Automation, Control and Intelligent Systems
2025, Vol. 13, No. 1, pp. 12-21
https://doi.org/10.11648/j.acis.20251301.12

Research Article

Radio Frequency Identification (RFID) Based Voting System Using Internet of Thing

Moradeke Grace Adewumi*

Department of Computing and Information Sciences, University of Lay Adventist of Kilgali, Kigali, Rwanda

Abstract

This project focuses on the development of a secured Radio Frequency Identification (RFID)-based electronic voting application using Flutter, Firebase and Arduino. The application aims to enhance the voting process by integrating RFID technology for user authentication, ensuring a secure and seamless experience for voters. The system employs RFID cards to authenticate users, allowing only authorized individuals to vote, with Firebase enforcing a single-vote policy to prevent electoral fraud. Most important features include real-time voting data updates, robust encryption protocols for safeguarding user interface designed for accessibility. The methodology encompasses hardware integration with RFID readers, microcontrollers, and software development leveraging Flutter for the client-side and Firebase for backend services. Extensive testing and security measures were carried out to ensure data integrity, privacy, and system reliability. This innovation addressed critical challenges in electronic voting, such as voter impersonation, multiple voting, and cybersecurity threats, contributing to the modernization of electoral processes while maintaining transparency and trust in democratic systems. By leveraging RFID for user authentication, the system ensures that only eligible voters can access the platform, maintaining the integrity and transparency of the voting process. Additionally, the application enhances user experience through a streamlined interface designed with Flutter, providing simplicity and accessibility for diverse users. The incorporation of Firebase as a backend ensures real-time data handling, robust authentication, and prevention of multiple votes.

Keywords

Cyber Security, Radio Frequency Identification Number, Electronic Voting, Leveraging

1. Background Study

The digital age has revolutionized various aspects of human interaction, including the political sphere where the concept of online voting is becoming increasingly popular. Voting systems are crucial in democratic societies, ensuring that citizens can participate in choosing their leaders and influencing important decisions. However, with the introduction of electronic and online voting, ensuring the security, integrity, and privacy of voters is critical to maintain trust in the democratic process. One way to enhance the security of these voting systems is through the development of an Authenticator App tailored specifically for voting system users. Traditional voting systems rely on physical presence at polling stations, where voters cast ballots either by paper or electronic machines. While secure, these methods can be inconvenient,

*Corresponding author: adewumi.moradeke@bouesti.edu.ng (Moradeke Grace Adewumi), moradekegraceadewumi@unilak.ac.rw (Moradeke Grace Adewumi)

Received: 3 February 2025; **Accepted:** 17 February 2025; **Published:** 11 March 2025

time-consuming, and prone to human errors in counting or handling the ballots. The increasing shift towards online or electronic voting (e-voting) introduces convenience but also brings challenges regarding voter authentication, data integrity, and fraud prevention. In an online voting system, voters can cast their ballots from remote locations using computers or mobile devices. The core challenge in such systems is ensuring that:

Only eligible voters can vote, each voter votes only once, voter identity is protected to prevent coercion and maintaining the secrecy of the ballot and the voting data remains tamper-proof and secure. To address these issues, many systems incorporate authentication mechanisms and an authenticator app plays a pivotal role by providing a second layer of security to the voting system, ensuring that only the rightful user can access the voting platform [3].

1.1. Current Challenges in Voting Systems

Despite the growing adoption of e-voting and online voting systems, there are several significant challenges as identified by [4] that must be addressed to ensure system integrity issues:

1) Voter Fraud: The potential for individuals to vote multiple times or impersonate other users is a primary concern in online voting systems.
2) Security Threats: Voting systems are increasingly becoming targets of cyber-attacks, including denial-of-service attacks, phishing schemes, and man-in-the-middle attacks, all of which aim to compromise the voting process.
3) Data Integrity: The security of the data transmitted and stored in the voting system is vital to ensure that votes are not tampered with or altered.
4) Voter Privacy: It is essential to maintain the anonymity of voters to prevent coercion or retaliation, a challenge that becomes more complex in the digital realm.

Several existing technologies and standards can be leveraged in the development of an authenticator app for a voting system [11].

1) OAuth and OpenID Connect: These are open standards for authorization and identity verification that can be integrated into the voting system's authentication process.
2) TOTP (Time-Based One-Time Password): This algorithm is commonly used in authentication apps like Google Authenticator and provides secure, time-limited OTPs.
3) Public Key Infrastructure (PKI): A system of digital certificates and keys that can be used to secure the communication between the voting system and the authenticator app.

Several countries and regions have explored the use of digital tools, including authenticator apps, in their voting systems [7]. Estonia is known for its advanced online voting system, where citizens use a national ID card to securely cast their votes. Though it uses a different method like digital signatures which serves as a strong example of the potential for technology in voting.

Internet of Things (IoT) involve use of technology in revolutionizing e-voting by enhancing the security and transparency of the electoral process. The incorporation of artificial intelligence (AI) and machine learning (ML) into e-voting systems enhances their effectiveness [6]. AI algorithms can scrutinize voting trends and identify anomalies, aiding in the avoidance of fraudulent actions and coercion. Machine learning methodologies can augment voter authentication systems, expand accessibility for varied populations, and optimize the efficiency of networks during high-demand voting intervals, hence this study.

1.2. Statement of the Problem

The advancement of technology has transformed the electoral process, leading to the adoption of electronic voting (e-voting) systems as a means to enhance accessibility and efficiency in elections. However, these systems face significant security challenges that jeopardize the integrity of the electoral process. One of the most pressing issues is the authentication of voters, which is critical for ensuring that only eligible individuals can cast votes, thereby preventing electoral fraud and maintaining public trust in democratic process. Current e-voting systems often rely on traditional authentication methods, such as single-factor authentication, which are inadequate in the face of increasingly sophisticated cyber threats. These methods expose e-voting systems to various vulnerabilities, including unauthorized access, vote tampering, and impersonation. [13] Highlights that many existing e-voting platforms lack robust security measures, making them susceptible to attacks that can compromise the integrity of the voting process. Hence the development of radio frequency identification-based voting system using internet of thing.

1.3. Motivation of the Study

E-voting systems are increasingly targeted by cyber threats, including identity theft, vote tampering, and system manipulation. An authenticator app provides multi-factor authentication (MFA) to secure voter identities to ensure that only authorized users access the system. This prevents unauthorized voting, reinforces voter integrity and prevent fraud manipulation.

1.4. Aim and Objectives

The primary aim of the study is to design a reliable authentication mechanism using RFID internet of things. The specific objectives is to ensure that only authorized individuals with unique RFID cards can access the voting system thereby preventing voters' impersonation and unauthorized

access from voting.

2. Literature Review

2.1. Overview of E-voting Systems

The advent of electronic voting systems has revolutionized the electoral process, promising enhanced efficiency, accessibility, and transparency. However, the implementation of secure e-voting systems has posed significant challenges, particularly concerning user authentication. An authenticator app designed for e-voting users can serve as a pivotal tool in ensuring secure and reliable voting processes. This literature review synthesizes key findings from recent research on e-voting security, with a particular focus on the role of authentication mechanisms, specifically those that could be integrated into an authenticator app.

2.2. Frameworks and Security Vulnerabilities

A framework for securing e-voting systems, which incorporates cryptographic techniques and decentralized architectures was proposed by [5]. They note that while their framework offers significant security advantages, the complexity of implementation poses challenges. An authenticator app that aligns with this framework could simplify the user experience while maintaining the necessary security measures.

Overview of security vulnerabilities in electronic voting systems and recommending more resilient designs [1]. They acknowledged the lack of real-world testing for proposed solutions, suggesting a gap in practical implementation that an authenticator app could address by providing a user-friendly interface for securely verifying voter identity. In order to address this issue, SecureBallot was proposed to secure open-source e-Voting system which can decouple the voter identification and voting phases by means of proven cryptographic technologies.

2.3. Addressing Security Threats

Various security threats that e-voting systems face were analysed and proposal for effective countermeasures were made by [9]. Their work highlighted the need for comprehensive security strategies, which could be augmented by an authenticator app that employs secure authentication mechanisms, such as time-based one-time passwords (TOTPs) or biometric verification and facial recognition system.

Discussion on current challenges in electronic voting and the innovations aimed at mitigating these issues were highlighted [14]. The risks associated with new technologies, which may inadvertently exacerbate existing problems were also discussed. The development of an authenticator app must therefore be approached with caution, ensuring that it enhances security without introducing new vulnerabilities.

2.4. Related Works in E-voting Systems

The development of an authenticator app for e-voting systems users is essential for enhancing the security and integrity of electronic voting processes. While blockchain technology offers promising solutions for secure e-voting, challenges related to authentication, scalability, and public trust remain. This literature review highlighted the critical role of secure authentication mechanisms and the need for comprehensive frameworks that incorporate usability, accessibility, and real-world applicability. Future research should focus on the practical implementation of authenticator apps, exploring their effectiveness in mitigating security threats and enhancing voter confidence in e-voting systems. Security concerns in e-voting, was addressed by emphasizing the importance of security and legal measures during voting. The study was based on ISO15408 certification process, a framework for independent security evaluations. The paper proposed a methodology that combines legal and technical requirements for e-voting security assessments, focusing on BPMN processes to model scenarios. A detailed analysis of a Solidity e-voting smart contract reveals its vulnerabilities and limitations. The research also produces a BPMN representation of an e-voting scenario, aligning logical behaviour with smart contract implementation. The aim was to bridge the gap between legal and technical aspects of e-voting in order to enhance security and transparency [8]. Blockchain-Based E-Voting Systems as a reviewed Technology [3]. The review explored potential solutions for secure and transparent e-voting systems using blockchain technology. They came up with enhanced security and anonymity. Nevertheless, scalability, cost-effectiveness, authentication, privacy, and security vulnerabilities in e-voting systems were not addressed in the study. Identification of e-voting auditing to balance the equation of Insecure Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging, and Monitoring [15]. He affirmed that the purpose of cyber attacks alone can threaten the stability of the country and disturb other factors. Exploration on Evaluating Electronic Voting Security comparative analysis [14]. The review and research done revealed that they conducted a comparative analysis of different e-voting systems, focusing on their security measures and vulnerabilities. They also point out inconsistencies in security measures among systems, and the necessity for better auditing processes. E-voting using internet of things to prevent security and privacy challenges [10]. The work discussed the security and privacy challenges associated with e-voting, offering solutions to enhance system integrity. They introduced a secure and transparent e-voting mechanism through IoT devices using Blockchain technology with the aim of detecting and resolving the various threats caused by an intruder at various levels in the voting system. However, lack of standardized protocols and potential for cyberattacks which are major vulnerabilities was not discussed. Framework for secure e-voting systems that includes cryptographic tech-

niques and decentralized architectures. However, the complexity of implementation and the need for widespread consensus on security standards are the major concerns [2]. Review on Security Vulnerabilities in E-Voting was carried out [12]. A thorough overview of vulnerabilities in electronic voting systems and recommendations for more resilient designs vying to make these recommendations a game-changing one was actualized. But then they were forced to acknowledge the lack of real-world testing of proposed solutions in various environments. An efficient unidirectional proxy re-encryption technique that facilitates the re-encryption of vote content and the authentication of users' identities was suggested by [5]. This resulted from the overhead burden on the voting system noted in the prior e-voting system encryption approach utilizing pairing operations. Consequently, it is imperative to devise a protocol that safeguards voter privacy while ensuring high efficiency for the proper execution of e-voting.

3. Methodology

3.1. Overview

Iterative Waterfall SDLC Model was adopted for this study, because it combines the sequential steps of the traditional Waterfall Model with the flexibility of iterative design and it also allows for improvements and changes to be made at each stage of the development process, instead of waiting until the end of the project.

1) Systematic Development in Phases: The project breaks down into distinct phases: requirements gathering, system design, development, implementation, testing, and results evaluation. These phases indicate a structured, step-by-step approach typical of the Iterative SDLC Model.
2) Incremental Refinements: The methodology focuses on integrating and testing individual components, such as the RFID reader, Firebase backend, and Flutter interface, before moving to a full system test. Each component was independently validated (e.g., unit testing, integration testing), which reflects iterative development and refinement.
3) Clear Functional Requirements: Functional and non-functional requirements were outlined in advance, indicating a planned and progressive approach.
4) Deliverables and Documentation: The project emphasizes documentation (e.g., detailed system design, hardware/software requirements, test results), a hallmark of Iterative SDLC.

3.2. System Design

The voting system is composed of some main components: the client-side application built with Flutter, the backend services provided by Firebase, cloud infrastructure by Blynk, arduino board and RFID card reader RFID integration for secure authentication. Users interact with the Flutter app, where they log in and vote using an RFID card. Firebase handles backend functionalities such as user authentication, data storage, and real-time updates. RFID technology ensures that only authorized users can log in and cast a vote, with Firebase enforcing single-use vote constraints.

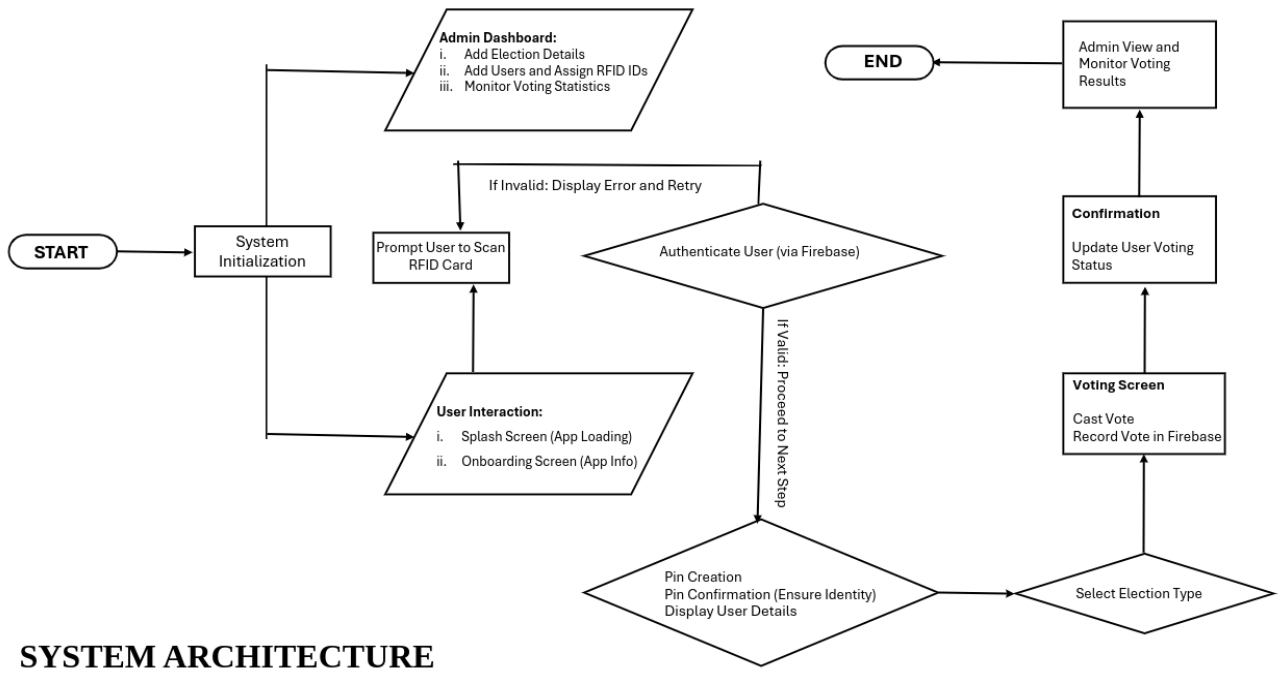

Figure 1. *The System Architecture of the E-Voting.*

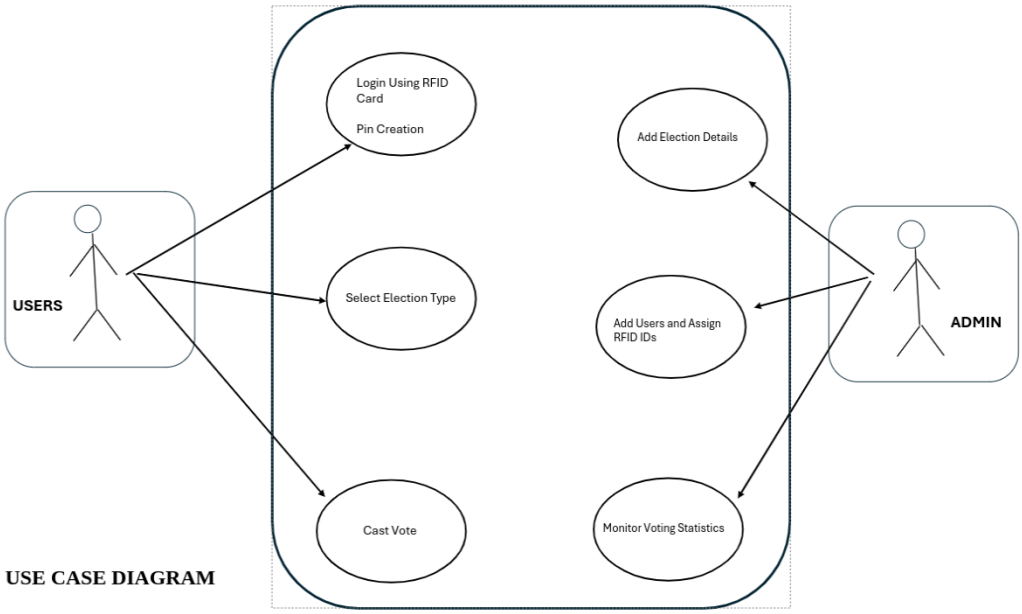

Figure 2. *Use Case Diagram.*

3.3. System Requirements

3.3.1. Hardware Requirements

a. RFID Reader (RFID-RC522) to read the card details assigned to a RFID card.
b. Mobile device (Android or iOS) with Flutter app support.
c. Arduino board and Jumper wires for the complete connection of all hardware components
d. Server or workstation for Firebase integration and development

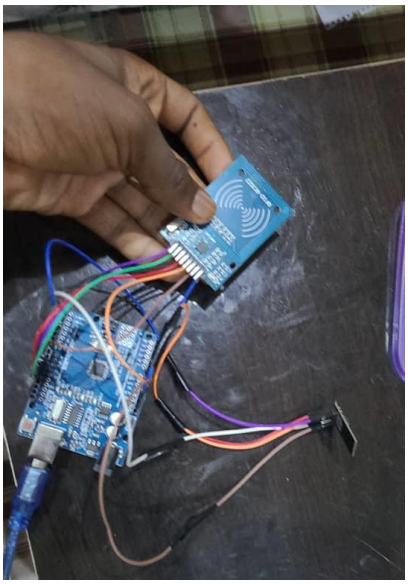

Figure 3. *The complete Arduino Board.*

3.3.2. Software Requirements

a. Flutter and Dart SDK (for app development)
b. Firebase (for authentication and data storage)
c. Android Studio (for coding and testing)
d. Important Flutter dependencies (for handling RFID data, getting HTTP requests and communicating with firebase): firebase_core (version 3.8.1), dio (version 5.7.0) and cloud_firestore (version 5.5.1)

3.3.3. Functional Requirements

a. User authentication through RFID cards.
b. Real-time voting access and restriction using Firebase.
c. Enforcement of single-vote functionality to prevent double voting.

3.3.4. Non-Functional Requirements

a. Performance: The app will provide a seamless, real-time user experience.
b. Reliability: Reliable RFID and Firebase integration ensures accurate vote counting and authentication.
c. Usability: The UI should be intuitive and user-friendly.
d. Security: Strong data protection to secure user authentication and voting data.

3.4. System Development

3.4.1. Programming Tools and Technologies

a. Flutter: Flutter is used for building a cross-platform mobile app that provides a smooth, responsive user interface.
b. Firebase: Firebase is used for backend services, including real-time database and authentication, ensuring se-

cure data handling.

c. Blynk.cloud is used as the cloud infrastructure that handles the collection of all hardware components and software data/information.

d. RFID Integration: RFID libraries are used to integrate RFID-based login functionality, allowing secure and reliable authentication of users.

3.4.2. Database Design

Firebase serves as a NoSQL database for storing user profiles, voting data, and RFID authentication status. The database schema includes collections for user information, RFID card status, and vote records. Each user's vote status is stored to prevent multiple votes.

User Interface (UI) Design:

The app interface is designed in Flutter, focusing on simplicity and ease of navigation to enhance user experience. UI principles, such as clarity and responsiveness, ensure the app is accessible and intuitive for all users.

3.5. Implementation Details

RFID Integration:

a. The RFID reader is configured to communicate with the Flutter app. RFID card data is captured and validated upon login.

b. A unique RFID card ID is checked against Firebase to confirm whether the user has access and if they have previously voted.

Firebase Setup:

a. Firebase Authentication is configured to store and manage user data securely.

b. Firebase real time Database is set up to store voting data and track whether each user has cast a vote.

Voting Process:

a. Upon successful RFID authentication, Firebase checks the user’s voting status.

b. If the user has not voted, they are granted access to the voting interface. After voting, their status is updated in Firebase to prevent further voting attempts.

Testing Procedures:

a. Unit Testing: Each module (e.g., RFID login, Firebase data retrieval) is tested independently.

b. Integration Testing: The interactions between Flutter, Firebase, and RFID are tested to ensure smooth operation.

c. System Testing: Full system testing is performed to verify end-to-end functionality, including user login, voting, and data validation.

3.6. Security Measures

1) Data Protection: Firebase provides data security and access control, ensuring that only authenticated users can access voting functionalities.

2) Authentication Security: RFID cards are used as a secure form of user authentication, minimizing the risk of unauthorized access.

3) Preventing Multiple Votes: Firebase stores each user's voting status, checking it before allowing access to the voting interface to ensure only one vote per user.

4. Results

Admin Dashboard 1 - Adding Election

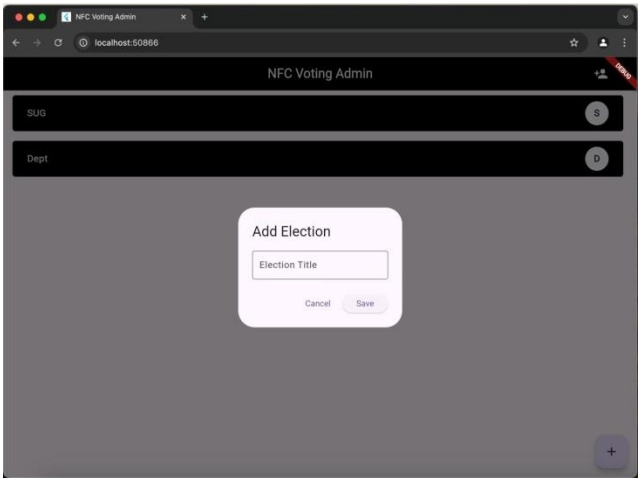

Figure 4. *The Admin dashboard.*

This determine where the admin will add type of election to be conducted.

Admin Dashboard 2 - Adding Users and their unique ID

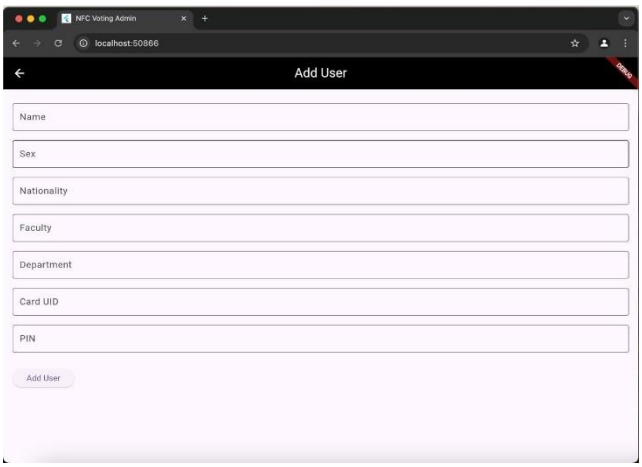

Figure 5. *Admin Dashboard 2.*

This is also part of the admin dashboard where the admin can add users and their unique identifications card (ID) for verifications.

Admin Dashboard 3 - Election Statistic Page

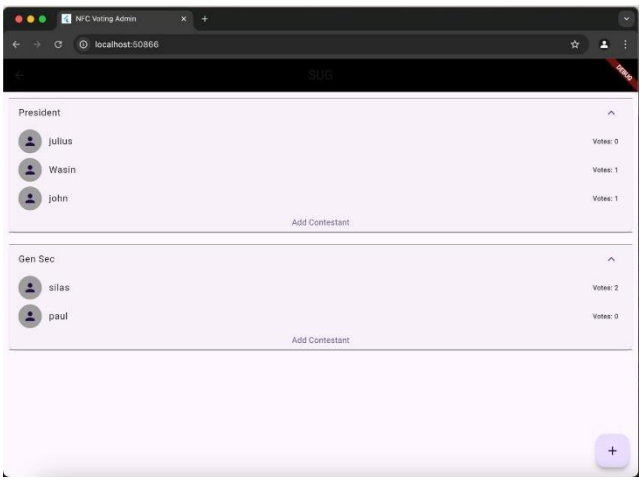

Figure 6. *Election Statistics Page.*

This is the page where admins can add positions contesting for and the candidates for each post. Admins can equally check the votes of each candidate here.

Splash Screen

Figure 7. *Loading page.*

This is just a screen that shows for a few seconds indicating the loading system.

ONBOARDING SCREEN

Figure 8. *Voting Process.*

This screen gives more information about the app to the user so they can understand the services the app offers.

Prompt Screen - Scan NfC enabled Card

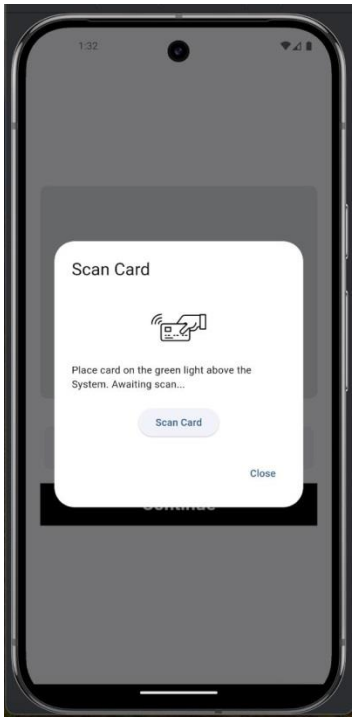

Figure 9. *The Scanning Stage.*

This screen prompts the user to scan their card on the RFID-RC522 card reader so the app can get their details using

the HTTP GET request.

Pop-Up Screen - Successful Login

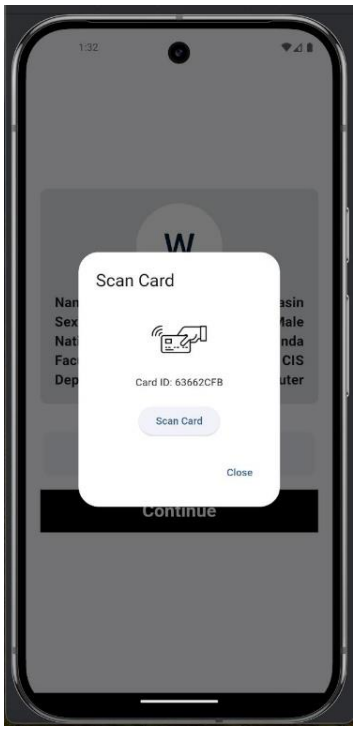

Figure 10. *Successful Login page.*

This screen shows the unique ID of the scanned card as a pop-up menu for successful login.

User Details -Pin Confirmation

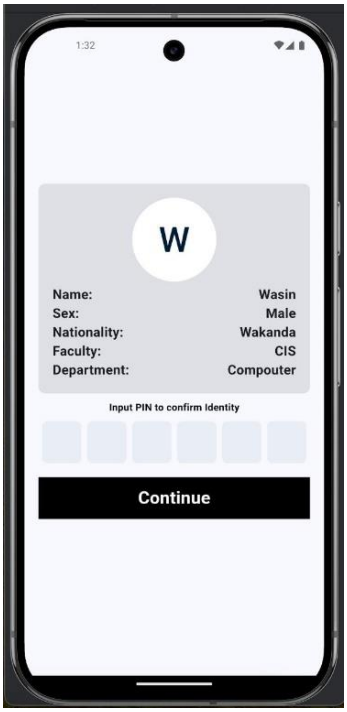

Figure 11. *Authentication Page.*

This page shows the users' details and also confirms if the user trying to vote is the owner of that card. So a pin is needed to confirm each user identity.

Vote Selection Screen

Figure 12. *Selection Page.*

This screen prompts the user to select the election he/she wants to participate in.

Election Page

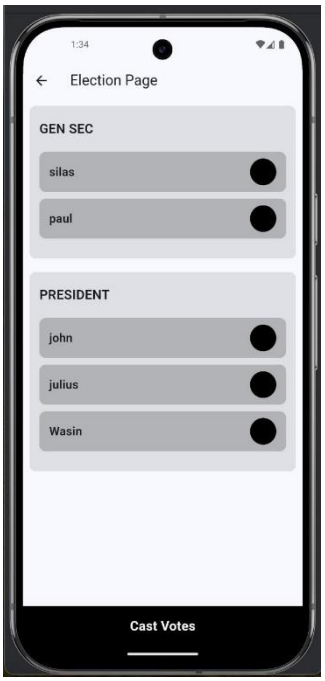

Figure 13. *Election Page.*

This is the screen whereby users are allowed to cast their votes and choose their favourite candidate for each post.

5. Discussion and Summary

5.1. Discussion

The results of the RFID-Based Voting System demonstrated the practicality and security of integrating internet of things into e-voting for enhancing the voting process. The system's ability to authenticate voters using RFID cards eliminates the risks associated with unauthorized access and multiple voting. The admin dashboard proved effective in managing elections, adding users, and monitoring live voting statistics. Features like the onboarding screen and NFC card prompt made the system intuitive for users, ensuring a seamless voting experience.

The integration of Arduino IoT components facilitated real-time data transfer between the hardware and software layers, ensuring instant verification and vote recording. This setup relied on cloud infrastructures like Firebase and Blynk, enabling real-time updates and secure data storage. Firebase's authentication and database functionalities ensured that each voter could only cast a single vote, addressing concerns of electoral fraud. The NFC reader linked with the Arduino further streamlined the authentication process, ensuring fast and accurate validation of voter credentials.

Despite the system’s successes, challenges like dependency on stable internet connections and the complexity of hardware-software integration were noted. The reliance on NFC and RFID technologies may exclude users in regions without access to such equipment, highlighting a limitation in scalability. However, these results validate the feasibility of RFID-based systems for secure, transparent, and efficient voting, with future opportunities for scalability and refinement to address these limitations.

5.2. Summary

The document outlines the development of an RFID-based voting system designed to enhance security and accessibility in electoral processes. It begins with an introduction to the challenges of traditional and electronic voting systems, emphasizing issues such as voter fraud, data integrity, and user privacy. It proposes an RFID-based authenticator app to address these problems, integrating multi-factor authentication (MFA) and other advanced security measures to ensure the system's reliability. The methodology highlights the system's core components, including a Flutter-based mobile application, Firebase for backend services, and RFID technology for secure authentication. The system is designed to allow users to log in with RFID cards, authenticate through Firebase, and cast a single vote, with Firebase ensuring that users cannot vote multiple times. The integration of real-time authentication, encryption protocols, and user-friendly design ensures both security and accessibility.

The project also includes detailed system requirements, covering hardware such as RFID readers and cards, and software like Flutter, Dart SDK, and Firebase. Functional requirements focus on user authentication, real-time voting access, and single-vote enforcement. Security measures, including data protection, RFID authentication, and prevention of multiple votes, are integral to the system. Testing procedures involve unit, integration, and system testing to ensure seamless interaction between components and overall functionality. The document also details various application screens, from the admin dashboard for election setup and user management to user interfaces for authentication, voting, and results display. The study underscores the importance of secure and user-friendly e-voting systems, advocating for the widespread adoption of technologies like RFID and Firebase to modernize electoral processes while maintaining voter trust and data integrity.

6. Conclusion

The document concludes by emphasizing the development of a secure and efficient voting application utilizing RFID technology, integrated with Flutter and Firebase. This innovative approach addressed the challenges associated with electronic voting, such as security vulnerabilities, voter impersonation, and data integrity. By leveraging RFID for user authentication, the system ensures that only eligible voters can access the platform, maintaining the integrity and transparency of the voting process. Additionally, the application enhances user experience through a streamlined interface designed with Flutter, providing simplicity and accessibility for diverse users. The incorporation of Firebase as a backend ensures real-time data handling, robust authentication, and prevention of multiple votes, safeguarding the electoral process. Overall, this project demonstrates a comprehensive solution to modern voting challenges, paving the way for scalable, secure, and user-friendly electronic voting systems.

Abbreviations

AI	Artificial Intelligence
BPMN	Business Processes Modeling Notation
IoT	Internet of Things
MFA	Multi-Factor Authentication
ML	Machine Learning
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification
SDLC	System Development Life Cycle
TOTP	Time-Based One-Time Password

Author Contributions

Moradeke Grace Adewumi is the sole author. The author

read and approved the final manuscript.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Agate, V., De Paola, A., Ferraro, P., Lo Re, G., & Morana, M. (2021). NDS LAB-Networking and Distributed Systems SecureBallot: A Secure Open Source e-Voting System http://www.diid.unipa.it/networks/

[2] Azameti, A. A. K., Koi-akrofi, G., Quist, S. C., & Dayie, R. (2022). Systematic Literature Review : A Novel Framework for Evaluating Electronic Voting Systems Artifacts.

[3] Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. (2024). Blockchain-Based E-Voting Systems: A Technology Review. Electronics (Switzerland), 13(1), 1-38. https://doi.org/10.3390/electronics13010017

[4] Jafar, U., Ab Aziz, M. J., Shukur, Z., & Hussain, H. A. (2022). A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems. Sensors, 22(19). https://doi.org/10.3390/s22197585

[5] Li, W., & Xiong, H. (2021). Efficient proxy re-encryption scheme for e-voting system. KSII Transactions on Internet and Information Systems, 15(5), 1847-1870. https://doi.org/10.3837/tiis.2021.05.015

[6] Mannonov, K. M. ugli, & Myeong, S. (2024). Citizens' Perception of Blockchain-Based E-Voting Systems: Focusing on TAM. Sustainability (Switzerland), 16(11), 1-19. https://doi.org/10.3390/su16114387

[7] Muñoz, L. A., Bolívar, M. P. R., & Villamayor Arellano, C. L. (2022). Factors in the adoption of open government initiatives in Spanish local governments. Government Information Quarterly, 39(4). https://doi.org/10.1016/j.giq.2022.101743

[8] Pastena, A. (2024). A methodology for vulnerability assessment and threat modelling of an e-voting platform based on Ethereum blockchain. Artificial Intelligence and Law, 12(December). https://iris.unicampania.it/handle/11591/519108

[9] Peelam, M. S., Kumar, G., Shah, K., & Chamola, V. (2024). DemocracyGuard: Blockchain-based secure voting framework for digital democracy. Expert Systems, March 2024, 1-27. https://doi.org/10.1111/exsy.13694

[10] Rathee, G., Iqbal, R., Waqar, O., & Bashir, A. K. (2021). On the Design and Implementation of a Blockchain Enabled E-Voting Application within IoT-Oriented Smart Cities. IEEE Access, 9, 34165-34176. https://doi.org/10.1109/ACCESS.2021.3061411

[11] Singh, I., Kaur, A., Agarwal, P., & Idrees, S. M. (2024). Enhancing Security and Transparency in Online Voting through Blockchain Decentralization. SN Computer Science, 5(7). https://doi.org/10.1007/s42979-024-03286-2

[12] Sunardi, Riadi, I., & Raharja, P. A. (2019). Vulnerability analysis of E-voting application using open web application security project (OWASP) framework. International Journal of Advanced Computer Science and Applications, 10(11), 135-143. https://doi.org/10.14569/IJACSA.2019.0101118

[13] Vladucu, M. V., Dong, Z., Medina, J., & Rojas-Cessa, R. (2023). E-Voting Meets Blockchain: A Survey. IEEE Access, 11(February), 23293-23308. https://doi.org/10.1109/ACCESS.2023.3253682

[14] Zhao, L. L. (2024). Ethnic votes and parties' mobilization: A case study of New Zealand. Politics and Policy, 52(3), 614-632. https://doi.org/10.1111/polp.12599

[15] Zissis Dimitrios. (2011). Methodologies and Technologies for Designing Secure Electronic Voting Information Systems. 263. www.syros.aegean.gr/documents/phd/phd_dzissis.pdf