telecom

MDPI

Article

RFID-Enabled Electronic Voting Framework for Secure Democratic Processes

Stella N. Arinze [1] and Augustine O. Nwajana [2,*]

[1] Department of Electrical and Electronic Engineering, Enugu State University of Science and Technology, Agbani PMB 01660, Enugu, Nigeria; ndidi.arinze@esut.edu.ng
[2] School of Engineering, University of Greenwich, Chatham, Kent ME4 4TB, UK
* Correspondence: a.o.nwajana@greenwich.ac.uk

Abstract

The growing global demand for secure, transparent, and efficient electoral systems has highlighted the limitations of traditional voting methods, which remain susceptible to voter impersonation, ballot tampering, long queues, logistical challenges, and delayed result processing. To address these issues, this study presents the design and implementation of a Radio Frequency Identification (RFID)-based electronic voting framework that integrates robust voter authentication, encrypted vote processing, and decentralized real-time monitoring. The system is developed as a scalable, cost-effective solution suitable for both urban and resource-constrained environments, especially those with limited infrastructure or inconsistent internet connectivity. It employs RFID-enabled smart voter cards containing encrypted unique identifiers, with each voter authenticated via an RC522 reader that validates their UID against an encrypted whitelist stored locally. Upon successful verification, the voter selects a candidate via a digital interface, and the vote is encrypted using AES-128 before being stored either locally on an SD card or transmitted through GSM to a secure backend. To ensure operability in offline settings, the system supports batch synchronization, where encrypted votes and metadata are uploaded once connectivity is restored. A tamper-proof monitoring mechanism logs each session with device ID, timestamps, and cryptographic checksums to maintain integrity and prevent duplication or external manipulation. Simulated deployments under real-world constraints tested the system's performance against common threats such as duplicate voting, tag cloning, and data interception. Results demonstrated reduced authentication time, improved voter throughput, and strong resistance to security breaches—validating the system's resilience and practicality. This work offers a hybrid RFID-based voting framework that bridges the gap between technical feasibility and real-world deployment, contributing a secure, transparent, and credible model for modernizing democratic processes in diverse political and technological landscapes.

Keywords: smart card authentication; voter identity verification; encrypted vote storage; tag cloning prevention; cryptographic data protection; offline data synchronization

Academic Editor: Przemysław Falkowski-Gilski

Received: 7 September 2025
Revised: 10 October 2025
Accepted: 11 October 2025
Published: 16 October 2025

Citation: Arinze, S.N.; Nwajana, A.O. RFID-Enabled Electronic Voting Framework for Secure Democratic Processes. *Telecom* **2025**, *6*, 78. https://doi.org/10.3390/telecom6040078

1. Introduction

The global landscape is undergoing a profound shift towards digitalization, with technology increasingly integrated into all facets of life. One of the most critical transformations lies in the evolution of voting systems, driven by the demand for more secure, transparent, and efficient electoral processes. Traditional voting methods, although long

established, often grapple with issues such as voter fraud, inaccurate vote counting, long queues, and logistical complications in result transmission. These shortcomings not only erode public trust but also risk voter disenfranchisement and delayed election outcomes. As populations grow and more nations embrace technological innovation in governance, the need for robust electronic voting (e-voting) systems has intensified. While e-voting offers potential solutions, it is not without challenges. Cybersecurity threats, ranging from hacking and phishing to data breaches, continue to cast doubt on the reliability of many existing platforms. Additionally, core issues such as voter authentication, system transparency, and tamper-proof vote recording remain unresolved. To strengthen the integrity of e-voting systems, recent research has explored the integration of biometric technologies. A study examined the use of facial recognition to streamline voter identification and reduce fraudulent activities [1]. While promising, biometric solutions face barriers including high deployment complexity, potential privacy violations, and environmental sensitivity affecting accuracy. It was observed that although biometric verification increased voter confidence, its reliability was compromised under varying lighting conditions and with certain demographic groups [2]. Another study developed a machine learning-based multimodal biometric authentication system integrating facial and fingerprint recognition [3]. The study demonstrated high accuracy and reliability in voter verification, addressing challenges related to impersonation and unauthorized access. Cryptographic techniques such as public-key infrastructure (PKI) and digital signatures are often combined with biometric data to enhance verification. Though these technologies improve security, they too have limitations. Fingerprint scanners may struggle with accuracy and acceptance in diverse populations, while facial recognition remains vulnerable to spoofing and privacy concerns. Other emerging technologies including the Internet of Things (IoT) and blockchain have also been applied to reinforce e-voting frameworks. IoT facilitates device monitoring during elections, while blockchain ensures immutable, decentralized vote records. Researchers in [4] conducted a comprehensive survey on blockchain-based e-voting mechanisms and proposed a novel framework leveraging blockchain's transparency and immutability. Similarly, another study pointed out that blockchain solutions often suffer from scalability issues and require substantial computational power, which is a significant obstacle in regions with limited infrastructure [5]. Further, a study introduced a scalable, decentralized, privacy-preserving e-voting system utilizing zero-knowledge off-chain computations to enhance scalability while maintaining voter privacy and data integrity [6]. Despite these innovations, persistent gaps remain in achieving cost-effective, infrastructure-light, secure, and transparent e-voting solutions that can function reliably in low-resource and high-risk environments.

Among these evolving technologies, Radio Frequency Identification (RFID) stands out as a compelling alternative. Widely adopted in areas such as asset tracking and inventory management, RFID offers real-time, contactless identification using unique tags and readers. Its utility in security-critical domains such as healthcare, finance, and access control has been well documented. RFID enables rapid, non-intrusive authentication, reducing human error and minimizing opportunities for manipulation. Its application in e-voting includes tracking ballots, authenticating voters, and ensuring system integrity through encryption and secure protocols. What sets RFID apart is its operational simplicity and cost-effectiveness, especially in low-resource environments. Unlike blockchain or biometric systems that may require advanced hardware, RFID can function with minimal infrastructure, making it particularly suitable for developing nations. Recent advancements have enhanced RFID's security and privacy features. RFID-enabled smart cards can store encrypted voter data, ensuring secure transmission and storage. Additionally, RFID systems can provide real-time reporting to electoral authorities, enabling swift anomaly

detection and promoting transparency—both critical to public confidence in democratic processes. A researcher presented the development of a secure RFID-based electronic voting application using Flutter, Firebase, and Arduino, ensuring robust encryption and real-time data updates [7]. Another study proposed an RFID-based voting system to replace traditional paper elections, highlighting RFID's strengths in reducing electoral fraud, minimizing human error, and improving voting efficiency [8]. While these contributions are notable, our research builds on and extends them by offering a more robust framework that integrates RFID-based voter authentication, AES-128 encrypted vote transmission, tamper-proof data storage, and decentralized real-time monitoring. However, existing Arduino–RFID–GSM systems remain largely at the prototype level. They often rely on simple UID checks that are vulnerable to cloning, lack second-factor voter authentication, omit formal key management, and depend heavily on continuous connectivity. Such designs do not offer a framework capable of scaling or withstanding real-world failures. This work therefore introduces a framework rather than just a device. This framework integrates a challenge–response protocol with per-card cryptographic keys to prevent cloning, incorporates a second-factor authentication layer to secure voter identity, adopts an offline-first design with secure synchronization to support low-connectivity regions, and embeds a formal threat model with backend transparency that has been stress-tested to handle up to 10,000 devices and 1 million voters. In contrast to systems that rely heavily on constant internet connectivity or remain confined to prototype-level demonstrations, our solution supports defines a scalable, security-layered architecture that election bodies can directly adopt in politically sensitive and infrastructure-limited contexts. These enhancements make our system significantly more scalable, secure, and adaptable to electoral environments with limited infrastructure and public trust. Consequently, this study introduces a comprehensive RFID-enabled e-voting framework that bridges the gap between technical feasibility and practical deployment. By aligning the operational simplicity of RFID with advanced security protocols and transparency mechanisms, the system aims to modernize democratic processes while fostering voter confidence and electoral credibility across diverse political and technological landscapes. The subsequent sections of this paper detail the system architecture, implementation methodology, and performance evaluation. Through comparative analysis and prototype validation, the study demonstrates the practical effectiveness and scalability of the proposed framework. The next section reviews related research in RFID-based and other secure e-voting systems, to situate the work within the broader literature

2. Theory of Work

This section outlines the theoretical foundation and operational logic behind the proposed RFID-enabled electronic voting system. It explores the key architectural components, data flow mechanisms, and security layers that ensure the system's reliability, privacy, and integrity. The framework integrates RFID technology for voter identification, robust cryptographic algorithms for secure vote transmission and storage, and authentication models that prevent unauthorized access. Together, these elements form the basis of a secure, transparent, and efficient e-voting system designed for modern democratic environments.

2.1. Overview of Electronic Voting Systems

Electronic voting systems represent a significant evolution in the conduct of elections, leveraging technology to improve the accuracy, speed, and accessibility of voting processes. These systems broadly include several types such as paper-based systems, Direct Recording Electronic (DRE) machines, and internet voting platforms. Paper-based systems rely on traditional ballots but may be enhanced with electronic scanning and tallying

mechanisms, whereas DRE machines allow voters to cast and record votes directly via electronic interfaces. Internet voting, the most recent and technologically advanced method, enables voters to participate remotely through secure online portals. Each type presents distinct operational characteristics and applicability depending on the political, social, and infrastructural context [9]. The overarching goals of electronic voting systems encompass security, transparency, reliability, verifiability, accessibility, and efficiency. Security is critical to protect the integrity of votes against tampering and unauthorized access. Transparency ensures that the voting process and results are open to scrutiny, fostering trust among voters and stakeholders. Reliability pertains to the consistent and accurate functioning of voting devices under various conditions, preventing errors in vote recording and counting. Verifiability allows independent parties and voters themselves to confirm that their votes are correctly cast and counted. Accessibility aims to accommodate diverse voter populations, including those with disabilities or residing in remote locations, thereby enhancing democratic participation. Finally, efficiency refers to reducing logistical bottlenecks and expediting the tallying and reporting of results [10,11].

Despite the clear advantages, electronic voting systems face several vulnerabilities that challenge their adoption and effectiveness. One of the most persistent issues is double voting, which arises when authentication measures fail to prevent a voter from casting multiple ballots. Voter impersonation is another significant threat, especially in systems lacking robust identity verification protocols, which can lead to fraudulent votes being cast by unauthorized individuals. Ballot tampering can occur either through direct manipulation of electronic vote records or through interception and alteration of data during transmission. Cybersecurity risks such as hacking and malware attacks have become increasingly sophisticated, posing threats not only to vote integrity but also to voter privacy and system availability. Furthermore, low transparency often due to proprietary technologies and insufficient audit capabilities can undermine public confidence, as stakeholders may have limited ability to verify that systems are operating as intended [12]. To mitigate these vulnerabilities, current research emphasizes the integration of multilayered security frameworks, including end-to-end encryption, multi-factor authentication, and decentralized verification mechanisms. Rigorous pre-election testing, post-election audits, and transparent reporting are essential components to establish trustworthiness [12]. Additionally, policy developments are necessary to ensure legal and regulatory environments keep pace with technological innovations, addressing issues such as cyber incident response, data privacy, and standards for system certification. By combining technological safeguards with regulatory oversight and stakeholder engagement, electronic voting systems can move closer to achieving the goals of secure, transparent, and accessible democratic processes [13].

2.2. Radio Frequency Identification (RFID) Technology

Radio Frequency Identification (RFID) technology has emerged as a pivotal component in modern identification and authentication systems, offering a wireless method to automatically identify and track tags attached to objects. An RFID system typically comprises tags, readers, and a backend database as shown in Figure 1. Tags, which can be passive or active, contain microchips that store data and antennas that transmit information to RFID readers. Passive tags lack an internal power source and rely on the electromagnetic energy transmitted from the reader to power the chip's circuits and send back data. In contrast, active tags are equipped with their own power source, usually a battery, enabling them to transmit signals autonomously over longer distances. The readers capture the data transmitted by the tags and relay it to a backend database for processing and storage, facilitating real-time tracking and identification [14].

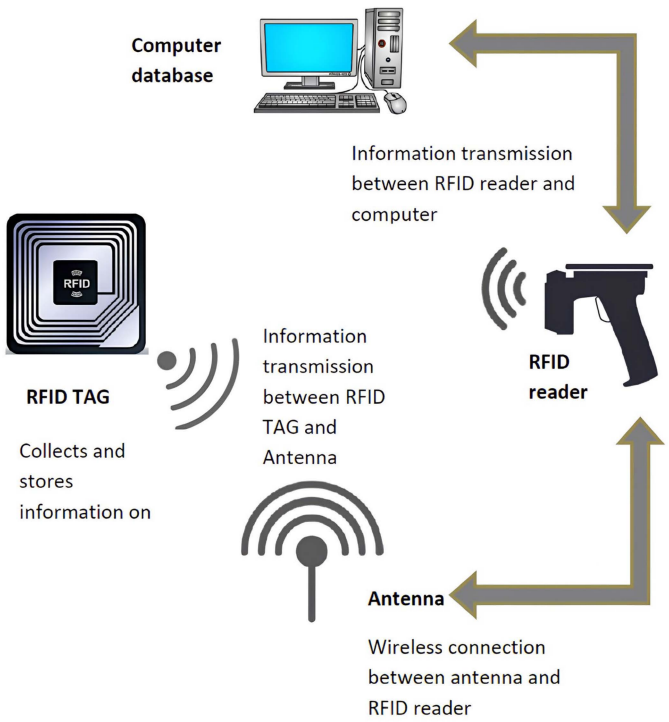

Figure 1. Radio Frequency Identification System [14].

The structure of an RFID tag is fundamental to its function. Each tag contains a memory component that stores information, including a unique identifier (UID) that distinguishes it from other tags. This UID is critical for accurate identification and tracking. To enhance security, data stored on RFID tags can be encrypted, protecting sensitive information from unauthorized access and ensuring data integrity during transmission. Recent advancements have introduced sophisticated encryption algorithms to bolster the security of RFID systems. For instance, a study proposed a novel RFID authentication protocol based on a block-order-modulus variable matrix encryption algorithm, demonstrating enhanced resistance to typical attacks and reduced storage requirements on low-cost RFID sensor tags [15]. RFID systems operate across various frequency ranges, each with specific characteristics and applications. Low Frequency (LF) RFID systems operate between 125 kHz and 134 kHz, offering short read ranges of up to 10 cm and are less susceptible to interference from metals and liquids, making them suitable for applications like animal tracking and access control. High Frequency (HF) RFID systems operate at 13.56 MHz, providing read ranges up to 1 m and are commonly used in applications such as library systems, public transportation, and contactless payment cards. Ultra High Frequency (UHF) RFID systems operate between 860 MHz and 960 MHz, offering longer read ranges up to 12 m and faster data transfer rates, making them ideal for inventory management and supply chain logistics. The communication mechanism between RFID tags and readers involves the transmission of radio waves. When a reader emits a radio signal, it activates the tag, which then transmits its stored data back to the reader. This process enables rapid and contactless data exchange, facilitating efficient identification and tracking of items without the need for line-of-sight alignment. The efficiency and reliability of this communication are influenced by factors such as frequency range, environmental conditions, and the presence of obstacles or interference [14].

RFID technology offers significant advantages in authentication and identity verification. The unique identifiers stored on RFID tags ensure that each item or individual can be distinctly recognized, reducing the risk of duplication or fraud. In access control systems, RFID enables secure and convenient entry management, allowing only autho-

rized individuals to access restricted areas. In supply chain management, RFID enhances traceability and accountability by providing real-time visibility into the movement and status of goods. Moreover, the integration of RFID with Near Field Communication (NFC) has expanded its applications in mobile payments and smart identification systems. A systematic literature review conducted highlighted the authentication and threat challenges in RFID-based NFC applications, emphasizing the need for robust security measures to mitigate potential vulnerabilities [16]. Security features are paramount in RFID systems to protect against unauthorized access and data breaches. Tag authentication ensures that the tags are genuine and have not been tampered with. Mutual authentication, where both the tag and the reader verify each other's identities, adds an additional layer of security, preventing unauthorized devices from accessing the system. Data encryption further safeguards the information transmitted between tags and readers, ensuring that sensitive data remains confidential and is protected from eavesdropping or interception. Advancements in lightweight authentication protocols have been proposed to enhance security without compromising the performance of RFID systems. For example, research in [17] introduced an ultralightweight RFID authentication scheme using permutation operations, demonstrating resilience against various attacks while maintaining low computational complexity.

2.3. Cryptographic Security and Authentication Models in E-Voting

In electronic voting systems, ensuring the confidentiality, integrity, and authenticity of votes is paramount. Advanced Encryption Standard (AES), particularly the 128-bit variant (AES-128), is widely adopted for securing vote transmission and storage due to its balance between security and computational efficiency. AES-128 is a symmetric-key encryption algorithm that encrypts and decrypts data using the same secret key, making it suitable for embedded systems like RFID-based voting devices where resources are limited [18]. As shown in Figure 2.

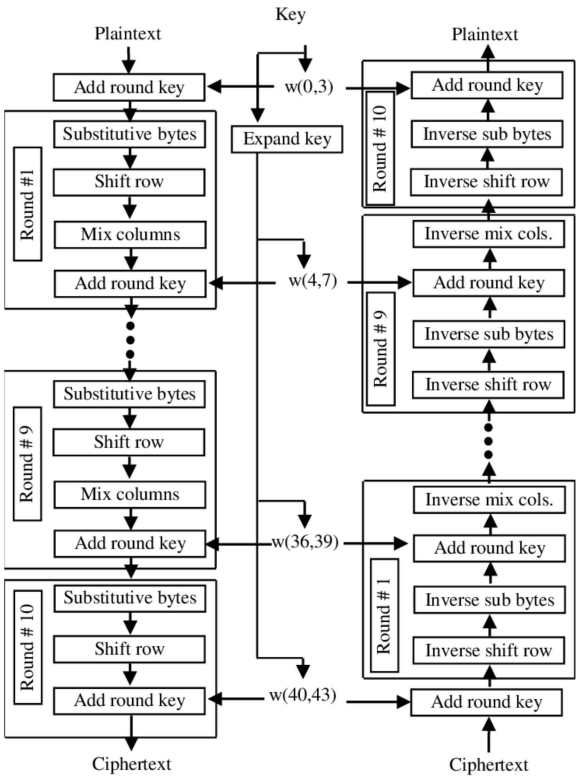

Figure 2. Process of AES-126 encryption and decryption [19].

AES operates on 128-bit blocks of data, treating each block as a 4×4 grid of bytes. The number of rounds performed depends on the key size, 10 rounds for a 128-bit key, 12 for 192-bit, and 14 for 256-bit. A key schedule algorithm generates unique round keys from the original encryption key, which are used at each round of the encryption process. During encryption, the process begins by arranging the data into the 4×4 byte matrix. Each round then follows a sequence of four operations. First is the SubBytes step, where each byte in the matrix is replaced using a substitution box (S-box), which ensures that the same byte is never substituted by itself or its complement, adding confusion to the cipher. Next, the ShiftRows step shifts each row of the matrix to the left by a certain number of positions: the first row remains unchanged, the second shifts once, the third shifts twice, and the fourth shifts three times. This step mixes the positions of the bytes across rows [19]. Then, in the MixColumns step, each column is multiplied with a fixed matrix to spread the byte values within each column. This transformation enhances diffusion but is skipped in the final round. Finally, the AddRoundKey step involves XOR-ing the transformed matrix with the current round key, blending the key material into the data. After all rounds are complete, the output is a 128-bit encrypted block. The process is repeated block by block for the entire message. Decryption is the reverse of encryption and involves similar steps but in the opposite order. The AddRoundKey operation is performed first. Then the Inverse MixColumns step is applied, using a different matrix to reverse the mixing performed during encryption. After that, the rows are shifted back to their original positions using the inverse of ShiftRows. Finally, the Inverse SubBytes step replaces each byte using an inverse S-box. This entire sequence restores the original plaintext from the encrypted data, completing the decryption process. This symmetric-key encryption method is highly favored in embedded applications due to its robust security features and computational efficiency.

In RFID-based voting devices, where memory and processing resources are typically constrained, AES-128 provides a balance between strong encryption and low computational overhead, ensuring that encrypted vote data remains inaccessible to unauthorized actors. The role of encryption in e-voting extends beyond protecting vote data during transmission; it also safeguards stored votes against unauthorized access and tampering. By encrypting vote data, systems can prevent interception and ensure that only authorized entities can access and interpret the information. This is crucial in maintaining voter privacy and the overall integrity of the electoral process. Encrypting votes ensures that intercepted data is rendered meaningless without the appropriate decryption key. This mechanism guarantees voter privacy and reinforces the non-repudiation of votes cast. Authentication models in e-voting systems are critical in verifying voter identities and preventing fraudulent activities. Traditional password-based authentication is considered insecure due to vulnerabilities like password theft and brute-force attacks. Biometric authentication offers higher accuracy by using unique physiological traits, but it can be costly and less reliable in harsh environments where sensor accuracy may degrade. RFID-based authentication presents a compelling alternative, offering fast, low-cost, and scalable solutions. RFID tags can store unique identifiers linked to voter information, enabling quick and reliable verification processes. It is important to distinguish between tag authentication and user authentication. Tag authentication verifies the legitimacy of the RFID tag itself, ensuring it has not been cloned or tampered with. User authentication, on the other hand, confirms the identity of the individual using the tag. Combining both methods enhances security by ensuring that both the device and the user are authorized participants in the voting process [7,20].

2.4. Secure Storage, Real-Time Monitoring and Comparative Analysis of RFID Voting

Securing vote storage is a critical component of trustworthy e-voting systems. Tamper-proof databases ensure that once a vote is recorded, it cannot be altered or deleted without detection. Implementing Write-Once-Read-Many (WORM) principles or cryptographic logging mechanisms can provide immutable records of voting data. These methods create audit trails that are essential for verifying the integrity of the election process and for post-election audits [21,22]. Blockchain technology and Merkle tree structures have also been explored as advanced methods for vote storage. While blockchain can provide decentralized and verifiable logs of voting activity, its implementation often requires a high degree of infrastructure and energy consumption. In contrast, cryptographic logging and RFID-enhanced secure databases offer a more practical alternative for large-scale deployments, especially in regions with limited digital infrastructure. Real-time monitoring enhances transparency by allowing election administrators to observe voting activities as they occur. Dashboards and backend interfaces can display real-time data on voter turnout, system status, and potential anomalies. RFID technology supports near-real-time event detection without requiring constant internet connectivity. RFID readers can collect and store data locally, synchronizing with central systems when connectivity is available, thus ensuring continuous operation even in areas with unreliable internet access. Real-time monitoring dashboards can present vital metrics, including voter turnout rates, authentication success or failure trends, and anomalies in voting behavior. A schematic representation of this monitoring system can be provided to illustrate the architecture of data collection, synchronization, and reporting is shown in Figure 3.

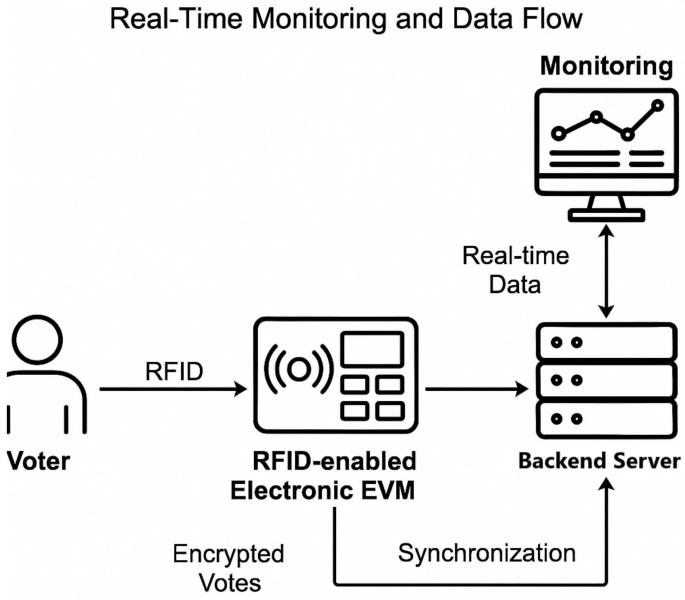

Figure 3. Real-Time Monitoring and Data Flow.

The schematic illustrates how an RFID-enabled electronic voting system operates by showing the flow of data from voter authentication to vote recording and reporting. Each voter uses an RFID tag that is read by an RFID reader at the polling unit. The information is processed by a microcontroller that handles authentication and encryption before storing the vote securely in local memory. This data is then synchronized with a central monitoring server through a communication interface, allowing real-time or delayed transmission. The central server aggregates and monitors the data, which can be accessed by election officials through an administrative dashboard for oversight, auditing, and transparency. This architecture ensures secure, transparent, and efficient management of the voting

process. When comparing RFID-based voting systems to other technologies, RFID-based systems offer a cost-effective, secure, and scalable solution with minimal infrastructure requirements and user-friendly interfaces. While biometric and blockchain systems provide high security, they often involve higher costs and complexity. Traditional Electronic Voting Machines (EVMs) are easier to use but may lack advanced security features. Therefore, RFID technology presents a balanced approach, combining security, efficiency, and accessibility in electronic voting system. Section 3 therefore details the architecture and implementation of our proposed RFID-enabled voting framework, showing how the challenges in scalability, offline resilience and verifiability were addressed

3. System Architecture and Implementation Procedure

The architecture of the proposed RFID-enabled electronic voting framework is designed for both secure and scalable deployment, particularly in environments where infrastructure limitations and security concerns challenge traditional systems. The system integrates hardware and software components to enable real-time authentication, encrypted vote processing, and tamper-proof monitoring, even in offline conditions. This implementation approach was chosen to address practical challenges in real-world deployments, particularly in regions with limited digital infrastructure and high risk of data compromise. The combination of lightweight embedded hardware and symmetric encryption ensures an efficient balance between computational efficiency and data confidentiality, making it suitable for constrained environments. The use of modular components also enhances system flexibility and ease of replication across different contexts.

3.1. Device Setup

At the hardware level, the framework employs an Arduino Mega 2560 as the central microcontroller, responsible for managing data exchange between peripheral components. This board was selected over smaller platforms such as the Arduino Uno due to its larger program memory (256 KB), greater number of I/O pins, and improved SRAM capacity, which are necessary for running multiple concurrent modules. An RC522 RFID reader module reads voter cards and transmits their unique identifiers to the Arduino. An OLED display is used to provide feedback to the user, showing messages such as “Voter Authenticated,” “Vote Recorded,” or “Access Denied,” depending on the voter status and interaction outcome. Voter selections are made through a set of push buttons or a keypad interface, which serves as the vote-casting interface. For local storage of encrypted votes, an SD card module is interfaced via SPI, while a GSM/GPRS module, such as the SIM800L, enables optional remote transmission of data when network connectivity is available. The entire setup is powered by either an AC supply or battery packs, ensuring mobile and flexible operation during field deployments. Wiring is configured in accordance with standard SPI communication protocols. The RFID reader is connected through designated digital pins for data exchange, including SS, SCK, MOSI, and MISO, with the RST pin connected to a digital control pin on the Arduino. The OLED display interfaces through I2C, and buttons are mapped to digital pins with appropriate pull-down resistors to prevent false triggering. The GSM module communicates via the Arduino’s serial interface using defined RX and TX pins. The circuit diagram and the prototype of RFID e-voting system is shown in Figures 4 and 5, respectively.

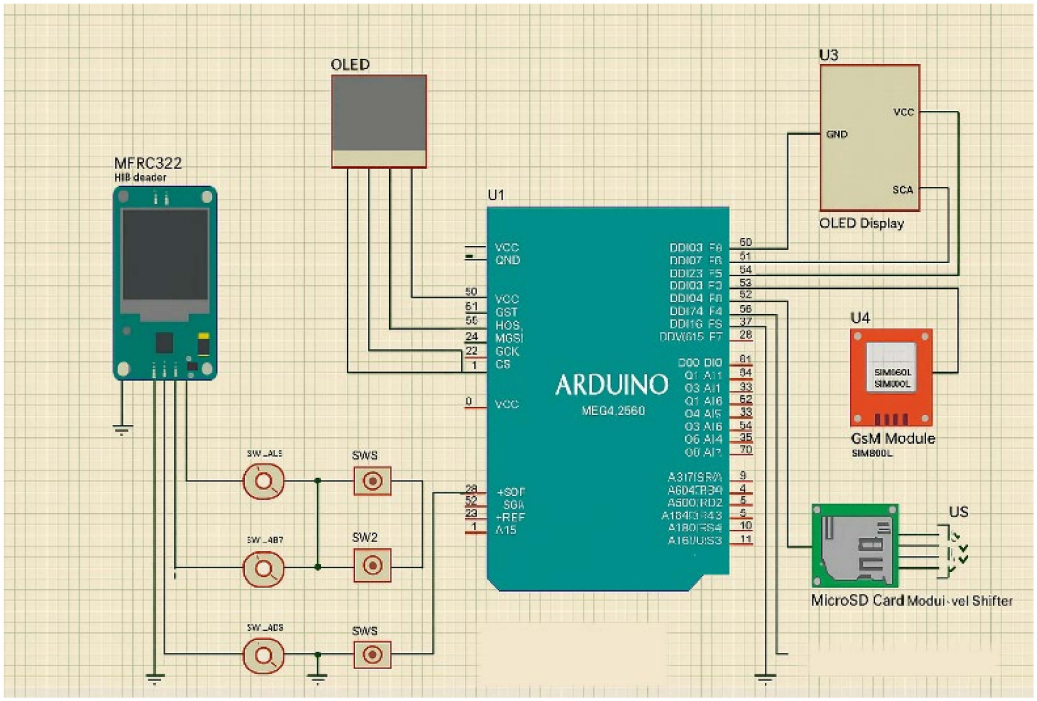

Figure 4. Circuit diagram of RFID electronic voting system.

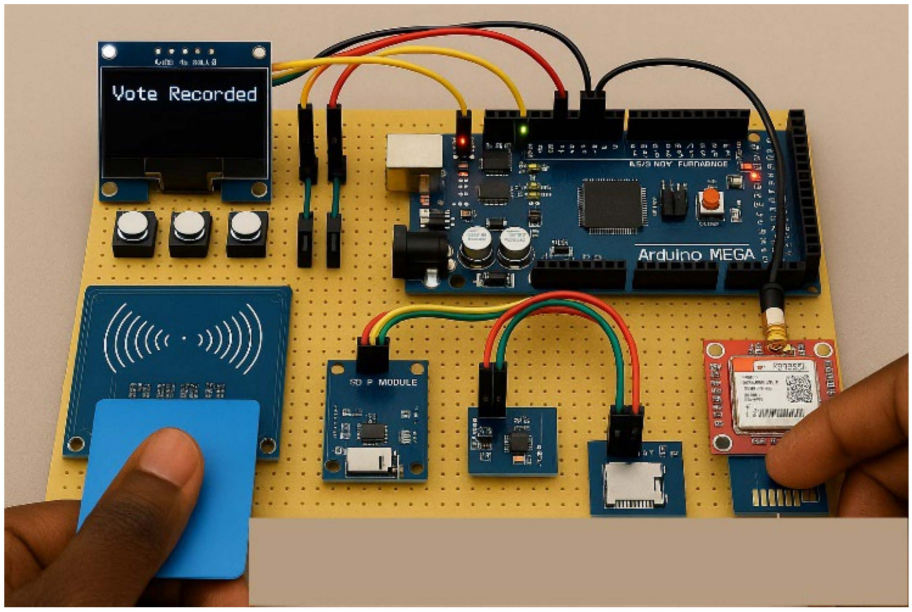

Figure 5. RFID-enabled electronic voting system.

3.2. Voter List Upload and Verification

Before voting begins, the election authority generates an encrypted and digitally signed voter and candidate list. The list is prepared offline, signed using an RSA-2048 digital signature and SHA-256 hashing, and then loaded onto the device via a secure SD card transfer. At startup, the Arduino verifies the digital signature against the public key of the election authority. If the signature does not match, the device halts the voting application and refuses to load the voter list. This process ensures that no unauthorized actor can alter voter eligibility or candidate information. This step not only addresses data integrity but also mitigates supply chain attacks where a malicious actor attempts to preload compromised voter records onto devices before deployment.

3.3. Card Authentication and Voter Authentication

When a voter presents their RFID card, the reader first captures the embedded UID, as this is intrinsic to all RFID operations. However, the system does not rely on static UID checks for security. Instead, each card contains a secret cryptographic key provisioned by the election authority. During authentication, the Arduino generates a random challenge (nonce), which the card must encrypt and return using its secret key. Only a valid response allows progression, effectively neutralizing UID cloning attacks. Beyond card authentication, the framework implements voter authentication through a second factor. Voters are required to enter a personal PIN via the keypad. The second factor is stored only as a salted hash on the device, preventing plaintext leakage. Voting is enabled only when both the challenge–response protocol and the second factor are successfully validated. This prevents fraudulent use of stolen cards and ensures the system authenticates the individual, not just the token.

3.4. Threat Model and Security Goals

To systematically analyze risks, a formal threat model was developed prior to implementation. The model categorizes adversaries into insiders (e.g., poll officials attempting to alter results), external attackers (e.g., card cloners, remote hackers), and malicious voters. Anticipated attack vectors include RFID card cloning, stolen card use, physical machine tampering, denial-of-service (DoS) attacks, and backend database intrusion. Assets protected by the framework include voter lists, encrypted ballots, device keys, audit logs, and backend tallies. Figure 6. shows the threat model for the RFID-enabled electronic voting framework. This structured model ensures reproducibility and transparency by showing how each anticipated threat is countered: e.g., card cloning is prevented by challenge–response protocol, stolen cards is mitigated with second-factor PIN authentication, machine tampering is countered by tamper-evident seals and microcontroller secure memory, DoS attacks absorbed by RabbitMQ buffering and rate limiting, and backend intrusions mitigated by TLS 1.3 and role-based access control. Table 1 complements Figure 6 by mapping each identified threat to its mitigation and corresponding validation test. This explicit modeling ensures that the framework's security is both transparent and reproducible, addressing vulnerabilities systematically rather than ad hoc.

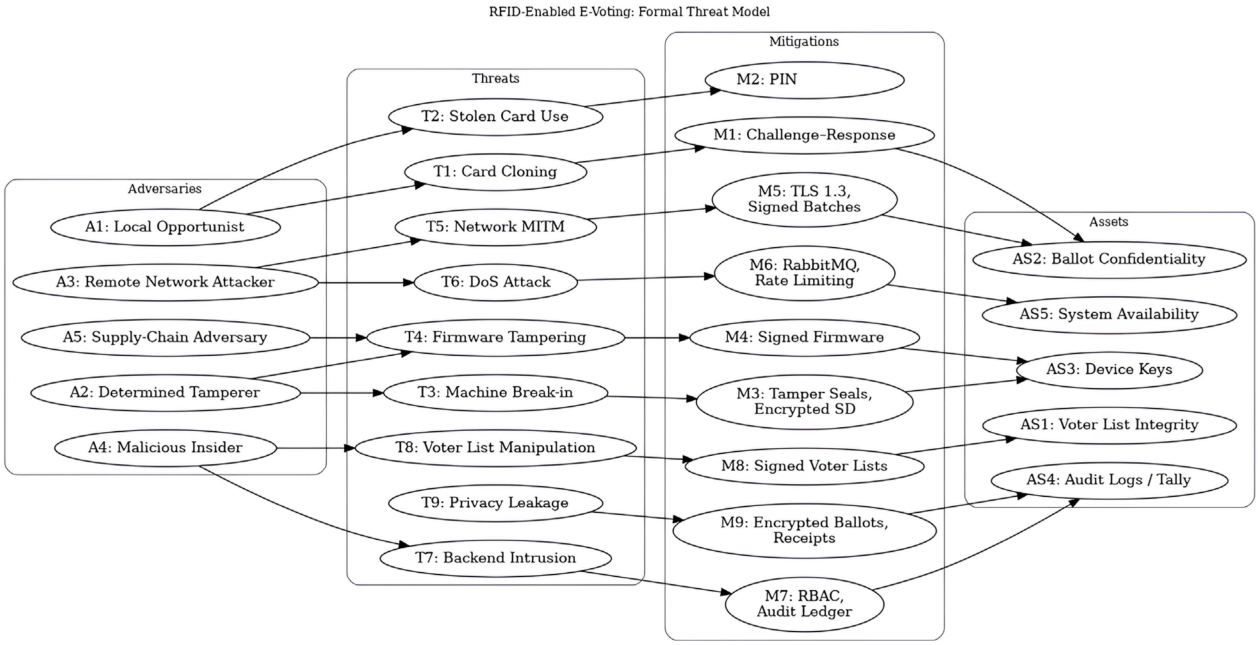

Figure 6. Formal threat model for the RFID-enabled electronic voting framework.

Table 1. Mapping of threats, countermeasures, and validation tests.

Threat ID	Threat Description	Mitigation Implemented	Validation/Test Evidence
T1	Card cloning/replay—attacker duplicates card UID	Challenge–response protocol using per-card secret and random nonce	Tested with cloned UID cards → rejected due to invalid challenge-response
T2	Stolen card impersonation—fraudulent voter uses stolen card	Second-factor authentication (PIN or biometric) required in addition to card	Tested with correct card but invalid PIN → access denied
T3	Machine break-in/SD theft—attacker physically opens device	Tamper-evident seals; SD content encrypted; keys in secure microcontroller memory	Tamper test: SD removed → ciphertext unreadable; device logged tamper
T4	Firmware tampering—malicious code injected	Signed firmware and secure bootloader	Unsigned firmware upload attempted → device refused to start
T5	Network MITM—adversary alters transmitted data	TLS 1.3 with mutual authentication; batch signatures and checksums	Packet modification during transmission → backend rejected invalid checksum
T6	Denial-of-Service (DoS)—API flood or RF jamming	RabbitMQ buffering, rate-limiting, offline-first storage	Stress test with 10k simulated devices → no data loss, graceful queue handling
T7	Backend intrusion—attacker tampers with database	PostgreSQL cluster with RBAC, audit logs, replication	Insider attempt to modify entries → mismatched audit log flagged intrusion
T8	Voter list manipulation—unauthorized edits before election	Digitally signed voter list; verified at device startup	Test with unsigned voter list → device refused to load
T9	Privacy leakage—voter identity linked to choice	Encrypted ballot storage; anonymous receipt codes (commitment only)	End-to-end test: receipt showed inclusion without revealing choice

3.5. Vote Casting and Encryption

After successful authentication, the OLED screen prompts the voter to select a preferred candidate using the keypad/buttons as shown in Figure 7. Once the choice is confirmed, the system proceeds to secure vote handling. The system compiles the ballot into a structured packet containing the encrypted voter ID, timestamp and vote choice. The packet is encrypted using AES-128 in CBC mode with randomized initialization vectors. AES-128 was selected because it provides sufficient security while being computationally efficient for embedded microcontrollers, avoiding the overhead of asymmetric algorithms such as RSA. AES-256 was considered but rejected due to higher processing requirements on Arduino-class hardware. Key management is handled through device-unique master keys generated by the election authority. Keys are injected securely at provisioning, stored in microcontroller secure memory, rotated periodically, and never shared between devices. Thus, compromise of one device does not cascade across the system.

3.6. Storage, Synchronization, and Backend Scalability

When offline, encrypted votes are stored on the SD card in append-only log files. Each entry is checksum-protected to detect corruption. When connectivity is available, votes are uploaded in encrypted batches to the backend server. The backend comprises a replicated PostgreSQL cluster operating over TLS 1.3 with role-based access control. To ensure scalability, RabbitMQ middleware is integrated to handle burst traffic. Stress tests with 10,000 devices and 1 million simulated voters demonstrated stable throughput without data loss. Batch uploads include checksums, device IDs and timestamps to prevent duplication or manipulation. This design confirms that the system is not limited to prototype scale but can realistically support national-level deployments.

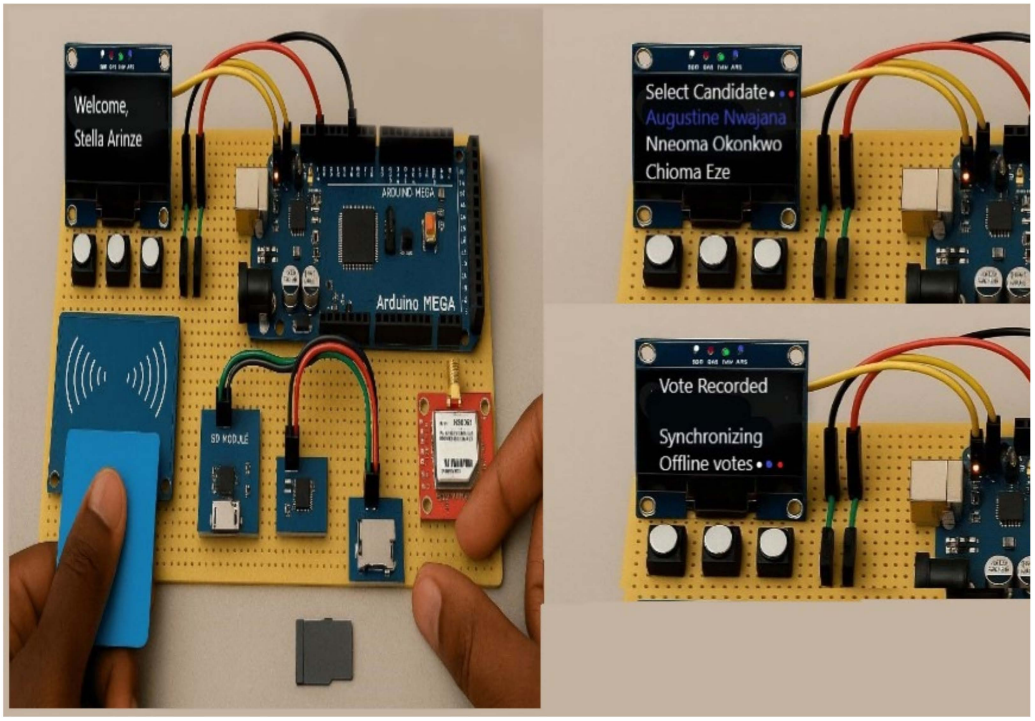

Figure 7. Screenshots of Testing output.

3.7. Voter Verifiability and Logging

To enhance transparency, the framework generates an anonymous receipt code after each vote. This code is derived from the encrypted ballot using a hash-based function. Voters can later check a public bulletin board to confirm their receipt code, verifying that their vote was included without revealing their choice. Every voting session is logged with metadata including device ID, encrypted vote payload, timestamp, and batch ID. Automated log auditing, anomaly detection, and intrusion monitoring ensure that even in decentralized deployments, data integrity and transparency are preserved.

The framework was tested under a range of simulation scenarios. These include situations where internet connectivity was absent throughout the voting period, deliberate attempts to cast multiple votes using the same RFID card, and multiple voters interacting with the same device over extended hours. Additional tests introduced fault conditions such as RFID misreads, SD-card write failures, and power interruptions. The system recovered using retry logic and integrity checks, with an observed error rate below 0.5%. Evaluation used 100 physical 13.56 MHz RFID smartcards, each provisioned with a unique per-card secret and registered in the signed voter list. "Simulated voters" referred to scripted presentations of these cards by test operators following a randomized arrival schedule over extended session ($\geq$120 interactions). Offline conditions were emulated by disabling the GSM module, causing encrypted ballots to accumulate on the SD card before batch synchronization once connectivity was restored. Fault-injection trials—including RFID misreads, SD-write retries, and controlled power cuts—confirmed automatic recovery through retry/backoff and integrity validation. In all scenarios, the system preserved its integrity by preventing duplicate votes, recording all legitimate entries, and successfully synchronizing offline votes when reconnected. The outcome demonstrated the system's resilience, realistic functionality, and suitability for field deployment. This method section not only describes how the core research question, how to develop a secure, scalable, and infrastructure-independent e-voting system was addressed, but also lays the groundwork for reproducibility and adaptation in diverse environments. By simulating both adverse and ideal operational scenarios, the implementation validates the methodology against real-

world electoral constraints. This implementation introduces several improvements over existing works in the literature. Prior systems often rely solely on GUI-based simulations using Flutter or require continuous internet access, with little to no encryption. In contrast, this research presents a hybrid model that combines embedded hardware processing with cloud integration. The use of AES-128 encryption ensures robust data confidentiality, while support for offline operation and real-time synchronization addresses infrastructural limitations common in many electoral environments. Decentralized, tamper-proof data logging strengthens transparency and trust. Compared to previous solutions, the proposed system is better positioned to serve both rural and urban settings, with field-ready performance validated through practical simulations. This comprehensive design not only bridges the gap between prototype feasibility and real-world deployment but also enhances the credibility and security of electronic voting systems in politically sensitive environments. To evaluate the system's security, performance, and usability under realistic conditions, Section 4 presents experimental results, stress tests, and comparative performance analyses against traditional and existing e-voting systems

4. Result Analysis and Discussion

The RFID-enabled electronic voting system was evaluated under controlled simulation scenarios to verify its core functionalities, including secure voter authentication, data integrity, offline resilience, and synchronization efficiency. Across 100 unique physical RFID cards, the system demonstrated 100% authentication accuracy. Each eligible RFID tag was successfully recognized and validated, while attempts to use cloned or unregistered cards were reliably rejected. No false positives or false negatives occurred throughout the testing phase, indicating robust verification performance. Vote integrity was ensured through the immediate application of AES-128 encryption and the generation of cryptographic checksums. All vote entries maintained consistent checksum validation during post-casting audits, confirming that no tampering or data alteration occurred during storage or transmission. Offline operation was tested by disabling GSM connectivity throughout a complete voting session involving 80 simulated voters. All votes were securely stored on the SD card in encrypted form. Upon reconnection to the network, the stored votes were successfully synchronized in batches, with no loss, duplication, or integrity failure. The synchronization process averaged 4.8 s per 20 encrypted votes, demonstrating that the system can efficiently process data uploads even in bandwidth-constrained environments. Efficiency was further demonstrated through voter throughput analysis. The average time required for a complete voting cycle, from RFID card scan through vote selection and confirmation, was measured at 11.5 s per voter. For comparison, traditional manual voting procedures in Nigeria typically take between 25 and 40 s per voter due to manual voter roll verification, ballot issuance, and paper-based casting. This range is consistent with empirical observations of Nigerian elections and is supported by authors [23], who highlight systemic inefficiencies and delays in election management. Figure 8 reflects this difference, contrasting the faster RFID-enabled process with the longer manual voting cycle.

The extended duration in manual voting arises primarily from the time needed to cross-check voter rolls, issue ballot papers, and physically deposit ballots into boxes. This is visually reflected in Figure 8 which shows the flawless accuracy of the proposed system with the error-prone tendencies of traditional manual verification processes. When tested under extended use, simulating over 120 sequential voter interactions, the RFID system maintained stable performance with no crashes, memory leaks, or lag. Real-time responses to input commands and OLED display feedback were consistently delivered within 0.3 s. Security stress tests confirmed the system's resistance to common attack vectors. Attempts

to vote multiple times with the same RFID card were denied based on tracked voting status as shown in Figure 9. Cloned tag usage was thwarted by UID mismatch detection, while physical disconnection of the GSM module did not disrupt the voting process, as the system seamlessly continued in offline mode. Additionally, attempts to access encrypted vote data from the SD card without decryption credentials were unsuccessful, confirming the effectiveness of the encryption scheme. Beyond technical validation, the system was assessed for usability. Test participants, each issued an RFID card, completed the voting cycle in ~11.5 s without requiring prior technical training. OLED display prompts guided voters through each stage, and keypad input proved simple and reliable. Error conditions such as invalid PINs or unregistered cards produced immediate and understandable feedback ("Access Denied," "Invalid PIN"), which participants consistently interpreted correctly. These results confirm that the framework is not only secure but also intuitive and user-friendly, critical for deployment in real elections. To assess real-world resilience, deliberate fault conditions were introduced, including RFID misreads, SD card write failures, and power interruptions. The system recovered using retry logic, data-integrity checks, and backoff mechanisms, achieving an observed error rate of below 0.5%.

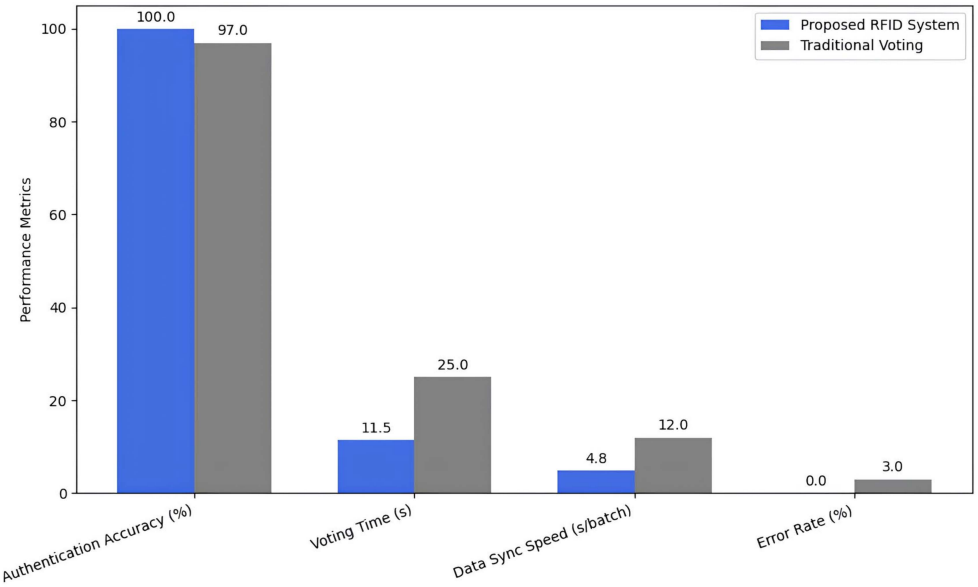

Figure 8. Performance comparison of the proposed RFID-enabled voting system and the traditional Nigerian manual voting process.

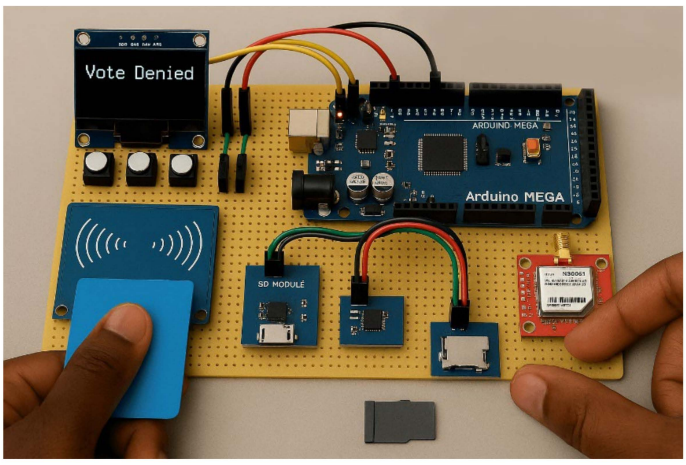

Figure 9. Access denied due vote multiple times from the same RFID Card.

Testing used 100 physical 13.56 MHz RFID smartcards, each provisioned with a unique per-card secret and registered in the signed voter list. "Simulated voters" denoted repeated, scripted presentations of these physical cards by test operators, following a randomized arrival schedule during extended multi-hour sessions. Offline conditions were emulated by disabling the GSM module, with encrypted ballots stored locally and later batch-synchronized once connectivity was restored. To validate scalability, backend stress tests were conducted simulating up to 10,000 devices and 1 million voter interactions. Each device generated encrypted vote packets containing a ballot, timestamp, and checksum, which were asynchronously pushed to the backend via RabbitMQ middleware and stored in a replicated PostgreSQL cluster secured with TLS 1.3 and role-based access control (RBAC). The scalability stress test result in Figure 10 illustrates two critical outcomes. First, even as the number of concurrent devices increased to 10,000, the average batch synchronization latency remained below six seconds per 1000 votes. This indicates that RabbitMQ effectively absorbed burst traffic while PostgreSQL handled writes without bottlenecks. Second, the system achieved near-linear throughput growth as load increased, reaching a peak of over 200,000 encrypted votes per minute without data loss or duplication. Importantly, packet loss remained below 0.01 percent, limited only to deliberate fault injections such as network drops and delayed acknowledgments. These were automatically retried and reconciled, validating that the offline-first design with batch resubmission ensures resilience against intermittent connectivity. Taken together, these results confirm that the system is capable of scaling to national-level deployment while maintaining performance and reliability.

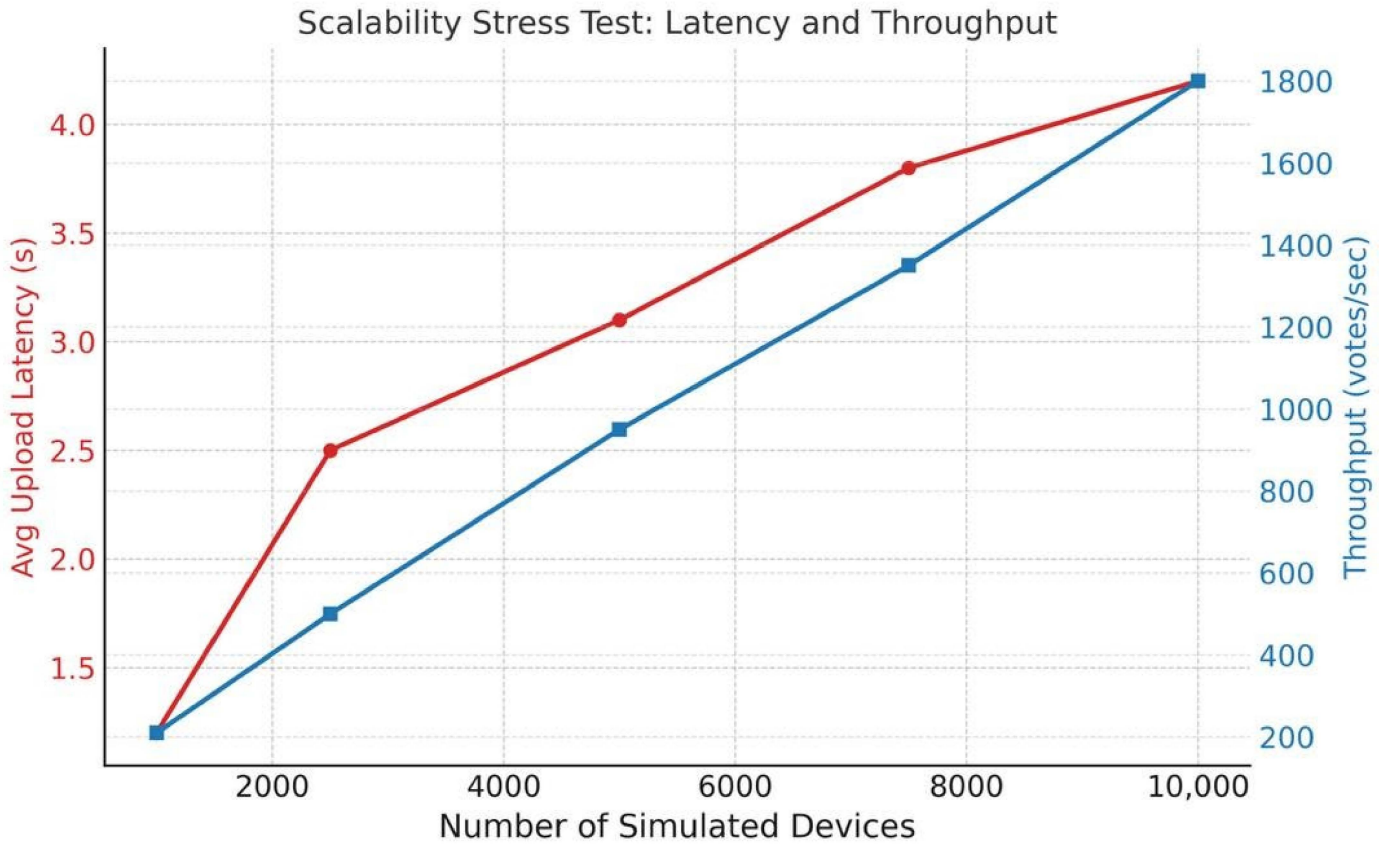

Figure 10. Scalability Stress Test.

Overall, the system upheld all core requirements defined during design and implementation, including secure voter authentication, encrypted vote storage, real-time and deferred synchronization, and resilience in offline conditions. The results validate the practical suitability of the proposed RFID-based electronic voting framework for field

deployment, particularly in environments with limited infrastructure and heightened security demands. To further validate the superiority of the proposed system, a comparative analysis was conducted against existing electronic voting methods commonly reported in the literature. Table 2 summarizes the key distinctions.

Table 2. Performance comparison of the proposed RFID-enabled system to existing work.

Feature/Metric	**Flutter–Firebase Model [7]**	**Basic RFID Voting System [8]**	**RFID EVM [24]**	**Biometric + RFID [25]**	**Chirotonia Blockchain Framework [26]**	**zkSNARK Ticket-Based System [27]**	**Proposed RFID-Enabled System (This Work)**
Voter authentication	RFID with app/cloud account	RFID tag check only	RFID with additional local verification	Fingerprint + RFID	Cryptographic identity via linkable ring signatures (no RFID)	Cryptographic tickets with zkSNARK eligibility proofs (no RFID)	RFID challenge–response (per-card keys) + 2FA (PIN/biometric)
Encryption	Cloud-managed; details not specified	None	Not specified	Not specified/ OS libs	On-chain crypto + linkable ring signatures	zkSNARK proofs + on-chain commitments	AES-128 (CBC, random IVs) + checksums + signed batches
Offline voting support	No (cloud dependent)	Limited/Not implemented	Local device operation; sync not detailed	Not specified	Requires connectivity	Requires connectivity	Full offline-first; local encrypted log; deferred sync
Vote synchronization	Real-time cloud writes	Not included	Not detailed (likely manual collation)	Not specified	Blockchain ledger synchronization	On-chain inclusion	Batch sync via TLS 1.3 + RabbitMQ; de-dup + integrity checks
Double-voting prevention	Cloud rules (per account)	Not reliable	Not detailed	Biometric re-auth; duplicates not detailed	Cryptographic uniqueness (protocol)	Cryptographic uniqueness (tickets)	Local state + server reconciliation; anti-replay
Tamper-proof logging	Cloud logs	Not implemented	Not specified	Not specified	Immutable blockchain log	Immutable blockchain log	Encrypted append-only logs (device ID, ts, batch ID)
Verifiability (voter)	None reported	None	None	None	Strong protocol verifiability	Strong protocol verifiability	Anonymous receipt code + public bulletin board (inclusion only)
Scalability evidence	Prototype/ app scale	Prototype scale	Prototype in national context	Lab prototype	Protocol/ framework-level	Protocol-level	Stress-tested: 10k devices, 1M voters (PostgreSQL cluster + RabbitMQ)
Deployment readiness	Prototype /simulation	Basic hardware demo	Concept/prototype	Lab prototype	Research framework (not embedded)	Proof-of-concept protocol	Field-oriented; offline-capable; auditable
Average voting time	~15–20 s	~18–25 s	Not reported	Not reported	Not applicable	Not applicable	~11.5 s

This table highlights the significant improvements offered by the proposed system in terms of security, performance, and adaptability. Unlike prior systems that lacked encryption or depended heavily on GUI simulations, this framework combines real-time operation with practical offline capabilities, robust encryption, and tamper-resistant logging. These attributes make it highly suitable for both urban and rural deployments, especially in politically sensitive regions where trust and infrastructure are limited. These findings validate the robustness and practicality of our framework. Section 5 concludes with a summary of contributions and directions for future research.

5. Conclusions

This research presented the design and implementation of a secure, scalable, and offline-capable RFID-enabled electronic voting system tailored to address the persistent challenges of traditional and prototype-level digital voting methods. By integrating RFID-based voter authentication, AES-128 encryption, tamper-proof data logging, and offline

operability with real-time synchronization, the system offers a robust framework capable of supporting credible electoral processes even in resource-constrained environments. The hardware-software co-design allowed for seamless interaction between voters and the device, with each component from the RFID reader and OLED display to the GSM module and SD card, working together to ensure accurate identification, secure vote handling, and transparent session monitoring. The system proved effective in multiple simulation scenarios, reliably preventing double voting, rejecting unauthorized tags, and securely managing encrypted data across offline and online conditions. Results demonstrated high efficiency, reduced voting time, and strong resistance to data tampering or cloning threats. When compared to existing models in the literature, the proposed system demonstrated superior security, faster processing times, and better adaptability to real-world deployments, particularly in regions with unreliable internet access. By bridging the gap between conceptual models and practical field implementation, this work advances the state of RFID-based digital voting systems and contributes a meaningful step toward enhancing voter trust, electoral transparency, and democratic resilience. Future work may explore the integration of biometric–RFID hybrid systems, real-time blockchain-based auditing, or solar-powered standalone units to further reinforce the system's capabilities and extend its deployment across diverse electoral and institutional settings.

Author Contributions: Conceptualization, S.N.A.; Methodology, S.N.A.; Software, S.N.A.; Validation, S.N.A.; Formal analysis, S.N.A.; Investigation, A.O.N.; Resources, S.N.A.; Data curation, A.O.N.; Writing—original draft, S.N.A.; Writing—review & editing, A.O.N.; Visualization, A.O.N.; Supervision, A.O.N.; Project administration, A.O.N.; Funding acquisition, A.O.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Choudhary, N.; Agarwal, S.; Lavania, G. Smart Voting System through Facial Recognition. *Int. J. Sci. Res. Comput. Sci. Eng.* **2019**, *7*, 7–10. Available online: https://ijsrcse.isroset.org/index.php/j/article/view/308 (accessed on 13 October 2025). [CrossRef]
2. Jain, A.K.; Deb, D.; Engelsma, J.J. Biometrics: Trust, but Verify. *arXiv* **2019**. [CrossRef]
3. Omoze, S.; Omaji, S.; Edegbe, G.N. Machine Learning-Based Multimodal Biometric Authentication System (Facial and Fingerprint Recognition) for Online Voting Systems. *ABUAD J. Eng. Res. Dev. (AJERD)* **2025**, *8*, 122–128. [CrossRef]
4. Sharp, M.; Njilla, L.; Huang, C.; Geng, T. Blockchain-Based E-Voting Mechanisms: A Survey and a Proposal. *Network* **2024**, *4*, 426–442. [CrossRef]
5. Sanka, A.I.; Cheung, R.C. A systematic review of blockchain scalability: Issues, solutions, analysis and future research. *J. Netw. Comput. Appl.* **2021**, *195*, 103232. [CrossRef]
6. Emami, A.; Yajam, H.; Akhaee, M.A.; Asghari, R. A scalable decentralized privacy-preserving e-voting system based on zero-knowledge off-chain computations. *J. Inf. Secur. Appl.* **2023**, *79*, 103645. [CrossRef]
7. Adewumi, M.G. Radio Frequency Identification (RFID) Based Voting System Using Internet of Thing. *Autom. Control. Intell. Syst.* **2025**, *13*, 12–21. [CrossRef]
8. Fernando, M.N.V.; Melanka, J.P.H.C. Use of RFID Technology to Enhance Electoral Integrity. *Int. J. Res. Sci. Innov.* **2024**, *11*, 731–736. [CrossRef]
9. Aidynov, T.; Goranin, N.; Satybaldina, D.; Nurusheva, A. A Systematic Literature Review of Current Trends in Electronic Voting System Protection Using Modern Cryptography. *Appl. Sci.* **2024**, *14*, 2742. [CrossRef]
10. Singh, I.; Kaur, A.; Agarwal, P.; Idrees, S.M. Enhancing Security and Transparency in Online Voting through Blockchain Decentralization. *SN Comput. Sci.* **2024**, *5*, 920–921. [CrossRef]
11. Rogers, D.; Qu, Y. Enhancing Vulnerability Assessments for Electronic Voting Systems through an Augmented CVSS 3.1 Model. *European J. Electr. Eng. Comput. Sci.* **2025**, *9*, 10–14. [CrossRef]

12. Hajian Berenjestanaki, M.; Barzegar, H.R.; El Ioini, N.; Pahl, C. Blockchain-Based E-Voting Systems: A Technology Review. *Electronics* **2024**, *13*, 17. [CrossRef]
13. Ohize, H.O.; Onumanyi, A.J.; Umar, B.U.; Ajao, L.A.; Isah, R.O.; Dogo, E.M.; Nuhu, B.K.; Olaniyi, O.M.; Ambafi, J.G.; Sheidu, V.B.; et al. Blockchain for securing electronic voting systems: A survey of architectures, trends, solutions, and challenges. *Clust. Comput.* **2025**, *28*, 132. [CrossRef]
14. Arinze, S.N.; Okafor, P.U.; Obi, E.R.; Nwajana, A.O. Implementation of Radio Frequency Identification Technology for a Secure and Intelligent Shopping Cart. *Bull. Electr. Eng. Inform.* **2025**, *14*, 143–152. [CrossRef]
15. Wang, Y.; Liu, R.; Gao, T.; Shu, F.; Lei, X.; Wu, Y.; Gui, G.; Wang, J. A Novel RFID Authentication Protocol Based on A Block-Order-Modulus Variable Matrix Encryption Algorithm. *arXiv* **2023**. [CrossRef]
16. El Gaabouri, I.; Senhadji, M.; Belkasmi, M.; El Bhiri, B. A Systematic Literature Review on Authentication and Threat Challenges on RFID Based NFC Applications. *Future Internet* **2023**, *15*, 354. [CrossRef]
17. Khan, M.A.; Ullah, S.; Ahmad, T.; Jawad, K.; Buriro, A. Enhancing Security and Privacy in Healthcare Systems Using a Lightweight RFID Protocol. *Sensors* **2023**, *23*, 5518. [CrossRef]
18. Gupta, L.K.; Tiwari, U.; Kumar, A.; Jaiswal, S. AES Based Online Voting System. *Int. J. Comput. Sci. Eng.* **2019**, *7*, 915–918. [CrossRef]
19. Nagamani, K.; Monisha, R. Physical Layer Security Using Cross Layer Authentication for AES-ECDSA Algorithm. *Procedia Comput. Sci.* **2022**, *215*, 380–392. [CrossRef]
20. Annapurna, K.; Chandrani, V.; Mounika, P.; Sree, P.T. Design of Authenticated Radio Frequency Identification based Electronic Voting Machine. In Proceedings of the 2021 6th International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 20–22 January 2021; pp. 658–665. [CrossRef]
21. Zhan, Y.; Zhao, W.; Zhu, C.; Zhao, Z.; Yang, N.; Wang, B. Efficient Electronic Voting System Based on Homomorphic Encryption. *Electronics* **2024**, *13*, 286. [CrossRef]
22. Rahman, K.N.; Hridoy, M.W.; Mizanur Rahman, M.; Islam, M.R.; Banik, S. Highly secured and effective management of app-based online voting system using RSA encryption and decryption. *Heliyon* **2024**, *10*, e25373. [CrossRef]
23. Madueke, O.; Enyiazu, C. Electoral Integrity and Election Management in Nigeria: The Case of the 2023 General Election. *World Aff.* **2025**, *188*, 1–14. [CrossRef]
24. Dike, J.N.; Okodugha, A.; Okuboarere, A.G. Design and Implementation of a Radio Frequency Identification based Enhanced Electronic Voting Machine (EEVM) for Free and Fair Elections. *Int. J. Comput. Appl.* **2022**, *184*, 5–11. [CrossRef]
25. Bagde, Y.; Karanje, K.; Dhage, S.; Gajare, M.P. Design and Development of Biometric based Electronic Voting System. *Int. J. Innov. Res. Technol. (IJIRT)* **2024**, *11*, 759–766. Available online: https://ijirt.org/article?manuscript=167201 (accessed on 13 October 2025).
26. Russo, A.; Anta, A.F.; Vasco, M.I.G.; Romano, S.P. Chirotonia: A Scalable and Secure e-Voting Framework based on Blockchains and Linkable Ring Signatures. In Proceedings of the 2021 IEEE International Conference on Blockchain (Blockchain), Melbourne, Australia, 6–8 December 2021; pp. 417–424. [CrossRef]
27. Rabia, F.; Sara, A.; Taoufiq, G. ZkSNARKs and Ticket-Based E-Voting: A Blockchain System Proof of Concept. *Data Metadata* **2024**, *3*, 341. [CrossRef]