Online Voting System

Vankudothu Likitha, Y Hemanth, S Poojith, K Jaideep and Vipul Dabhi

March 28, 2024

Online Voting System

Y Hemanth
Department of Computer Science Engineering and Technology Parul Institute of Engineering and Technology
Vadodara, India
200303124544@paruluniversity.ac.in

S Poojith
Department of Computer Science Engineering and Technology Parul Institute of Engineering and Technology
Vadodara, India
200303124471@paruluniversity.ac.in

Vankudothu Likitha
Department of Computer Science Engineering and Technology Parul Institute of Engineering and Technology
Vadodara, India
200303124518@paruluniversity.ac.in

K Jaideep
Department of Computer Science Engineering and Technology Parul Institute of Engineering and Technology
Vadodara, India
200303124275@paruluniversity.ac.in

Prof. Dr. Vipul Dabhi
Department of Computer Science Engineering and Technology Parul Institute of Engineering and Technology
Vadodara, India
vipulkumar.dabhi23496@paruluniversity.ac.in

Abstract— **The proposed system represents a comprehensive and secure approach to the electoral process, consisting of three integral sections: admin, voter, and candidate. The admin section serves as the gateway for inputting crucial voter and candidate information into a centralized database. When registering as a voter, individuals provide their facial features, enabling a sophisticated biometric identification process. This ensures a high level of accuracy and security in verifying the identity of each voter. Meanwhile, candidate registration is a straightforward process that involves gathering essential information to establish a comprehensive database of potential representatives. During the actual voting process, an advanced live camera system is employed to conduct facial recognition scans. This innovative technology plays a pivotal role in authenticating voters based on their distinct facial features. The system then employs the Facenet classification method to assess the eligibility of each voter. If deemed eligible, a unique voter ID block is generated and subsequently added to the Blockchain. This integration with Blockchain technology introduces an extra layer of security, rendering the records immutable. Through the application of SHA-512 hashing, the voter ID block becomes impervious to any attempts at tampering or unauthorized alterations, guaranteeing the integrity of the electoral records. This multifaceted system not only ensures a highly accurate and secure voting process but also establishes a robust foundation for transparent and trustworthy elections.**

Keywords— AdminSection, VoterRegistration, Candidate Registration,FacialRecognition,Biometric,IdentificationCentralized Database,Live Camera System,Facial Recognition Scans.

I. Introduction

Across democracy, electoral protection is an trouble of country wide security. The laptop safety area has been operating at the possibilities of digital voting machine, with an aim of decreasing the fee of election and growing the safety of the election. From the start of the democratic elections, the voting machine become primarily based on pen and paper. Instead of pen and paper currently the Indian election makes use of evm machines,that are liable to vote casting fraud and device tampering. Electronic voting machine are taken into consideration invalid and anybody with bodily get entry to that device can tamper with the gadget ,as a result affecting all votes casted. Enter blockchain era. A blockchain is a disbursed, immutable, incontrovertible, public ledger**.**In the realm of democracy, safeguarding electoral processes is paramount for national security. Over time, the landscape of voting mechanisms has evolved, transitioning from traditional pen-and-paper methods to electronic voting machines (EVMs) in many countries, including India. However, the adoption of EVMs has introduced concerns regarding the integrity and security of the electoral process. Electronic voting machines, while offering the promise of increased efficiency and potentially reduced costs, also present significant vulnerabilities to various forms of tampering and electoral fraud. Unlike traditional paper ballots, which are tangible and relatively straightforward to secure, EVMs are susceptible to manipulation due to their digital nature. Any individual with physical access to an EVM could potentially tamper with the device, compromising the validity of the entire voting process and undermining the democratic principles it is meant to uphold.

In response to these challenges, the field of computer security has been actively exploring the potential of blockchain technology as a means of enhancing the security and reliability of electronic voting systems. Blockchain, often described as a distributed, immutable, and tamper-evident public ledger, offers several features that make it an attractive solution for addressing the shortcomings of traditional EVMs. One of the key advantages of blockchain technology is its decentralized nature. By distributing copies of the ledger across a network of nodes, blockchain eliminates the need for a centralized authority, reducing the risk of single points of failure and making it more resistant to manipulation or tampering. Additionally, the immutability of blockchain ensures that once data is recorded on the ledger, it cannot be altered or erased retroactively, providing a transparent and verifiable record of all transactions. In the context of electronic voting, blockchain could be leveraged to create a transparent and secure voting system where each vote is recorded as a transaction on the blockchain. This would enable voters to verify that their votes have been accurately recorded and counted, while also providing election authorities and other stakeholders with a tamper-proof audit trail of the entire voting process.

Furthermore, blockchain technology can help mitigate the risk of unauthorized access or tampering by implementing robust encryption and cryptographic techniques to secure the integrity of the voting process. By encrypting voter identities and ballot information, blockchain-based voting systems can ensure the privacy and anonymity of voters while still maintaining the integrity and security of the electoral process. While blockchain technology holds great promise for revolutionizing electronic voting systems and enhancing electoral security, it is essential to recognize that its implementation poses its own set of challenges and considerations. Issues such as scalability, interoperability, and accessibility must be carefully addressed to ensure that blockchain-based voting systems are practical, inclusive, and resistant to potential attacks or vulnerabilities. The adoption of blockchain technology has the potential to significantly enhance the security, transparency, and integrity of electronic voting systems, thereby safeguarding the democratic process and bolstering national security efforts. However, it is essential to approach the implementation of blockchain-based voting systems thoughtfully and collaboratively, taking into account the complex technical, social, and political factors involved in modern electoral processes.

II. LITERATURE SURVEY

The proposed system described above presents an innovative approach to modernizing the electoral process, incorporating elements of biometric identification, facial recognition technology, and blockchain integration to enhance security, accuracy, and transparency. To conduct a literature survey on this topic, we can explore relevant research articles, conference papers, and academic publications that discuss similar systems or components. Research in biometric authentication methods, such as facial recognition, fingerprint scanning, and iris recognition, can provide insights into the efficacy and challenges of implementing such technologies in electoral processes. Studies examining the use of biometrics for identity verification and authentication in various domains, including government services and financial transactions, can offer valuable lessons for the electoral context.

Literature on facial recognition algorithms, techniques, and applications can inform the design and implementation of the facial recognition system described in the proposed electoral process. Research exploring the accuracy, reliability, and ethical considerations of facial recognition technology, particularly in diverse demographic settings, can help evaluate its suitability for use in elections. Academic papers discussing the use of blockchain technology for enhancing the security and transparency of elections can provide theoretical frameworks and practical insights into its implementation. Studies examining blockchain-based voting systems, decentralized identity management, and cryptographic techniques for securing electoral data can offer valuable perspectives on the integration of blockchain in the proposed system.

Literature on security measures and protocols for safeguarding electoral processes against fraud, tampering, and cyberattacks can inform the design and implementation of secure voting systems. Research on cryptographic techniques, such as hashing algorithms and digital signatures, can provide guidance on ensuring the integrity and authenticity of electoral records stored on the blockchain. Case studies of real-world implementations of similar voting systems or technologies, along with evaluations of their effectiveness, usability, and acceptance by stakeholders, can offer practical insights and lessons learned. Comparative analyses of different voting technologies, including traditional paper-based systems, electronic voting machines, and blockchain-based platforms, can help assess the advantages and limitations of each approach. By conducting a comprehensive literature survey encompassing these key areas, researchers can gain a deeper understanding of the proposed system's technological components, security mechanisms, and potential implications for electoral integrity and democratic governance. Additionally, identifying gaps and challenges in existing literature can guide future research directions aimed at further advancing the development and deployment of secure and transparent electoral systems.

The requirement for users to authenticate themselves using both their unique IDs and passwords serves as an additional layer of security, forging an unbreakable link between each vote and its rightful owner. Through this stringent authentication protocol, the system not only safeguards the anonymity of voters but also guarantees the accuracy and reliability of the results. Moreover, the implementation of robust encryption algorithms and stringent access controls further fortifies the system's defenses, rendering it impervious to even the most sophisticated cyber threats. In addition to its unparalleled security measures, the online voting system also offers unparalleled convenience and accessibility to voters. By eliminating the need for physical presence at polling stations, the system enables individuals from all walks of life to participate in the democratic process from the comfort of their homes or workplaces. This democratization of the voting process not only enhances voter turnout but also promotes inclusivity and civic engagement.

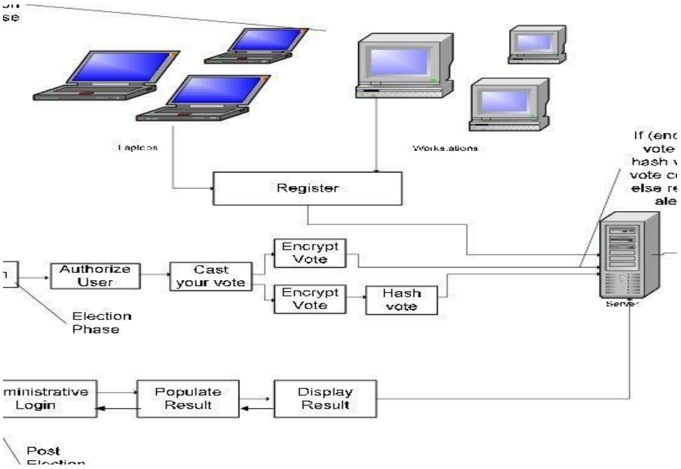
In conclusion, the proposed online voting system represents a paradigm shift in the realm of democratic governance, offering a potent combination of convenience, accessibility, and, above all, security. Its innovative features, such as the unique ID generation process and stringent authentication protocols, ensure that each vote is sacrosanct and that the electoral process remains beyond reproach. As we embrace the digital age, it is imperative that we harness the transformative power of technology to strengthen and safeguard our democratic institutions, and the online voting system stands as a testament to our unwavering commitment to upholding the principles of democracy in the digital era.The transition from traditional paper-based voting systems to online voting holds immense potential in revolutionizing democratic processes. The contemporary age of rapid technological advancement demands modernization in various sectors, including electoral processes. In countries like India, where manual methods still prevail, there are numerous challenges inherent in the paper-based ballot system. These challenges include logistical difficulties, delays, and the possibility of errors in counting and recording votes. However, the adoption of an online voting system offers a solution to these challenges by providing a streamlined and efficient process. An online voting system encompasses procedures such as voter registration, casting votes, and result declaration within a digital framework. This digitalization not only enhances accuracy but also empowers voters to participate conveniently from their own devices or through government-provided resources. By enabling citizens to engage in the electoral process from anywhere with internet access, online voting increases voter turnout and accessibility, thus strengthening democracy.

Moreover, the transition to an online voting system has significant implications for reducing the risk of corruption within the electoral process. Advanced technology, combined with secure authentication measures, establishes robust safeguards against fraudulent activities. Integration with established online databases, such as NADRA's, enhances the system's ability to efficiently register and verify voters aged 18 and above. This integration streamlines the registration process while fortifying the integrity of the voter database, thereby minimizing the potential for duplicate or fraudulent registrations. However, the adoption of online voting also raises concerns regarding cybersecurity, privacy, and inclusivity. Addressing these concerns requires comprehensive measures to ensure the security and integrity of the voting process, protect voters' privacy, and promote inclusivity by accommodating diverse demographics, including those with limited access to technology. The adoption of an online voting system represents a significant step towards modernizing and democratizing electoral processes. By leveraging technology to overcome the limitations of traditional methods, online voting promises enhanced accuracy, accessibility, and integrity, ultimately strengthening democratic governance.

III. HARDWARE AND SOFTWARE USED

1. HARDWARE TECHNOLOGY

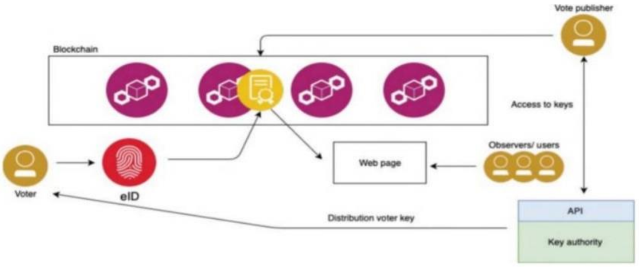
Hardware requirements refer to the specific physical components necessary to support the operation and functionality of a computer system or electronic device. These components encompass various elements such as the central processing unit (CPU), random-access memory (RAM), storage devices (e.g., hard disk drives, solid-state drives), input/output (I/O) devices (e.g., keyboard, mouse, monitor), and networking hardware (e.g., network interface cards, routers). Each hardware component plays a crucial role in facilitating different aspects of computing tasks, from processing and storing data to interacting with users and communicating with external devices or networks. Moreover, the selection of appropriate hardware components is essential to ensure optimal performance, reliability, and compatibility with the software applications or systems that will be utilized. Additionally, hardware requirements may vary depending on the specific requirements and intended use cases of the computer system or electronic device. For example, a high-performance gaming computer may require more powerful CPU and graphics processing units (GPUs) to handle resource-intensive gaming applications, while a server system may prioritize factors such as storage capacity, data redundancy, and network bandwidth for efficient data storage and access. Understanding the hardware requirements and capabilities is essential for designing, configuring, and maintaining computer systems that meet the desired performance, reliability, and scalability criteria for their intended applications and usage scenarios



2. SOFTWARE TECHNOLOGIES

System software serves as the foundation of a computer system, providing essential functionalities to manage and operate hardware components effectively. This category includes operating systems (e.g., Windows, macOS, Linux), device drivers, firmware, and utility programs. The operating system acts as an intermediary between the user and the hardware, facilitating communication and coordination between various system components. It manages system resources, such as memory allocation, file system operations, and peripheral device management, to ensure smooth and efficient operation of the computer system. Device drivers enable communication between the operating system and hardware devices, allowing them to function correctly and interact with software applications. Additionally, firmware provides low-level control and initialization routines for hardware components, such as BIOS (Basic Input/Output System) or UEFI (Unified Extensible Firmware Interface), ensuring proper booting and initialization of the system.

On the other hand, application software encompasses a wide range of programs and tools designed to perform specific tasks or functions for the user. This category includes productivity software (e.g., word processors, spreadsheets, presentation software), multimedia applications (e.g., video players, image editors, music players), communication tools (e.g., email clients, web browsers, instant messaging applications), and specialized software for various domains or industries. Application software enables users to accomplish diverse tasks, ranging from creating documents and managing data to accessing information, communicating with others, and entertainment purposes. These programs leverage the capabilities provided by the underlying system software and hardware infrastructure to deliver functionality tailored to the user's needs and preferences.



3. PROPOSED SYSTEM

In our proposed blockchain-based voting system, the collaboration between the vote publisher and the key authority is crucial for ensuring the integrity and security of the voting process. The key authority plays a central role in generating and distributing cipher keys to both voters and the vote publisher. These cipher keys are essential for encrypting and decrypting the votes, ensuring that the voting data remains confidential and tamper-proof. The distribution channel for these cipher keys must be securely established to prevent any potential third-party interference or tampering. This may involve the use of cryptographic protocols, secure communication channels, and robust authentication mechanisms to safeguard the confidentiality and integrity of the cipher keys during transmission.

Moreover, transparency and auditability are fundamental principles in the design of our blockchain-based voting system. By utilizing a public blockchain, the stored data, including the encrypted votes, remains accessible and verifiable by any interested observer. This transparency ensures that the voting process is open to scrutiny and enhances trust in the integrity of the election results. Additionally, the use of smart contracts embedded with the voting configurations helps automate and enforce the rules and procedures governing the elections, reducing the risk of human error or manipulation. Overall, our proposed system aims to provide a secure, transparent, and tamper-resistant platform for conducting various types of elections, fostering trust and confidence in the democratic process.

4. EXSITING SYSTEM

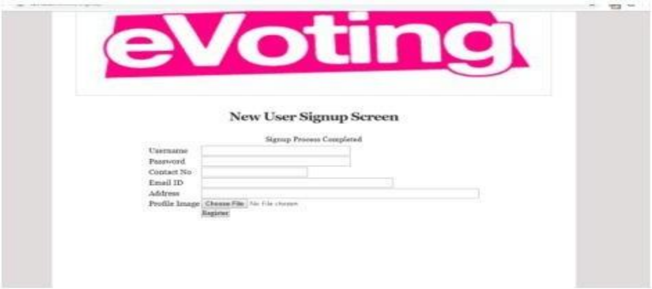
Blockchain technology has gained significant attention in recent years as a secure and transparent solution for various applications, including online environments. Our e-voting system leverages blockchain to address several critical challenges in traditional voting systems. One of the primary advantages of using blockchain in our system is the elimination of the need for trust in a centralized authority that oversees the elections. With blockchain, the integrity and immutability of the voting process are ensured through decentralized consensus mechanisms, where multiple nodes validate and record each vote transaction. This decentralized nature of blockchain mitigates the risk of manipulation or interference by any single entity, including the authority responsible for conducting the elections. As a result, the election results are tamper-resistant and trustworthy, instilling confidence among voters in the integrity of the electoral process.

Furthermore, transparency is a cornerstone feature of our e-voting system facilitated by blockchain technology. By recording all voting transactions on a public ledger, the entire voting process becomes transparent and auditable to all participants. Each vote is cryptographically secured and timestamped, ensuring its authenticity and preventing any unauthorized modifications. Additionally, the decentralized nature of blockchain allows for real-time monitoring and verification of the voting process by interested stakeholders, including voters, election observers, and regulatory authorities. This transparency fosters trust in the fairness and accuracy of the electoral system, empowering voters to participate with confidence knowing that their votes are being securely recorded and counted. Overall, the integration of blockchain technology in our e-voting system addresses the challenges of centralized control and lack of transparency, paving the way for more secure and democratic elections.

IV. IMPLEMENTATION

The Admin module serves as the backbone of the e-voting system, providing administrators with the necessary tools to manage the electoral process efficiently. Administrators can add new party and candidate details to the system, ensuring that the electoral options are comprehensive and up-to-date. Additionally, administrators have access to view party details and monitor the vote count in real-time. To access the Admin module, users must log in using predefined credentials, with the username set as 'admin' and the password as 'Admin'.

On the other hand, the User Module caters to individual voters participating in the electoral process. Users are required to sign up with the application, providing their unique user ID and uploading a face photo captured from a webcam for authentication purposes. Once registered, users can log in using their credentials to access the voting functionality. The login process validates the user ID, ensuring that only authorized users can cast their votes. Upon successful login, users can proceed to the cast vote module, where they can select their preferred candidates or parties to cast their votes securely and confidentially. By segregating administrative tasks into the Admin module and providing a streamlined user experience through the User Module, our e-voting system ensures efficient management and seamless participation in the electoral process.



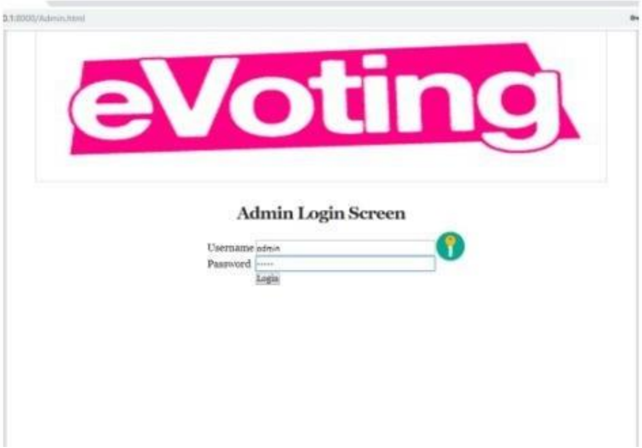
New User Signup Screen

Signup Process Completed

Username
Password
Contact No
Email ID
Address
Profile Image Choose File No file chosen

V. RESUL

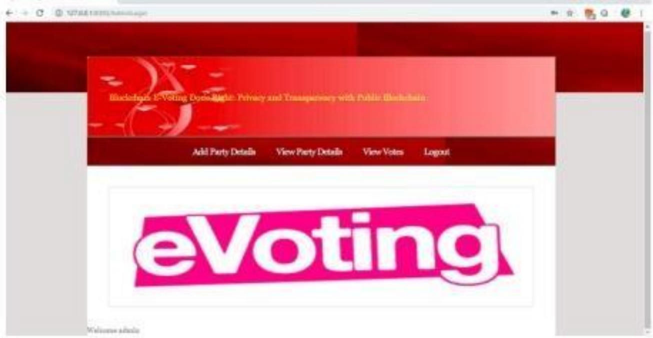
In this project we are using public python Blockchain API’s to store and manage voting data as Blockchain provides secure and tamper proof of data storage and to implement this project we have designed following modules. Admin module: this user responsible to add new party and candidate details and can view party details and vote count. Admin login to system by using username as ‘admin’ and password as Admin’User Module: this user has to signup with the application by using username as his ID and then upload his face photo which capture from webcam. After registering user can go for login which validate user id and after successful login user can go for cast vote modulewhich execute following functionality.



Admin Login Screen

Username admin
Password .....

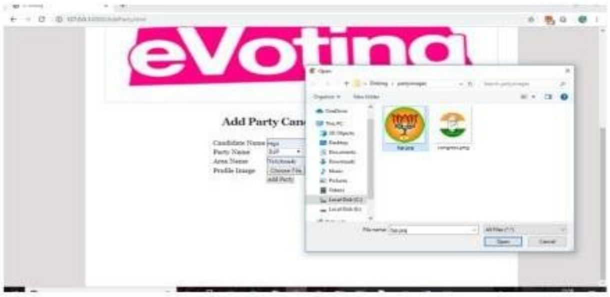
The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product .


Blockchain E-Voting Done Right: Privacy and Transparency with Public Blockchain

Welcome admin

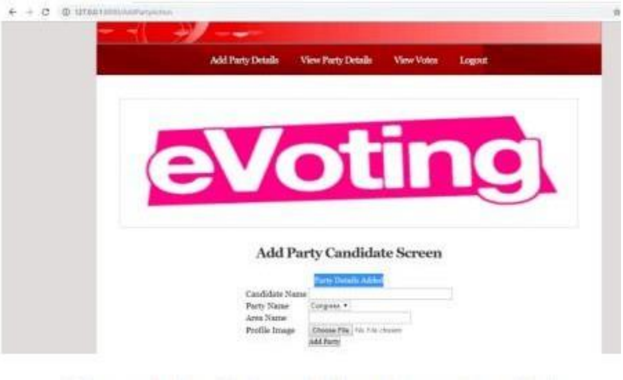
Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs.

All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .add the open button the click



Candidate Name
Party Name BJP
Area Name Tolichowki
Profile Image Choose File

Here ‘open’button then click on ‘add party’

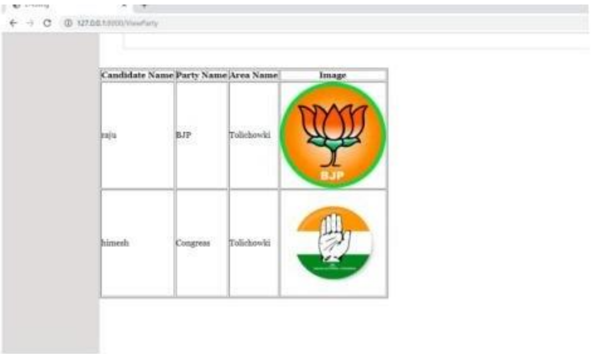


Add Party Candidate Screen

Party Details Added

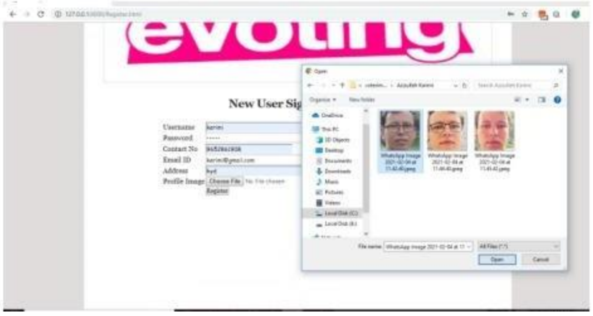
Candidate Name
Party Name Congress
Area Name
Profile Image Choose File No file chosen

Now click on “view party details”



Candidate Name	Party Name	Area Name	Image
raju	BJP	Tolichowki	
himesh	Congress	Tolichowki	

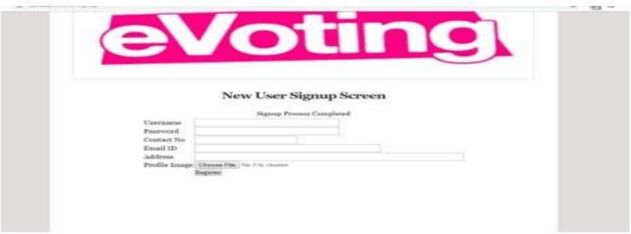
Figure 4.6: ’click on Logout’



New User Sig

Username karimi
Password ......
Contact No [illegible]
Email ID karimi@gmail.com
Address hyd
Profile Image Choose File No file chosen

Face photo captured by webcam

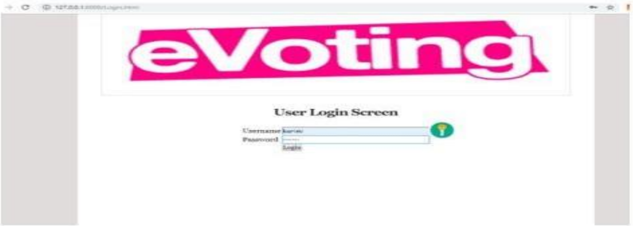


New User Signup Screen

Signup Process Completed

Username
Password
Contact No
Email ID
Address
Profile Image Choose File No file chosen

Figure 4.8: Login as this user to cast Vote



User Login Screen

Username karimi
Password ......

Figure 4.9: First Authenticate User

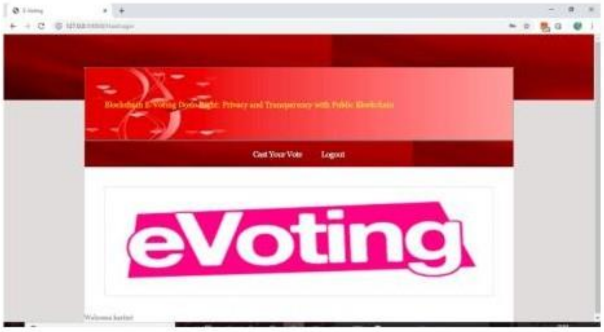

Blockchain E-Voting Done Right: Privacy and Transparency with Public Blockchain
Cast Your Vote
Logout
eVoting
Welcome karimi

Figure 4.10: ‘Cast Your Vote’

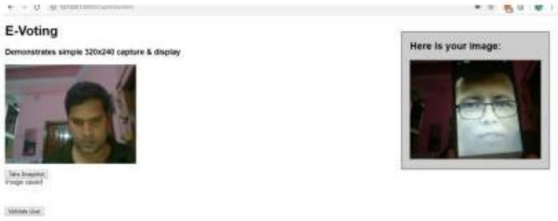
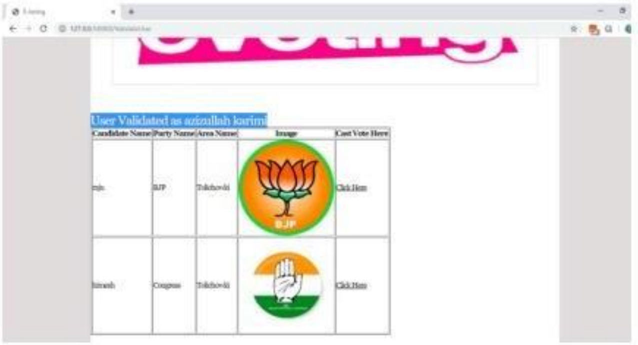


Figure 4.11: Enter Caption



User Validated as azizullah karimi

Candidate Name	Party Name	Area Name	Image	Cast Vote Here
[illegible]	BJP	Tolichowki		Click Here
[illegible]	Congress	Tolichowki		Click Here

Figure 4.12: user is identified

CONCLUSION

The implementation of an online voting system represents a significant leap forward in modernizing and streamlining the electoral process. It holds the potential to greatly enhance accessibility for voters, particularly those facing physical or logistical barriers. By leveraging digital technology, citizens can exercise their democratic right from the convenience of their own homes, thereby expanding the reach of democratic participation. Additionally, online voting systems can expedite the counting and announcement of election results, potentially reducing the time and resources traditionally associated with manual vote tabulation. However, it is crucial to approach the adoption of online voting with cautious optimism, as it introduces new challenges related to cybersecurity and ensuring the integrity of the voting process. A robust system must be developed and continuously updated to safeguard against potential threats and guarantee the trustworthiness of election outcomes.

REFERENCES

[1] AMNA Qureshi, ”SEVEP: Verifiable secure and privacy preserving remote polling with untrusted computing devices”, Future Network Systems and Security Feb, vol. 22, 2019.

[2] S. Ganesh Prabhu, Rachel, Agnes Shiny and A. R. Roshinee, ”Tracking Real Time Vehicle And Locking System Using Labview Applications”, In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 55-57, 2020.

[3] Annoshmitha Das, VOT-EL: Three Tier Secured State-Of-The-Art EVM Design Using Pragmatic Fingerprint Detection Annexed with NFC Enabled Voter-ID Card, IEEE, 2016.

[4] shani Mandal, Secure and Hassle Free EVM through deep learning face recognition, IEEE, Feb 2019.

[5] R. Maheswar and G. R. Kanagachidambaresan, ”Sustainable development through Internet of Things”, Wireless Networks, 2020.

[6] A Framework for the Analysis of Internet Voting Systems” by Alessandro Acquisti, Stefan Brands, and David Chaum.

[7] ”E-Voting: Risk and Opportunities” by Jordi Barrat i Esteve, Joan Borrell i Sole, and Josep M. Reniu i Vilamala.

[8] The Threat of Strategic Voting in a Blockchain-based Proxy Voting System” by Florian Breuer, et al year 2015.

[9] Towards Trustworthy Elections: New Directions in E-Voting” by Jeremy Clark, Aleks Essex, and Carlisle Adams year 2018.

[10] The Impact of Technology on the Administration of Elections” by Thad Hall year 2012.

[11] ”Remote Electronic Voting: Traps and Pitfalls” by David L. Dill.

[12] ”Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy” by Josh Benaloh, Eric Lazarus, and Brent Waters.

[13] ”An Analysis of the Helios Voting System” by Rivest, R. L., Shen, E., Wagner, D.

[14] Election Audits with Fault-Tolerant Devices” by James A. Clarke, et AI.

[15] ”Scantegrity: End-to-End Voter-Verifiable Optical-Scan Voting” by David Chaum, Aleks Essex, and Ron Rivest.

[16] Voting Technologies and Trust: E-Voting’s Role in Restoring Trust in Elections” by Sharon L. Jones.

[17] ”Modeling and Analysis of an Internet Voting Protocol” by Yue Zhang, et al 2016.

[18] STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System” by Dana DeBeauvoir, et al 2017.

[19] ”On the Notion of Coercion-Resistance in Voting” by Olivier Pereira and Bogdan Warinschi year 2016.

[20] ”Webvotetrust: A Web-based Voting System Supporting Trust in Electoral Processes” by Feng Hao, et al year 2015.

[21] ”On the Security of Return Codes of Mixnets” by Olivier Pereira and Jean-Jacques Quisquater year 2012.

[22] Cryptographic Voting Protocols: A Systems Perspective” by Aggelos Kiayias and Hong-Sheng Zhou year 2011.

[23] The ThreeBallot Voting System: A Secure Internet Voting Scheme” by Ron Rive year 2010.

[24] The Estonian Internet Voting System and its Security and Trustworthiness” by Tanel Tammet and Helger Lipmaa.

[25] ”The Unwitting Insider: An Analysis of Privacy Risks and Remedies in

[26] ”Cross-Border Internet Voting: Transparency and the Role of Governments” by Benoˆıt NadeauDostie, et al

[27] Scalable and Transparent Computational Integrity with Random Beacon” by Joshua A. Krollet al year 2018.

[28] ”Performance Optimizations for Homomorphic Encryption” by Jack Doerner, et al year 2010 pp(23-45)

[29] ”A Privacy-Focused Design for Remote E-Voting” by Sergiu Bursuc, et al.

[30] Scalable and Transparent Computational Integrity with Random Beacon” by Joshua A. Kroll, et al year 2021 pp (19-28)

[31] Tanmay Kadam” Online Voting System”, International Journal of Engineering Trends and Technology (IJETT), V37(5),273-276 July 2016. ISSN:2231-5381. www.ijettjournal.org

[32] Kohno, T., Stubblefield, A., Rubin, A. D., Wallach, D. S. (2004). Analysis of an Electronic Voting System. IEEE Symposium on Security and Privacy (pp. 27-40)

[33] Juels, A., Catalano, D., Jakobsson, M. (2005). Coercion-Resistant Electronic Elections. Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (pp. 61-70)

[34] Ryan, P. Y. A., Schneider, S. A. (2008). A Practical Verifiable Voting System. Proceedings of the 18th USENIX Security Symposium (pp. 363-378)

[35] Mobile Development of Android-Based Beginner E-Voting System November 2022

[36] Secured Aadhar Based E-Voting Application using RSA October year 2019

[37] Web Base Online Election Management Systems: Technical Review July 2023

[38] 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) Published: 2017

[39] Secure Digital Voting System Based on Blockchain Technology January 2021

[40] DOI: 10.4018/978-1-7998-5351-0.ch071 Secure Digital Voting System Based on Blockchain Technology January 2018