JOURNAL OF CULTURAL ANALYSIS AND SOCIAL CHANGE

Journal of Cultural Analysis and Social Change,
2026, 11(1), 3537-3550
ISSN: 2589-1316

Strengthening Electoral Trust in the DRC: Evidence from a Multimodal Biometric and RFID Voting Prototype

Lingole Mbembo Justin[1,2,3], MinSam Ko[4], Nyazabe Sllife[5,2]*, Ngomabinda Alex[2], Nkwimi Bilangoma Grevi[1,2], Mwandoki Mwamunzoyo Jerome[6]

[1] *Department of Applied Artificial Intelligence, Hanyang University, South Korea, Email: lingolejustin2020@gmail.com*
[2] *Department of Management Information Systems and Business English, University of Kinshasa, Democratic Republic of the Congo.*
[3] *National Institute of Art, Kinshasa, Democratic Republic of the Congo.*
[4] *Professor, School of ICT, College of Computing, Hanyang University, South Korea.*
[5] *Graduate School of Global Digital Innovation, KAIST, South Korea.*
[6] *Policy Competency Based on ICT Convergence, Handong Global University, South Korea. Email: songazilagracia333@gmail.com*

*__Corresponding Author:__ snyazabe@gmail.com

Citation: Justin, L. M., Ko, M. S., Sllife, N., Alex, N., Grevi, N. B. and Jerome, M. M. (2026). Strengthening Electoral Trust in the DRC: Evidence from a Multimodal Biometric and RFID Voting Prototype, *Journal of Cultural Analysis and Social Change*, 11(1), 3537-3550. https://doi.org/10.64753/jcasc.v11i1.4758

Published: April 09, 2026

ABSTRACT

Electoral processes in the Democratic Republic of the Congo (DRC) continue to face concerns related to transparency, voter authentication, and the prevention of duplicate registration and multiple voting. While electronic voting devices have been introduced, persistent operational and credibility challenges indicate that authentication remains a critical weakness in the electoral chain. This study proposes and evaluates a multimodal electoral authentication framework that combines fingerprint recognition, facial recognition, and RFID-enabled voter cards to strengthen voter verification during registration and voting. The study draws on two sources of evidence. First, a survey of 160 Congolese respondents examined perceptions of prior electoral processes and attitudes toward biometric authentication in elections. Second, a functional prototype was developed and assessed through usability testing with 25 participants using the Post-Study System Usability Questionnaire (PSSUQ). Descriptive results show strong respondent concern regarding the integrity of current electoral safeguards and generally positive attitudes toward biometric-supported voting authentication. Across the prototype tests, fingerprint authentication received the highest overall usability rating, followed by RFID and facial recognition. The findings suggest that multimodal authentication may offer a promising pathway for strengthening electoral verification in high-risk contexts such as the DRC. However, the results should be interpreted as exploratory given the limited usability sample and controlled testing environment. The study contributes a context-sensitive technical framework and empirical baseline for future electoral technology research and pilot implementation.

Keywords: Electoral Integrity, Biometric Authentication, RFID Technology, Electronic Voting Systems, Multimodal Authentication, Democratic Republic of the Congo.

INTRODUCTION

Electoral legitimacy depends not only on the formal conduct of voting but also on the credibility of voter registration, voter authentication, results management, and public transparency. In the Democratic Republic of the Congo (DRC), recurring controversies surrounding election administration have kept public confidence in electoral institutions under pressure (JUMA, 2019; Mavungu, 2013; Berwouts & Reyntjens, 2019). International observation of the December 2023 general elections documented important transparency and procedural concerns, including

deviations in results management and broader weaknesses in the administration of the electoral process (The Carter Center, 2024).

Although the DRC has introduced election technologies, including electronic voting devices (Ali-Diabacté, 2020; Martin Milolo, 2019), technology adoption alone does not guarantee electoral integrity, as the effectiveness of such systems depends on their design, governance, and implementation context (Alvarez, Hall, & Trechsel, 2009). Election technology can support voter registration, authentication, and results transmission, but its value depends on whether it enhances transparency, accountability, accessibility, and operational reliability across the electoral chain (IFES, 2022).

In the DRC context, one persistent weakness concerns the prevention of duplicate registration and multiple voting. The Carter Center's final report on the 2023 general elections highlights important transparency and implementation challenges, while also indicating that voter authentication remains insufficiently automated at the point of voting (The Carter Center, 2024). Furthermore, following the 2023 elections, the Independent National Electoral Commission (CENI) reported the cancellation of votes for 82 candidates due to electoral fraud, including the misuse of voting equipment and unauthorized voting practices (CENI, 2024).

Biometrics are widely used for identity management because they support de-duplication of registries and person-level identification (IFES, 2011; Jain et al., 2011). In electoral contexts, biometric systems are primarily introduced to reduce duplicate registrations and strengthen voter verification. However, the design and deployment of such systems must account not only for security but also for inclusion, usability, privacy, and operational feasibility. In particular, facial recognition technologies may exhibit performance variability and demographic bias, raising important concerns about reliability in high-stakes applications such as elections (NIST, 2020). Furthermore, election technologies should remain accessible to persons with disabilities and should not compromise the independence or secrecy of the vote (IFES, 2023).

The Congolese electoral system is structured around two interconnected phases: voter enrollment and voting. These phases are interdependent, meaning that weaknesses in voter registration directly affect the integrity of the voting process. During enrollment, eligible citizens are authenticated and added to the voter registry, with the objective of preventing duplicate entries and ensuring voter eligibility.

However, existing reports suggest that the current system lacks sufficiently robust automated mechanisms to prevent duplicate registration and multiple voting (The Carter Center, 2024). As a result, vulnerabilities may arise where individuals obtain multiple voter cards or attempt to vote more than once. To mitigate this risk, CENI conducts post-enrollment fingerprint checks to detect duplicate records, although the effectiveness of this approach remains uncertain in the DRC context.

Since 2018, Electronic Voting Machines (EVMs) have been introduced to improve electoral administration. However, these systems do not include automated voter authentication at the point of voting. Instead, eligibility verification relies on manual checks performed by election officials, including voter card verification and name-list validation.

This human-dependent process may increase vulnerability to procedural inconsistencies and manipulation, particularly in contexts where institutional controls are limited (The Carter Center, 2024). Reports from the 2023 elections indicate instances of electoral irregularities, including the misuse of voting equipment and unauthorized voting practices. A CENI report from January 2024 further confirmed that 82 candidates were disqualified due to electoral fraud involving unauthorized use of election materials. These issues highlight persistent weaknesses in the current system and reinforce the need for more robust voter authentication mechanisms.

Despite growing interest in biometric and technology-enabled electoral systems, important gaps remain in the literature. There is limited empirical research grounded in the socio-institutional realities of the DRC, where electoral mistrust and operational constraints shape the feasibility of technological reform. In addition, many prior studies emphasize system architecture while paying insufficient attention to citizens' perceptions and usability considerations. Moreover, although multimodal authentication systems are often presented as conceptually superior, the literature provides limited guidance on which authentication modality should be prioritized under practical constraints such as speed, ease of use, and operational feasibility.

Accordingly, this study addresses two main questions: (1) How do Congolese respondents perceive the weaknesses of the current electoral system and the acceptability of biometric and RFID-supported voter authentication? (2) Among fingerprint recognition, facial recognition, and RFID authentication, which modality demonstrates the strongest usability performance in a prototype evaluation?

To address these questions, this study combines a perception survey with a prototype-based usability assessment of a multimodal biometric and RFID authentication system. By integrating contextual analysis, user perceptions, and system-level evaluation, the study contributes both empirically and practically to the design of more secure and context-appropriate electoral authentication mechanisms in developing country contexts.

LITERATURE REVIEW

Election Technology and Electoral Integrity

Electoral technologies have been increasingly adopted to enhance the efficiency, transparency, and credibility of election processes, particularly through improvements in voter registration, results transmission, and verification mechanisms (International IDEA, 2011; IFES, 2022; UNDP, 2015). These technologies support critical functions such as voter registration, voter authentication, ballot casting, and results transmission. However, prior research consistently emphasizes that the adoption of technology alone does not guarantee electoral integrity. Instead, the effectiveness of electoral technologies depends on their design, governance, transparency, and alignment with institutional contexts (Alvarez et al., 2009; IFES, 2022).

In many developing democracies, weaknesses in voter registration systems and identity verification processes create vulnerabilities such as duplicate registration and multiple voting, thereby undermining electoral integrity (International IDEA, 2016; IFES, 2015; UNDP, 2017). These challenges have motivated the adoption of biometric-based solutions aimed at strengthening voter identification and reducing fraud. However, the literature also highlights that technological solutions must be evaluated not only in terms of security but also in terms of accessibility, usability, cost, and institutional feasibility (IFES, 2022).

Biometric Authentication in Electoral Systems

Biometric authentication has emerged as a widely adopted approach for identity verification due to its ability to uniquely identify individuals based on physiological or behavioral characteristics, thereby enhancing the reliability of identification systems (Jain et al., 2004; World Bank, 2018; IFES, 2020). Common biometric modalities include fingerprint, facial recognition, and iris recognition. These systems are particularly relevant in electoral contexts, where accurate voter identification is essential to prevent impersonation and duplicate voting (Jain et al., 2011; IFES, 2011).

Prior studies have demonstrated that biometric systems can significantly improve the reliability of voter registration and authentication processes. For example, biometric-based voter registration systems have been shown to reduce duplicate entries and enhance trust in electoral systems (Umar et al., 2022). However, biometric technologies are not without limitations. Issues such as data quality, environmental conditions, and user variability can significantly affect system performance, particularly in contexts where users may have worn fingerprints or limited familiarity with digital systems (Jain et al., 2004; NIST, 2015; World Bank, 2018; IFES, 2020).

Moreover, recent evaluations of facial recognition technologies have raised concerns about performance variability across demographic groups, highlighting potential risks related to fairness and reliability in high-stakes applications such as elections (NIST, 2020; Rhue, 2023). These limitations suggest that relying on a single biometric modality may not be sufficient in complex real-world environments.

RFID Technology in Electoral Systems

Radio-Frequency Identification (RFID) technology has been proposed as a complementary mechanism to enhance voter identification and streamline electoral processes, particularly through its ability to support automated identification and improve operational efficiency in election management systems (Want, 2006; IFES, 2011; UNDP, 2015). RFID systems enable the storage and retrieval of voter information through embedded chips, allowing for faster and more efficient authentication at polling stations (Borba et al., 2018).

In electoral contexts, RFID can support voter tracking and reduce administrative delays, thereby improving the overall voting experience. Some studies suggest that RFID-based systems can help detect attempts at multiple voting by identifying repeated use of voter credentials across polling stations (Arinze and Nwajana, 2025). However, the adoption of RFID technology also introduces challenges related to system interoperability, infrastructure requirements, and data security.

Furthermore, concerns regarding privacy and unauthorized data access remain critical considerations in the deployment of RFID-enabled electoral systems. These issues highlight the need for careful system design and governance when integrating RFID into electoral processes.

Multimodal Biometric Systems: Opportunities and Trade-offs

To address the limitations of single-modality systems, recent research has increasingly explored multimodal biometric authentication, which combines multiple identification methods (e.g., fingerprint and facial recognition) to enhance accuracy, robustness, and system reliability (Ross & Jain, 2003; World Bank, 2018). The integration of multiple modalities is intended to improve system robustness by reducing reliance on any single authentication method (Adjei et al., 2020).

Empirical studies have shown that multimodal systems can enhance security and reduce the likelihood of fraud by requiring multiple layers of verification (Nagaraj et al., 2022; Padmavathi et al., 2023). For example, bimodal

systems combining fingerprint and facial recognition have been proposed to improve voter authentication accuracy and prevent impersonation (Awotunde, 2017).

However, multimodal systems also introduce important trade-offs. Increased system complexity may lead to longer processing times, higher implementation costs, and greater operational challenges. In addition, usability differences across modalities can significantly affect user experience. Some studies suggest that fingerprint authentication tends to be more reliable and user-friendly, while facial recognition may face challenges related to environmental conditions and user acceptance (Umar et al., 2022).

Research Gap and Contribution

Despite the growing body of research on biometric and RFID-based electoral systems, several gaps remain. First, there is limited empirical evidence grounded in the socio-institutional context of the DRC, where electoral challenges and governance conditions differ significantly from those in other regions. Second, existing studies often emphasize technical system design while paying limited attention to user perception, usability, and real-world adoption considerations. Third, although multimodal systems are widely proposed as superior solutions, there is insufficient clarity regarding which authentication modality should be prioritized under practical constraints such as cost, speed, and ease of use.

This study addresses these gaps by combining contextual analysis, user perception data, and prototype-based usability evaluation to assess both the acceptability and operational performance of multimodal biometric authentication in the DRC electoral context.

METHODOLOGY

Research Design

This study adopts an exploratory quantitative research design combining two complementary components: (1) a perception survey assessing respondents' experiences with the current electoral system and their attitudes toward biometric authentication, and (2) a prototype-based usability evaluation of a multimodal biometric and RFID authentication system.

This dual approach enables the study to examine both user perception and system-level performance, which are essential dimensions in evaluating electoral technologies in real-world contexts (IFES, 2022).

Study Context and System Rationale

The study is grounded in the electoral context of the Democratic Republic of the Congo, where challenges such as duplicate registration, multiple voting, and limited automation in voter authentication have been documented (The Carter Center, 2024).

The proposed system (prototype) was designed to address these vulnerabilities by integrating biometric authentication (fingerprint and facial recognition) with RFID-based voter identification, thereby introducing a layered authentication mechanism intended to reduce fraud and improve verification reliability.

Survey Data Collection

A structured survey questionnaire was administered to assess respondents' perceptions of the current electoral system and their attitudes toward biometric and RFID-based authentication technologies. A total of 160 valid responses were collected using a non-probability sampling approach. The instrument measured key variables, including perceived electoral fraud, trust in the system, awareness of biometric technologies, and overall technology acceptance. In addition, the questionnaire captured respondents' prior experiences with electoral processes, their perceptions of electoral integrity, and their attitudes toward the adoption of biometric and RFID-enabled identification mechanisms. Table 1 summarizes the demographic information.

Table 1. Demographic Information

Measurements		Frequency	%
Location	Urban	100	62.5
	Rural	60	37.5
Familiarity with touch screen devices	Very Low	10	6.3
	Low	15	9.4
	Moderate	50	31.3
	High	55	34.4
	Very High	30	18.8

Age	18–30	80	50
	31–45	50	31.3
	46–60	25	15.6
	>60	5	3.1
Gender	Male	85	53.1
	Female	70	43.8
	prefer not to say	5	3.1
Education	No formal education	5	3.1
	Primary school	30	18.8
	Secondary school	60	37.5
	Bachelor's degree	45	28.1
	Master's or higher	20	12.5
Total		160	100

System Design and Implementation

Based on insights derived from the literature review, contextual analysis, and survey findings, a multimodal biometric-RFID authentication system was designed and implemented.

The system integrates three authentication components:

- Fingerprint recognition (primary authentication method)
- Facial recognition (secondary or fallback authentication method)
- RFID-based voter identification

The system was implemented using:

- Programming languages: C# and Python
- Database management system: SQL Server
- Fingerprint SDK: ZKTeco SDK
- Libraries: OpenCV, Emgu CV, DeepFace, AxZKFPEngXControl

These technologies were used to enable biometric capture, identity verification, and liveliness detection, ensuring a functional and testable prototype.

Usability Evaluation

The usability of the proposed system was evaluated through controlled testing involving 25 participants from Hanyang University. The objective of this evaluation was to provide initial insights into the usability and operational performance of the three authentication modalities under controlled conditions.
Usability was assessed using the Post-Study System Usability Questionnaire (PSSUQ), a validated instrument widely used to measure user satisfaction and perceived system usability in human–computer interaction research (Lewis, 1995).

Usability Metrics

The evaluation focused on seven key usability dimensions:

- Ease of Use: The degree to which the system is intuitive and easy to operate
- Speed: The time required to complete the authentication process
- Effectiveness: The accuracy and reliability of user authentication
- Ease of Scanning: The ability of the system to capture biometric or RFID data efficiently
- Error Message Clarity: The clarity and usefulness of system feedback in case of errors
- Error Recovery and Retry: The system's ability to allow users to recover from errors smoothly
- System Performance: The overall stability and consistency of system operation

These dimensions collectively capture key aspects of usability, including efficiency, reliability, user interaction quality, and error handling.

Data Analysis

Data collected from both the survey and usability testing were analyzed using JASP statistical software.

- Survey responses were analyzed using descriptive statistics to assess general trends in perceptions and attitudes.
- Usability data were analyzed by comparing mean scores across the three authentication modalities (fingerprint, facial recognition, and RFID).

Given the exploratory nature of the study and the relatively small sample size for usability testing, the results are interpreted as indicative rather than confirmatory.

SYSTEM ANALYSIS AND DESIGN

Overview of the Electoral Process in the DRC

The electoral process in the Democratic Republic of the Congo is structured around two main phases: voter enrollment (registration) and voting. These phases are closely interconnected, as the integrity of the voting process depends heavily on the accuracy and reliability of the voter registration stage.

During enrollment, eligible citizens are registered and their personal information is recorded in electoral databases. This phase is intended to ensure that only eligible voters are included in the voter registry and to prevent duplicate registrations. The voting phase involves the identification of registered voters and the casting of ballots using electronic voting devices (EVDs), followed by ballot printing and physical submission.

Despite these mechanisms, prior reports have highlighted limitations in voter authentication and fraud prevention, particularly regarding duplicate registration and multiple voting (The Carter Center, 2024).

Existing Enrollment System

The current enrollment system implemented by the Independent National Electoral Commission (CENI) involves biometric data capture and local database verification.

When an individual presents for registration, biometric data, typically fingerprints and facial information, are collected and checked against the local enrollment database to detect potential duplicates. If a duplicate is detected, the registration is rejected. Otherwise, the individual is successfully registered, and a voter card is issued.

At the end of the enrollment period, local databases are consolidated into a central database, where additional checks are performed to identify duplicate records. In cases of duplication, only the most recent registration is retained, and a list of duplicate entries may be published by CENI (The Carter Center, 2024).

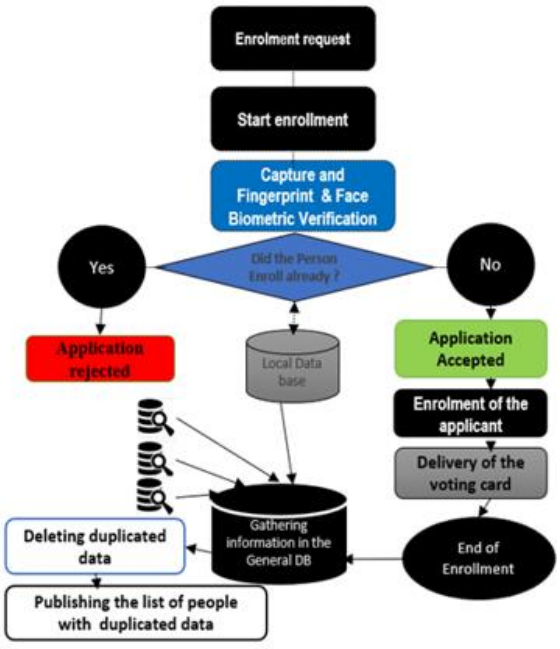

Figure 1. Existing voter enrollment process in the DRC

Existing Voting System

The voting process in the DRC relies on EVDs to facilitate ballot selection. Upon arrival at a polling station, voters present their voter cards to election officials, who manually verify their eligibility by checking their names against voter lists.

Once verified, voters use the EVD to select their preferred candidates across multiple election categories. After confirming their selections, a ballot is printed and deposited into a ballot box. Finally, indelible ink is applied to the voter's thumb to indicate that the individual has already voted.

Although this system introduces elements of digital support, voter authentication at the polling station remains largely manual. This reliance on human verification may increase vulnerability to procedural inconsistencies and unauthorized voting practices, particularly in environments where oversight mechanisms are limited (The Carter Center, 2024).

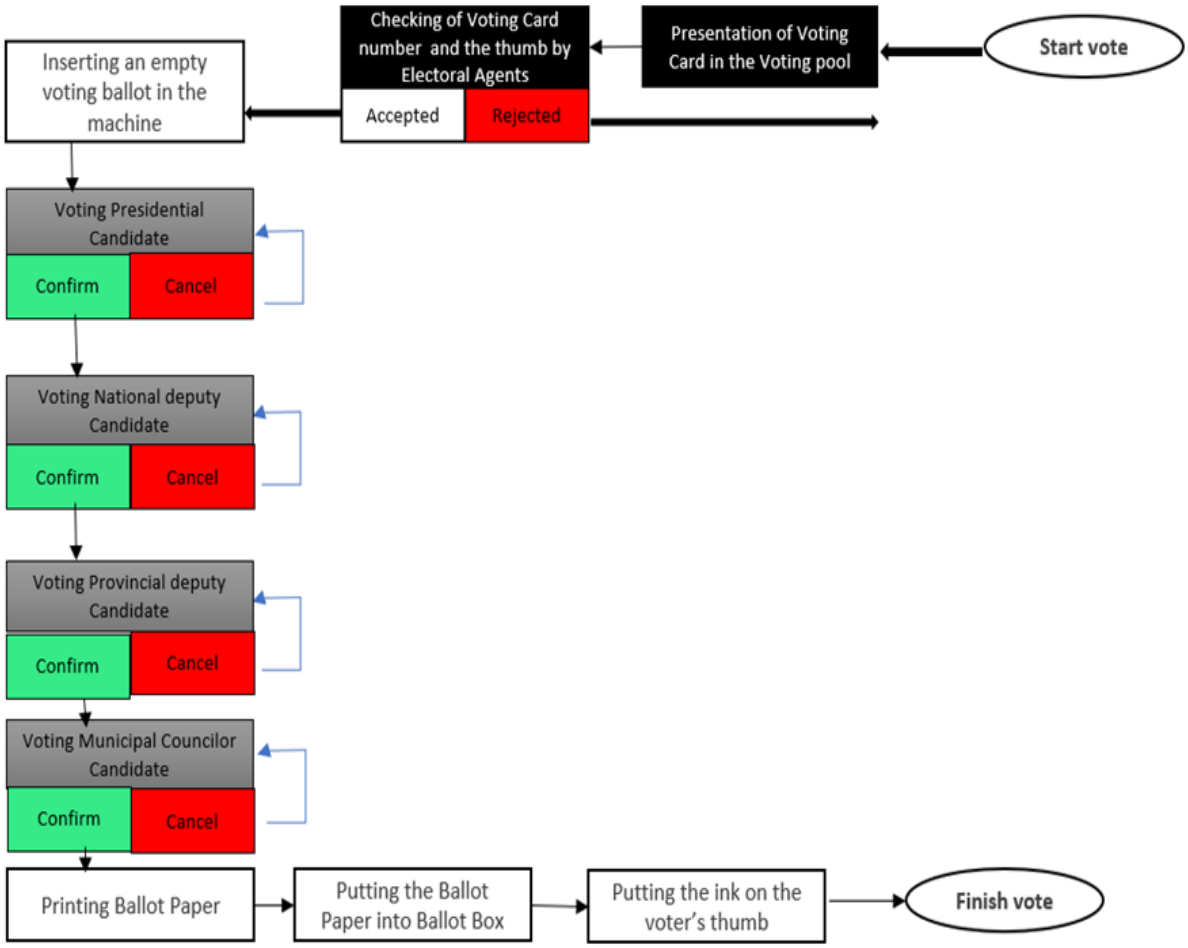

Figure 2. Existing voting process workflow in the DRC

Limitations of the Existing System

The analysis of the current electoral system reveals several critical limitations. First, the system lacks automated voter authentication, relying primarily on manual verification rather than real-time biometric validation at the point of voting. This shortcoming increases the risk of multiple voting, as the absence of automated checks during the voting process may allow individuals to cast more than one ballot. In addition, duplicate registrations are typically detected only after the enrollment phase, rather than being prevented in real time. Furthermore, the system's strong dependence on human agents heightens its vulnerability to human error and potential manipulation. Taken together, these limitations underscore the need for a more robust and automated authentication mechanism capable of strengthening electoral integrity.

Proposed Multimodal Enrollment System

To address the limitations identified in the existing system, this study proposes an enhanced enrollment architecture that integrates biometric authentication with RFID technology. The proposed system introduces several key improvements. First, it incorporates a centralized and synchronized database that enables real-time data exchange between enrollment centers and the central repository, thereby reducing the risk of duplicate registration. Second, it adopts a multimodal biometric verification approach by combining fingerprint and facial recognition to strengthen identity validation and improve system reliability. Third, it introduces RFID-enabled voter cards to replace traditional cards, facilitating more secure and efficient identification during the electoral process. Collectively, this design aims to enhance the accuracy, efficiency, and security of voter registration.

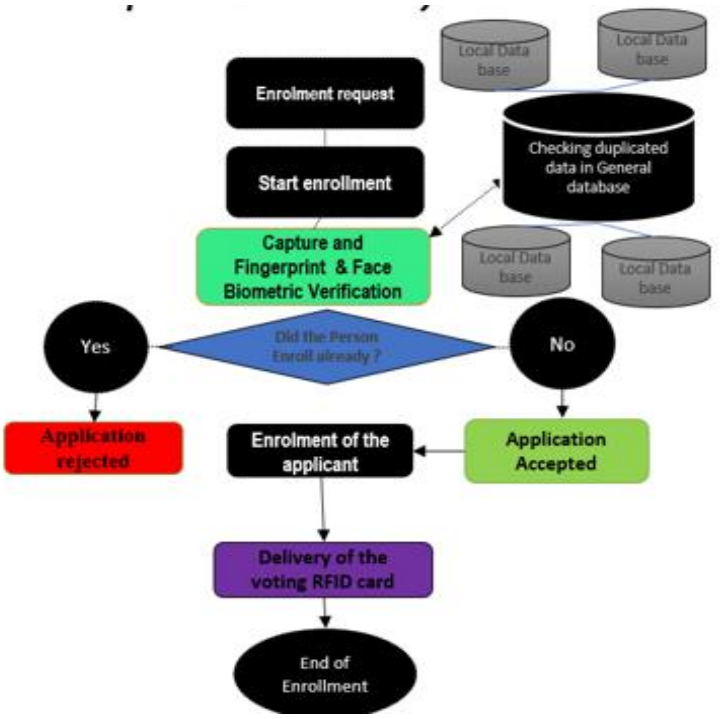

Figure 2. Proposed multimodal biometric-RFID enrollment system architecture

Proposed Voting System

The proposed voting system introduces a layered authentication process to enhance voter verification at polling stations.

Upon arrival, the voter initiates authentication by scanning their RFID-enabled voter card. The system verifies whether the individual is registered and whether they have already voted. If the voter is eligible, the system proceeds to biometric authentication.

Fingerprint recognition is used as the primary authentication method. In cases where fingerprint verification fails, facial recognition is employed as a secondary method. Only after successful authentication is the voter granted access to the voting interface.

After authentication, the voting process follows a structure similar to the existing system, including candidate selection, confirmation, ballot printing, and submission.

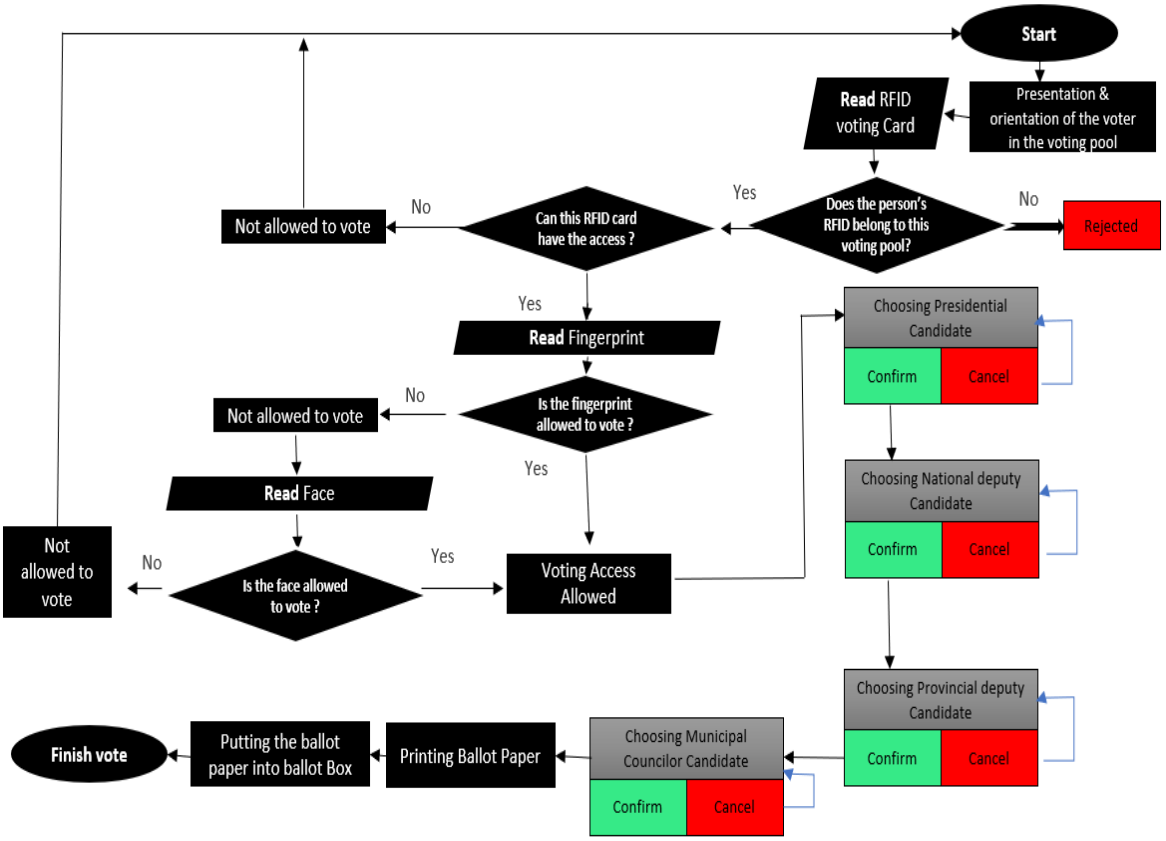

Figure 3. Proposed multimodal voting authentication workflow

Key Improvements of the Proposed System

Compared to the existing system, the proposed architecture introduces several key improvements. First, voter verification is automated, shifting authentication from reliance on human agents to a system-driven process, thereby enhancing consistency and reducing the likelihood of human error. Second, the system enables real-time verification, which effectively prevents multiple voting by ensuring that each individual can cast a ballot only once. Third, security is strengthened through the integration of multimodal authentication, combining RFID-based identification with biometric verification to reduce dependence on a single authentication mechanism. In addition, the automation of core processes improves operational efficiency by minimizing delays and reducing manual intervention.

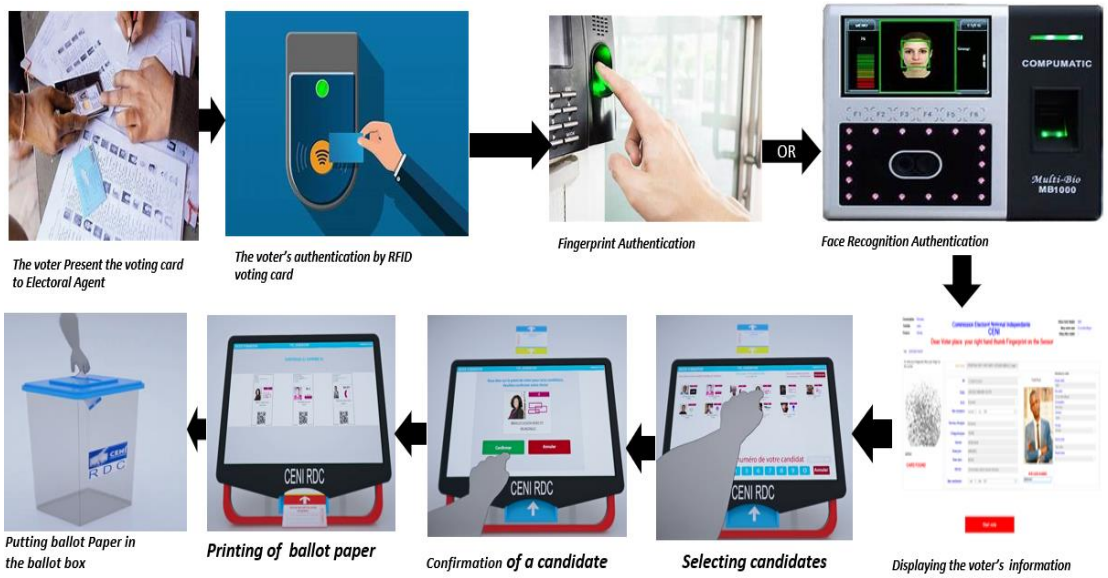

Figure 4. Physical Description of Scenario of the Proposed Voting System

Finally, the system eliminates the need for ink-based marking by digitally tracking voting status, thereby enhancing traceability and reliability. Collectively, these improvements are expected to strengthen electoral integrity, reduce the risk of fraud, and improve the overall robustness of the voting process.

Figure 5. The Verification Form

FINDINGS AND DISCUSSION

Empirical Findings

Perceptions of the Current Electoral System

The survey results reveal substantial dissatisfaction among respondents regarding the effectiveness of the current electoral system in preventing fraud and ensuring electoral integrity. A majority of respondents (68.2%) reported dissatisfaction with their overall experience of the voting process. In addition, 73.8% indicated that they had observed or were aware of instances of multiple voter registration, while 60.6% reported having witnessed or experienced multiple voting without detection by electoral authorities. Furthermore, 63.7% of respondents expressed the view that the current system is ineffective in detecting duplicate voter records.

Taken together, these findings suggest that perceived weaknesses in voter registration and authentication mechanisms remain a critical concern among respondents. While these results do not establish the actual prevalence of electoral fraud at the national level, they provide strong evidence of low institutional trust and perceived system vulnerability, which are key determinants of electoral legitimacy.

Perceptions of Biometric and RFID-Based Authentication

The findings indicate a generally positive attitude toward the adoption of biometric and RFID-based authentication technologies in the electoral process. A significant proportion of respondents expressed confidence in the potential of such technologies to reduce electoral fraud, with 73.1% supporting fingerprint authentication, 61.9% supporting facial recognition, and 60% supporting the integration of RFID with biometric systems.

In addition, 78.1% of respondents reported awareness of biometric authentication technologies, while 87.5% and 84.7% expressed comfort with the use of fingerprint and facial recognition, respectively, for voter identification. These findings suggest that technological acceptance is not a primary barrier to the adoption of biometric systems in the DRC context.

Usability Evaluation of Authentication Modalities

The usability evaluation results demonstrate clear differences in performance across the three authentication modalities. As shown in Table 5, fingerprint authentication achieved the highest overall usability score (93.8%), followed by RFID (92.5%) and facial recognition (88.5%).

Across the evaluated dimensions, including ease of use, speed, effectiveness, and system performance, fingerprint authentication consistently outperformed facial recognition, while RFID demonstrated strong performance particularly in speed and operational efficiency. These results suggest that fingerprint-based authentication provides the most balanced performance in terms of usability and reliability within the tested prototype environment.

To provide a detailed view of system performance across the three authentication modalities, the results are presented separately for fingerprint, facial recognition, and RFID-based authentication. The usability results for fingerprint authentication are presented in Table 2.

Table 2. Usability evaluation results for fingerprint authentication

	Valid	Missing	Mean	Std. Deviation	Minimum	Maximum
Fingerprint_Ease_of_use	25	0	4.800	0.408	4.000	5.000
Fingerprint_speed	25	0	4.760	0.436	4.000	5.000
Fingerprint_authentication_effectiveness	25	0	4.800	0.408	4.000	5.000
Fingerprint_easy_scanning	25	0	4.680	0.557	3.000	5.000
Fingerprint_telling_error_msg	25	0	4.640	0.569	3.000	5.000
Fingerprint_easy_recovering_error	25	0	4.400	0.707	3.000	5.000
Fingerprint_peformance	25	0	4.760	0.436	4.000	5.000

The results for facial recognition authentication are summarized in Table 3.

Table 3. Usability evaluation results for facial recognition authentication

	Valid	Missing	Mean	Std. Deviation	Minimum	Maximum
Face_recog_ease_of_use	25	0	4.200	0.957	1.000	5.000
Face_recog_speed	25	0	4.480	0.918	1.000	5.000
Face_recog_effectiveness	25	0	4.600	0.866	1.000	5.000
Face_recog_easy_scanning	25	0	4.560	0.870	1.000	5.000
Face_recog_telling_error	25	0	4.320	0.900	1.000	5.000
Face_recog_easy_recovering_error	25	0	4.240	1.012	1.000	5.000
Face_recog_perfotmance	25	0	4.600	0.764	2.000	5.000

The usability performance of RFID-based authentication is presented in Table 4.

Table 4. Usability evaluation results for RFID-based authentication

	Valid	Missing	Mean	Std. Deviation	Minimum	Maximum
Rfid_ease_in_use	25	0	4.640	0.638	3.000	5.000
Rfid_speed	25	0	4.600	0.645	3.000	5.000
Rfid_effectiveness	25	0	4.640	0.638	3.000	5.000
Rfid_easy_scanning	25	0	4.680	0.557	3.000	5.000
Rfid_error_msg	25	0	4.400	0.764	3.000	5.000
Rfid_easy_recovering	25	0	4.480	0.770	3.000	5.000
Rfid_performace	23	2	4.739	0.689	3.000	5.000

Table 5. Comparative usability performance of authentication modalities

Authentication method	Ease of use	Speed	Effectiveness	Easy scanning	Giving error message	Easy recovering and retry	Performance	Mean of Means	%
Fingerprint	4,8	4,76	4,8	4,68	4,64	4,4	4,76	4,6914286	93,829
Facial Recognition	4,2	4,48	4,6	4,56	4,32	4,24	4,6	4,4285714	88,571
RFID Card	4,64	4,60	4,64	4,68	4,4	4,48	4,939	4,6255714	92,511

DISCUSSION

Interpreting System Vulnerabilities and Trust Deficit

The findings highlight a critical gap between the intended design of the electoral system and its perceived effectiveness among users. The high proportion of respondents reporting exposure to multiple registration and voting suggests that perceived system vulnerabilities are widespread, which may undermine public trust in electoral outcomes.

This aligns with prior research emphasizing that electoral legitimacy is not only determined by procedural correctness but also by citizens' confidence in the system's integrity (IFES, 2022). In this context, the absence of automated voter authentication mechanisms at the point of voting appears to be a key structural limitation.

Acceptance of Biometric Technologies in Electoral Contexts

The positive perception of biometric authentication observed in this study is consistent with existing literature suggesting that biometric systems can enhance voter confidence by improving identity verification and reducing opportunities for fraud (IFES, 2011; Jain et al., 2011).
Importantly, the findings indicate that respondents are not only aware of biometric technologies but are also largely willing to adopt them in electoral processes. This suggests that social acceptance is unlikely to be a major barrier to implementation in the DRC.
However, it is important to note that acceptance alone does not guarantee successful deployment. Prior research emphasizes that the effectiveness of election technologies depends on governance, transparency, and institutional capacity rather than technology alone (Alvarez et al., 2009).

Multimodal Authentication: Performance and Trade-offs

The usability results provide important insights into the relative strengths of different authentication modalities. While multimodal systems are often presented as superior solutions, the findings demonstrate that not all modalities contribute equally to system performance.
Fingerprint authentication emerged as the most reliable and user-friendly method, confirming prior studies that highlight its robustness and widespread usability (Umar et al., 2022). In contrast, facial recognition showed comparatively lower usability scores, which may reflect known challenges related to environmental conditions, user interaction, and performance variability across populations (NIST, 2020).
RFID technology demonstrated strong performance in terms of speed and operational efficiency, supporting its role as an effective complementary mechanism rather than a standalone authentication solution. This aligns with prior research emphasizing RFID's contribution to improving system efficiency and reducing processing time (Borba et al., 2018).
Taken together, these findings suggest that a hybrid approach, prioritizing fingerprint authentication while integrating RFID and facial recognition as complementary layers, offers a more balanced and context-appropriate solution.

Theoretical and Practical Contributions

This study makes three key contributions. First, it provides empirical evidence from the DRC context, addressing a significant gap in the literature, which has largely focused on other regions with different institutional conditions. Second, it integrates user perception and system usability analysis, offering a more comprehensive evaluation framework compared to prior studies that focus primarily on technical system design. Third, it contributes to the ongoing debate on multimodal biometric systems by demonstrating that the effectiveness of such systems depends not only on combining multiple technologies but also on prioritizing the most reliable and user-friendly modalities.

Practical Implications

The findings have several important practical implications for policymakers and electoral management bodies such as CENI. First, from a policy perspective, the strong support for biometric systems indicates that electoral reform initiatives incorporating biometric authentication are likely to be both socially acceptable and politically feasible. Second, from an operational standpoint, the implementation of such systems would require substantial investments in capacity building, infrastructure development, and robust data management frameworks to ensure system reliability and security. Third, from a technical perspective, system design should prioritize fingerprint authentication as the primary identification method, while integrating RFID and facial recognition as complementary layers to enhance system robustness and resilience. Collectively, these implications provide actionable insights for the effective design and deployment of technology-enabled electoral systems.

Limitations and Future Research
Despite its contributions, this study has several limitations.
First, the survey sample may not fully represent the diverse demographic and geographic characteristics of the DRC population, limiting the generalizability of the findings. Second, the usability evaluation was conducted in a

controlled environment with a relatively small sample, which may not fully capture real-world operational challenges.

Third, the study does not address certain structural issues, such as automated age verification, due to the absence of a comprehensive national database of birth records. This represents an important avenue for future research, as the establishment of a unified and reliable citizen identification system could strengthen the country's digital sovereignty and unlock the potential for a wide range of digital-based initiatives.

Fourth, the implementation of biometric and RFID-based systems involves significant financial and logistical costs, which may pose challenges in resource-constrained environments.

Future research should focus on large-scale pilot testing, integration with national identity systems, the development of complementary verification mechanisms, including age validation and fraud detection algorithms, and an empirical analysis based on a theory- or context-driven research model.

CONCLUSION

This study examined the potential of a multimodal biometric and RFID-based authentication system to address persistent challenges in the DRC's electoral process. The findings highlight significant dissatisfaction with the current system and strong support for technological solutions aimed at improving voter authentication.

The usability evaluation demonstrates that fingerprint authentication offers the most reliable and user-friendly solution, while RFID and facial recognition provide valuable complementary functions. Rather than presenting technology as a complete solution, this study emphasizes that effective electoral reform requires the integration of appropriate technologies with robust governance and institutional frameworks.

Acknowledgement

This work was supported by Culture, Sports and Tourism R&D Program through the Korea Creative Content Agency grant funded by the Ministry of Culture, Sports and Tourism in 2023 (RS-2023-00224524). It was also supported in part by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2020S1A5B8104091).

REFERENCES

Adjei, J. K., Opare, K., & Asamoah, D. (2020). A secure biometric-based electronic voting system using multimodal authentication. International Journal of Computer Applications, 175(43), 1–8. https://doi.org/10.5120/ijca2020920203

Ali-Diabacté, T. (2020). Operational and procedural integrity of elections in the Democratic Republic of Congo. Journal of African Elections, 19(1), 52–65. https://doi.org/10.20940/JAE/2020/v19i1a3

Alvarez, R. M., Hall, T. E., & Trechsel, A. H. (2009). Internet voting in comparative perspective: The case of Estonia. PS: Political Science & Politics, 42(3), 497–505. https://doi.org/10.1017/S1049096509090787

Arinze, S. N., & Nwajana, A. O. (2025, October). RFID-enabled electronic voting framework for secure democratic processes. In Telecom (Vol. 6, No. 4, p. 78). MDPI.

Awotunde, J. B. (2017). Automated voting system using bimodal identification and verification technique. Annals of Computer Science Series, 15(1), 1–8.

Berwouts, K., & Reyntjens, F. (2019). The Democratic Republic of Congo: The great electoral robbery (and how and why Kabila got away with it). Africa Policy Brief, 25(25), 1–6.

Borba, P., Alves, J., & Nardelli, P. H. J. (2018). RFID-based solutions for secure and efficient identification systems. IEEE Communications Magazine, 56(2), 118–124. https://doi.org/10.1109/MCOM.2018.1700646

International Foundation for Electoral Systems. (2011). Biometrics in elections. https://www.ifes.org/sites/default/files/migrate/biometrics_in_elections_2011_0.pdf

International Foundation for Electoral Systems. (2015). Voter registration and identification: Key concepts and issues. https://www.ifes.org

International Foundation for Electoral Systems. (2020). Biometric technology in elections. https://www.ifes.org

International Foundation for Electoral Systems. (2022). Lessons on the use of technology in elections and the impact on electoral dispute resolution. https://www.ifes.org/sites/default/files/2022-12/Lessons%20on%20the%20Use%20of%20Technology%20in%20Elections%20and%20the%20Impact%20on%20EDR_Final.pdf

International Foundation for Electoral Systems. (2023). Five principles for the use of technology in elections. https://www.ifes.org/sites/default/files/2023-10/Five_Principles.pdf

International IDEA. (2011). Introducing electronic voting: Essential considerations. https://www.idea.int

International IDEA. (2016). Voter registration in Africa: A comparative analysis. https://www.idea.int

Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern recognition letters, 79, 80-105.

Jain, A. K., Ross, A., & Nandakumar, K. (2011). Introduction to biometrics. Springer. https://doi.org/10.1007/978-0-387-77326-1

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4–20. https://doi.org/10.1109/TCSVT.2003.818349

Juma, P. Z. (2019). La problématique de la crise de légitimité et la fraude électorale en République Démocratique du Congo.

Lewis, J. R. (1995). IBM computer usability satisfaction questionnaires: Psychometric evaluation and instructions for use. International Journal of Human-Computer Interaction, 7(1), 57–78. https://doi.org/10.1080/10447319509526110

Mansingh, B. P., & Titus, J. (2020). A secured biometric voting system using RFID linked with the Aadhaar database. In Proceedings of the IEEE International Conference on Advanced Computing and Communication Systems (ICACCS) (pp. 24–30).

Mavungu, M. E. (2013). Fraud and repression in the 2011 elections in the Democratic Republic of Congo. Journal of African Elections, 12(3), 25–50.

Milolo, M. (2019). Le numérique dans la gestion du système électoral: L'expérience de la machine à voter en RDC.

Møller, J., & Skaaning, S.-E. (2013). Regime types and democratic sequencing. Journal of Democracy, 24(1), 142–155. https://doi.org/10.1353/jod.2013.0010

Nadar, G. R., Paulraj, R., Rajesh, M., Kiruthika, S. V., & Jasmine, I. (2017). Smart voting machine based on fingerprints and face recognition. International Journal of Engineering Research & Technology.

Nagaraj, P., Muneeswaran, V., Ramu, B., Pavan, C. S., Yoganand, E., & Prakash, K. G. (2022). Voting system using facial and fingerprint authentication. In Proceedings of the International Conference on Data Science, Agents and Artificial Intelligence (ICDSAAI) (pp. 1–6). https://doi.org/10.1109/ICDSAAI55433.2022.10028783

Najam, S., Shaikh, A. Z., & Naqvi, S. (2018). A novel hybrid biometric electronic voting system: Integrating fingerprint and face recognition. Mehran University Research Journal of Engineering and Technology, 37(1), 59–68. https://doi.org/10.22581/muet1982.1801.05

Narayana, D. S., & Sarma, G. S. (2022). A fair and secure electronic voting system authentication with biometric information. International Journal of Scientific Research.

National Institute of Standards and Technology. (2015). Biometric performance evaluation. https://www.nist.gov

National Institute of Standards and Technology. (2020). Face recognition vendor test (FRVT) part 3: Demographic effects. U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8280

Olumide, S. A., Olutayo, K. B., & Adekunle, S. E. (2020). A review of electronic voting systems: Strategy for a novel approach. International Journal of Information Engineering and Electronic Business, 12(1), 19–29. https://doi.org/10.5815/ijieeb.2020.01.03

Padmavathi, J., Jahnavi, M., Hemanth, M., Rama Rao, S. V., & Sunitha, R. (2023). A secured hybrid biometric-based e-voting system for election processes. Industrial Engineering Journal, 52(3), 1–10.

Rhue, L. (2023). The anchoring effect, algorithmic fairness, and the limits of information transparency for emotion artificial intelligence. Information Systems Research, 35(3), 1479–1496.

Ross, A., & Jain, A. K. (2003). Information fusion in biometrics. Pattern Recognition Letters, 24(13), 2115–2125. https://doi.org/10.1016/S0167-8655(03)00079-5

Sudeepthi, K., & Lingala, G. (2020). Secured e-voting system using two-factor biometric authentication. In Proceedings of the IEEE International Conference on Computing Methodologies and Communication (pp. 1–4).

The Carter Center. (2024). Final report: General elections in the Democratic Republic of the Congo, December 2023. https://www.cartercenter.org/wp-content/uploads/2024/07/drc-final-report-2023.pdf

Umar, B. U., Olaniyi, O. M., Olatunde, A. B., Isah, A. A., Haq, A. K., & Ajayi, I. T. (2022). A bi-factor biometric authentication system for secure electronic voting. In Proceedings of IEEE NIGERCON 2022. https://doi.org/10.1109/NIGERCON54645.2022.9803174

United Nations Development Programme. (2015). Information technology and elections management. https://www.undp.org

United Nations Development Programme. (2017). Electoral integrity and inclusive participation. https://www.undp.org

Want, R. (2006). An introduction to RFID technology. IEEE Pervasive Computing, 5(1), 25–33. https://doi.org/10.1109/MPRV.2006.2

World Bank. (2018). Principles on identification for sustainable development: Toward the digital age. https://id4d.worldbank.org

