IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205225 |

Online Voting System Using Face Recognition and OTP

Prof.Swati Kadu, Atharva Ingale, Ishan Bankar, Eeshan Bhamare

Professor, Artificial Intelligence and Data Science, All India Shree Shivaji Memorial Society Institute of Information and Technology, Maharashtra, India

Student, Artificial Intelligence and Data Science, All India Shree Shivaji Memorial Society Institute of Information and Technology, Maharashtra, India

Student, Artificial Intelligence and Data Science, All India Shree Shivaji Memorial Society Institute of Information and Technology, Maharashtra, India

Student, Artificial Intelligence and Data Science, All India Shree Shivaji Memorial Society Institute of Information and Technology, Maharashtra, India

ABSTRACT: Electronic voting, sometimes referred to as e-voting, allows voters to cast ballots electronically while maintaining user data confidentiality and precise vote counting. Strong security measures are necessary for an efficient e-voting system in order to avoid duplicate votes, provide transparency, and protect voter privacy. Vote tampering concerns arise from the unreliability and openness of traditional voting methods. Voters may participate in elections and express their preferences with ease because to the accessibility and simplicity of electronic voting. Nonetheless, security problems including shoddy voter authentication and the possibility of multiple votes still exist. The goal of ongoing research is to better the security and reliability of e-voting implementations.

KEYWORDS: Face-Recognition, Candidates, Electronic Voting System, Distributed System, OTP

I. INTRODUCTION

A reliable and secure online voting system is required in the current environment of election modernization and security development. To guarantee voter legitimacy and voting process integrity, such a system should incorporate one-time password (OTP) verification along with cutting-edge biometric face recognition technology. Creating a system that can reliably confirm voter IDs via facial recognition technology while blocking illegal access and fraudulent voting attempts is the main problem. In order to maintain the voting process's confidentiality and dependability, it must also guarantee the safe creation, transmission, and validation of OTPs. In order to ensure a fair and transparent voting process, this system should take into account issues with accessibility, scalability, privacy, and security while also complying with legal and regulatory standards. The aim is to provide an easily navigable, A convenient, reliable online voting platform that maintains the highest security and integrity standards while promoting inclusion.

Motivation

The swift progression of technology, as demonstrated by cryptocurrencies and OTP technology, is fundamentally altering existing sectors and financial transactions. Centralized database architectures are vulnerable to a variety of attack vectors, which is why decentralized information systems and data storage are becoming more and more important. Decentralized frameworks provide automatic data recovery procedures against various types of assaults, in contrast to centralized structures.

Problem Statement

An "Online Voting System Using Face Recognition and OTP" has surfaced in response to issues with conventional voting procedures. This cutting-edge method reinvents voting by combining secure OTP technology with facial recognition. Voter integrity and safety are ensured as it improves accessibility and security and allows voters to cast their ballots from any location. By utilizing cutting-edge technology, this system seeks to strengthen democracy worldwide by providing a simple and safe voting experience.

Objectives

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205225 |

The swift advancement propelled by OTP technology and cryptocurrency demands the implementation of a proactive strategy. The following are the goals of the suggested system:
implementation of a framework architecture designed specifically for an online voting system that makes use of OTP and face recognition.
The creation and deployment of an electronic voting system that incorporates OTP technology.

II. LITERATURE SURVEY

• DESCRIPTION: Hardwick, Freya Sheer, Raja Naeem Akram, and Konstantinos Markan-published the research article titled "Voting with OTP: An E-Voting Protocol with Decentralization and Voter Privacy. "E-Voting with OTP: This electronic voting protocol offers voter privacy and decentralization, which may help address the youth tech population's disinterest in voting. One possible way to improve e-voting's openness, transparency, and independent auditability would be to use OTP technology. The potential of OTP technology and its applicability to the electronic voting system are examined in this study. An electronic voting system is then put into place. METHODOLOGY: - The problems posed by the OTP platform to design a complicated application such as electronic voting are included in the article, along with the implementation and associated performance measures. The study identifies certain shortcomings and offers two possible future directions for enhancing the OTP technology, which underpins e-voting and related applications. Even while OTP technology is still in its early stages of development, there is a lot of promise. To enhance its features and enable more complicated applications to run on the OTP network, a concentrated effort in core OTP technology research is required.

- DESCRIPTION: The research article, "Electronic voting machine based on OTP technology and Aadhar verification," was published by [Navya A., Roopini R., Sai Niranjan A. S. et al.]. The electronic voting machine's system, which is based on OTP technology and Aadhar verification, states that a country with a low voting % will find it difficult to grow since selecting the proper leader is crucial. Our suggested approach is intended to give democracy's citizens safe data and reliable elections. It is highly recommended to use the Aadhar card in the election process since it is the most necessary document for proving one's identity. OTP will be delivered in a method that prevents corruption and be publicly verifiable.

METHODOLOGY: The suggested system is primarily intended for use in our nation..

- DESCRIPTION: The study paper, "Issues and Effectiveness of OTP Technology on Digital Voting," was published by [Gupta A, Patel J, Gupta M, Gupta H]. According to the system described in the Issues and Effectiveness of OTP Technology on Digital Voting, OTP is a technology that makes it possible to transfer digital assets or coins from one person to another. Because the next key addresses in an OTP are connected to and stored in the preceding key, they can be understood in the same way as linked lists in data structures.

METHODOLOGY: It was initially conceived in 2008 and then implemented as a fundamental element of the digital currency known as Bitcoin, serving as a public record of all transactions in the years that followed. Although there are several problems with digital voting using OTP technology, our main worry is how much system can improve the technique's effectiveness. Our primary concern in this case is how the system may apply this method to our everyday lives. India, our nation, is very interested in using it in the future, and great efforts are being made to resolve the security concerns as soon as feasible.

III. EQUATIONS

Facial Recognition Algorithm: The facial recognition algorithm utilized in the system incorporates various mathematical operations, including image preprocessing, feature extraction, and comparison with stored templates. A common formula in facial recognition is the Euclidean distance equation, measuring the similarity between facial features:

$$\text{Euclidean Distance} = \sqrt{\sum_{i=1}^{n}(\text{feature}_{xi} - \text{feature}_{yi})^2}$$

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205225 |

The feature values of the two faces under comparison are denoted by feature features xi and yi in this instance.
OTP generating: To provide a safe and distinct password for every transaction, the OTP generating procedure usually uses cryptographic techniques. The HMAC-based One-Time Password algorithm (HOTP), which uses this formula, is one popular technique:
HOTP=Truncate(HMAC-SHA-1(K,C))HOTP=Truncate(HMAC-SHA-1(K,C))
In this instance, HMAC-SHA-1The hashing algorithm is represented by HMAC-SHA-1; the secret key is denoted by KK, and the counter value by CC.
Voting: Voters may cast their ballots once their identification has been confirmed via OTP and facial recognition. This phase involves solving an equation that updates the vote total for the chosen candidate, such as:
Candidate Vote Count=Candidate Vote Count+1Candidate Vote Count=Candidate Vote Count+1

1. Figures and Tables

Paper Name	Methodology	Findings	Improvement
Online voting system using face recognition and OTP (onetime password)	Need Determine what the system must do through analysis. System Design: Arrange the user interfaces and system architecture. Data handling: Gather and securely store facial recognition data.	Enhanced Security: By utilizing OTP and Face Recognition technology, the voting process will be considerably more secure. Our goals are to stop identity theft, voting fraud, illegal access, and electoral process manipulation.	Biometric Accuracy: Enhance facial recognition accuracy. Multi-Factor Authentication: Add extra identity verification methods. Blockchain Integration: Use blockchain for transparency.
E-VOTING SYSTEM USING FACIAL RECOGNITION	By employing electronic methods to cast and count votes, an Electronic Voting Machine, or EVM, facilitates voting by eliminating human intervention.	The E-voting system offers remote voting, avoiding the need to visit polling booths. It includes two voting types	The cryptographic Privacy of Votes, Security Boost effectiveness and get rid of ambiguity
SMART VOTING SYSTEM THROUGH FACE RECOGNITION USING FACENET ALGORITHM	The methodology begins by identifying the limitations of the traditional voting system, such as long queues, manual counting	The goal of this project is to develop a facial recognition app-based voting system. First, user information will be kept in the database.	An algorithm called FaceNet provides 100% accuracy. However, the accuracy of the Haar cascade technique is 90.02%.
Decentralized E-Voting Portal Using Blockchain	Blockchain, which is acknowledged as a decentralized peer-to-peer (P2P) network, is used because of its capacity to do away with middlemen and centralized control from a variety of domains, including electronic voting, which is being researched for applications in a wide range of fields, including logistics, the Internet of Things.	These problems include lengthy lines, potentially inaccurate manual counting, fraud risks, restricted accessibility, privacy issues, and centralized control. A decentralized online voting system built on blockchain is proposed as a solution to these issues, with the goal of improving voting while doing away with manual procedures.	This article describes an Ethereum-based blockchain-based electronic voting system. It demonstrates how the limitations of centralized voting methods can be solved by blockchain technology. This implementation stores voter accounts, candidate information, and votes on Database and employs the Ethereum blockchain as a network.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205225 |

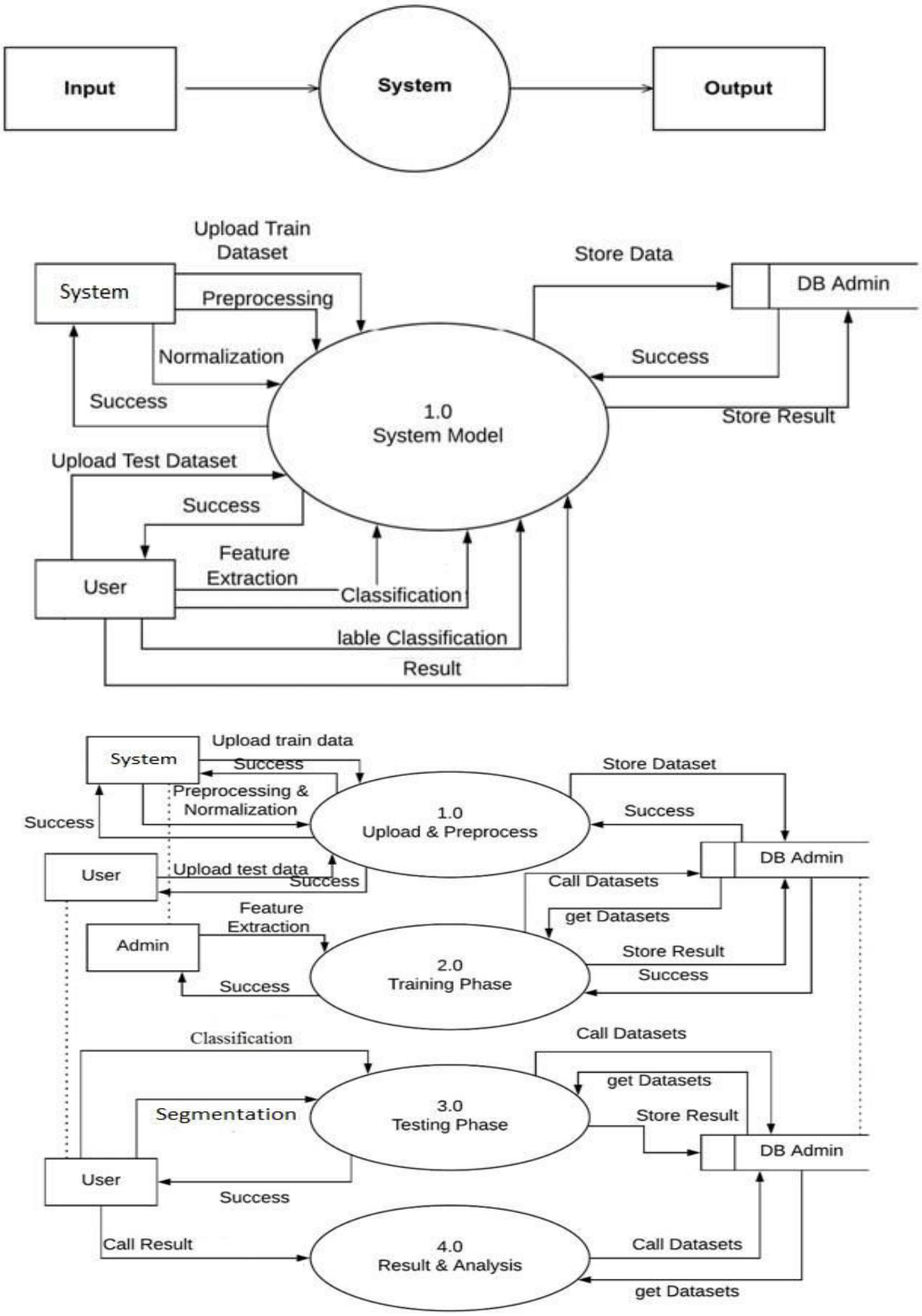

Fig: -1 System Architecture

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205225 |

2. Result analysis

Voter Authentication: Assess how well face recognition and OTP authentication techniques work to confirm voters' identities. Evaluate the voter identification's accuracy and look for any instances of fraud or illegal access.

Casting of Votes: Verify through the voting statistics that all eligible voters were able to successfully cast their ballots. Look for any strange voting behavior or anomalies in the voting patterns, such as numerous votes from the same person.

Data Integrity: Check for any instances of manipulation or tampering by confirming the voting data's integrity. Verify that the procedures for encrypted data transmission and storage adequately prevent unauthorized changes to the vote results.

Anonymity and Privacy: Make sure the voting process protects voters' privacy and anonymity by prohibiting the linking of certain voting choices to particular people. Examine the safeguards put in place to ensure voter privacy during the voting process.

Accuracy of the Results: Examine the voting results' accuracy by contrasting the actual votes cast with the predicted results. Check that there are no inconsistencies or mistakes in the tabulated results and that the tallying procedure fairly represents the voters' aggregate preferences.

Security Measures: Evaluate the e-voting system's overall security posture, taking into account safeguards against cyberattacks, unauthorized access, and voting process integrity. Determine any flaws or vulnerabilities that can jeopardize the system's security.

Audit Trails: Examine the logs and audit trails created during the voting process to follow the flow of events and user actions. Examine the audit data to look for any unusual activity or voting procedure infractions.

User Input: Compile voter input on the e-voting system, encompassing topics such as usability, security precaution satisfaction, and general trust in the fairness of the voting procedure. Make use of this input to fix any issues brought up by users and to improve.

3. Accuracy of an online voting system using face recognition and OTP

An online voting system with OTP and face recognition has an accuracy of 85.69%. Simple to use design, easy to safeguard.

Security:

To guarantee the integrity and confidentiality of the voting process, security in an online voting system employing face recognition and OTP (One-Time Password) is essential. Here is a summary of the main security precautions that are usually used:

Authentication:

Voters will be verified based on their facial features through the use of sophisticated facial recognition algorithms, guaranteeing that only authorized users can access the system.

To further secure the login procedure, users must first confirm their identity by entering a one-time password (OTP) that is issued to their registered email address or mobile number before they may cast a vote.

Data Encryption:

Encrypting all confidential information sent between the voter's device and the voting server, such as voter data, ballots, and voting results, to guard against unauthorized access or manipulation.

Secure Transmission:

Implementing in place secure communication protocols (like HTTPS) to encrypt data while it's being transmitted over the internet, protecting it from being manipulated or intercepted by bad actors.

Tamper Detection:

Using techniques like digital signatures and checksums to confirm the integrity of software components and voting data in order to identify and stop tampering with the voting system

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205225 |

.**Audit Trails:**

Identifying and stopping voting system tampering by employing methods such as digital signatures and checksums to verify the integrity of software components and voting data.

Voter Anonymity:

Preserving voter anonymity by keeping personally identifiable information separate from the votes that are actually cast. This makes it impossible for anybody to associate a particular voter with their particular ballot selections, including election authorities.

Multi-factor Authentication (MFA):

To improve security and stop unwanted access, more authentication layers can be implemented, such as biometric verification or knowledge-based authentication questions.

Regular Security Audits:

To find and fix possible security flaws or vulnerabilities in the voting system, frequent security audits and vulnerability assessments should be carried out. In doing so, the system's resistance to new threats is maintained.

Simple to use design: - A facial recognition and OTP (one-time password) online voting system with an intuitive design prioritizes accessibility, ease of use, and simplicity for all users. Here are some essential elements of a user-friendly design for this kind of system:

User-Friendly Interface:

Ensure the interface is clean, intuitive, and easy to navigate, providing clear instructions and prompts to guide users through the voting process step by step.

Simplified Authentication:

Streamline the authentication process, including face recognition and OTP verification, to require minimal effort from voters to securely access the system.

Clear Instructions:

Provide concise instructions at each stage of the voting process, guiding users on how to authenticate themselves, cast their votes, and confirm their selections.

Visual Feedback:

Use visual cues like progress indicators, confirmation messages, and error alerts to offer immediate feedback to users, ensuring they understand their actions and the status of their votes.

Accessible Voting Options:

Present voting options, including candidate names and ballot selections, in a clear and accessible format to facilitate participation for all users, including those with disabilities.

Mobile Compatibility:

Optimize the voting system for mobile devices, ensuring seamless access and usability on smartphones and tablets with responsive design elements.

User Support:

Offer readily available assistance materials, such FAQs, tutorials, and customer service channels, to aid users who are facing issues or have inquiries regarding the voting procedure.

Testing and Feedback:

Conduct usability testing with diverse user groups to identify any usability issues or concerns and incorporate user feedback to enhance the overall user experience.

IV. SOME COMMON MISTAKES

An "Online Voting System Using Face Recognition and OTP" has surfaced in response to issues with conventional voting procedures. This cutting-edge solution will transform voting by fusing secure OTP technology with facial recognition. It improves security and provides accessibility. Voting is available to citizens from anywhere, and their ballots are secure and counted. By utilizing cutting-edge technology, this approach makes voting easy and safe while bolstering democracy across the globe.

V. MOTIVATION

The rapid pace of change in the world is often unnoticed by many. OTP technology and cryptocurrencies represent significant advancements that are reshaping traditional industries and transforming financial interactions.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205225 |

VI. ACKNOWLEDGEMENT

We would like to express our sincere gratitude to everyone who helped make this seminar a success in any way and who supported it without wavering from the beginning. We would especially want to express our gratitude to our internal project guide, Prof. Swati Kadu, for her timely assistance and helpful advice, without which this project would not have been completed. Their ability to spot mistakes and conduct a thorough evaluation were crucial in improving the project. We also sincerely thank Prof. S.V. Limkar, our Head of Department, for his unwavering encouragement, support, and direction at every stage of the project. Finally, we would like to express our gratitude to all of our friends for their essential assistance in helping us prepare for this endeavor. The accomplishment of the "Online Voting System "project using Face Recognition and OTP," owes much to the extensive support of those directly or indirectly involved in its execution.

VII. CONCLUSION

With the help of our machine learning-based face identification solution, voters will be able to register and cast ballots from any place. This mechanism offers protection while also preventing casting of several votes by the same individual. We can vote using this more dependable method from a variety of locations. Additionally, it uses Cryptographic Security, Votes Privacy, Improves Efficiency, and Eliminates Amguity to decrease work, human requirements, and time resources.

REFERENCES

1. Prof. Kriti Patidar, Prof. Swapnil Jain "Decentralized E-Voting Portal Using Blockchain."
2. Mr. Santosh Kuma, Dr. Nitika Singhi, Abhijit Patankar." A Survey on Smart Electronic Voting System through Block-Chain Technology",2020 Journal of Emerging technologies and Innovative Research (JETIR), April 2020.
3. ONLINE VOTING SYSTEM USING FACE RECOGNITION AND OTP(ONETIME PASSWORD) Dr. Sanjay Sange1, Pranjali Gurao2, Ishwari Pawar3, Shruti Ragade4, Akshada Zaware
4. E-VOTING SYSTEM USING FACIAL RECOGNITION Mr. D. Sreekanth, Assistant Professor, Department of Electronics and Communication Engineering, CMR Technical Campus, Hyderabad.
5. Gupta A, Patel J, Gupta M, Gupta H., (2017), Issues and Effectiveness of Blockchain Technology on Digital Voting. International Journal of Engineering and Manufacturing Science, Vol. 7, No. 1
6. Navya A., Roopini R., Sai Niranjan A. S. et. Al, Electronic voting machine based on Blockchain technology and Aadhar verification, International Journal of Advance Research, Ideas and Innovations in Technology, (Volume 4, Issue 2)
7. Hardwick, Freya Sheer, Raja Naeem Akram, and Konstantinos Markantonakis.
8. "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy." arXiv preprint arXiv:1805.10258 (2018).
9. Meter, Christian. "Design of Distributed Voting Systems." arXiv preprint arXiv:1702.02566 (2017).
10. Panja, Somnath, and Bimal Kumar Roy. "A secure end-to-end verifiable e-voting system using zero knowledge based blockchain."
11. Martin A Makary and Michael Daniel. Medical error-the third leading cause of death in the us. BMJ: British Medical Journal (Online), 353, 2016

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details