Secure Biometric E-Voting System Interim Report
Student - Alexander Gordon 2502331
Supervisor - Oluwafemi Samuel

Aims and Objectives

This project addresses three key issues within the UK electoral system, including voter impersonation, ballot tampering, and slow vote counting [15] [14]. The UK continues to rely heavily on paper ballots and manual counting, a voting system that has changed very little since 1888 (Electoral Commission, 2025; Open Rights Group, 2025) [18]. While confirmed cases of postal vote impersonation are reported to be very low, with under 1000 being convicted between 2008 to 2013, the current system makes impersonation difficult to detect or prove [14]. This is due to voters typically being identified only by name, address and signature [14]. Ballot tampering is also a concern due to the physical handling of paper ballots, particularly during transportation and counting [14]. Although safeguards exist, reliance on human handling introduces the possibility of error or misconduct [14]. Additionally, manual counting of millions of ballots is time consuming, with recounts in close elections further delaying results, increasing costs and creating uncertainty that can lead to challenges to electoral integrity [15].

Public trust is essential to the effective functioning of government. Unexpected delays or perceived weaknesses in election security can reduce confidence in outcomes, even when no wrongdoing has occurred. In a modern country such as the UK, a voting system that appears slow or outdated risks increasing public suspicion and disengagement.

The aim of this project is to explore and design an electronic voting system that strengthens voter authentication through biometric verification. It also aims to protect user information using encryption. This will address the issues of ballot tampering and the voter impersonation while eliminating delays in ballot counting.

1. To evaluate and select a biometric authentication technology that balances cost-effectiveness with accuracy, ensuring a False Acceptance Rate (FAR) below 0.1% to minimise voter impersonation risks.
2. To design and implement a secure database architecture using deterministic searchable indexing and multi-layered encryption (symmetric and deterministic) that protects voter data from unauthorized access while maintaining system functionality.
3. To develop a biometric voter authentication mechanism that prevents duplicate voting by recording successful authentications in an encrypted, tamper-resistant audit trail.
4. To implement secure data transmission protocols using TLS and certificate pinning between the voting application, biometric devices, and database servers to prevent man-in-the-middle attacks and data interception.

Background Research

Biometric Research

The three main biometric authentication methods are used today include fingerprint, facial recognition, and iris scanning [2]. Fingerprint and facial ID are widely used in smartphones, resulting in extensive research focused on lowering costs while maintaining low false

acceptance rates (FAR). Iris scanning never made it into mass production in smart phones due to its costly and complex nature, requiring the use of deep neural networks and high computational power to work [3][5].
When selecting a biometric system, cost is a critical factor, particularly for a government deploying it nationwide. Governments aim to minimise expenses while maintaining effectiveness. Iris scanners perform poorly in this regard. According to the *Safe and Sound Security Biometric Access Control System Pricing Guide for 2025*, iris scanners cost between "1500 USD to 3000 USD" [21], making nationwide deployment at polling stations extremely expensive.
Facial recognition systems cost "1000 USD to 2500 USD" [21], which remains a major expense when scaled across thousands of polling stations. Fingerprint systems are significantly cheaper at 200 USD to 1500 USD" [21], making them far more attractive from a budget perspective.
Accuracy must also be evaluated based on software quality and FAR, which occurs when a system incorrectly grants access. Since scans are verified against stored templates, even expensive hardware is ineffective without reliable software.
Iris scanners offer the highest accuracy, with FAR values between "0.0001% to 0.01%" [2], due to advanced software and precise iris capture [3][5]. Facial recognition performs worse, with FARs of "0.1% to 1.0%" [2], despite its cost. Accuracy can degrade due to "occlusion, lighting, aging, pose variation, and plastic surgery" [4]. Facial systems are also vulnerable to spoofing, with Equal Error Rates (EER) reaching "8%" in some advanced systems [8].
Fingerprint scanners provide a strong balance, achieving FARs between "0.1% and 0.01%" [2], offering an excellent cost-to-accuracy ratio. The fingerprint scanner is not infallible though as matter on the finger or moisture can affect performance, these issues are easily resolved by cleaning or drying [6].
Although fingerprints can be stolen, vulnerability depends on scanner type. Optical scanners may accept fake prints as it only accepts an image of the fingerprint, while capacitive scanners reject them by detecting electrical conductivity [7].
Based on this analysis, fingerprint scanners are the most practical option, offering the best balance of cost and accuracy. While future research may reveal additional factors, fingerprint scanning is currently the most effective solution.

Security Research

With the public trusting its information to the government, it is essential that this data is always protected, even from employees. This makes database security research especially interesting, as it focuses on hiding personal data even from the database management system. The research identified several key methods for securing data:

- Deterministic searchable indexing
- Column-level encryption using Deterministic and Symmetric encryption
- Transport Layer Security (TLS) and Pinning
- Key Management System (KMS)

Deterministic searchable indexing allows specific rows of data to be located in a database [9]. It works by hashing values unique to each row, preferably encrypted, and using that hash to retrieve the row later [9]. This keeps information encrypted while still making it accessible when needed.
Column-level encryption combines deterministic and symmetric encryption [11]. Symmetric encryption will protect personal information like National Insurance numbers and other

identifiers, while deterministic encryption will be used for less sensitive data such as county [11]. Deterministic encryption also speeds up lookups. Keys for multi-column encryption will be managed by a KMS, allowing external parties to securely encrypt or decrypt data [11]. Finally, TLS and pinning provide a secure connection between the application and the database. TLS protects data in transit at the transport layer, but it can still be vulnerable to man-in-the-middle attacks [10]. Pinning addresses this by verifying the server using a specific certificate or public key [10], ensuring the server is trusted and data cannot be intercepted.

The research has significantly changed the original project plan. Pinning and deterministic indexing were not initially considered but including them results in a much stronger database design. All of these methods are compatible with PostgreSQL, which will host the project.

Existing Platforms

To develop a secure and reliable e-voting system, past implementations must be examined to identify strengths and limitations. Malaysia introduced a smart card known as MyKad in 2001, which stores a voter's fingerprint and is used to authenticate access to a voting booth [16]. On the day, the voter's fingerprint is matched against the fingerprint stored on the MyKad, and a successful match allows the voter to proceed [16].

Although this system provides strong voter authentication, it does not prevent duplicate voting, as no mechanism exists to record whether a person has already voted [16]. Furthermore, the process remains paper-based and therefore retains limitations that this project seeks to address. Nevertheless, MyKad's effectiveness as an authentication method is demonstrated by its widespread use in other Malaysian public services [16].

Building on the biometric authentication that Malaysia have implemented, modern electronic voting systems aim to move beyond paper-based processes by integrating secure digital architectures that address both voter authentication and integrity. Designs commonly include encrypted ballot casting, tamper-resistant storage and verifiable tallying to ensure that each vote accurately counted [20]. However, challenges remain in ensuring system scalability for large countries, protecting sensitive voter data, and maintaining public trust in automated processes [17][19].

Research into various electoral systems has identified several key considerations. These include the high security of biometric authentication, the significant importance of data protection, and the fact that biometric data may be stored either physically or electronically.

Main features

The proposed application will provide a stable and secure voting platform that uses biometric scans to authenticate voters. It will be intuitive and easy to set up, with a strong focus on data security using encryption.

Features

- **Voter Authentication**
  Users can authenticate their identity using biometric scanning before voting.
- **Biometric Device Integration**
  The application will support biometric scanners and receive biometric data securely.
- **Secure Data Storage**
  Voting data will be encrypted and protected, ensuring only authorised officials can access it.
- **Official Access Control**
  Election officials must log in to enable the voting process and manage sessions.
- **Cross-Platform Compatibility**
  The application will work on both Windows and macOS.
- **Government-Style User Interface**
  The interface will be inspired by British Government websites to ensure clarity and accessibility.

Progress to date

To date, the project has focused on building a strong foundation in understanding the problem of current electoral systems and the potential e-voting technologies that address it. This has included reviewing past and current voting systems that align with aspects of the project's aim. Initial research has made good progress in identifying suitable technologies, outlining both the advantages and drawbacks of the biometric options considered. Based on this research, the project is currently leaning towards fingerprint scanning technology due to benefits such as low production cost and strong FAR performance. With further research underway, a final decision is close to being made.

Another key area of progress has been system security. Research has identified a stable and well-tested approach to protecting user data from unauthorised access while still allowing for system maintenance. As security is a core aim of the project, having a clearer idea of the system structure has enabled early experimentation and improved understanding of potential weaknesses in the security design.

Ongoing review of current literature has also been established following advice from previous students on the importance of starting early. Relevant sources are being collected and stored with clear notes on how they support different aspects of the project. One of the main challenges faced so far has been deciding which biometric technology to use. Each option has its own strengths and limitations, making the decision process complex and requiring extensive research.

Personal reflection

Currently the project is researched extensively, and there is a clear idea on what it's going to look like and what's to be involved. The project is on track for what I wish to achieve in terms of outcome and grade. The hardest part has been the research as I have never done it before, but it has gone surprisingly well. I managed to find everything I'm looking for and had positive improvements to the project plan. I'm most happy with my research.

Plans for the remainder

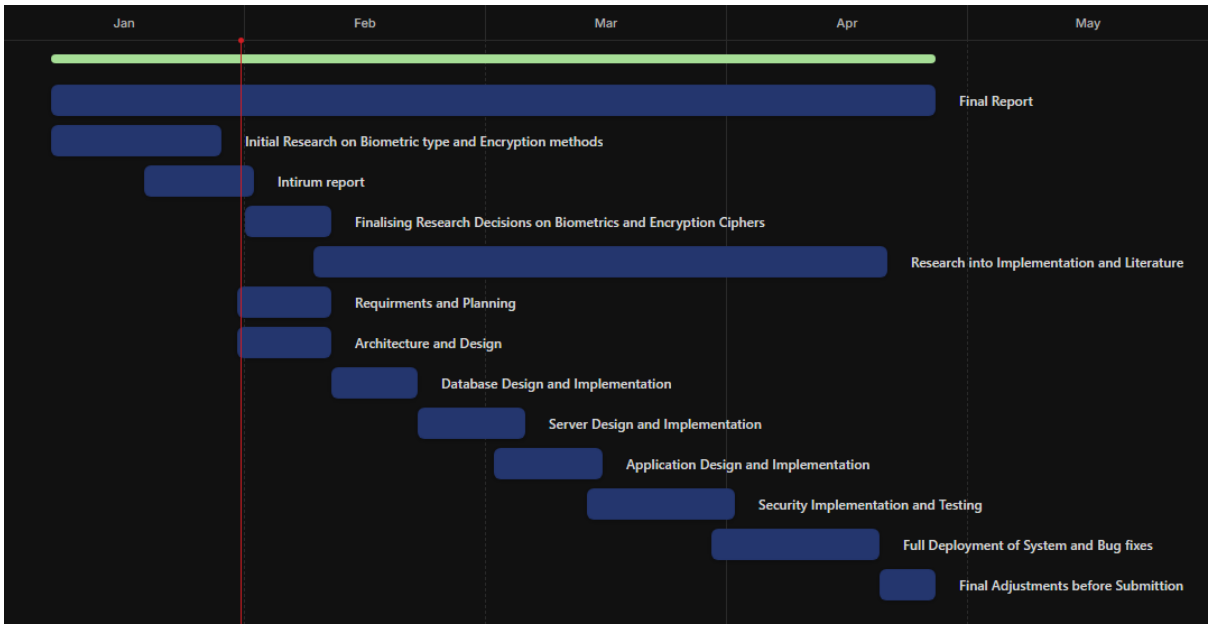

Fig. 1. Gantt chart outlining plans for the project

For the remainder of the project, the work will focus on finalising research, then fully designing and implementing the system, while documenting the process. The initial milestones will centre on planning a well-structured system, including defining clear requirements and producing an architecture that the system will be based on. The development methodology will be agile.

The next set of milestones will focus on implementing the core components of the system. This will begin with database implementation, followed by server development and then application-level functionality. Following this structure ensures that the expected data models are defined early and remain consistent, reducing the need for major changes as implementation progresses.

Subsequent milestones will focus on security measures, including strengthening encryption and securing data transmission. This phase will lead into final testing, where the system will be deliberately stressed in order to identify weaknesses and potential vulnerabilities.

The final milestones will involve full system deployment and resolving any issues identified during testing. This stage will focus on refining and polishing the system in preparation for final submission.

Regarding risk, no risks were identified in the planning or research stages of the project.

References

[1]
K. K. Sadasivuni, M. T. Houkan, M. S. Taha, and J.-J. Cabibihan, "Anti-spoofing device for biometric fingerprint scanners," *IEEE Xplore*, Aug. 01, 2017. https://ieeexplore.ieee.org/abstract/document/8015898.

[2]
R. Alrawili, A. A. S. AlQahtani, and M. K. Khan, "Comprehensive survey: Biometric user authentication application, evaluation, and discussion," *Computers and Electrical Engineering*, vol. 119, no. A, p. 109485, Oct. 2024, doi: https://doi.org/10.1016/j.compeleceng.2024.109485.

[3]
K. Nguyen, H. Proença, and F. Alonso-Fernandez, "Deep Learning for Iris Recognition: A Survey," *ACM computing surveys*, vol. 56, no. 9, pp. 1–35, Apr. 2024, doi: https://doi.org/10.1145/3651306.

[4]
S. Anwarul and S. Dahiya, "A Comprehensive Review on Face Recognition Methods and Factors Affecting Facial Recognition Accuracy," *Lecture Notes in Electrical Engineering*, vol. 597, pp. 495–514, Nov. 2019, doi: https://doi.org/10.1007/978-3-030-29407-6_36.

[5]
Hosam El-Sofany, Belgacem Bouallegue, and Yasser M Abd El-Latif, "A Proposed Biometric Authentication Hybrid Approach Using Iris Recognition for Improving Cloud Security," *Heliyon*, vol. 10, no. 16, pp. e36390–e36390, Aug. 2024, doi: https://doi.org/10.1016/j.heliyon.2024.e36390.

[6]
W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and Accuracy of Fingerprint-Based Biometrics: A Review," *Symmetry*, vol. 11, no. 2, p. 141, Jan. 2019, doi: https://doi.org/10.3390/sym11020141.

[7]
Y. Yu, Q. Niu, L. Xiaoshi, J. Xue, W. Liu, and D. Lin, "A Review of Fingerprint Sensors: Mechanism, Characteristics, and Applications," *Micromachines (Basel)*, vol. 14, no. 6, pp. 1253–1253, Jun. 2023, doi: https://doi.org/10.3390/mi14061253.

[8]
L. Li, P. L. Correia, and A. Hadid, "Face recognition under spoofing attacks: countermeasures and research directions," *IET Biometrics*, vol. 7, no. 1, pp. 3–14, Jan. 2018, doi: https://doi.org/10.1049/iet-bmt.2017.0089.

[9]
P. G. M. R. Alves and D. F. Aranha, "A framework for searching encrypted databases," *Journal of Internet Services and Applications*, vol. 9, no. 1, Jan. 2018, doi: https://doi.org/10.1186/s13174-017-0073-0.

[10]
D. Diaz-Sanchez, A. Marin-Lopez, F. A. Mendoza, P. A. Cabarcos, and R. S. Sherratt, “TLS/PKI Challenges and Certificate Pinning Techniques for IoT and M2M Secure Communications,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3502–3531, 2019, doi: https://doi.org/10.1109/comst.2019.2914453.

[11]
E. Mohamed, “Future Trends and Real-World Applications in Database Encryption,” *Int. J. Electr. Eng. and Sustain.*, vol. 3, no. 1, pp. 28–39, Nov. 2023, Available: https://ijees.org/index.php/ijees/article/view/106

[12]
A. A. Alyousif, A. A. Yassin, and H. M. Mohammed, “Enhancing Searchable Symmetric Encryption Performance through Optimal Locality,” *Informatica*, vol. 49, no. 7, Feb. 2025, doi: https://doi.org/10.31449/inf.v49i7.5925.

[13]
H. Chen, Y. Yang, and S. Lv, “Revisiting frequency-smoothing encryption: new security definitions and efficient construction,” *Cybersecurity*, vol. 7, no. 1, Aug. 2024, doi: https://doi.org/10.1186/s42400-024-00208-w.

[14]
E. Hill, M. Sobolewska, S. Wilks-Heeg, and M. Borkowska, “Explaining electoral fraud in an advanced democracy: Fraud vulnerabilities, opportunities and facilitating mechanisms in British elections,” *The British Journal of Politics and International Relations*, vol. 19, no. 4, pp. 772–789, Jun. 2017, doi: https://doi.org/10.1177/1369148117715222.

[15]
N. Johnston, *EU referendum – the count*, Briefing Paper no. 7588, House of Commons Library, London, UK, May 12, 2016.

[16]
R. Ismail, N. N. Zulkifli, M. M. Magiman, and Mohd, “A Smart Card (MyKad) and Fingerprint Authentication for E-Voting System,” *International Journal of Engineering Research & Technology*, vol. 11, no. 11, Nov. 2022, doi: https://doi.org/10.5281/zenodo.18398554.

[17]
P. Fantozzi, M. Iecher, L. Laura, M. Naldi, and V. Rughetti, “Electronic Voting Worldwide: The State of the Art,” *Information*, vol. 16, no. 8, p. 650, Jul. 2025, doi: https://doi.org/10.3390/info16080650.

[18]
P. Norris, "Will New Technology Boost Turnout? Evaluating Experiments in UK Local Elections," in *Electronic Voting and Democracy: A Comparative Analysis*, N. Kersting and H. Baldersheim, Eds. London, UK: Palgrave Macmillan, 2004, pp. 193–225.

[19]
T. Treier and K. Düüna, “Identifying and Solving a Vulnerability in the Estonian Internet Voting Process: Subverting Ballot Integrity Without Detection,” *IEEE Access*, vol. 12, no. 10.1109/ACCESS.2024.3521337, pp. 197766–197782, 2024, doi: https://doi.org/10.1109/access.2024.3521337.
[20]
Q. Han, X. Zhang, S. Lu, X. Zhao, and Z. Yan, “An SGX-based online voting protocol with maximum voter privacy,” *Journal of Systems Architecture*, vol. 151, p. 103144, Jun. 2024, doi: https://doi.org/10.1016/j.sysarc.2024.103144.

[21]
A. Devasia, “Biometric Access Control System Price: Full Guide (2024),” *Safe and Sound Security*, May 29, 2024. https://getsafeandsound.com/blog/biometric-access-control-system-price/