SMART BLOCKCHAIN AND IOT BASED COUPLED SECURITY MECHANISM FOR VOTING SYSTEMS TO PREVENT ELECTION DATA TAMPERING

Abstract

The alleged advantages of electronic voting initiatives, their wider adoption, and implementation methods that are taking longer than anticipated are briefly discussed in this study. The venerability and usability of the electronic voting system are hampered by a number of technological, social, and cultural issues. Given the various legal and regulatory platforms, one of them is the evaluation and standardization of e-voting systems, which remains a significant obstacle to be overcome. This subject has only been briefly discussed in the literature on electronic voting. We also used bilinear pairing to establish the security of the network mechanism; bilinear pairing possesses the benefit of low both encryption and decryption volume of data, which lowers the volume of information kept in nodes. This proposal effectively created a block chain-based network authentication system for voting mechanisms. In addition, more features like ranking and ballot counting will enhance the efficiency of counting votes and support electronic voting systems.

Keywords: : Block Chain, Node MCU, Web Server, IoT, e-Voting.

Authors

R. Karuppusamy
Assistant Professor
Department of Electronics and Communication Engineering
Hindusthan Institute of Technology
Coimbatore, Tamil Nadu, India.

A. Abdul Hayum
Assistant Professor
Department of Electronics and Communication Engineering
Hindusthan Institute of Technology
Coimbatore, Tamil Nadu, India.

A. Vidhyasekar
Assistant Professor
Department of Electronics and Communication Engineering
Hindusthan Institute of Technology
Coimbatore,Tamil Nadu, India.

B. Paulchamy
Professor and Head
Department of Electronics and Communication Engineering
Hindusthan Institute of Technology
Coimbatore, Tamil Nadu, India.

B. Hakkem
Assistant Professor
Department of Electronics and Communication Engineering
Hindusthan Institute of Technology
Coimbatore,Tamil Nadu, India.

Copyright © 2024 Authors

I. INTRODUCTION

The application of information and communication technology (ICT) in democratic and governance procedures is known as "e-voting," a combination of the words "democracy" and "electronic." It is also referred to as "internet democracy" or "digital democracy." ICTs (information and communication technologies) have recently had a significant impact on the daily lives of billions of people. ICT was generally expected to have an impact on democratic processes and public elections at the beginning of the twenty-first century, as part of what has come to be known as the "e-voting system." However, security problems that could have compromised the outcome of the elections have been reported. E-voting is undoubtedly a multidimensional field that involves a complex interplay of technical as well as nontechnical difficulties that frequently revolve around the issue of security systems. The need to concurrently satisfy the opposing needs of integrity and privacy. Given that the legitimacy of democracy is seen as the primary result of voting procedures, attacks and cheating that might prove exceedingly difficult to undo after elections are over must be avoided. the existence of an easily verifiable, straightforward, understandable, and practical traditional voting method. devices used by voters, 25–35% of which could be contaminated with malware.

Employing block chain technology, this study has created a system for voting with safety features. All transaction's details are kept in each node, eliminating the need for a central database to store data about transactions. Additionally, the block chains strictly allow the addition of facts and do not permit the alteration of original data. Instead, they use a distributed ledger model that supports any type of transactions via P2P architecture. The block chains have a number of benefits, including [1] they adopt a distributed framework that stores data in various nodes; [2] every node can jointly keep the public record so that other nodes continue to replicate and make use of it if any node's ledger is never lost; and [3] the block chains make use of cryptography techniques, such as hash technology and elliptic curve cryptography, to guarantee network security.

In addition to preventing system shutdown, our suggested block chain-based voting method also enables any user to carry out voting authentication. We hope that the in-depth analysis and final suggestions can serve as a helpful resource of information for authorities as well as scholars in order to set up an appropriate range of implementation for voting and eventually contribute to a reliable and protocol zed expansion of electronic voting systems. In this paper, we aim to contribute to this understudied the topic through implementing the aforementioned practical assessment framework to an e-voting.

II. RELATED WORKS AND CRYPTOGRAPHIC FOUNDATIONS

Related Works: Bräunlich, Grimm, and Richter in 2013 [20], where the authors proposed the first multidisciplinary partnership to convert legal demands into technical standards and which had previously been applied for various fields such as smart devices. With our suggested plan, it will be easier to count ballots for electronic voting while also saving time. Therefore, it is essential to upgrade network security in the voting process and replace conventional voting with it.

This paper suggests a network security mechanism for electronic voting systems that employs block chain technology to improve visibility and impartiality. The system uses a

Copyright © 2024 Authors

number of weighted states, each of which is used to determine whether a vote was successful or unsuccessful when it surpasses the default value.

III. THE PROPOSED SCHEME

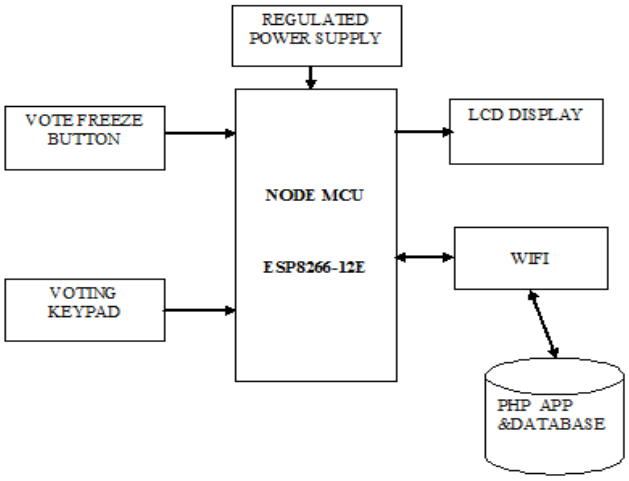

Figure 1: Block Diagram of Proposed Method

The step-down transformer supplies power to the node. In most cases, we use a 230v, 50 Hz power supply, however it needs to be altered in order to give the device the necessary power supply. The step-down transformer converts 230v AC to 12v AC (12VRMS while the peak is approximately 17V). whereas a 5V DC power supply is needed. The rectifier is used to convert AC to DC. Here, AC is converted to DC using a bridge rectifier.

A bridge rectifier is made up of four diodes coupled in a bridge-like fashion. Diodes D2 and D4 conduct during the positive half cycle, and diodes D1 and D3 conduct during the negative half cycle. As a result, AC gets changed into DC. Since the DC that was produced in this case contained pulses, it was referred to as pulsing DC power. Given that the voltage drop across the diodes is 1.4V, the rectifier circuit's output voltage peak is 15V. For the purpose of eliminating ripples, the pulsating direct current is filtered by a resistor capacitor-coupled filter. Thus, the capacitor's charging and discharging will convert the pulsing DC to pure DC. Additionally, the voltage is sent to voltage regulator IC7805 so that it can step down 15V to 5V dc.

The Node MCU receives the stepped-down power. The 16*2 LCD display (I2C LCD display) and push buttons are both attached to the node. It is possible to employ digital or the I2C protocol communication. In this case, the LCD display is connected to the module using I2C communication. The ESP8266 has been linked to an I2C LCD display.

The four The I2C interface lines are linked to SDL, SCL, VCC, and GND, which together make up 3.3V. The module's D2 pin is connected to the module's SDL pin, which is linked to the I2C lcd's SCL wire. The push button wires are linked to pins D5, D6, and D7. The candidates' votes are registered using these push buttons. After verification, the voter may express their preference by depressing the pushbuttons attached to the modules. They

Copyright © 2024 Authors

voted for candidate A, B, or C, respectively. Voters can verify that they voted by reading the displays thank-you note once the ballot has been correctly recorded. The polling station officer can end the voting period by pushing the ballot freeze button after the election is over. The node module keeps track of the votes given to each contender. The officers can access the web page created to view the total votes received for each candidate immediately after voting ends.

The website page is loaded with the module's data. The page is accessible via the link, and all data is transferred via serial communication via the cluster MCU IoT module.
Through the use of this IoT module, the unique URL link is obtained. We can access this information at any moment using this URL.
The URL of the server for the proposed methodology is
http://contraptions.in/_iot_blockchain_voting/

Our data is maintained in a secure manner using this cloud storage. The user may input their information and password whenever the web page is opened by clicking this link. After this connection setup, a web page can be accessed via a WiFi hotspot linked to the module. The originally created database and the damaged database are both included on the web page. The corrupted database aids in locating the damaged block of the vote so that it can be changed.

The original database is compared to the corrupted one to determine the difference. As a result, since the hashing algorithm is being used, any modification in a block will cause the algorithm code to be modified in every block, making it possible for the user to determine which block the data was recently altered. So, the votes are still in a fairly solid position.

IV. RESULT AND DISCUSSION

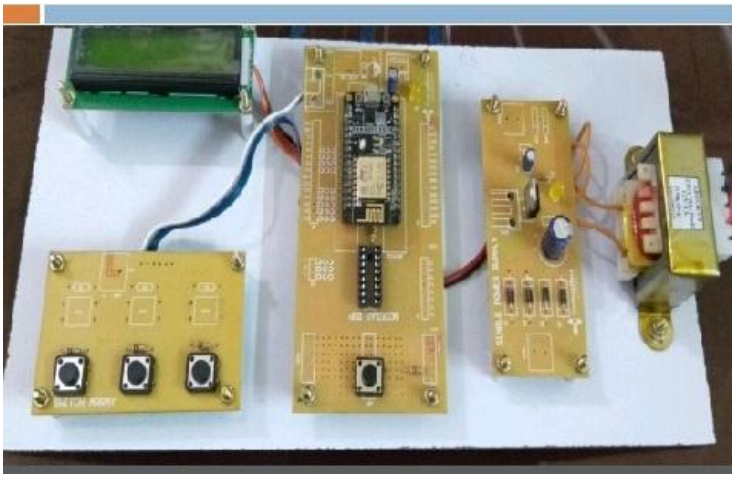

Figure 2: Hardware

Copyright © 2024 Authors

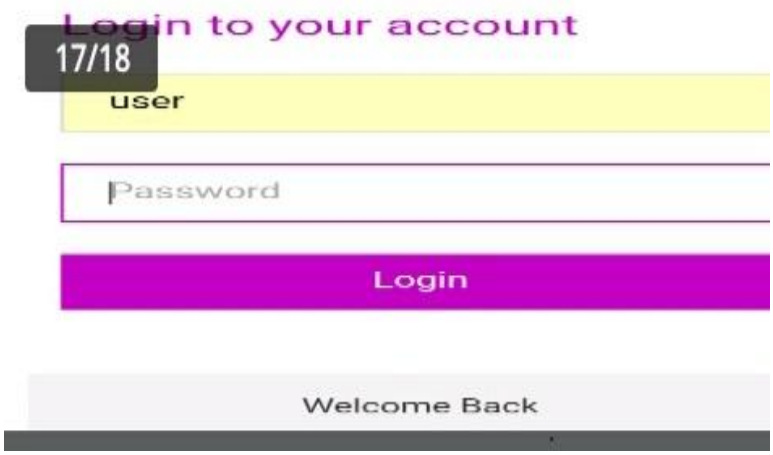

Figure 3: Webpage link

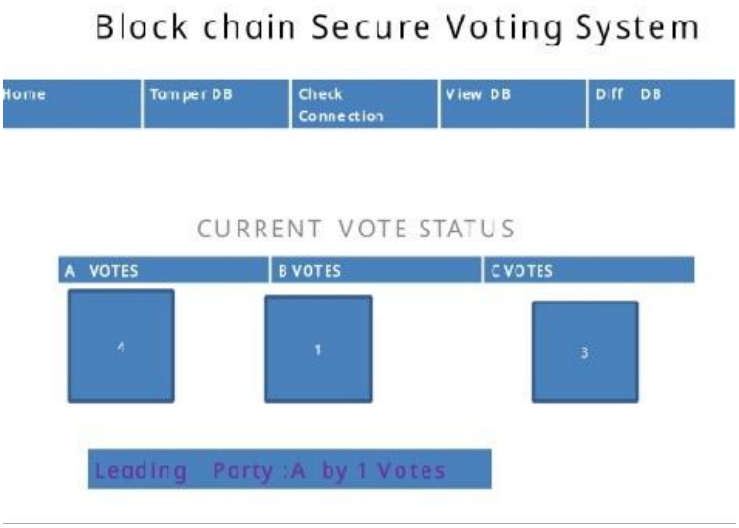

Figure 4: Output of the Developed Prototype

V. CONCLUSION

We used bilinear pairing to establish the network security mechanism as part of this project, which was successful in developing a block chain-based network security system to protect electoral systems. Bilinear pairing has the benefit of low both encryption and decryption data volume, which lowers the volume of stored data in specific nodes. Additionally, additional elements like ranking and ballot counting will enhance the efficiency of vote counting and support electronic voting systems. The future possibilities and process of further advances for the aforementioned technology, such as the one created in this project, are only limited by the imagination. An alternative course of action that can be taken to enhance the system created in this project. E-voting would become more effective with the addition of biometric information, eliminating corruption by a third intermediary person.

Copyright © 2024 Authors

REFERENCES

[1] Drew Springall et al., "Security Analysis of the Estonian Internet Voting System," CCS'14, November 3–7, 2014, Scottsdale, Arizona, USA.
[2] U. S. V. Foundation, "The Future of Voting," 2015. [Online]. Available: https://www.usvotefoundation.org/e2e- viv/summary.
[3] "The FREAK Attack," 2015. [Online]. Available: https://censys.io/blog/freak.
[4] David Adrian et al., "Imperfect Forward Secrecy: How Diffie Hellman Fails in Practice," Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security October 2015.
[5] X. Wang and H. Yu, "How to Break MD5 and Other Hash Functions," Annual International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2005: Advances in Cryptology – EUROCRYPT 2005 pp 19-35S.
[6] Shafi Goldwasser and Yael Tauman Kala, On the (In) security of the Fiat-Shamir Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS'03) 0272-5428/03 $17.00 © 2003
[7] Dirk Achenbach, et.al, "Improved Coercion Resistant Electronic Elections through Deniable Re- Voting," USENIX Journal of Election Technology and Systems (JETS) Volume 3, Number 2 August 2015

Copyright © 2024 Authors