iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.68176

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 13 Issue IV Apr 2025- Available at www.ijraset.com

Fingerprint-Based Voting System Using C#: A Secure Biometric Approach to Modern Elections

Tarun Kancherla
Department of Computer Science and Business Systems Mahatma Gandhi Institute of Technology, Hyderabad, India

Abstract: ***Integrity in elections is fundamental to democratic processes, yet traditional voting systems face significant vulnerabilities such as rigging and voter fraud. This paper introduces a biometric voting so- lution leveraging fingerprint recognition to enhance electoral transparency developed using C# and SQL Server Studio to improve electoral transparency and security. The proposed system employs bio- metric authentication to uniquely identify voters, effectively eliminating impersonation and multiple voting incidents. System performance evaluations demonstrate a biometric matching accuracy of 98%, underscoring the practicality and efficiency of biometric systems in real- world electoral environments.***

Keywords: Fingerprint Authentication, Biometric Security, Electronic Voting, C#, Election Integrity

I. INTRODUCTION

Free and fair elections form the bedrock of a functioning democracy. How- ever, electoral integrity is often compromised by practices such as voter im- personation and multiple voting. This research project introduces a biometric fingerprint-based voting system designed using C#, addressing these prevalent security challenges.

II. LITERATURE REVIEW

Traditional Electronic Voting Machines (EVMs) are susceptible to security breaches and electoral fraud. Previous studies emphasize the potential of biometric authentication but also highlight issues such as accuracy and false identifications. This paper bridges existing research gaps by presenting a comprehensive biometric-based solution implemented on contemporary programming platforms.

III. METHODOLOGY

A. *System Requirements*

1) Software: Windows 11, Microsoft Visual Studio 2022, SQL Server 2022

2) Hardware: Intel i5 (5th Gen), 4GB RAM, 20GB Storage

B. *Implementation*

The voting system is implemented in C# leveraging the .NET Framework and Pattern Recognition. Fingerprint Recognition libraries. SQL Server securely stores biometric data and voting records.

IV. SYSTEM ARCHITECTURE

The proposed architecture integrates biometric scanning, authentication al- gorithms, secure data handling, and intuitive voter interfaces. The biometric data flow involves voter fingerprint capture, biometric verification, vote cast- ing, secure database storage, and final result generation.

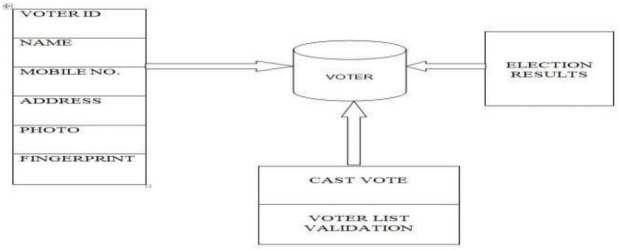


Figure 1: Proposed Fingerprint Voting System Architecture – The diagram outlines how voter data flows through biometric validation before casting and result generation.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

V. IMPLEMENTATION AND TESTING

Fingerprint authentication utilized minutiae-based matching algorithms. The system's response time for fingerprint verification was recorded using a Stop- watch utility integrated within the application, averaging 0.85 seconds per voter. The tests involved 100 fingerprint samples to ensure accuracy and reliability.

Table 1: System Test Cases and Results

Test Case	Description	Result
TC01	Invalid fingerprint	PASS
TC02	Attempted voting before election date	PASS
TC03	Re-voting attempt	PASS
TC04	Wrong login credentials	PASS
TC05	Invalid voter ID format (varchar)	FAIL

VI. RESULT AND ANALYSIS

1) Authentication Accuracy: Achieved 98% biometric matching accu- racy.
2) Authentication Speed: Average matching time was 0.85 seconds per voter.
3) Error Rates: False Acceptance Rate (FAR) at 1% and False Rejection Rate (FRR) at 2%.
4) System Performance: Average CPU usage was 14%, RAM usage averaged at 120MB, indicating efficient resource management.

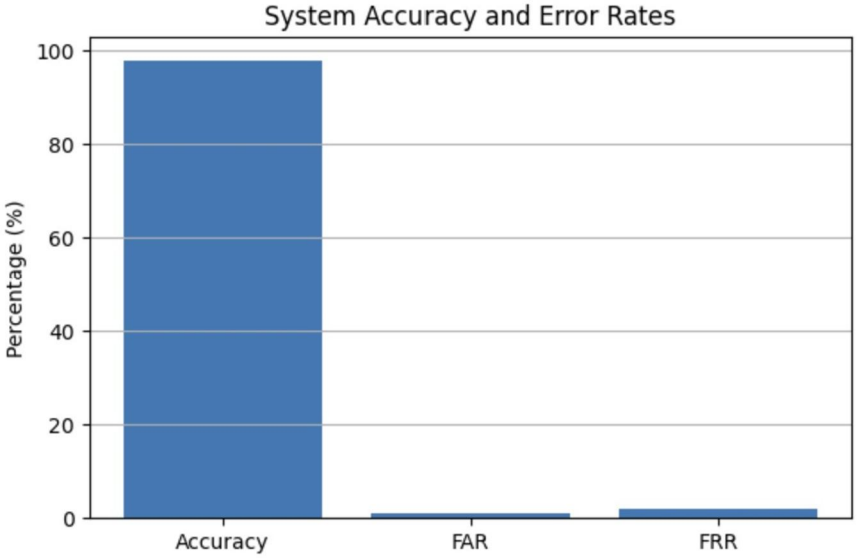


Figure 2: Authentication Accuracy and Error Rate – The system achieved 98% accuracy, with FAR at 1% and FRR at 2%.

VII. DISCUSSION

The developed biometric system significantly reduces fraud risk, ensuring voter authentication is swift and reliable. Its practical performance demonstrates readiness for actual electoral processes, though reliance on biometric hardware and data security requires robust management strategies.

VIII. CONCLUSION

The fingerprint-based voting system demonstrates robust security, efficiency, and accuracy, validating biometric solutions as superior alternatives to con- ventional methods. The developed prototype underscores its suitability for deployment in electoral systems, enhancing democratic integrity.

IX. FUTURE SCOPE

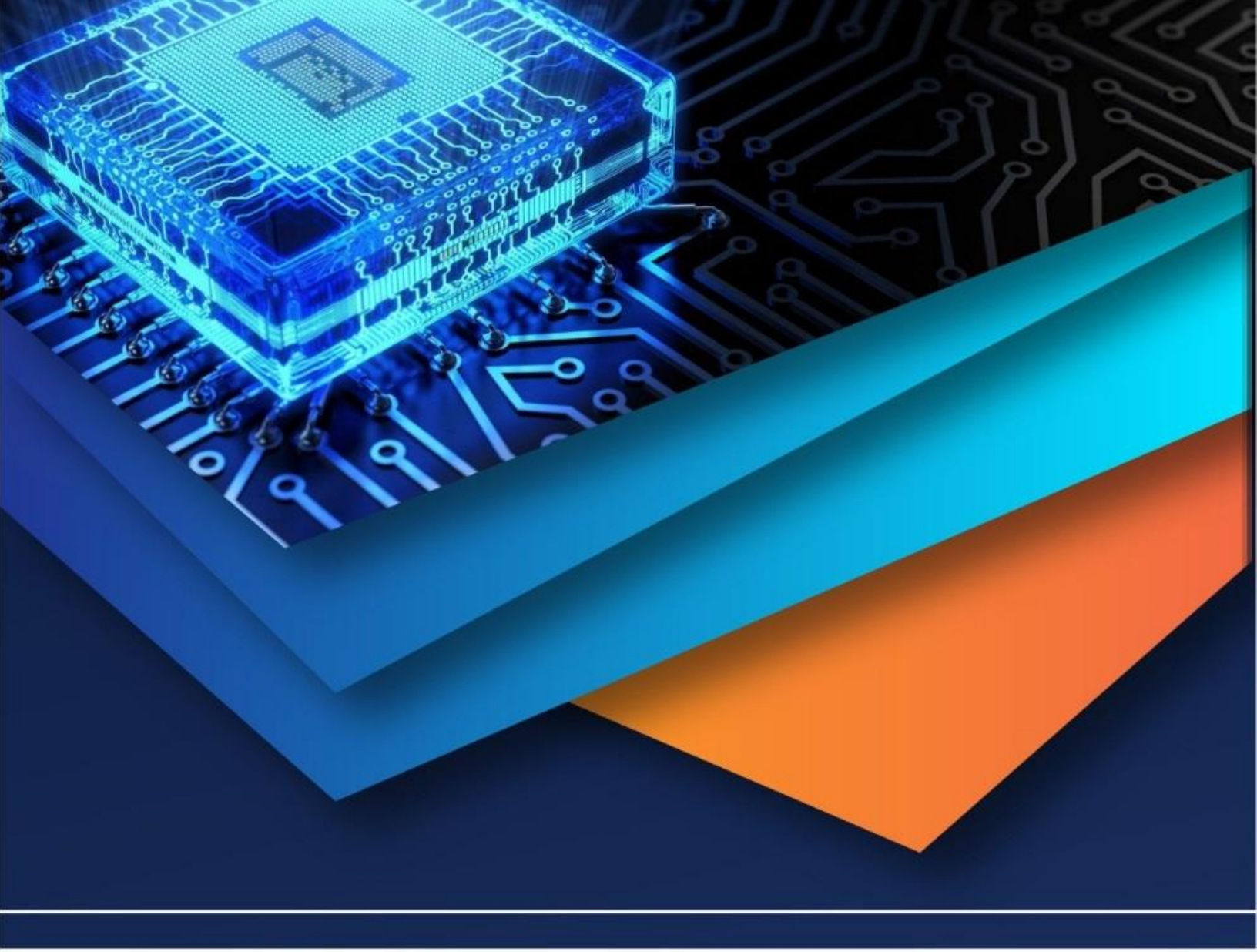
Future enhancements include mobile biometric verification, cloud-based in- frastructures, blockchain for transparency, and incorporation of additional biometric methods such as iris scans for greater security.

X. ACKNOWLEDGMENT

The author expresses sincere gratitude to Mrs. B. Swetha, Assistant Professor, Department of IT, MGIT, Hyderabad and Ms. M. Var- alakshmi, Assistant Professor, Department of IT, MGIT, Hyder- abad, for their invaluable guidance and support throughout the project.

REFERENCES

[1] A. Jain, A. Ross, and S. Prabhakar, ”An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, Jan. 2004.
[2] M. Tariq and Z. Khan, ”A Secure and Transparent Biometric Voting System,” in Proc. 2020 International Conference on Emerging Trends in Smart Technologies (ICETST), IEEE, pp. 1–6, 2020.
[3] S. Anil, A. Kaur, and R. Aggarwal, ”Fingerprint based voting system for election process,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, no. 3, pp. 1071–1074, 2015.
[4] S. P. Mudholkar, R. S. Deshmukh, and S. R. Chaudhari, ”Biometric Authentication Techniques for Intrusion Detection Systems: A Review,” International Journal of Computer Applications, vol. 3, no. 6, pp. 28–32, 2010.
[5] Y. H. Kim, H. J. Kim, and K. H. Park, ”Blockchain-based voting system design using fingerprint authentication,” in Proc. 2019 IEEE Interna- tional Conference on Consumer Electronics (ICCE), pp. 1–2.
[6] M. A. Khan and M. F. Azeem, ”Biometric Fingerprint Identification for E-Voting System Using Cryptographic Technique,” in Proc. 2022 International Conference on Computational Intelligence and Computing Applications (ICCICA), pp. 154–159.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY