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

R.Karuppusamy**1** A.Abdul Hayum2 A.Vidhyasekar**3** B.Paulchamy4

Assistant Professor, Department of Electronics and Communication Engineering1,2,3

Professor and Head, Department of Electronics and Communication Engineering4

Hindusthan Institute of Technology, Coimbatore - 641 032, Tamil Nadu, India**1, 2, 3, 4**

Corresponding author mail id: aabdulhayum@gmail.com

**ABSTRACT:**

 In this paper brief the claimed benefits of e-voting initiatives, wider adoption of e-voting mechanisms and implementation processes is slower than expected. Several technical, social, and cultural challenges hinder venerability and applicability of e-voting system. Amongst them, the evaluation and harmonization of e-voting systems, given different legal and statutory frameworks, is still an important challenge to overcome. Only a few works have addressed this topic in the field of e-voting. This proposed successfully developed a block chain-based network security mechanism for voting systems we have also employed bilinear pairing in establishing the network security mechanism; bilinear pairing has the advantage of low encryption and decryption data volume, which reduces volume of stored data in nodes. Additionally, added mechanisms such as ballot counting and ranking to our scheme and improve the speed of vote counting and complement electronic voting systems.

**Key Note**: Block Chain, Node MCU, Web Server, IoT, e-Voting.

**1. INTRODUCTION**

 E-voting (a combination of the words democracy and electronic), also known as internet democracy or digital democracy, is the use of information and communication technology (ICT) in political and governance processes The Information and Communication Technologies (ICT) have had a huge impact in the day by day lives of billions of citizens in recent years. In the early 2000s, it was widely anticipated that ICT would also influence public elections and democratic processes, an integral part of what has been labelled e-voting system. Nonetheless, security flaws have been reported, which might have jeopardized elections’ results certainly, e-voting is a multifaceted discipline that needs to take into account a complex combination of technical and nontechnical issues that often evolve around the topic of security system. The need to fulfil simultaneously two antagonistic properties: integrity and privacy. The consideration of democracy’s legitimacy as the main outcome of electoral processes, which results in the need of preventing any potential attacks and frauds that could be very difficult to revert once elections are over. The existence of a traditional voting system which is reasonably verifiable, simple, intuitive, and functional. Voters’ devices, of which 25-35% may be infected by malware technology,

This study has developed a voting system with network security mechanism using block chain technology. The block chains adopt a distributed ledgers model that allow for any form of transaction via P2P architecture; every transaction’s details are stored in each node so the block chains do not require a centralized database for transaction data storage, and the block chains only allow addition of information and not modification of original data. The block chains enjoy the following features: [1] they adopt a distributed architecture that store data in different nodes; [2] all the nodes jointly maintain the public ledger so that if any node’s ledger is ever lost, other nodes can still replicate and use it; and [3] the block chains employ cryptography techniques including hash technology and elliptic curve cryptography to ensure network security.

Our proposed block chain-based voting system not only prevents system shutdown, but also enables any user to conduct voting authentication. In this paper we aim at contributing to this unexplored topic by applying the aforementioned practical evaluation framework to a e-voting, We hope that the thorough analysis and the final recommendations can become a relevant source of information for officials and researchers in order to establish a safe range of implementation for Voting and ultimately contribute to a secure and protocol zed expansion of e-voting systems.

**2. RELATED WORKS AND CRYPTOGRAPHIC FOUNDATIONS**

**2.1 Related Works**

 One of the most relevant Bräunlich, Grimm and Richter in 2013 [20], in which the authors presented the first interdisciplinary collaboration to transform legal requirements into technical criteria and which had been previously used for other sectors such as smart devices. Our proposed scheme can effectively reduce time complexity in counting ballots for e-voting. Hence, it is imperative to replace traditional voting with electronic voting and enhance network security in electronic voting.

This study proposes a voting system network security mechanism based on block chain technology that improves transparency and impartiality in electronic voting system. It utilizes several states, each one weighted, so that when the weighted value is exceeds the default value, the system deems the voting a failure

**3. THE PROPOSED SCHEME**

****

**Figure 1: Block Diagram of Proposed Method**

The power to node is provided by the step down transformer. In general we use the power supply of 230v ,50 Hz but it has to be changed to provide the required power supply to the device.230v AC is converted to 12v AC(12VRMS where the peak is around 17V) using the step down transformer. Whereas the required power supply being 5V DC .To converts AC to DC we use rectifier. Here bridge rectifier is used to convert AC to DC.

Bridge rectifier consists of 4 diodes which are connected in the form of bridge. During positive half cycle, diodes D2 and D4 conduct and during negative half cycle diodes D1 and D3 conduct. Thus AC is converted into DC. Here the obtained DC is not pure as it contains pulses, hence called pulsating DC power. Whereas the voltage drop across the diodes is 1.4V, therefore the peak voltage at the output of the rectifier circuit is 15V.This pulsating DC is filtered using resistor capacitor –coupled filter for removing the ripples. Thus the charging and discharging of the capacitor will make the pulsating DC to pure DC. Further the voltage is given to voltage regulator IC7805 for 15V to be stepped down to 5V dc.

The stepped down power is supplied to the Node MCU. The node is connected to the push buttons and 16\*2 LCD display (I2C LCD display). Either I2C communication or digital communication can be used. Here we have used the I2C communication to connect the LCD display to the module .the I2C lcd display is connected to ESP8266.

The four wires in the I2C are connected to SDL, SCL, VCC, GND which comprises of 3.3V. the wire from SCL in I2C lcd is connected to the pin D1 of the ESP8266,and the pin from SDL is connected to D2 in the module. To the pins D5, D6, D7 the wires from the push buttons are connected. These push buttons are used to register the candidates vote. after checking the candidate is allowed to cast their votes by pressing the push buttons connected to the modules. They cast their vote either to the candidate A, B or C .when their vote has been casted successfully the voters can notify that the they voted by the thank you description in the display. After the completion of the election the officer in the polling booth can close the voting session by pressing the vote freeze button. The vote casted to each candidate is registered in the node module. The total votes delivered to each candidate can be viewed immediately or after the completion of the election by the officers through the web page developed.

The data’s from the module are loaded to the web page. The user can access the page using the link these entire data’s are sent to the node MCU IoT module by using serial communication.

The separate URL link is getting by using this IoT module. Using this link we can view those data’s at anytime and anywhere.

The URL of the server for the proposed methodology is

“http://contraptions.in/\_iot\_blockchain\_voting/”

 This cloud storage is used for maintaining our data’s in a secured manner. When the page is opened through this link the user is allowed to enter the user name and password provided to them. Wifi hotspot is connected to the module after this connection setup the web page can be accessed .the web page comprises of the original database and the corrupted database. The corrupted data base helps to find the block where the vote has been corrupted thus it can be modified.

The difference is identified by the original database against the corrupted one. Thus the data can’t be corrupted any occasion as the hash algorithm is used thus any change in block will change the algorithm code in every block which makes the user to identify in which block the data has been corrupted. Thus the votes remain very much secured.

 **4. RESULT AND DISCUSSION:**



**Figure 2: Hardware**



**Figure 3: Webpage link**



**Figure 4: Output of the Developed Prototype**

**5. CONCLUSION**

 This project successfully developed a block chain-based network security mechanism for voting systems we have also employed bilinear pairing in establishing the network security mechanism; bilinear pairing has the advantage of low encryption and decryption data volume, which reduces volume of stored data in particular nodes. Additionally, added mechanisms such as ballot counting and ranking to our scheme and improve the speed of vote counting and complement electronic voting systems. For the above device such as the one developed in this project only the sky is the limit with regards to its future potential and further advancements process. A different path that can be followed to improve the system developed in this project. Addition of the biometric details would make the e voting an efficient thus preventing the corruption by the third intermediate person.

**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