8, July 2021: 3199-3204

Research Article

An Enhanced Security Mechanism For Voting System To Prevent Election Data Tampering Using Iot And Blockchain

Ms.S.RADHIKA[1], Ms.M.YUVARANI[2], Mr.C.MATHIYALAGAN[3],Ms.M.ELAKKIYA[4]*

[1,2,3]Assistant Professor,Department of EEE,Builders Engineering College,Tirupur,Tamilnadu
[4]*Assistant Professor, Department of EEE, Velalar college of Engineering and Technology,Erode, Tamilnadu.

Abstract

The victory of any democracy depends on the justice of its elections. Building a confined voting system that maintains isolation of votes while still given that plainness to the voters has been a valiant for an extremely long time. The modern enhance in malpractices such as EVM tampering and booth capturing has raised questions about the truthfulness of the election progression. In spite of the claimed income of e-voting initiatives, wider gratitude of e-voting mechanisms and achievement processes is slower than predictable. By developing a secure electronic voting system that offers the fairness and privacy which also provide transparency and flexibility. Amongst them the assessment and organization of e-voting systems, given varied authorized and legal frameworks is still an important contract with to conquer. Blockchain ability originates from the primary architectural sketch of the crypto currency bitcoin. With the use of block chains a confined and hard system for digital voting can be devised. The paper presents in wisdom valuation of the scheme which successfully demonstrates its usefulness to appreciate an end-to-end provable e-voting scheme.

Keywords: Blockchain, PHP, Data tampering, e-voting

I. INTRODUCTION

Voters can give their vote from remote location with the help of some smart devices like smart-phones; tablet etc…to find out the best suitable candidate in an organization, country or university. The movement from paper based voting system to electronic system brings new enhancement such as real time counting ,instant result, environment friendly, transparent, less error and decentralized. With the development in the digital voting system there a number of security issues and attacks are coming. In any electronic voting system the authentication, accuracy, consistency and verifiability are the basic system requirements.

The Protection can be given by these two techniques Blockchain and IoT which uses a database to prevent data tampering in the electronic voting system. If any tamper happens it will give indication to the responsible authorities. This database can be written in any of the Programming Language.

E-voting systems will be beneficial to all people who are involved in elections in addition ideal e-voting systems have transparency, completeness(only voters have the right to vote and their votes are correctly counted),and verifiability then a better solution is required.

II. RELATED WORK

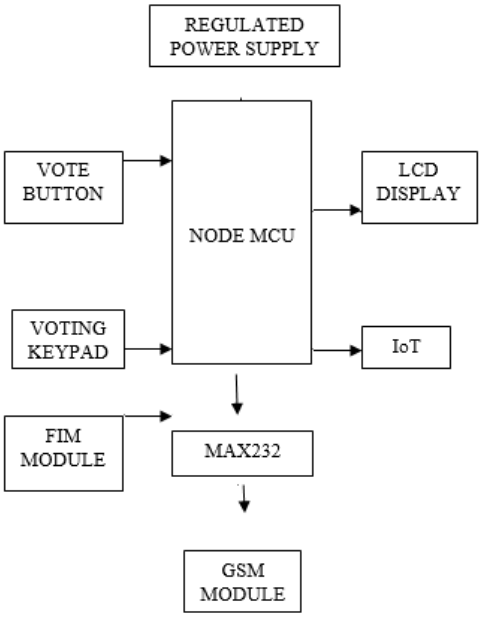
A. Present System

Electronic Voting mechanism is a effortless electronic mechanism used to confirmation votes in place of papers and boxes which were worn earlier in predictable voting system. There have been common studies on by computer technologies to obtain better elections. Although there has been cryptographic explore on electronic voting and there are unique approaches such as voter demonstrable assessment trail. A demonstrable review follow does not, by itself, address voter separation concerns or common other bother on elections. It has been the subject of lively research for decades with the objective to reduce the cost of running an voting while ensuring the election honesty by fulfilling the safety, retreat and observance requirements. Smart contracts are programmable contracts that regularly perform when pre-defined conditions are met. It offers some opportunities to organize a safe e-voting system in some association or country.

B. Drawbacks

- Vulnerability
- It is not secure
- Votes can be tampered
- Reliability is less

III. PROPOSED SYSTEM



The Regulated Power Supply is used to run the Node MCU. It is a low cost open source IoT platform and also a development board, firmware based in the widely used ESP8266-12E WiFi module. The

button is designed for single purpose, internet enabled functions. When the button is pressed a connection is made to a web server which will perform the desired task. ”Blocks” on the block chain are made up of digital pieces of information and stored in the database. FIM Module 3030 is a standalone Fingerprint identification module composed of optic sensor and processing board.PHP is a server side scripting language designed for web development and also used as general purpose programming language.

A. BLOCKCHAIN TECHNOLOGY

Blockchain is literally just a chain of blocks. When we say the words “block” and “chain” in this context, we are actually talking about digital information (the “block”) stored in a public database (the “chain”).

A single block on the block chain can actually store up to 1 MB of data. Depending on the size of the transactions, that means a single block can house a few thousand transactions under one roof.

Their computer receive a copy of the block chain that is updated automatically whenever a new block is added, sort of like a Facebook News Feed that live updates whenever a new status is posted.

B. INTERNET OF THINGS

The Internet of Things is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators and network connectivity which enable these objects to connect and exchange data. Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing internet infrastructure.

The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer based systems and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities.

APPLICATIONS

The ability to network embedded devices with limited CPU, memory and power resources means that IoT finds applications in nearly every field. Such systems could be in charge of collecting information in settings ranging from natural ecosystems to buildings and factories, thereby finding applications in fields of environmental sensing and urban planning.

C. PHP

The proposed system that is going to be described in this phase is done using the PHP database.PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language.

IV. METHODOLOGY

This paper consists of the following parts

A. NodeMCU ESP8266-12E

FEATURES

- Microcontoller : ESP-8266 32-bit
- Clock Speed : 80 MHz
- USB Converter : CP102
- USB Connector : Micro USB
- Operating Voltage : 3.3 V
- Hardware serial ports: 1
- Digital I/O : 11
- PWM I/O with digital: 10
- Analog inputs : 1(10-bit)
- Flash Memory : 4 MB
- Instruction RAM : 64 KB
- Data RAM : 96 KB
- Communications : Serial,SPI,I2C and 1-Wire via software libraries
- WiFi : Built-in 802.11

Besides adding WiFi capability, the main claim fame for the ESP8266 processor over the AVR processor of the standard Arduino that it has a larger 4 MB of Flash Memory and runs at clock speeds of 80 MHz and can sometimes optionally be over clocked to 160 MHz and therefore has a very fast processing speed.

B. FINGERPRINT SENSOR

FIM Module 3030 is a stand-alone fingerprint

Identification module composed of optic sensor and processing board. With high speed CPU and optimized fingerprint Algorithm.FIM 3030 module series boosts high identification rate and supports high speed 1:N identification, upload ability and download ability of data, providing optimal condition for application to access control system, door lock.

FIM 3030 Module has function of fingerprint enrolment, identification partial and entire deletion and reset in a single board, it does not require connection with a separate PC, thereby offering convenient development environment.

Special Features

- Built-in fingerprint identification function
- Provides the minimum recognition time through optimized fingerprint technology
- Excellent weak, dry and wet fingerprint recognition

- Storage of verification log (2,000ea)
- RS-232 Serial Interface
- RoHS
- Sensor Cable : FPCB

C. LCD DISPLAY

A Liquid-Crystal Display (LCD) is a flat-panel display or other electronically modulated optical device that uses the light-modulating properties of liquid crystals. Liquid crystals do not emit light directly, instead using a backlight or reflector to produce images in color or monochrome. LCDs are available to display arbitrary images(as in a general purpose computer display)or fixed images with low information content, which can be displayed or hidden, such as preset words ,digits, and 7-segment displays, as in a digital clock.

D. WiFi Module

The ESP8266 integrates 802.11 b/g/n HT40 Wi-Fi transceiver so it can not only connect to a WiFi network and interact with the internet but it can also set up a network of its own allowing other devices to connect directly to it. This makes the ESP8266 Node MCU even more versatile.

E. Memory

It has 128 kB of internal RAM and 4 MB of flash memory used for program and data storage just enough to handle with the large strings that make up web pages, XML data and everything we throw at IoT devices.

F. Serial Communication

- The board includes CP2102 USB-to-UART Bridge Controller which converts USB signal to serial and allows your computer to program and communicate with the ESP8266 chip.
- Its communication speed is 4.5 Mbps.
- Flow Control Support.

CONCLUSION

Inspite of technology development there is still a data tampering threat in the elections but it can be solved by using this block chain technology in a proper way also it is highly secure. It prevents all sorts of misusage. It can be easily interfaced. Blockchain technology enables safety and cost proficient election. It’s possible to send hundreds of transaction per second on to the block chain which utilize everything. Also it has a fingerprint reader which ensures that one person cannot vote additional than once. It stores every data and monitored by the responsible authorities.

REFERENCES

1. Lijun Wu,Kun Meng,Shou Xu,Shuqin Li Meng Ding, and Yanfeng Suo. Democratic Centralism: A hybridnblockchain architecture and its applications in energy internet. In Energy Internet(ICEI), IEEE International Conference,IEEE,2017.
2. Rifa Hanifatunnisa and Budi Rahardjo.Blockchain based e-voting recording system design. In Telecommunication System Services and Applications(TSSA),2017 11th International Conference,IEEE,2017.
3. Hiroki Watanabe,Shigeru Fujimura,Atushi Nakadira,Yasuhiko Miyazaki,Akihito Akutsu and Jay Junichi Kishigami.

Blockchain contract: A complete consensus using blockchain.In Consumer Electronics(GCCE),4th Global Conference,IEEE 2015.

4. Ashish Singh,Kakali Chatterjee ,"SecEVS:Secure Electronic Voting system using Blockchain Technology" International Conference on Computing,Power and Communication Technologies(GUCON),2018.
5. Fridrik,P.Hjalmarsson,Gunnlaugur,Mohammad Hamdaqa,Gisli,"Blockchain based E-Voting System" International Conference on Computing,2018
6. J Alex Halderman and Vanessa Teague. The new south wales ivote system: Security failures and Verification flaws in a live online election.In International Conference on E-voting and Identity,2015.
7. Yi Liu and Qi Wang. An e-voting protocol based on blockchain.
8. Stefano Bistarelli,Marco Mantilacci,Paolo Santancini, and Francesco Santini.An end to end voting system based on bitcoin.In proceedings of the symposium on applied computing,2017.
9. Douglas W Jones.Threats to voting systems.In NIST workshop on threats to voting systems,2005.
10. Kibin Lee, Joshua I James,Tekachew Gobena Ejeta and Hyoung Joong kim.Electronic voting service using blockchain,2016.
11. Shajan Joseph, A Rajaram, "A Novel Enhanced SVM cluster based secure and effective routing protocol for node authentication in Mobile Ad Hoc Networks," International Journal of Computer Technology and Applications (IJCTA), 10(19): 25-39, 2017.
12. Premanand, R.P., Rajaram, A. Enhanced data accuracy based PATH discovery using backing routeselectionalgorithm in MANET. Peer-to-Peer Netw. Appl. 13, 2089–2098 (2020).https://doi.org/10.1007/s12083-019-00824-1
13. Rajaram.A., Dr.S.Palaniswami . Malicious Node Detection System for Mobile Ad hoc Networks. (IJCSIT)International Journal of Computer Science and Information Technologies, Vol. 1 (2) , 2010, 77-85
14. Dr.S.Palaniswami, Ayyasamy Rajaram. An Enhanced Distributed Certificate Authority Scheme for Authentication in Mobile Ad hoc Networks. The International Arab Journal of Information Technology (IAJIT).vol.9 (3),291-298.