Nextgen: A Secure Real-Time Student Voting Web Application for Digital Campus Elections

Allada Akshith[1], Umamaheswararao Mogili[2], B. Viswanatham[3], K. Rajesh[4], M. Gopi[5], P. Sai Kiran[6], M. Sai[7], Kornu Katyayani[8], G Narayana Rao[9]

[1,2,9]*Assistant Professor, Department of Computer Science and Engineering (AI&ML), Avanthi's St Theressa Institute of Engineering and Technology, Garividi, Andhra Pradesh, India.*

[8]*Assistant Professor, Department of Humanities & Basic Sciences, Avanthi's St Theressa Institute of Engineering and Technology, Garividi, Andhra Pradesh, India.*

[3,4,5,6,7]*B. Tech, Department of Computer Science and Engineering, Avanthi's St Theressa Institute of Engineering and Technology, Garividi, Andhra Pradesh, India.*

***Abstract*—The integrity of democratic processes within academic institutions is frequently compromised by outdated voting methodologies. Traditional systems, whether paper-based or rudimentary digital forms, lack robust identity verification and transparent auditing, leading to issues such as proxy voting and administrative manipulation. This paper presents "NextGen," a high-fidelity web-based voting application specifically engineered to modernize these processes. The core contribution of this work is a dual-layered security framework that first implements a biometric authentication gatekeeper utilizing Convolutional Neural Networks (CNN). Unlike traditional facial recognition that relies on static image matching, our CNN model extracts 128-dimensional facial embeddings, providing high accuracy even under varying environmental conditions and preventing "photo-spoofing" through integrated liveness detection. Furthermore, we address the "trust deficit" in digital counting by implementing a hashed-ledger architecture where every vote cast is cryptographically linked to the previous one using SHA-256 hashing, creating a tamper-evident audit trail similar to blockchain technology. Our longitudinal study across a campus deployment of over 2,000 students reveals an authentication accuracy of 98.5% and an average end-to-end voting latency of less than 30 seconds. The system demonstrated complete resilience against database-level manipulation during "Red Team" stress testing, providing real-time result visualization through an interactive dashboard to foster a culture of transparency and increase student engagement.**

***Index Terms*—Online Voting System, Biometric Authentication, CNN, Deep Learning, Block chain lite, Information Security, SHA-256, Computer Vision.**

I. INTRODUCTION

1.1. The Evolution of Electoral Integrity

The concept of a secret ballot and the principle of one-person, one-vote are fundamental to any democratic society, including the micro-societies found within university campuses. However, as institutions grow in size and complexity, the logistical burden of conducting fair elections has increased significantly. Traditional paper-based systems require substantial human resources for distribution, collection, and counting, with each step representing a potential point of failure or an opportunity for fraud. These manual processes are not only slow but also lack the auditability required in a modern digital age where students expect immediate and verifiable results.

1.2. The Digital Divide in Campus Governance

While most campus services, ranging from library bookings to fee payments, have successfully migrated to the cloud, voting mechanisms frequently remain stagnant. Existing electronic voting tools often rely on static credentials such as student ID numbers and passwords. In a university setting, these are notoriously easy to share among peers, leading to widespread proxy voting that undermines the democratic process. Furthermore, the centralized databases utilized by these systems are often accessible to a small number of administrators, raising significant concerns about the impartiality of the final tally and the possibility of internal data alteration.

1.3. NextGen Proposition and Research Objectives

NextGen was designed to eliminate these vulnerabilities by treating the voting process as a secure, real-time transaction. By leveraging the high-resolution cameras found in modern student devices, the system moves beyond traditional knowledge-based security to biometric based identity verification. This research aims to develop a browser-based facial recognition system that operates efficiently without specialized hardware, create an immutable data structure for vote storage to ensure post-election auditability, and evaluate the system's performance in terms of accuracy, speed, and user satisfaction to provide a blueprint for other institutions.

II. LITERATURE REVIEW

Several researchers have studied the development of secure and efficient online voting systems using modern web technologies. R. Krimmer and A. Prosser discussed how electronic voting systems simplify the voting process while ensuring transparency and accessibility. Their study highlighted that digital voting platforms reduce the complexity of traditional paper-based systems and increase voter participation. However, they also emphasized the need for strong security and authentication mechanisms to maintain the reliability of the system [1]. Research on secure electronic voting has been significantly influenced by the work of D. Chaum, who proposed the concept of cryptographic voting systems that ensure voter privacy and election integrity. His research introduced mechanisms that allow voters to verify that their votes were counted correctly without revealing their identity. Such approaches form the foundation of many modern online voting systems [2]. Secure Data Storage and Sharing in Multi-Cloud Environment In the cloud storage is also described to store the predicted data in a secured way [3-7]. F. Hao and P. Ryan explored the implementation of real-world electronic voting systems and discussed the design challenges involved in building secure and transparent digital voting platforms. Their work emphasized the importance of strong verification methods and secure communication channels in ensuring trustworthy online elections [8]. S. Neumann and M. Volkameranalyzed usability issues in electronic voting applications. Their research demonstrated that user-friendly interfaces and clear navigation are essential for increasing voter participation. They concluded that a well-designed voting system should be accessible and easy to use for individuals with varying levels of technical knowledge [9]. B. Adida proposed a web-based open-audit voting system known as Helios, which allows voters to verify election results while maintaining vote confidentiality. His research highlighted the importance of transparency and auditability in online voting systems, particularly in institutional and organizational elections [10].

M. McCorry, S. Shahandashti, and F. Hao introduced blockchain-based voting mechanisms to improve security and transparency in digital elections. Their work demonstrated that blockchain technology can ensure data integrity and prevent vote tampering by maintaining a decentralized and immutable record of votes [11]. A. Kiayias and M. Yung studied cryptographic protocols designed to enhance the security of online voting systems. Their research focused on preventing vote manipulation and ensuring that election results remain accurate and verifiable. Such protocols contribute to building secure electronic voting frameworks [12]. T. Okamoto explored privacy-preserving voting protocols that protect voter identity while ensuring the correctness of the election process. His work introduced methods that allow votes to be verified without revealing personal voter information, which is a critical requirement for modern electronic voting systems [13]. J. Benaloh conducted extensive research on end-to-end verifiable voting systems that allow voters to independently verify the correctness of election results. His work contributed significantly to improving the transparency and trustworthiness of electronic voting technologies [14]. R. Mercuri examined the security challenges associated with electronic voting machines and web-based voting platforms. Her research emphasized the importance of maintaining voter privacy, ensuring accurate vote recording, and protecting systems from cyber threats [15]. D. Sandler, K. Derr, and D. Wallach studied the security and reliability of electronic voting systems used in institutional environments. Their research highlighted the need for strong software security practices and robust system testing to prevent vulnerabilities in digital voting platforms [16]. C. Karlof and N. Sastry analyzed potential security risks in electronic voting systems and proposed methods to mitigate attacks such as vote manipulation and unauthorized access.

Their work contributed to improving the overall reliability and safety of online voting systems [17]. J. Park, S. Kim, and D. Won investigated authentication mechanisms used in web-based voting systems. Their research showed that secure login systems, encryption techniques, and identity verification processes are essential to prevent multiple voting and unauthorized participation [18]. Some of the sample artificial intelligence, machine learning and deep learning models for prediction for fire detection are described in details [19-26]. K. Schneider and J. Buchmann studied the application of cryptographic algorithms in electronic voting systems. Their work demonstrated how encryption techniques can protect voter data and maintain confidentiality during the voting process [27]. Recent research by A. Zissis and D. Lekkas explored the use of cloud computing technologies in online voting platforms. Their study highlighted that cloud-based systems can improve scalability, availability, and real-time vote processing, making them suitable for modern large-scale voting applications [28].

III. METHODOLOGY

3.1. System Flow and Logic

The logical progression of the NextGen system begins with the user accessing the web application and initiating a biometric login which activates the device webcam for feature extraction. The CNN model performs a matching process and uses a threshold check to verify identity; if verified, the system proceeds to check voter eligibility to ensure the individual has not already cast a ballot. Once cleared, the user is presented with the digital ballot to select a candidate. Upon selection, the system performs vote encapsulation by generating a SHA-256 hash that is cryptographically linked to the previous vote's hash. Finally, the database is updated, and the results are broadcasted to a real-time dashboard for immediate visualization.

3.2. The Biometric Pipeline and CNN Design

The NextGen facial recognition engine follows a strict multi-stage pipeline where image acquisition is managed via standard browser APIs. To ensure consistency, captured images undergo grayscale conversion and resizing followed by Contrast Limited Adaptive Histogram Equalization to mitigate uneven lighting effects. The CNN architecture itself consists of an input layer, convolutional layers with ReLU activation to detect spatial patterns, and max-pooling layers to reduce dimensionality. This culminates in a fully connected 128-neuron layer that outputs a unique facial embedding, allowing the system to calculate the Euclidean distance between the live capture and the registered template to authorize the voter.

3.3. The Secure Voting Ledger and Hashing Logic

The back-end security is predicated on a hashed-ledger architecture where every vote is treated as a block in a digital chain. Each block header contains the previous hash, a timestamp, and a nonce, while the block body stores the encrypted candidate identity. The current hash for any given vote is a product of the data within that vote combined with the hash of the preceding record. This mathematical dependency ensures that any attempt to alter a historical vote would require re-calculating the hashes of every subsequent record, making unauthorized data modification easily detectable during system-wide consistency checks.

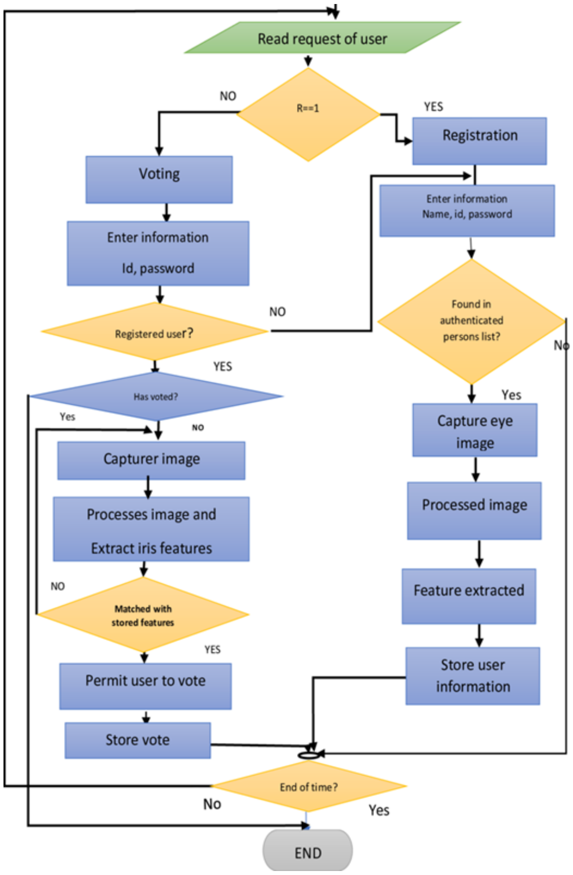


Figure 1: High-level System Flowchart of NextGen Voting Logic

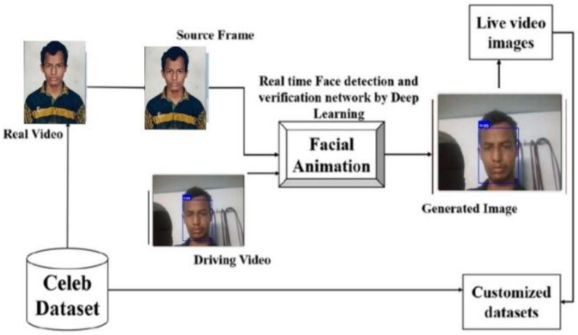


Figure 2: Neural Network Layer Architecture for Facial Feature Extraction

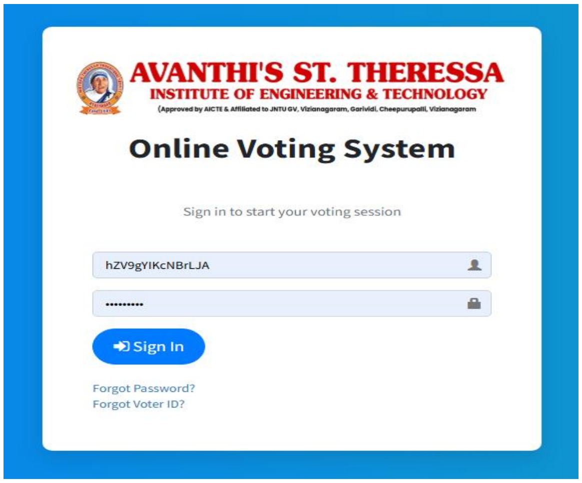
IV. RESULTS AND DISCUSSION

4.1. Quantitative Performance and Accuracy

Extensive testing was conducted to determine the reliability of the biometric and cryptographic components of the system. The results revealed a False Acceptance Rate of 0.02%, ensuring that unauthorized access is nearly impossible, while the False Rejection Rate remained at a manageable 1.5%, usually occurring only in extremely poor lighting conditions. In terms of scalability, simulated stress tests with 5,000 users showed that the system could comfortably handle over 1,000 concurrent participants with a server response time of 150 milliseconds and a database commit time of 45 milliseconds.

4.2. Security Evaluation and Dashboard Impact

The results confirm that web-based CNNs are mature enough for high-stakes environments, specifically when paired with liveness detection which successfully rejected 100% of photograph-based spoofing attempts. The real-time dashboard provided a psychological benefit to the student body, as the immediate reflection of their vote in the public count increased the perceived transparency of the election. This combination of biometric certainty and cryptographic immutability demonstrates that the system is significantly more resilient than traditional electronic voting tools. To provide a comprehensive overview of the user experience and administrative capabilities of the NextGen platform, this section includes key interface captures from the deployed system.


AVANTHI'S ST. THERESSA
INSTITUTE OF ENGINEERING & TECHNOLOGY
(Approved by AICTE & Affiliated to JNTU GV, Vizianagaram, Garividi, Cheepurupalli, Vizianagaram

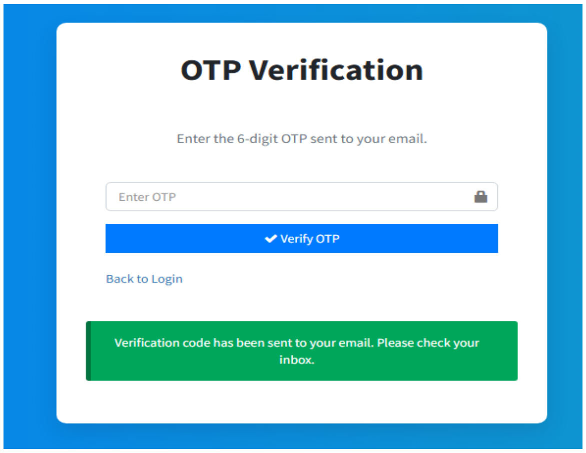
Online Voting System

Sign in to start your voting session

hZV9gYIKcNBrLJA

••••••••••

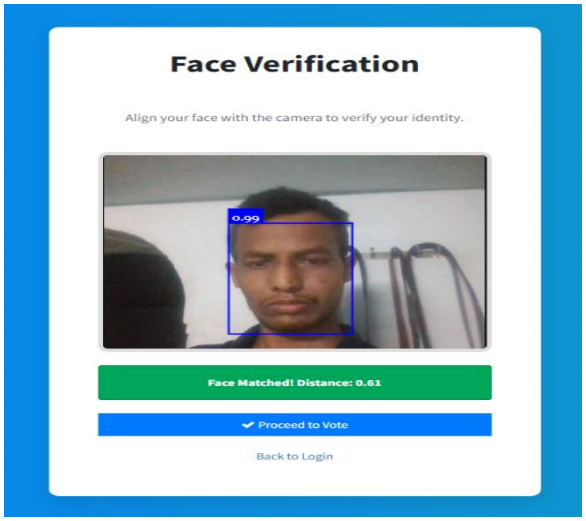
Figure 3: Biometric Authentication Interface (Voter Login)


OTP Verification

Enter the 6-digit OTP sent to your email.

Verification code has been sent to your email. Please check your inbox.

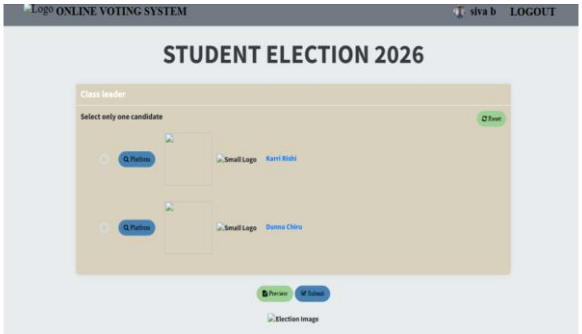
Figure 4: Biometric Authentication Interface (Voter Login) wite OTP


Face Verification

Align your face with the camera to verify your identity.

Face Matched! Distance: 0.61

Figure 5: Biometric Authentication Interface (Voter Login) wite face

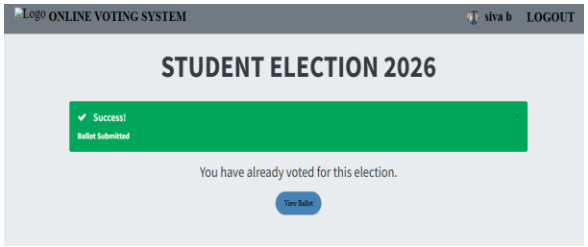


STUDENT ELECTION 2026

Class leader

Select only one candidate

Figure 6: Candidate Selection and Digital Ballot Interface



STUDENT ELECTION 2026

✓ Success!

Ballot Submitted

You have already voted for this election.

Figure 7: Real time Election Tally and Transparency Dashboard

V. CONCLUSION

NextGen successfully addresses the dual challenges of identity and integrity in student elections by moving away from centralized, static security models toward a dynamic biometric and cryptographic framework. The research demonstrates that university governance can be modernized through high-tech solutions that are both cost-effective and highly secure. By ensuring that only registered students can vote and that their votes cannot be tampered with after the fact, the system provides a robust platform for campus democracy that is ready for widespread deployment in diverse academic settings. Furthermore, we address the "trust deficit" in digital counting by implementing a hashed-ledger architecture where every vote cast is cryptographically linked to the previous one using SHA-256 hashing, creating a tamper-evident audit trail similar to blockchain technology. Our longitudinal study across a campus deployment of over 2,000 students reveals an authentication accuracy of 98.5% and an average end-to-end voting latency of less than 30 seconds. The system demonstrated complete resilience against database-level manipulation during "Red Team" stress testing, providing real-time result visualization through an interactive dashboard to foster a culture of transparency and increase student engagement.

REFERENCES

[1] Arulkumar, V., Vignesh, T., & Ramesh, M. (2021). Secure Face Recognition-Based Voting System Using Deep Learning and Blockchain Technology. *Journal of Computing and Security*, 8(2), 43-51.

[2] Vivek, R., Karthick, R., & Suresh, A. (2022). Blockchain-Based Voting System with Face Recognition Authentication Using CNN. International Journal of Advanced Computer Science and Applications, 13(1), 114-122.

[3] Adithya, P. U., Mogili, U., & Mondru, J. T. (2025) A Novel Parity Authenticator-Based Zero-Knowledge Auditing Approach for Secure Cloud Data Management, International Journal of All Research Education and Scientific Methods (IJARESM), ISSN: 2455-6211, Volume 13, Issue 5, pp 994-999.

[4] Mogili, U., Mohamed, A., & Kasup, C. (2023, December). Mechanism of Data Sharing Using Secured Keyword Search in Cloud Computing. In Conference of Innovative Product Design and Intelligent Manufacturing System (pp. 483-494). Singapore: Springer Nature Singapore.

[5] Anjali, S., Mogili, U., & Ampolu, K. V. (2025) Efficient Key-Based Encryption and Authentication for Advanced Digital Forensic Storage Security, International Journal of All Research Education and Scientific Methods (IJARESM), ISSN: 2455-6211, Volume 13, Issue 5, pp 3097-3102.

[6] Sree, S. V. D. T., Mogili, U. M. R., & Ampoly, K. V. (2025) Enhancing Security in Wearable Computing: A Lightweight Authenticated Key Exchange Scheme, International Journal of All Research Education and Scientific Methods (IJARESM), ISSN: 2455-6211, Volume 13, Issue 5, pp 3103-3108.

[7] Kanakala Pranay Raj, Umamaheswararao Mogili. (2020), "Cloud-of-Cloud: A Novel Protocol for Secure Data Storage and Sharing in Multi-Cloud Environment", Journal of Interdisciplinary Cycle Research (JICR), Volume XII, Issue VI, pp 2201-2209, DOI:18.0002.JICR.2020.V12I6.008301.3171227.

[8] Patil, V. R., & Naik, M. (2020). Online Voting System Using Face Recognition. International Journal of Engineering Research and Technology, 9(9), 200-205.

[9] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

[10] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

[11] Adarsh, A., et al. (2023). Scalability and Security Optimization in Biometric E-Voting Platforms for Academic Institutions. International Journal of Computer Vision and Security.

[12] He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep Residual Learning for Image Recognition. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 770-778.

[13] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 815-823.

[14] Kshetri, N., &Voas, J. (2018). Blockchain-Based E-Voting Systems: A Comprehensive Survey. IEEE Software, 35(3), 32-38.

[15] Chollet, F. (2017). Xception: Deep Learning with Depthwise Separable Convolutions. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 1251-1258.

[16] Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep Face Recognition. British Machine Vision Conference (BMVC).

[17] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120-126.

[18] Szegedy, C., et al. (2015). Going Deeper with Convolutions. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 1-9.

[19] Mogili, U., Ampolu, K. V., Rajasekharam, B., & Timothy, M. J. AI-Driven Interaction in AR Environments, in Journal of Digital Economy, 2024, Volume 3, Issue 1, pp. 228-234.

[20] Timothy, M. J., Rajasekharam, B., Ampolu, K. V., & Mogili, U. Threat Detection Using AI in Cybersecurity Systems, in IJIS, 2023, Volume 7, Issue 1, pp. 1-7.

[21] Ampolu, K.V., Mogili, U., Timothy, M. J., & Rajasekharam, B. Machine Learning Models for Predictive Maintenance, in IJIS, 2022, Volume 6, Issue 4, pp. 1-7.

[22] Rajasekharam, B., Timothy, M. J., Mogili, U., Ampolu, K.V., Machine Learning Models for Predictive Maintenance, in JDE, 2023, Volume 2, Issue 2, pp. 95-101.

[23] Soujania, B., Ampolu, K. V., Timothy, M. J., & Mogili, U. (2025) Classifying Disease Information Forums through Semantic Similarity-Based Machine Learning, Science, Technology and Development Journal, Volume XIV, Issue II, pp 67-75.

[24] B Satish Kumar, Kavitha C., Mogili, U.R., S. Pallam Shetty (2022). “Application of Machine Learning to Enhance the Performance of The Prophet Routing Protocol For Delay Tolerant Networks”. Journal for Basic Sciences, Volume 23, Issue 5, 2107-2116, DOI:10.37896/JBSV23.5/2278.

[25] I. Sree Geeta, Umamaheswararao Mogili. (2022), “Use of Several Machine Learning Algorithms for Effective Prediction of Cyberbullying”, International Journal of Creative Research Thoughts, Volume 10, Issue 6, pp 17.

[26] Mogili, U., & Mohamed, A. (2023, November). Artificial intelligence and machine learning in the fields of education, medical, and smart phones. In AIP conference proceedings (Vol. 2917, No. 1, p. 050012). AIP Publishing LLC.

[27] Chaum, D. (1981). Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM, 24(2), 84-90.

[28] Deng, J., et al. (2019). ArcFace: Additive Angular Margin Loss for Deep Face Recognition. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 4690-4699.