iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XI **Month of publication:** November 2023

DOI: https://doi.org/10.22214/ijraset.2023.56932

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XI Nov 2023- Available at www.ijraset.com

A Review of Digital Voting Systems using Aadhar Authentication

Mr. Sanket Kumbhar[1], Mr. Sainath Mohite[2], Mr. Bhushan Dandavate[3], Mr. Hrishikesh Kamble[4], Prof. J. T. Patil[5]
Information Technology, Dr. J.J. Magdum College of Engineering, Jaysingpur.

Abstract: Utilizing India's Aadhar system for secure and effective voter identification, a digital voting system with Aadhar authentication is an electronic voting mechanism. Voters use their Aadhar cards, which are connected to personal and biometric data, to authenticate themselves. With the preservation of data confidentiality and privacy, this system seeks to expedite the voting process, lessen voter fraud, and guarantee correct voter identification.
Keywords: Blockchain, Machine learning, Biometric, Communication.

I. INTRODUCTION

In a world where technology has transformed practically every aspect of our lives, democratic processes are no exception. The integration of technology with the time- honoured institution of voting is a compelling innovation that has the potential to bring in a new age of safe, efficient, and inclusive electoral processes. The Digital Voting System with Aadhar authentication is at the vanguard of this innovation, promising to transform the way we exercise our democratic rights. This thorough review article sets out to investigate the many facets of this transformational notion, from its promises and benefits to the crucial problems and consequences it holds for modern democracies.

Aadhar, India's pioneering biometric identification system, has been praised as one of the world's most ambitious digital endeavours. It was launched in 2009 and has quickly expanded to over a billion registered users, radically changing the way people identify their identities. Aadhar provides each individual a unique 12-digit identity number and secures it with a variety of biometric data, such as fingerprints and iris scans. This large library of personal information is the foundation of Aadhar authentication.

Aadhar's incorporation into the electoral process offers the prospect of a safer, more effective, and inclusive voting procedure. The fundamental idea behind this method is that voters will use their Aadhar cards for biometric verification, which may be used to verify identities and prevent identity fraud while also protecting the integrity of the election process.

A digital voting system that uses Aadhar authentication has several potential advantages. They consist of greater voter identification accuracy, heightened security, expedited administration, and higher voter turnout. But there are several obstacles in the way of putting such a system into place, including worries about cybersecurity, data privacy, and fair access for all residents.

Our goal as we go through this review paper is to assess digital voting systems that use Aadhar authentication seriously as they are right now. In order to illuminate this novel approach's revolutionary potential in electoral processes and its wider implications for democratic government, this research aims to offer a thorough examination of its advantages and disadvantages.

In modern democracies, digital voting systems have the potential to revolutionize the electoral process, making it more efficient, inclusive, and trustworthy. Their importance lies in adapting democratic practices to the realities of the digital era while upholding the core principles of free and fair elections.

A. Digital Voting Technologies

1) *Electronic Voting Machines (EVMs):* Electronic voting machines (EVMs) are electronic devices that are used in polling stations to cast and tally votes during elections. They are intended to take the place of traditional paper ballots and manual vote counting. EVMs have received popular acceptance in a number of nations, most notably India, the United States, and Brazil. To modernize the election process and make it more efficient, accessible, and easy, digital voting technologies have been created. Electronic voting machines (EVMs), internet voting systems, and mobile voting applications are three popular forms of digital voting technology.
2) *Online Voting Systems:* Online voting systems, often known as internet voting, allow residents to vote via the internet, removing the need for them to attend actual polling places. Online voting has grown in popularity in many nations and areas, particularly among rural and foreign voters.
3) *Mobile Voting System:* Mobile voting apps are smartphone applications that allow people to vote via their mobile devices.

©IJRASET: All Rights are Reserved

While mobile voting applications are still in the experimental stage in many places, they offer the potential to boost voter accessibility and engagement.

B. *Basics Of Different Voting Systems*

1) *EVM Based System:* An EVM Based System is one in which we employ a machine to conduct the voting process in India. EVMs are made up of two parts: the control unit and the ballot unit, which are linked by a cable. The control unit is overseen by the polling officer. The ballot unit is where voters casts their ballots. On the day of the election, these units are sealed and immediately unsealed. The main objection levelled regarding EVMs is that they employ internal microprocessors that may be tampered with.
2) *Paper Ballot System:* In this system, voters are given a paper ballot (typically a piece of paper) with the names of all candidates. These paper ballots are available at the polling place. The key drawbacks of such a method are the lengthy time necessary to compute votes, personnel, paper waste, ease of manipulation, and so on.
3) *Head Count Method:* This method is more commonly used in the Upper and Lower Houses of the Indian Parliament to determine the number of members in support of a motion and vice versa. We have a leader who initiates voting and declares the results. It is a model of trust and authority. The members trust the speaker,and the constitution gives him the ability to conduct voting and report results.
4) *Database Approach:* In this case, we have a centralized database that is administered by an authority that has the authority to alter thedatabase. The database is made up of rows and columns. When a voter votes, the relevant candidate's count increases by one. This method allows for vote backtracking.

C. *What is Aadhar?*

Aadhaar is a 12-digit personal unique identification number issued by the UIDAI (Unique Identification Authority of India) on behalf of the Government of India. This number will be used as confirmation of identity and address across the country. Anyone who is a citizen of India who fulfils the UIDAI verification process, regardless of gender or age, can apply for Aadhaar. Aadhaar enrolment is free for everyone. Every Aadhaar number is unique to a person and is valid forlife. In the future, Aadhaar will grant you access to services such as banking, mobile phones, and other government and non-government facilities.

II. RELEVANCE OF WORK

[8] This study provides an attempt to use blockchain featuressuch as encryption and transparency fundamentals to create an effective electronic voting mechanism. The multichain platform was used to implement the specifics of the proposed electronic voting proposal. The system is built in a controlledenvironment with a web-based application written in Java EEand run on the NetBeans platform with a Glassfish server native. MySQL is the database used by the program. The researchers adopted the multichain platform because it was appropriate for cryptocurrencies. [9] In this study, the researchers created a synchronous model for voting records based on distributed ledger techniques, as well as a model forthe user's encoded data using the elliptic curve to provide authentication and non-repudiation, as well as the ability for voters to change their votes before a previously set deadline. The system was built on the Linux (Ubuntu) platform. Each block includes the voter ID, vote, new voter signature, timestamp, and preceding block hash. It is safer and more anonymous when combined with other voting systems since each user uses an identification rather than his genuine identity, and decentralization is done without the involvement of a third party. The findings suggest that the method is secure and practical, and that it addresses the issueof voting fraud during electronic voting. [10] The ring structure is used in this study to provide voter anonymity, while blockchain technology is used to ensure integrity and transparency. To produce the signature, the user must use hisprivate key safely while also entering the public keys of the other ring members for the input algorithm. The amount of anonymity of the voter determines the number of keys chosen. If the chosen group is small, the possibilities of hiding the voter's identity increase significantly. The capacity to examine the voter's rights and anonymity, as well as the voter's ability to check the legitimacy of his vote, are some of the benefits of this technique. [11] The notion of block formation and block sealing is introduced in this study. Its utility is to make the blockchain more customisable; utilizing the consortium blockchain was recommended. [12] The election commission oversees the whole election process. EC stands for Election Commission. The EC creates the election,activates it, and then closes it after a set length of time. During the voting process, the EC watches the entire procedure and releases the results after the election. Another key responsibility of the EC is to compile a voter list before to the election by conducting a voter registration drive. Vi's personal information is stored by EC. In the proposed system, EC is seen as a trustworthy entity that assures the vi's information are tamper resistant. From the polling station to the constituency, the

EC employs various staff (for example, the returning officer, the assistant returning officer, and the presiding officer). In the system, voters can vote in person at a polling centre or online over the internet. To vote online, users must first verify themselves, then load election ballots, vote, and then view the results after the election. However, ifa voter wishes to vote at a polling centre, he or she must provide his or her National Identity (NID) Card and pass the authentication procedure before proceeding with the voting process. The suggested approach secretly inserts the vis into the V U. The authentication unit and the V U are two distinctunits in the voting system. Vis enters the V U completely anonymously. Permission to create a block is given upon authentication. The vi NID number is used to generate a newblock by producing the hash value from the preceding block's hash value. After inserting the vote inside the block, no one can trace back to the individual who created the block. From block construction to vote addition, the vi handles everything in our system; no other entities (e.g., presiding officer, agent, returning officer) are involved. [13] The blockchain-based implementation of an e-voting application. The data held on the Ethereum blockchain is decentralized and safe, and the blockchain code is shared and unchangeable. The Ethereum Blockchain enables us to develop code that can be deployed to the blockchain and executed by nodes on the network. Thecode in this application writes to the decentralized application utilizing the Ethereum blockchain's smart contract protocol. Ethereum allows you to create code and have it executed on the Ethereum virtual computer smart contracts. [13] The program uses Ethereum Blockchain technology as both a network and a decentralized database to store voter accounts, votes, and candidate information. Blockchain offers a decentralized approach that makes the network dependable, secure, versatile, and capable of supporting real-time services. The voter recognizes his vote is going to the correct candidate and that he only has one vote because the program does not allow for multiple votes. Using this strategy, electronic voting might be very reliable.

III. LITERATURE REVIEW

Traditional article-based voting methods or mechanisms may contribute to climate change and forest loss. To address this issue, article-based methods are being replaced with sophisticated e-voting procedures. As a result, in order to establish a secure voting method [1] By removing inbuilt limits, they presented a rank choice e-voting process. Every vote is encrypted using the EL Gamal procedure to ensure itsconfidentiality. Furthermore, proofs are generated upon the storing of each vote, which verifies the counting procedure without decrypting the information. The hypothesized mechanism is validated by comparing experimental findings to known mechanisms. The encryption and decryption of material at each node may raise the network's computational and communicational overhead. Furthermore, in an e-voting system, candidates who cast ballots and submit information must be protected. [2] have presented a crypto-biometric strategy for online voting methods. The palm vein and palmprint are the two-key crypto-biometric approaches suggested by the authors, who employed gabor lter with a threshold measure. Furthermore, after embedding in a biometric vector using a fuzzy commitment approach, the transmitted information is encrypted using a random key. [3]have demonstrated the transparency and organizational mechanism of countrywide e-voting in the context of securityissues and needs. The authors presented an instance in which Brazil pioneered the countrywide adoption of voting more than 20 years ago. Though the article-less voting process improves the ease and accessibility of consumers in distant regions. However, the article less e-voting systems have significant security issues such as verifiability, integrity, and voter unlikability. Furthermore, in order to confirm the genuine voter throughout the election process, the two key security problems in e-voting systems are authenticity and vote manipulation. Several researchers have developed safe e-voting systems; however, none of the solutions are practicable owing to the small size of computing equipment.

[4] The word and concept of "smart contracts" are credited toNick Szabo, a law and computer science graduate. His statedpurpose with smart contracts is to apply highly advanced legal procedures to the construction of Internet-based electronic commerce protocols between strangers. Ethereum provides an open-source blockchain platform for the deployment of smart contracts. To build these contracts, Ethereum established a new programming language called Solidity (akin to JavaScript). We deploy our e-voting systemas a permissioned blockchain smart contract system. SectionIII will go over the functions in depth. Each election in Netvote is represented by a series of smart contracts that are instantiated on the Ethereum blockchain by election administrators using the Admin dApp. Each ballot smart contract refers to a single ballot. Multiple ballots can be listedtogether using a voter pool smart contract, with each voter pool smart contract representing, for example, each polling station. As a result, an individual voter registers at the polling location and then interacts with the voter pool smart contract via the voter dAapp. Netvote uses a Vote Gateway to give voters with privacy during a private election. Each individual voter communicates a cryptographically signed vote token tothe Vote Gateway for verification via the voter dApp.[4] Thenew protocol, like the AV-net protocol, does not require a trusted third party or a private channel.

Participants transmit two-round public messages to execute the protocol, although it is substantially more efficient in terms of the number of rounds, computational cost, and bandwidth utilization. In general, the new protocol classified electronic voting into two categories:

- Decentralized elections, in which the protocol is mostly controlled by the voters.
- Centralized elections in which trustworthy authority handle the process.

[5] Once a voter has voted, the poll worker will update the voter's registration to reflect that a vote has been cast. Any votes cast by this person beyond this point will be disqualified. The same is true for individuals who vote by mail as well as those who vote in person on election day. Strict voter registration regulations also serve to ensure that each individual may only vote once.

Asymmetric cryptography, often known as public-key cryptography, is a cryptographic system in which each participant has a pair of keys. In cryptography, a key is a set of characters in a certain sequence. These keys are used to indicate the transformation of data in order for it to be jumbled or disguised in such a way that anybody who does not have the key would be mathematically unable to decipher the information. Because keys are not designed to be read or recalled by humans, the majority of keys have a low human readability. One of these keys is designated as the private key and should be kept confidential. The second is a public key that should be made public.[5] The Authentication Server is exclusively responsible for validating the identity of a voter. The voter will be needed to present proof of identification, most likely an ID or similar document of this type. In addition to this identifying information, the voter will transmit their blindfolded public key to the Authentication Server for signing. The Authentication Service will get the blinded public key as well as the information verifying the voter's identity. It is critical that this step be done using a blind signature to ensure voter confidentiality.[6] The Access Control Management layer is intended to help layer 1 and layer 3 by providing services necessary for these levels to perform their expected responsibilities. These services involve the defining of roles, access control policies for those roles, and voting transaction definitions. The layer 1 access control functions are supported by the role definition and maintenance, whereas the layer 3 blockchain-based transaction mapping and mining is supported by the voting transaction definitions. Overall, this layer supports the proposed system's cohesive function by supplying the foundations required by individual levels.

[6] The Ledger Synchronization layer uses one of the current database technologies to synchronize the Multichain ledger with the local application specific database. Votes are stored in the database's data tables in the backend. Voters may trace their votes using the unique identification that is assigned to them whenever their vote is mined and published to the blockchain ledger. The votes' security considerations are based on block-chain technology, which uses cryptographic hashes to safeguard end-to-end communication. Voting results are also saved in the application's database to allow auditing and other activities in the future.

[7] Voters, a vote administrator (VA), a front-end smart contract server (SCA), and multiple smart contract validation nodes compose the voting system. The job of a smart contract validation node is to precisely imitate the execution of smart contract codes. Many stakeholders might manage the validation nodes for practical voting, suggesting that all ballots on the blockchain have been certified by diverse stockholders. [7] we use the Hyperledger Fabric blockchain technology, which is based on Byzantine Fault Tolerance (BFT), to deploy our voting system in a real-world setting.[8]To be able to access and authenticate the system, the voter needs have an identifying number, some personal information, or a secret key. The system should require voters to produce secret codes upon registration in order for them to vote with them. By utilizing these codes, eligible persons should be able to vote in elections effortlessly. In addition to retaining log records of all activities conducted by the administrator, it is critical to securely preserve election results.At this point, blockchain systems can be rather useful since they allow votes to be preserved on blockchain systems as a new transaction.

IV. CHALLENGES AND CONCERNS

Implementing digital voting systems with Aadhar identification raises various issues and concerns that must be properly addressed to preserve the election process's integrity, security, and fairness.

The following is an examination of these issues and concerns:

1) *Data Security and Privacy:* Aadhar contains sensitive biometric and personal information. Concerns have been raised about how this data is safeguarded and if it is accessible to hackers or unauthorized access. There is a danger of data breaches and identity theft, which might jeopardize voters' anonymity and personal information.
2) *Exclusion and Accessibility:* If Aadhar authentication becomes necessary, some parts of the population, notably those without Aadhar cards, may be barred from voting. Concerns have been raised concerning the accessibility of the digital voting method for elderly or technologically impaired voters.

3) *Cyber security Risks:* Digital voting systems are vulnerable to assaults such as hacking, distributed denial-of-service (DDoS) attacks, and voting data manipulation. To avoid tampering with election results, it is critical to ensure the security of the system and voter data.
4) *Reliability of Authentication:* The accuracy and dependability of Aadhar authentication may be a source of worry. False positives and false negatives might result in eligible voters being denied access to the system or unauthorized persons getting access.
5) *Transparency is Lacking:* Transparency in the digital voting process, including vote validation and tabulation, is critical for maintaining public trust. Concerns may occur if the system is opaque.

A. *Benefits and Advantages*

Because Aadhar authentication is based on biometric and demographic data, it is impossible forunauthorized people to impersonate legal voters. Thisreduces the possibility of fraudulent votes. Biometricauthentication (fingerprint and iris scans) gives an additional degree of protection by guaranteeing that the voter matches the registered voter. Aadhar authentication can aid in the elimination of multiple voting instances by assuring that each voter can vote only once, limiting the likelihood of duplicate votes. Using Aadhar data to streamline voter registration canreduce the need for human data entry and verificationby providing accurate and up-to-date demographic information. Voter impersonation, or voting on behalf of another person, becomes more difficult with Aadhar identification since biometric verification needs the presence of the registered voter.

V. FUTURE WORK

The creation and implementation of a digital voting system based on Aadhar authentication necessitates a multifaceted strategy that includes technology, regulation, public awareness, and partnership. Continuous development, flexibility, and a dedication to tackling issues are required forthe future success of such a system. Create and put in place advanced security mechanisms to protect the voting process from cyber threats, identity theft, and data breaches. It is critical to do ongoing research on encryption systems and safe data transfer. Implement robust privacy protection procedures to address and mitigate privacy risks. Techniques such as differential privacy should be researched and developed in order to anonymize voter data while preservingthe legitimacy of the vote. Create user-friendly interfaces andtechnologies for those with impairments, non-technical users, and those without cell phones or computers. It is critical to ensure that the system is inclusive and accessible to alleligible voters. Promote digital literacy and voter education to guarantee that all citizens can successfully use the digital voting system. This includes user awareness campaigns, training programs, and user support. Before wider adoption, conduct thorough testing and pilot programs in controlled environments to detect and correct system vulnerabilities and operational concerns. Collaborations with academic institutions and security professionals may be required. Investigate the use of blockchain technology to secure and transparently record and count votes. By establishing a tamper-proof log, blockchain can improve the integrity of thevoting process.

VI. CONCLUSION

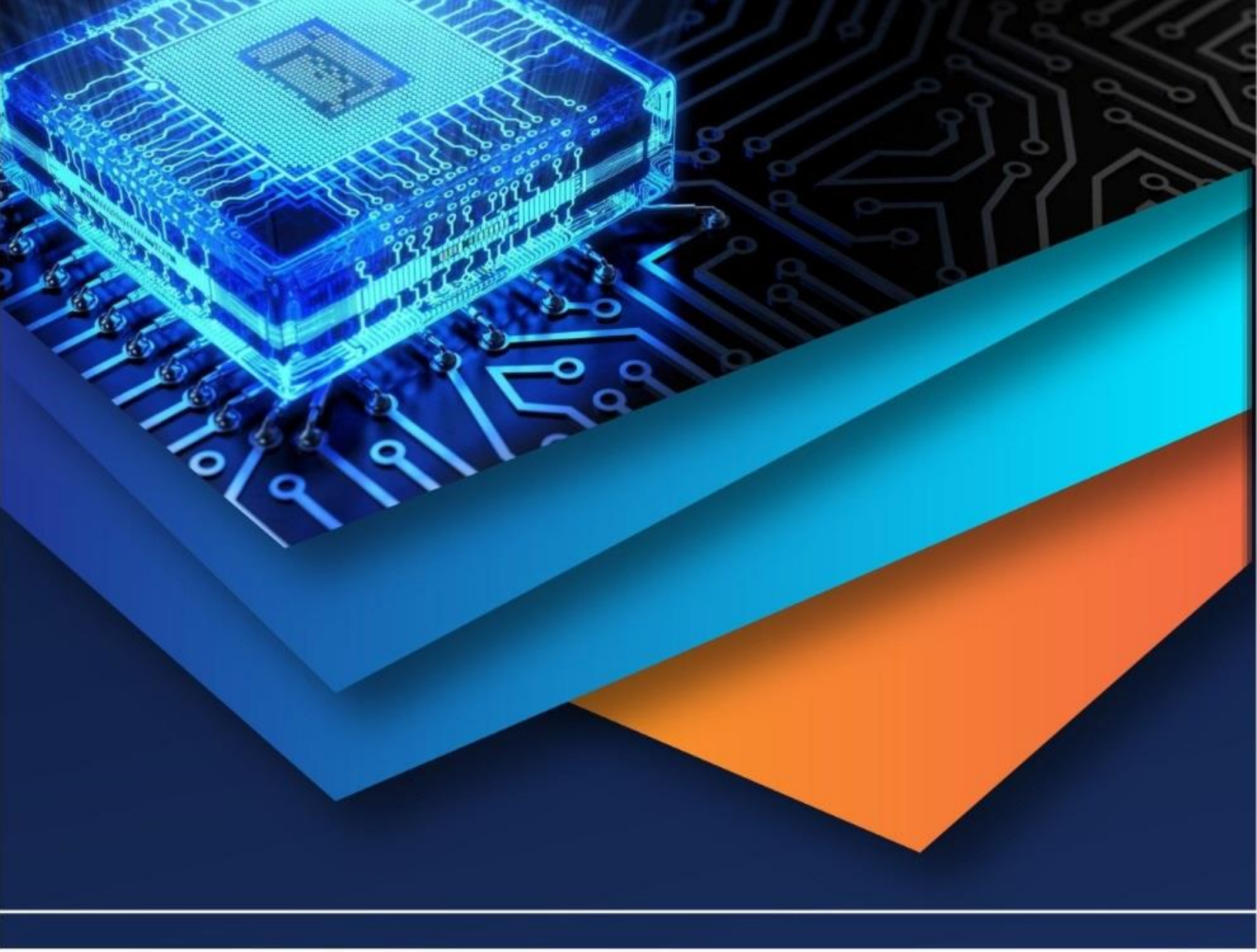
Our research presents various studies to demonstrate and study the benefits and drawbacks of both traditional and blockchain E-voting systems. The analysis and final results of our study show that the government's decision-makers and major election stakeholders lack the necessary information to hold a successful E-voting system in national elections. This study examines the experiences of several national elections in many important nations, as well as how they were plagued by challenges and failed experiments. Then came blockchain technology, which is a novel solution to the difficulties of electronic voting systems, and numerous tests on blockchaintechnology are being undertaken at the national andindividual levels by researchers. Finally, a digital voting system that uses Aadhar authentication has the potential to improve the security and accessibility of the voting process. It does, however, provide serious issues in terms of privacy, technology, and legal considerations. A multidisciplinaryapproach and a commitment to addressing these obstacles will be required for successful implementation. This field of research is dynamic and susceptible to continual investigationand development as technology and society advance.

REFERENCES

[1] X. Yang, X. Yi, S. Nepal, A. Kelarev, and F. Han, ``A secure veri_able ranked choice online voting system based onhomomorphic encryption,"IEEE Access, vol. 6, pp. 20506_20519, 2018.
[2] A. Meraoumia, H. Bendjenna, M. Amroune, and Y. Dris,``Towards asecure online E-voting protocol based on palmprint features," in Proc. 3rd Int. Conf. Pattern Anal. Intell.Syst. (PAIS), Oct. 2018, pp. 1_6.
[3] D. F. Aranha and J. van de Graaf, ``The good, the bad, and the ugly:Two decades of E-voting in Brazil," IEEE Secur.Privacy, vol. 16, no. 6,pp. 22_30, Nov. 2018.

[4] Blockchain-Based E-Voting System Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson School of Computer Science Reykjavik University, Iceland {fridrik14, gunnlaugur15}@ru.is of Science and MathematicsUniversity of Minnesota, Morris Morris, Minnesota, USA 56267 schu4276@morris.umn.edu
[5] Electronic Voting System Implementation Through BitcoinBlockchain Technology Cassandra Schultz Division
[6] Secure Digital Voting System based on Blockchain Technology Kashif Mehboob Khan1, Junaid Arshad2,Muhammad Mubashir Khan1 1 NED University of Engineering and Technology, Pakistan 2 University of WestLondon, UK.
[7] Secure Electronic Voting (E-voting) System Based on Blockchain on Various Platforms K. Varaprasada Rao and Sandeep Kumar Panda
[8] Khan, K. M., Arshad, J., and Khan, M. M. "Secure digital voting system based on blockchain technology" (Khanet al., 2018).
[9] Haibo Yi, "Securing e-voting based on blockchain in p2p network "(Yi, 2019)
[10] Oleksandr Kurbatov, Pavel Kravchenko, Oleksiy Shapoval, Nikolay Poluyanenko, Mariana Malchyk, Alina Sakun and Vladyslav Kovtun "Anonymous Decentralized E voting system" (Kurbatov et al., 2019).
[11] P. Raghava, P. Uday Kiran, Vimali. J.S, "TrustworthyElectronic Voting using Adjusted Blockchain Technology" (Shahzad & Crowcroft, 2019).
[12] Towards A Privacy-Preserving VotingSystemThrough Blockchain Technologies Rabeya Bosri, Abdur Razzak Uzzal, Abdullah Al Omar, and A S M Touhidul Hasan Department of Computer Science and Engineering University of Asia Pacific Dhaka, Bangladesh, Md. Zakirul Alam Bhuiyan Department of Computer and Information Sciences Fordham University New York, NY 10458, USA

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)