e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

ADVANCED DOUBLE AUTHENTICATION SYSTEM FOR SMART VOTING SYSTEM USING FINGERPRINT AND GSM

Mrs. Subha Indu S[*1], Prasanth S[*2], Shanmathi S[*3], Vidhya Lakshmi M[*4]

[*1]Assistant Professor, Department Of Software Systems, M.Sc Computer Science

Sri Krishna Arts And Science College, India.

[*2,3,4]Post Graduate Student, Department Of Software Systems, M.Sc Computer Science

Sri Krishna Arts And Science College, India.

ABSTRACT

Ensuring the integrity and security of the voting process is of paramount importance in any democratic society. Traditional voting systems often face challenges related to authentication and security. This paper presents an innovative solution, an Advanced Double Authentication System, designed to enhance the security and reliability of smart voting systems. The proposed system leverages two-factor authentication through fingerprint recognition and GSM (Global System for Mobile Communications) technology. The first layer of authentication in this system involves biometric verification using fingerprint recognition. Each eligible voter's unique fingerprint is registered in the system, and during the voting process, their identity is confirmed through a fingerprint scan. This biometric authentication adds an extra layer of security, ensuring that only authorized individuals can cast their votes. The second layer of authentication employs GSM technology to enhance the transparency and real-time monitoring of the voting process. After successful fingerprint verification, the voter's selection is securely transmitted to a central server via the GSM network. This allows for instant data transfer, reducing the likelihood of data tampering or manipulation. Additionally, voters receive an acknowledgment message on their mobile devices, providing them with a verifiable record of their vote.

Keywords: Voting System, Internet Of Things, GSM, Arduino, Sensors.

I. INTRODUCTION

The integrity and credibility of electoral processes are fundamental pillars of any democratic society. In recent years, technological advancements have opened up new possibilities for improving the security and efficiency of voting systems. One such innovation is the integration of biometrics and mobile communication technologies into the traditional voting framework. This paper introduces an Advanced Double Authentication System for Smart Voting, which combines fingerprint recognition and GSM (Global System for Mobile Communications) technology to enhance the security, transparency, and accessibility of the voting process. Traditional voting systems have long grappled with challenges related to authentication and the prevention of fraudulent activities. Voter impersonation, ballot stuffing, and unauthorized access to polling stations are just a few of the issues that have raised concerns about the reliability of electoral outcomes. In response to these challenges, governments and organizations worldwide are exploring cutting-edge solutions that leverage technology to fortify the electoral process.

Advanced Double Authentication System represents a pioneering approach that addresses the aforementioned challenges by incorporating two robust authentication layers. Firstly, it employs biometric authentication through fingerprint recognition. This method ensures that only eligible voters, whose fingerprints are registered in the system, can cast their ballots. Fingerprint recognition provides a highly accurate and unique identifier for each individual, minimizing the risk of identity fraud and unauthorized voting. Secondly, the system leverages GSM technology, a ubiquitous and secure communication platform. After successful fingerprint.

II. LITERATURE SURVEY

[1]"Biometric Authentication in Voting Systems":

Chenna, D., Ramesh, N., & Verma, S. (2017) examined the importance of biometric authentication, including fingerprint recognition, in enhancing the security and accuracy of electronic voting systems. Kumar, P., & Kumar, M. (2018) proposed a biometric-based voting system with fingerprint recognition, highlighting its potential to reduce voter fraud and enhance voter verification.

[2]"Mobile Technology in Voting":

Kasana, A., & Khan, A. (2018) explored the integration of mobile technology, particularly GSM-enabled smartphones, to enable secure and accessible voting systems. Singh, N. K., & Chauhan, K. (2019) discussed the feasibility of mobile-based voting systems, emphasizing the role of GSM technology in facilitating secure data transmission.

[3]"Security and Authentication":

Aggarwal, N., & Oberoi, S. S. (2016) investigated security enhancements in e-voting systems, including biometric authentication, to ensure the integrity of votes. Joshi, M., & Choudhary, A. (2017) focused on secure authentication methods in electronic voting, including the use of fingerprint recognition and secure communication channels like GSM.

[4]"Real-Time Monitoring and Transparency":

Thakur, M., & Verma, A. K. (2018) discussed the significance of real-time monitoring in electronic voting systems and how GSM technology enables instant data transfer and transparency. Chandra, R., & Sharma, R. (2016) examined real-time auditing and monitoring mechanisms in e-voting systems to ensure transparency and accountability.

[5]"Case Studies and Implementations":

Some literature includes case studies and practical implementations of advanced double authentication systems in real-world voting scenarios, showcasing their effectiveness and challenges faced during deployment.

III. EXISTING SYSTEM

In existing system of advanced double authentication systems for smart voting utilizing fingerprint recognition and GSM technology were being actively explored and developed in various regions worldwide.

However, specific implementations can differ significantly based on local requirements and technological infrastructure. Typically, an existing system of this nature comprises several key components. It includes a biometric database that stores registered voters' fingerprint data, ensuring secure and unique identification during the voting process. Additionally, fingerprint scanners are deployed at polling stations for voter authentication. Voters, often using GSM-enabled mobile devices, access a dedicated secure mobile application for voting. Votes are transmitted in real-time via the GSM network to a central server that securely stores and manages voting data. The system emphasizes robust security measures, including encryption and authentication protocols, and enables real-time monitoring of the voting process. It adheres to legal and regulatory frameworks while providing accessibility features for a wide range of voters. Audit trails and validation procedures are implemented to maintain transparency and integrity. However, it's crucial to recognize that the state of such systems can evolve rapidly, and the specifics may have changed since then. Therefore, consulting the latest information and local authorities is essential to understanding the current landscape of advanced double authentication systems for smart voting.

DISADVANTAGES OF EXISING SYSTEM

- Cost and Infrastructure
- Voter Registration Challenges
- Security Risks
- Maintenance and Updates

IV. PROPOSED SYSTEM

The proposed advanced double authentication system for smart voting, integrating fingerprint recognition and GSM technology, envisions a pioneering approach to revolutionize the security and efficiency of electoral processes. In this innovative system, the initial layer of authentication harnesses biometric data, with eligible voters registering their unique fingerprints during the enrolment process. When it comes time to cast their votes, these individuals will undergo a meticulous fingerprint recognition process to verify their identities, drastically reducing the risk of impersonation and unauthorized voting. Moreover, our system leverages the ubiquity and reliability of GSM technology to facilitate real-time data transmission. After successful fingerprint authentication, voters can securely transmit their choices to a centralized server via the GSM network. This immediate data transfer ensures the integrity of the voting process by minimizing the possibility of data tampering or manipulation. Additionally, voters receive confirmation messages on their GSM-enabled mobile devices, granting them a tangible record of their participation, thus enhancing transparency and trust in the electoral process. This combined use of fingerprint recognition and GSM technology not only strengthens the security of the voting system but also advances accessibility and inclusivity. It represents a significant step forward in addressing the challenges posed by traditional voting systems, marking a decisive move toward more secure, transparent, and convenient democratic elections.

ADVANTAGES OF PROPOSED SYSTEM

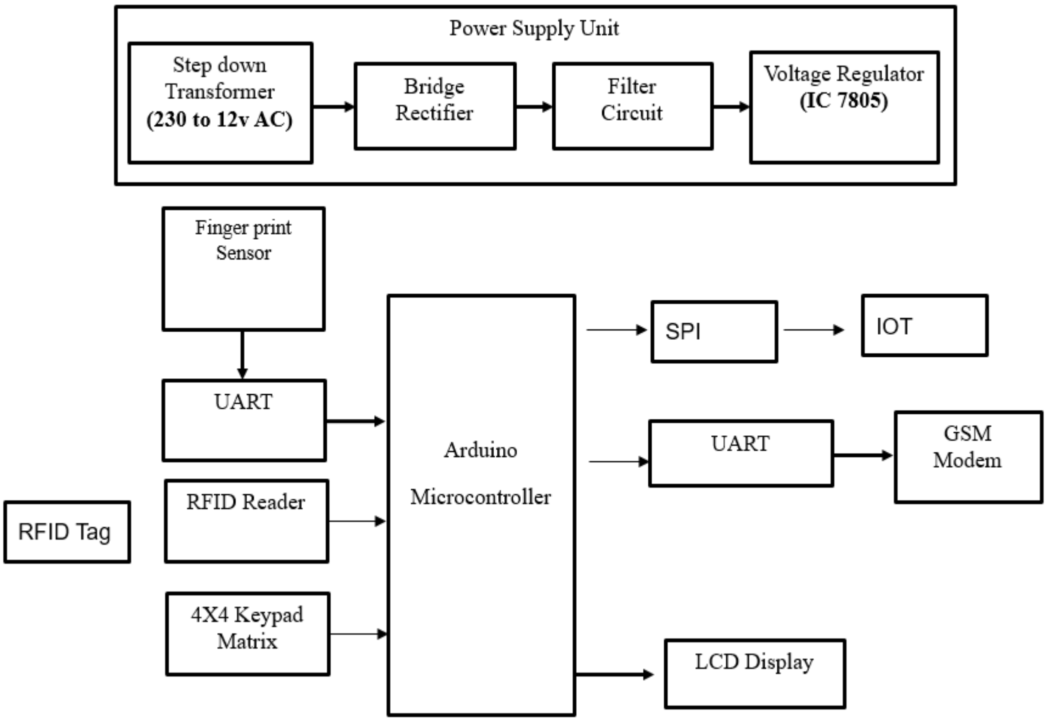
- Enhanced Security
- Biometric Authentication
- Reduced Fraud and Errors:
- Minimized Human Errors

V. POBLEM DEFINITION

The problem definition for an advanced double authentication system for smart voting, integrating fingerprint recognition and GSM technology, revolves around the imperative to enhance the integrity, security, and inclusivity of the electoral process. At its core, this multifaceted challenge encompasses the need to accurately verify the identities of voters while preventing any potential instances of unauthorized access or fraudulent participation. It also encompasses the critical aspects of safeguarding sensitive biometric data, particularly fingerprint information, from breaches or misuse while navigating the complex landscape of data privacy and protection regulations.

Moreover, this problem definition underscores the importance of ensuring that the proposed system is accessible to all eligible voters, including those with disabilities and those lacking access to GSM-enabled devices or stable internet connectivity. Technical complexities such as the reliability of fingerprint recognition, secure data transmission via GSM networks, and the scalability of the system for large-scale elections are additional dimensions of this challenge. Furthermore, the need for comprehensive user education and training, legal and regulatory compliance, fostering public trust, and optimizing resource allocation must all be addressed. Ultimately, the successful development and implementation of this advanced voting system hinge on effectively tackling these multifarious challenges to create a more secure, transparent, and inclusive democratic process.

VI. BLOCK DIAGRAM

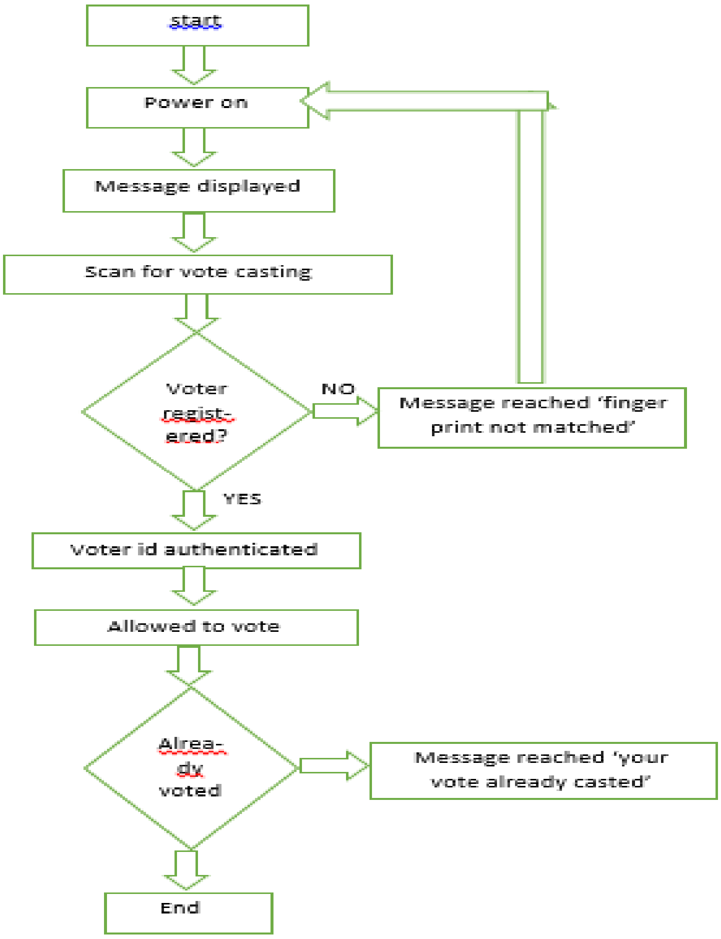


VII. WORKING PRINCIPLE

Incorporating fingerprint recognition and GSM technology, follows a rigorous and secure working process to ensure the integrity of the electoral system. It commences with the voter registration phase, where individuals provide their personal information and have their fingerprints captured and securely stored in a dedicated biometric database. When it's time to cast their votes, registered voters proceed to a polling station, where they undergo a two-step authentication process. First, they present themselves to election officials, providing their voter identification. The pivotal double authentication begins with the placement of their fingers on a fingerprint scanner, which captures their fingerprint data for verification. Upon successful fingerprint authentication, voters are granted access to a secure mobile application on a GSM-enabled device. Within this application, they select their preferred candidates or choices, ensuring the secrecy of their vote. Once the selections are made, the system encrypts the voting data, transmitting it securely via the GSM network to a central server in real-time.

At the central server, the transmitted data is received, decrypted, and processed to accurately record each voter's choices. Simultaneously, election authorities and observers can access a real-time monitoring dashboard, providing them with valuable insights into the progress of the voting process. This comprehensive working process not only enhances security but also promotes transparency and efficiency, resulting in a more trustworthy and accessible electoral system.

VIII. FLOW CHART



IX. CONCLUSION

In conclusion, the advanced double authentication system for smart voting, integrating fingerprint recognition and GSM technology, represents a significant leap forward in the evolution of secure and efficient electoral processes. This innovative system addresses critical challenges in modern elections, such as identity verification, data security, accessibility, and transparency, by leveraging cutting-edge biometric authentication and real-time data transmission capabilities. By combining the reliability of fingerprint recognition with the ubiquity of GSM technology, this system offers a robust and multi-layered approach to verifying voter identities, significantly reducing the risk of impersonation and fraud. Moreover, the immediate and secure transmission of voting data ensures the integrity of the process, minimizing the potential for data manipulation or tampering. One of the most noteworthy aspects of this system is its commitment to inclusivity. It allows a broader spectrum of voters, including those in remote areas and individuals with disabilities, to participate in the democratic process using their familiar mobile devices. Furthermore, the system provides a tangible and auditable record of participation, enhancing public trust and confidence in electoral outcomes. While challenges and considerations persist, particularly in the realms of data privacy, system scalability, and regulatory compliance, the benefits of this advanced double authentication system are undeniable. It exemplifies the potential to transform elections into more secure, transparent, and accessible events, reinforcing the cornerstone of democracy. As technology continues to evolve, so too will the possibilities for improving the electoral process, ensuring that every voice is heard and every vote counts in the most reliable and secure manner possible.

X. FUTURE ENHANCEMENT

The future of the advanced double authentication system for smart voting, integrating fingerprint recognition and GSM technology, holds immense potential for transformative enhancements in the realm of electoral processes. Firstly, continuous biometric authentication could become a norm, ensuring that a voter's identity remains securely verified throughout the entire voting session, reducing the risk of unauthorized use or tampering. Embracing zero-knowledge proofs can provide an elegant solution for voters to prove their eligibility without revealing their identities, reinforcing privacy while maintaining robust security. Incorporating artificial intelligence and machine learning algorithms will enable real-time anomaly detection, swiftly identifying irregular voting patterns or attempted fraud, thus safeguarding the integrity of the process. The integration of blockchain technology into the voting system can bring about end-to-end verifiability, ensuring that each vote is transparently recorded and independently auditable.

XI. REFERENCES

[1] Baig, Hidayat, Taslim, B. Jeba, Rajesh, A. Prof., and J. and Prof., "Secure Voting Using Smartphone Applications" International Journal of Future Revolution in Computer Science, Communication Engineering (IJFRSCE) skin. 14:20 - 23 Lub Ob Hlis 2016.

[2] Hemlata Sahu, Anupam Choudhray "Kev Pov Npav Kev Siv GSM Facilities" International Journal of Science and Engineering Volume 2, Issue 10, October 2011 ISSN 2229-5518 br>.

[3] Soumyajit Chakraborty, Siddhartha Mukherjee, Bhaswati Sadhukhan, Kazi Tanvi Yasmin, "Biometric Voting System siv Adhar kart hauv tib neeg" 2016.

[4] Dentles, S Sankarayan Gentles, S Sankarayanan, "Secure Mobile Voting with Biometrics", 2nd Asia-Himalayan International Conference, Kaum Ib Ris 4-6, 2011.

[5] Dr. Mehboob Karim, Nabila Shahnaz Khan, Ashratoz Zaban, Shasmoi Kendu, Asibel Islam, Brazab Nayak, "Proposed Framework for Biometric Electronic Voting System", IEEE International Conference 2017.

[6] Karthik, Tanpura, and B. Naveen Kumar. "Electronic voting security based on biometric authentication technology" (2016).

[7] M. yingyeh and K. Gbolagade, "Background of Biometric Electronic Voting in Ghana", Global Journal of Advanced Research in Computer Science and Software Engineering, Volume 3. Issue July 2013.

[8] Hasta, K., Day, A., Shrivastava, A., Jeddah, P., and Shelke, S.N. (December 2019). Fingerprint based secure voting. 2019 International Conference on Advances in Computing, Communication and Control (ICAC3) (p. 172) 1-6). IEEE.

[9] J. American Art. Meftaul Islam, EVM and Digital Bangladesh Department of International Relations, 2011 (Accessed: 22 September 2017). [Online]. Source: http://www.thedailystar.net/news-detail-215643A. Karnik, "Effectiveness of TCP Congestion Control with Rate Feedback: TCP/ABR and TCP/IP Switch Rate," M. Eng. Thesis, Indian Institute of Science, Bangalore, India, January. 1999.

[10] V. Kirtika Priya, V. Vimaladevi, B. Pandimeenal, T. Dhivya, "Arduino Based Smart Electronic Voting Machine", 2017 International Conference on Electronic Trends and Bilisim (ICEI) Xyo: 2017, Conference Papers, Inc. Publisher: IEEE.

[11] Shankar, A., Pandiaraja, P., Sumathi, K., Stephen, T., Sharma, P. (2021). Privacy-protected e-voting cloud system using personal encryption. Peer-to-Peer Networks and Applications, 14(4), 2399-2409.

[12] Reddy, G.S., Radha, S., Taufiq, K.T., Reddy, K.D.S., Reddy, K.P.K. and Nagabushanam., P. (January 2022). Security-based electronic voting using Xilinx devices. 2022 2nd International Conference on Power Engineering Applications and Control and Internet of Things in Face-Fab Facilities (PARC) (pp. 1-4). IEEE.

[13] Roman "Security Aspects of Internet-Based Voting" Master of Arts in Algorithms and Technologies in Telecommunications and Networks, 2010, pp. 14.14.329-332.

[14] A. Pirathepan, S. Sasikaran, P. Thanushkanth, S. Tharsika, M. Nathiya, C. Sivakaran, N. Thiruchchelvan, K. Thiruthanigesan, "Arduino Innovation", Sri Lanka Institute of Technology, Anuradhapura University College, Jaffna. Sri Lanka University of Technology, Sri Lanka.