Iris Detection for Secure Voting System

D Manichakradeep[1], Mr.Matru Dhanavath[2], U Jayanth[3], G Manideep[4], B Dileep[5]
[2]*Assistant Professor, Department of CSE (Cyber Security), Sphoorthy Engineering College, Hyderabad, Telangana, India*
[1,3,4,5]*Students, Department of CSE (Cyber Security), Sphoorthy Engineering College, Hyderabad, Telangana, India*

***Abstract*—When democracy comes to mind, the security of each and every single vote strikes the mind. Traditional electronic voting systems —and even modern systems that depend on PINs or fingerprints— still have weak spots. Passwords can easily be shared, and fingerprint scanners can be fooled by personification attacks (like fake silicone prints) or fail to read worn-out fingers. In this project, we decided to tackle this problem by using human iris. The iris is unique to every person and practically impossible to fake. To make this idea a reality, we built complete, standalone voting framework. We utilized Convolutional Neural Networks (CNNs) to scan and process a voter's iris in real-time. Instead of saving this sensitive biometric info out in the open, we encrypted everything using strong AES-256 encryption before storing it in a local SQLite database. Furthermore, we built a tamper-proof audit log using SHA-256 hash chaining, meaning every single action is recorded. Nobody, not even an administrator, can secretly change or delete a vote without breaking the cryptographic chain. Our testing showed that the system is incredibly accurate and fast, proving that next-generation voting machines can be highly reliable and extremely protective of user privacy.**

I. INTRODUCTION

Elections form the foundation of any democratic society, and ensuring their transparency and security presents a significant challenge. Switching from paper ballots was a big improvement because it made the counting process quicker and prevented people from hiding extra ballots physically. However, electronic voting machines come with their own group of digital dangers. How can we ensure with absolute certainty that the person pressing the button in the voting booth is indeed who they say they are?

Most modern systems try to solve this by using either basic ID checks or fingerprint scanners. Both have real-world problems. Fingerprints change over time, especially for people who engage in heavy manual labor. Facial recognition, which is also a common option, has a hard time working in poor lighting conditions and can be fooled by good-quality pictures. The human iris is formed before we are born and remains almost the same throughout our whole lives. It has complex, random textures that offer a perfect way to verify an identity. In this project, we created an electronic voting machine that is very secure and operates locally. We aimed for a system that does not require a continuous connection to a cloud server while voting is taking place, which lowers the risk of network attacks. By integrating sophisticated deep learning for the iris scanning and robust cryptography for the database, we established a situation where a ballot is closely linked to a verified person, and the information stays protected from harmful intruders.

II. LITERATURE REVIEW

Numerous scholars have studied ways to enhance electronic voting. Much of the recent research concentrates significantly on technologies such as blockchain and homomorphic encryption. These mathematical approaches are excellent for guaranteeing that a vote, once submitted, is accurately recorded. However, they completely disregard what occurs within the actual voting booth. If an unauthorized individual utilizes another person's smart card or takes their password, the blockchain will simply log a fraudulent vote flawlessly.

We also investigated different biometric methods. Early systems for iris recognition relied on complex mathematical formulas like Hamming distance. While they performed admirably in controlled settings, they

struggled with issues in everyday scenarios where people blink, use glasses, or encounter intense lighting. Recently, deep learning and convolutional neural networks (CNNs) have been developed to manage these real-world flaws. Our research builds on these contemporary deep learning approaches but advances further. We not only recognize the voter; we incorporate that recognition method within a secure, offline database that employs strict role-based access controls.

III. HOW OUR SYSTEM WORKS

We created the system to have a "defense-in-depth" structure. This essentially implies that if an intruder manages to penetrate one layer, they will instantly encounter another barrier. As shown, the system is divided into several key components:

1) The Camera System: Records the video stream and swiftly focuses on the eye.
2) The AI System: A simple Convolutional Neural Network (CNN) converts the visual input into a distinct numerical representation.
3) The Secure Repository: An SQLite database that keeps all information safe with AES-256 Galois/Counter Mode (GCM)encryption.
4) The User Portals: Special screens designed for Voters and Administrators featuring added protection such as TOTP.
5) The Audit Ledger: An ongoing procedure that continuously documents all information safely.

IV. TECHNOLOGY UNDER THE HOOD

A. Locating and Handling the Iris

Initially, we employ Haar cascade classifiers to examine the real-time video stream and identify the eyes. After detecting the eye, we apply Daugman's rubber-sheet model to "flatten" the round form of the iris into a flat, rectangular image. This procedure is essential as it guarantees the image appears identical to the computer, no matter how much the pupil expands or contracts.

B. Deep Learning Comparison

Rather than using standard bit-matching, we input that flat image into our CNN. The network examines the intricate patterns and produces a very precise numeric array. To confirm the identity of the voter, we compute the Euclidean distance between the current scan and the stored encrypted scan. We intentionally establish our threshold firmly to ensure that no impostors are allowed.

C. The Cryptographic Audit Trail

Our goal was to guarantee complete non-repudiation. Each time an individual logs in, submits a vote, or attempts to reset the system, the event is safely recorded. To prevent a dishonest admin from erasing their actions, we implement SHA-256 hash chaining. Imagine it as a chain formed from digital steel. Log 2 is mathematically linked to Log 1. If anyone modifies the information in Log 1, it disrupts the connection for the entire remaining chain.

V. SECURITY AND THREAT MITIGATION

This project was developed with the belief that someone will eventually attempt to physically break into the machine.
Protecting the Hard Drive: If a person takes the computer after election day, they cannot simply access the database to find out who cast votes for which candidate. The voting data and biometric profiles are securely encrypted while stored. Protecting Against Internal Threats: Even if a system administrator chooses to act improperly, they are unable to discreetly erase the votes to manipulate the system. Activating the harmful "Vote Reset" mode necessitates a multi-factor TOTP verification, and any attempt is permanently recorded in the unchangeable audit log prior to the execution of the reset function.

VI. REAL-WORLD TESTING AND RESULTS

We tested the system thoroughly using regular, inexpensive computer equipment (an Intel Core i5 without a separate graphics card) to demonstrate its ability to function in rural voting places without costly server units.
1) Pace: Even with strong encryption and the AI operating in the background, confirming a voter typically takes under 450 milliseconds.
2) Accuracy: We rigorously tested the system particularly to examine the False Acceptance Rate (FAR). During our evaluations, the system consistently did not mistake one individual for another

(keeping the FAR almost zero). The False Rejection Rate (FRR) remained well under 1%.

3). System Comparison

Fingerprint EVMs: Quick, yet they have a significant rejection rate (FRR ~3.5%) and can be easily deceived using silicone.

4). Face Recognition: Very vulnerable to changes in lighting; moderate chance of spoofing using iPads or photos.

5). Our CNN Iris System: Exceptionally high entropy, almost zero false acceptance, and integrated offline encryption, making it the most secure choice available.

VII. CONCLUSION

We initiated this initiative to address the obvious weaknesses found in today's physical voting machines. By shifting from simple passwords, relying on the distinct characteristics of the human iris, and supporting this with advanced learning and top-tier encryption, we established a voting system that citizens can believe in. The system clearly shows that it is possible to achieve high-level security without sacrificing speed. This framework guarantees strict compliance with the principle of "one individual, one vote," which upholds user confidentiality and ensures the ballot box's integrity.

REFERENCES

[1] S. M. Bellovin and M. A. Blaze, "Cryptographic Hash Functions for System Auditing," IEEE Security & Privacy, vol. 3, no. 5, 2005.

[2] J. Daugman, "How iris recognition works," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21-30, 2004.

[3] K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," in Proc. CVPR, 2016.

[4] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," Pattern Recognition Letters, vol. 79, pp. 80-105, 2016.

IX About the authors

Mr. Matru Dhanavath, M. Tech, (Ph.D.) , Assistant professor, Department of Computer Science and Engineering-Cyber security, Sphoorthy Engineering College

U. Jayanth, Student, Department of Computer Science and Engineering-Cyber security, Sphoorthy Engineering College

D. Mani Chakra Deep, Student, Department of Computer Science and Engineering- Cybersecurity, Sphoorthy Engineering College

G. Manideep, Student,
Department of Computer Science and Engineering-Cyber security,
Sphoorthy Engineering College

B. Dileep, Student,
Department of Computer Science and Engineering-Cyber security,Sphoorthy Engineering College