Review Article *Open Access*

Journal of Economics and Social Dynamics

ISSN: 3069-6577

DOI: *doi.org/10.63721/25JESD0110*

Securing the Vote through Multimodal Biometric Authentication: Evidence from the DRC's Electoral System

Lingole Mbembo Justin[1,3], Nyazabe Sllife[1], Min Sam Ko[2], Grace-Roven Tshimanga[1], Nkwimi Bilangoma Grevi[1,3] and Kinguangu Nguala Dieu-Merci[1]

[1]Department of Management Information Systems and Business English, University of Kinshasa
[2]Professor, School of ICT, College of Computing, Hanyang University
[3]Department of Applied Artificial Intelligence, Hanyang University

Citation: Lingole Mbembo Justin, Nyazabe Sllife, Min Sam Ko, Grace-Roven Tshimanga, Nkwimi Bilangoma Grevi, et al. (2025) Securing the Vote through Multimodal Biometric Authentication: Evidence from the DRC's Electoral System. J of Eco and Soc Dynamics 1(2), 1-16. WMJ/JESD-110

Abstract

Electoral processes in the Democratic Republic of the Congo (DRC) have faced persistent challenges since the first democratic elections in 2006, particularly regarding transparency and trust. Despite the introduction of electronic voting machines in 2018 and 2023, concerns remain over electoral fraud, notably the lack of robust mechanisms to prevent multiple registrations and votes by the same individual. These vulnerabilities continue to undermine public confidence in the Independent National Electoral Commission (CENI).

This study proposes a multimodal biometric authentication system to enhance the credibility and security of the electoral process. The proposed system integrates fingerprint and facial recognition technologies with RFID (Radio-Frequency Identification) card functionality, aiming to secure both voter registration and voting phases.

To evaluate public perception, a survey was conducted among Congolese citizens to assess their experiences with past elections and their trust in CENI's fraud prevention capabilities. Findings revealed widespread dissatisfaction and a strong interest in adopting biometric technologies.

A prototype of the system was developed and tested with 25 graduate students at Hanyang University. Among the three authentication methods, fingerprint recognition yielded the highest user satisfaction (93.8%), followed by RFID (92.5%) and facial recognition (88.5%), indicating strong potential for improving usability and trust in future DRC elections.

***Corresponding author:** Nyazabe Sllife, Ph.D. Candidate, Graduate School of Global Digital Innovation, University in Daejeon, South Korea.

Review Article *Open Access*

Submitted:09.09.2025 **Accepted:** 20.09.2025 **Published:** 29.09.2025

Introduction

The Democracy is a system of government in which state power is vested in the people or the general population of a state. In democracy, rulers are elected through competitive elections while more expansive definitions link democracy to guarantees of civil liberties and human rights in addition to competitive elections. Among elements of democracy, the election is the heart or the key element. And good elections are the ones presenting trust that each vote is recorded and tallied with accuracy, impartiality, freedom, fairness and peacefulness. However, In Democratic Republic of the Congo, the election issues have always been subjects of debates and contradictions after the publication of results by the CENI (Commission Electorale Nationale Independent) which can be translated in English as Independent National Electoral Commission. In the first two elections (in 2006 and 2011) the electoral system was manual where the voter could select his or her chosen candidates on the voting ballot and by putting a check mark next to the candidate's photo. These elections were characterized by the terrible frauds and the lack of transparency according to [1-3].

Finally in 2018, the Congolese CENI introduced the voting Machine in the Voting process. According to Ali-Diabacté, 2020, Martin Milolo, 2019 the Congolese Electoral system recognized some improvement comparing to the manual system introduced in 2006 and 2011 elections. The machine helps the voter to select his/her chosen candidate, once clicked on the button validate, the chosen candidate's number of voices will increment and then a ballot paper will be printed, containing the voter's choice [4,5].

Furthermore, the Fourth elections which took place on December 20, 2023: used the same system of 2018 and was Characterized by the massive cheating where some voting machines were found in some candidates' house. The recent report of the CENI published on January 5, 2024 Press release n°002/CENI/2024, mentioned the cancellation of votes of 82 candidates due to cheating and the illegal use of CENI kits (Source: www.ceni.cd.)

The Congolese electoral system, like many others worldwide, is divided into two interconnected phases: voter enrollment and voting. These phases are interdependent, which means that the failure of the first (enrollment) leads to the failure of the second (voting). Enrollment, or voter registration, is the stage where eligible citizens are authenticated and added to the voter list, ensuring that only those meeting the criteria can participate in elections. This phase also establishes preventive mechanisms to mitigate potential fraud during voting. However, studies indicate that the current Congolese electoral system lacks robust automatic detection methods to prevent individuals from registering multiple times. So, this allows dishonest individuals to potentially obtain multiple voting cards and vote multiple times. To counter this, CENI, the Congolese electoral commission, conducts post-enrollment fingerprint checks to detect duplicated data, a method whose effectiveness within the DRC's electoral context remains uncertain.

Since 2018, the introduction of Electronic Voting Machines (EVMs) aimed to enhance election integrity, but the system still fails to prevent multiple voting, as these machines do not authenticate voters. The current system does not mandate voter authentication before casting votes, instead relying on manual checks by CENI agents.

Voters are required to present their voting cards, after which agents decide eligibility by checking names against a list, marking names, and applying ink to thumbs after vote. However, this human-dependent process is vulnerable to corruption, with reports indicating instances of CENI agents allowing multiple votes in exchange for bribes. Some candidates even misuse voting machines at home, casting multiple votes undetected. Reports and studies indicate that some candidates exploit these vulnerabilities by bribing agents or using voting machines at home, resulting in fraudulent votes. A CENI report from January 2024 underscores these issues, revealing that 82 candidates were disqualified for electoral fraud involving unauthorized CENI equipment usage. This pattern of repeated voting and systemic exploitation has highlighted critical flaws in the existing system. Recognizing these vulnerabilities, this research seeks to design and

implement a secure electoral system using biometric authentication (fingerprint and facial recognition) alongside RFID (Radio-Frequency Identification) technology in order to prevent the multiple enrollment and multiple voting during the elections. The paper deals with the question rather the current methods applied by the Congolese CENI guarantee the security against electoral fraud or not. And we look at the Congolese people's perception and degree of awareness on E-voting using the Biometric authentication methods (Fingerprint and Facial recognition) combined with RFID technology. And finally, we are searching to know how effective is a biometric-based electoral system combined with RFID technology, basing in the context of DR Congo. After the experiment we are going to compare the three aforementioned methods, and say which methods is more user-friendly or more effective compared to the others.

Literature Review

In the realm of democratic governance, the integrity and security of electoral processes serve as the key element, underpinning the legitimacy of elected governments and the trust of citizens in their democratic institutions. However, traditional paper-based electoral systems have encountered numerous challenges over the years, ranging from instances of fraud and voter impersonation to logistical inefficiencies. These shortcomings have necessitated the exploration of innovative technology-based solutions aimed at fortifying electoral integrity and bolstering public confidence in the electoral process.

Among the technological advancements proposed to address these challenges, biometric authentication and radio-frequency identification (RFID) technology have emerged as promising avenues for enhancing the security and efficiency of electoral systems. Biometric authentication, encompassing methods such as fingerprint, facial recognition and iris, offers a unique and reliable means of verifying individual identities, thereby mitigating the risk of fraudulent voting practices. Similarly, RFID technology, which utilizes radio waves to transmit data stored on cards or tags, presents opportunities to streamline voter registration and authentication processes, while also enabling real-time tracking of voter participation. In the subsequent lines, we will delve into the theoretical underpinnings of biometric authentication and RFID technology, examining their potential applications in electoral systems.

Biometric authentication is increasingly being employed to enhance security and efficiency in electronic voting systems. Biometrics refers to the automatic recognition of individuals based on their physiological or behavioral characteristics. Common biometric traits include fingerprints, facial recognition, and iris scans [6]. The primary advantage of biometric authentication is that it offers a unique and difficult-to-fake identification mechanism, reducing the risk of electoral fraud.

Jain, Ross, and Nandakumar (2016) assert that biometric data, such as fingerprints and facial features, possess characteristics that are highly distinctive and virtually impossible to replicate. This uniqueness forms the basis of biometric authentication systems, enabling them to accurately verify the identity of individuals with a high degree of certainty. Guerin and Tran (2017) also emphasize that integrating biometric data into voter registration and verification processes could significantly enhance voter confidence by ensuring that each individual can only participate once in the election process. Moreover, biometric authentication offers additional benefits beyond security.

To complement biometric authentication, RFID technology is also gaining popularity in voting systems. outlined that RFID can serve as a secondary layer of security, verifying the voter's identity through a unique card, which helps maintain secure access to the voting platform [7].

The combination of fingerprint, facial recognition, and RFID offers a multi-modal authentication approach, which significantly strengthens security by requiring multiple identity proofs, thus mitigating risks of voter fraud and impersonation. In assessing the usability of different biometric methods, studies have demonstrated that while fingerprint and facial recognition are effective, they vary in terms of user satisfaction and ease of use [7]. found that fingerprint authentication was particularly user-friendly and efficient, whereas facial recognition, while accurate, faced challenges related to user experience.

Olumide S. et al., 2020 Numerous studies highlight the effectiveness of biometric systems, such as fingerprint and facial recognition, in preventing impersonation and ensuring secure voter identification. However, many existing systems struggle with challenges like high costs and technical limitations. reviewed the challenges associated with traditional and electronic voting systems, particularly in emerging democracies [8].

Radio-frequency identification (RFID) technology has emerged as a promising tool for improving the efficiency, security, and transparency of electoral systems. By leveraging RFID-enabled cards or tags, electoral authorities can streamline voter registration and authentication processes, while also enhancing the integrity of elections. One of the key advantages of RFID technology lies in its ability to securely store and transmit voter information. Borba, Alves, and Nardelli (2018) emphasize that RFID cards can serve as secure repositories for voter data, including personal details and eligibility status. This information is encoded onto RFID chips embedded within the cards, ensuring its integrity and confidentiality. During the authentication process at polling stations, RFID readers can quickly access this data, allowing election officials to verify the identity of voters with ease and accuracy.

Magaye (2019) highlights the utility of RFID in preventing instances of multiple voting by detecting attempts to cast ballots at multiple polling stations. Moreover, RFID technology offers benefits beyond authentication and tracking. The efficiency and speed of RFID-enabled authentication processes reduce wait times at polling stations, enhancing the overall voting experience for citizens (Borba, Alves, & Nardelli, 2018).

Despite these advantages, the adoption of RFID technology in electoral systems presents certain challenges and considerations. Technical issues, such as ensuring the interoperability and compatibility of RFID hardware and software systems, require careful attention (Magaye, 2019). Moreover, concerns regarding data privacy and security must be addressed to safeguard voter information against unauthorized access or manipulation.

The integration of biometric authentication and radio-frequency identification (RFID) technology represents a significant advancement in enhancing the integrity, efficiency, and security of electoral systems. By combining the strengths of biometric recognition methods, such as fingerprint and facial recognition, with the capabilities of RFID-enabled voter cards, electoral authorities can establish a comprehensive authentication mechanism that addresses key challenges and vulnerabilities in traditional electoral processes.

Adjei, Opare, and Asamoah 2020 underscore the synergistic benefits of integrating biometric authentication and RFID technology in electoral systems. At polling stations, RFID readers can quickly access this information, facilitating rapid and accurate verification of voter identities Adjei, Opare, & Asamoah, 2020. This seamless integration of biometric and RFID technologies streamlines the authentication process, reducing wait times and administrative burdens for both voters and election officials. Moreover, the integration of biometric authentication and RFID technology enables comprehensive voter tracking and monitoring throughout the electoral process.

The article by Awotunde, 2017 contributes significantly to discussions on the adoption of bimodal biometric systems in electoral processes. Awotunde's research specifically addresses common electoral challenges, such as impersonation and double voting, that affect election credibility. The study proposes an automated voting system using bimodal biometric identification, integrating both fingerprint and facial recognition technologies. This approach aims to improve voter verification accuracy and reduce electoral fraud by ensuring each voter is uniquely identifiable, thereby preventing duplicate registrations and voting. Awotunde's system is designed to reduce electoral fraud by ensuring that each voter can only register and vote once, mitigating the risks associated with duplicate or multiple voting, which are common in manual systems. While focused on Nigeria, the study's proposed system and findings are applicable to other regions facing similar electoral challenges [9].

Nagaraj et al. 2022 presents a novel e-voting system employing both fingerprint and facial recognition authentication to address common challenges like multiple voting and voter impersonation, critical issues

within the broader context of voting security. Several studies have explored biometric voting systems. proposed a bi-factor biometric authentication system combining fingerprint and iris recognition for electronic voting in Nigeria. This system addresses the common issues associated with fingerprint recognition, such as the inability to authenticate voters due to damage to the skin, especially in labor-intensive sectors. By integrating iris recognition, they achieved a system with 94% accuracy, with response times of 9 seconds for fingerprint verification and 20 seconds for iris recognition [6]. This research highlighted the limitations of using only fingerprint authentication, particularly in cases where voters' fingerprints may degrade due to labor-intensive work. Such a system could be highly relevant to the DRC/CENI, particularly in rural areas where voters may face similar challenges with fingerprint recognition.

In a related study, Hazzaa et al. 2012 developed a web-based voting system that also utilized fingerprint recognition [10]. Another study by Nadar et al. 2017 introduced a smart voting machine that integrated both fingerprint and face recognition [11]. Although this system improved security, it faced challenges such as delays in authentication due to the complexity of biometric verification.

Najam et al., 2018 proposed an electoral system using Fingerprint and facial recognition-based methods are used for voter identification. the idea was of comparing the Eigen-vectors of the extracted features with the biometric template pre-stored in the election regulatory body database. Then, the results of the proposed system showed that the proposed cascaded design-based system performed better than the systems using other classifiers or separate schemes i.e. facial or fingerprint-based schemes [12].

Padmavathi et al. (2023) proposed a secure hybrid biometric e-voting system employing RFID, fingerprint, and facial recognition techniques. The combination of these technologies ensures precision in voter identification, reducing the chances of fraudulent activities. The system's ability to prevent unauthorized voting and provide quick and accurate results [13].

Research made by emphasizes the need for robust multi-modal biometric systems, combining fingerprint, face, and RFID for enhanced security. Each method addresses specific vulnerabilities in voting processes, like preventing multiple registrations and ensuring voter authenticity [8].

Mansingh et al. 2020 explored a biometric voting system linked to India's Aadhar database using RFID technology. This system uses RFID tags for voter identification combined with fingerprint authentication, ensuring secure and verifiable voter participation [15].

In conclusion, the integration of biometric authentication and RFID technology offers a comprehensive solution to enhance the integrity, efficiency, and security of electoral systems. By combining the strengths of biometric recognition methods with the capabilities of RFID-enabled voter cards, electoral authorities can establish a robust authentication mechanism that safeguards against identity fraud, streamlines voter registration processes, and facilitates real-time monitoring of voter participation. Through strategic deployment and ongoing evaluation, the integration of biometric and RFID technologies has the potential to advance the credibility and transparency of electoral processes, thereby strengthening democratic governance and citizen trust in electoral institutions.

This literature of review presents the following gaps:

- While the literature discusses the potential benefits of biometric authentication and RFID technology in electoral systems, there is limited or Lack of Specific Empirical Studies Focusing on Socio-Political Context of elections in DRC and the CENI.
- The literature emphasizes the importance of integrating biometric authentication and RFID technology to enhance electoral integrity. However, there is a gap in the literature regarding the comprehensive evaluation of these technological solutions, including their effectiveness and the Cost Issues.
- The literature highlights the role of electoral management bodies such as CENI in implementing technology-based solutions. However, there is a gap in the literature regarding Lack of Detailed Studies Involving Election Officials

and Voters perception and awareness in adopting these Technologies.

- The literature talks about the use of the authentication using fingerprint, facial recognition and RFID technology, however most of the work don't say which methods must be prioritized, especially in some cases such as the cost issues.

Methodology

This study employs a structured and systematic approach to design, implement, and evaluate a new biometric-RFID hybrid voting system aimed at enhancing the security and integrity of electoral processes. The methodology involves seven key steps, as outlined below:

First, **The Literature Review & Case Studies:** A comprehensive review of existing literature and case studies was conducted to establish a theoretical foundation for the research. This step focused on analyzing prior work on biometric authentication, RFID technologies, and their applications in electoral systems. The objective was to identify gaps in the literature and draw insights applicable to the Democratic Republic of Congo (DRC) electoral context.

Second, **The Study of the Existing System:** An in-depth analysis of the current electoral system used by the Independent National Electoral Commission (CENI) in the DRC was undertaken. This step involved identifying vulnerabilities, inefficiencies, and challenges, such as voter impersonation, double voting, and logistical bottlenecks, that hinder the credibility of elections.

Third, the Survey on People's Experiences and Awareness: A survey was conducted to gather data on voter experiences and their awareness on biometric and RFID technologies in elections.

- **Research Design:** Mixed-methods approach (qualitative and quantitative).
- **Sampling:** 160 randomly selected Congolese participants.
- Data Collection: A structured questionnaire was used to collect information on voter challenges, perceptions of electoral fraud, and attitudes toward technology integration.

The fourth step was the Design and Implementation of the New System: Based on insights gained from the literature review, system analysis, and survey, a new biometric-RFID hybrid electoral system was designed and implemented. The system integrates:

- **Biometric technologies:** Fingerprint and facial recognition for voter identification.
- **RFID technology:** For efficient voter tracking and authentication.The system's design aimed to address challenges such as voter impersonation, multiple voting, and logistical inefficiencies.
- **Implementation:** we used C# and Python programming languages and SQL-server Express as the database management system.

The fifth step was the System Usability Testing: The usability of the proposed system was evaluated using a sample of 25 Hanyang University students to simulate real-world usage.

This test aims to evaluate the effectiveness of the designed system in terms of the ease of use, speed, effectiveness, easy scanning, error message telling, error recovery and retry, and the performance for each of the three authentication methods proposed in this work, namely: the Fingerprint, facial recognition and RFID card.

- **Tools Used:** ZKTeco 4500 & 9500 fingerprint readers, Windows RFID card reader, and ArduCam for facial recognition.
- **Method:** Post-Study System Usability Questionnaire (PSSUQ) was used to measure system usability and user satisfaction.

Research Type: The research type was Quantitative. To ensure this study follows a quantitative approach, each question utilized a Likert scale, allowing respondents to rate their responses as follows: Strongly Disagree (1), Disagree (2), Neutral (3), Agree (4), and Strongly Agree (5). Each numerical value corresponds to the level of agreement or satisfaction voters assigned to the specified criteria for each authentication method, providing measurable data for analysis.

Next, comes the Data Analysis: Data collected from the surveys and system usability tests were analyzed using JASP software. The 3 three aforementioned methods were separately analyzed, and the analysis focused on the Assessing the effectiveness of the proposed system in addressing electoral challenges and Measuring usability metrics of the biometric and RFID components by basing on these the following 7 criteria:

- **Ease of Use:** This aims to measure how simple and intuitive each authentication method is for users. It evaluates how easily users can interact with the system without extensive instructions or assistance.
- **Speed:** This refers to the time it takes for each method to authenticate a user. Faster systems enhance user experience by reducing waiting times. The speed evaluation compares how long it takes for each authentication method to process after the user interacts with the system.
- **Effectiveness:** Effectiveness measures how accurately and reliably each method can verify a user's identity. A high effectiveness rating means fewer false positives or negatives.
- **Easy Scanning:** This assesses how easily the system can capture and process the biometric data or scan the RFID card. It focuses on the user's experience during the scanning phase during the enrollment and authentication.
- **Error Message Telling:** This checks how well the system communicates errors to the user. Clear, helpful error messages help users understand issues and correct their actions. For Example, in our system, if fingerprint scanning fails, the system should display a message like "Finger not properly placed" instead of just showing "Error."
- **Error Recovery and Retry:** This aspect tests how effectively the system allows users to recover from errors and retry the authentication process without frustration. It ensures that users have a clear and efficient path to correct mistakes. For example: In facial recognition or fingerprint scanning if the system fails to detect a face or fingerprint, it should prompt the user to reposition or try again without making the process cumbersome.
- **Performance:** The Performance refers to how well the system functions in various conditions over extended use. For example, for fingerprint authentication, performance could assess how consistently the scanner works for different people and how it holds up under frequent use.

The Seventh and the Final Step Dealt with Results and Discussion: The findings from the data analysis were used to evaluate the system's ability to enhance electoral security, reduce fraud, and improve voter experience. The results are discussed in the context of the DRC's electoral system, providing insights into the feasibility and scalability of implementing the proposed solution.

The Existing System of the CENI

The Congolese electoral system, like many others worldwide, is made of two important phases, namely the enrollment (voter registration) and the Voting. The phases are interconnected and interdependent, which means that the failure of the first (enrollment) leads to the failure of the second (voting). Enrollment, or voter registration, is the stage where eligible citizens are authenticated and added to the voter list, ensuring that only those meeting the criteria can participate in elections. This phase also establishes preventive mechanisms to mitigate potential fraud during voting. And the voting is the phase where enrolled people present to the voting pool to choose their desired candidates.

In this section we are presenting both the existing enrollment and voting phase of the actual electoral system of the CENI.

The Existing Enrollment System of the CENI

The following chart summarizes the existing system of the CENI:

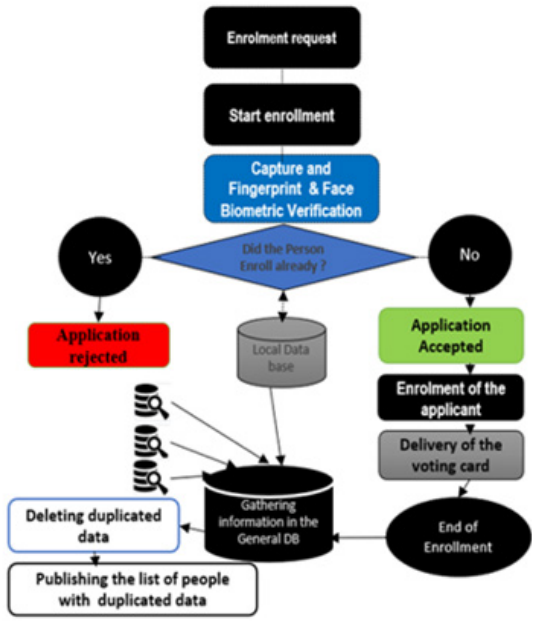

Figure 1: The Existing Enrollment System

The existing enrollment system begins with a person presenting themselves at a registration pool to request enrollment. Upon initiating the enrollment process, the system captures the individual's fingerprints and facial biometrics for verification to ensure they have not already been enrolled. This verification is conducted against the local database of the enrollment center. A duplicate check is then performed; if the individual already exists in the system, the application is rejected, and duplication is flagged in the local database. If no duplication is found, the application is accepted, and the person is officially enrolled. Following approval, the person's details are stored in the local database, and a voter card is printed and delivered to them. At the end of the enrollment process, all local database information is sent to the general database, where duplicate data is consolidated and removed. Finally, the CENI publishes a list of individuals with duplicate data, highlighting rejected and accepted enrollments, with only the most recent enrollment being validated. [15]

The Existing Voting System of the CENI

The voting process as presented in the final report of DRC elections by Carter Center, 2024 is presented as follows:

The CENI deployed one voting machine per polling station to facilitate voting at stations. After identification by means of a voter card, each voter is given a ballot paper to insert into the EVD (Electronic Voting Device), at which point he can then select his preferred candidates for presidential, parliamentary, provincial, and communal (where applicable) elections on the touch screen. A Voter makes his selection by pressing on the candidate's picture or tapping the number allocated to that candidate [16].

Depending on the number of candidates in a constituency, some voters are obliged to scroll through several screens to view the entire list of options for a given election (or he can also directly tap the number ascribed to the candidate of their choice). After selecting a candidate, the voter can either approve the selection from a pop-up box or go back to the previous step and modify his selection. A voters can also cast a blank vote as a means of abstaining from that particular contest. After completing these steps for each election type, the machine presents a final summary of the candidates and prints a ballot showing the voter's selections. Voters then cast his ballot in a single ballot box. After voting, the ink is put on the voter's thumb to show that he already voted.

This process is summarized in the following chart:

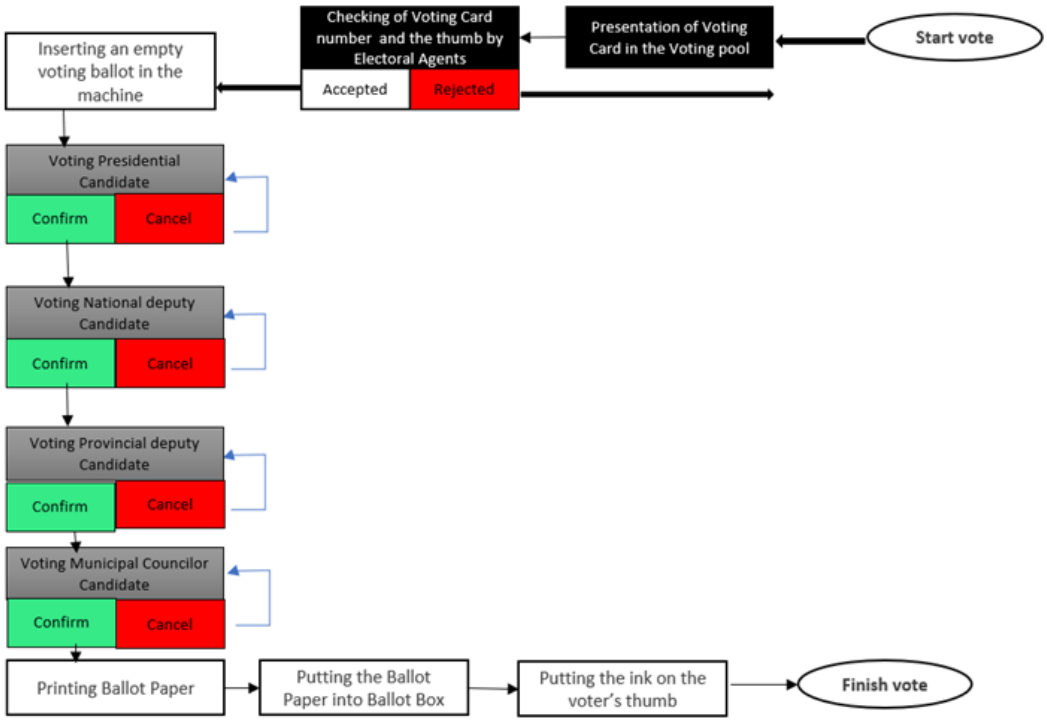

Figure 2: The Existing voting system

The Proposed System

After a deep study on the existing and the insights from the Congolese experiences in the previous elections we have proposed the new system architecture. And some key differences are provided compared to the existing system. The proposed system includes both the enrollment and voting phases.

The Proposed Enrollment System

Figure 3: The proposed enrollment system

Key Differences:

- The general database is more integrated in the proposed system, ensuring centralized data handling during enrollment. This implies the interconnexion of different centers of enrollment during the voter registration phase.

- The proposed system uses RFID voting cards instead of a simple voting card, adding an extra layer of security and efficiency during voting processes.
- The proposed system focuses on data synchronization between local and general databases to avoid duplication. This means that comparing to the former enrollment system where the integration of data was done after the enrollment period for all the country; but in the proposed architecture, the integration of data from local enrollment centers to the main data base will be done immediately.

The Proposed Voting System

Related to the failures noticed in the existing voting system characterized by: the multiple voting, fraud, the lack of the authentication methods, slowness, corruption of agents, etc, the following system is able to solve these problems.

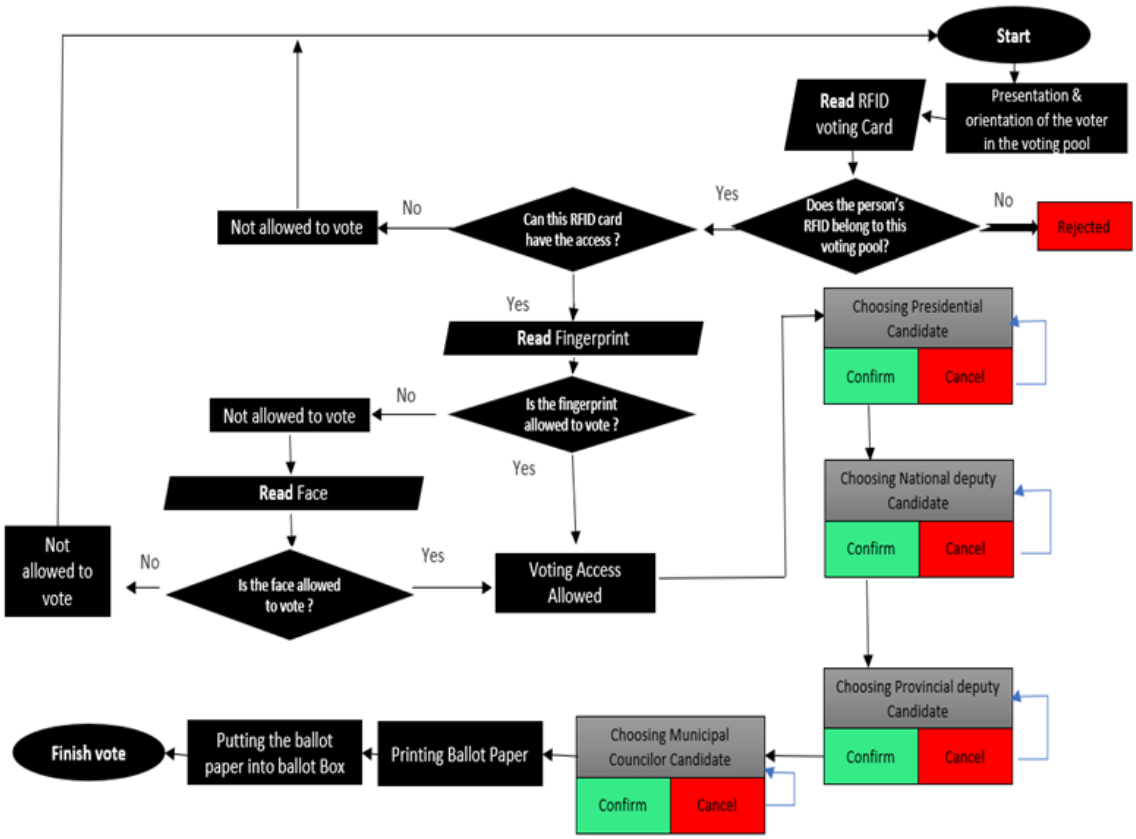

Figure 4: The Existing voting process

The Proposed Voting System Architecture process presented in the figure 12 can be interpreted as follows: once the voter is present in the voting pool, then he's going to be guided by the agents of the CENI. Then he will be asked to read his voting card to the sensor in order to have the access to the system. So, the system reads the RFID card, and checks if the voter belongs to the voting pool. If the voter's RFID voting card is not recognized as part of the voting pool, then the person's card is rejected. But in case that the voter's RFID voting card is recognized as part of the voting pool, then the system will check if the person voted already or not. If the voter voted already, then the voter is not allowed to vote. Unless the person voted already, then the system proceeds to read the fingerprint. If the fingerprint is not recognized, then, voting access is denied, but it gives the possibility of authenticating by using the facial recognition. But if the fingerprint is recognized, then the system allows access to voting. As an additional layer of security, the system performs facial recognition in the case the fingerprint fails. If the face is not recognized, voting is denied. If recognized, the voter is granted access to proceed with voting. After authentication, the voter chooses candidates for the following positions (same as the existing system): Presidential Candidate, National Deputy Candidate, Provincial Deputy

Candidate, and the Municipal Councilor Candidate. Similar to the existing system, the voter must confirm or cancel after each selection. A ballot paper is printed and placed in the ballot box, marking the end of the voting process.

This architecture is physically showed or described in the figure 5.

Figure 5: Physical Description of Scenario of the Proposed Voting System

Comparing to the existing voting system, the proposed system presents the following key differences:

The Verification before Voting: while the existing voting system requires human to decide if the person can vote or not, in proposed system, this will depend on the system. Which means that the person will place his RFID on the sensor and the system will proceed to the verification and decide rather the person can vote or not.

Figure 6: The verification form

- **Biometric authentication requirement:** Another difference that the proposed system provides is the authentication by fingerprint or facial recognition. This will prevent anyone to proceed to multiple voting.

- Elimination of the requirement of putting the ink after voting: after voting, the voter will not be supposed to put the ink on the thumb, because, one validates the vote, the person will not be given the possibility of voting again.

Findings and Discussion

Findings

The main objective of this research was to analyze and provide a system able to help the independent National Electoral Commission (CENI) of Democratic Republic of the Congo to provide free, fair, and credible elections without any fraud by enhancing the security, accuracy, and efficiency of the voting and enrollment processes. Throughout this research, we first, investigated to know if methods applied by the DR Congo's Independent National Electoral Commission (CENI) really guarantee the security against fraud during both enrollment and voting phases by preventing multiple enrollments and multiple voting. Second, we investigated Congolese people's awareness, perception or what they think of the biometric-based and RFID technology electoral system, basing on their experiences in previous elections. Third, we investigated if the biometric-based (fingerprint and facial recognition authentication) system with RFID cards is effective in preventing voter fraud and ensuring a one-to-one person vote and enrollment, basing on the actual context of Democratic Republic of the Congo, in other to decide which method is the best for the elections in the context of DRC. So, basing on these three research questions, the research we conducted present the following findings:

Concerning the integrity or effectiveness of methods provided by the CENI for preventing the multiple enrollment and multiple voting, the results present the following findings: About 68.2% of our respondents are not satisfied with the overall experience with the voting process in the previous elections. 73.8% have witnessed the Multiple Enrollment and 60.6% of our respondents experienced or witnessed the multiple voting Without being detected by the CENI. And 63.7% of our respondents Confirm the failure of the actual system in detecting Duplicated data. so, these findings support the hypothesis that current methods are ineffective, failing to detect and eliminate duplicate registrations and votes, which jeopardizes election integrity.

Regarding Congolese people's awareness, perception or what they think of the biometric-based and RFID technology electoral system, the results can be presented as follows: The findings indicate that people generally have a positive view of biometric-based systems. A majority of respondents (73.1%, 61.9%, and 40%) think that using fingerprint and facial recognition along with RFID technology can greatly help reduce electoral fraud. And 62.5% of our respondents insisted on the aspect that a strict penalty for anyone one making fraud. The 78.1% of respondents are aware of biometric authentication methods (fingerprint & face recognition) and RFID. The 87.5% of the respondents are comfortable with the idea of using Fingerprint authentication for vote and enrolment. And 84.7% of the respondents are comfortable with the idea of using facial recognition for vote and enrolment. And 60% of people believe that the combination RFID cards with biometrics can reduce the electoral fraud.

Concerning the Effectiveness of the Biometric System with RFID, after testing system, the results from the users' feedback were analyzed separately as mentioned above, following the three authentication methods , namely: fingerprint, facial recognition and RFID technology. The results of the user satisfaction and the system usability from descriptive analysis can be presented as follows:

Concerning the Effectiveness of the Biometric System with RFID, after testing system, the results from the users' feedback were analyzed separately as mentioned above, following the three authentication methods , namely: fingerprint, facial recognition and RFID technology. The results of the user satisfaction and the system usability from descriptive analysis can be presented as follows:

The data analysis results related to the fingerprint can be presented as follows:
Table 1: Presentation of the Fingerprint Authentication Results

Descriptive Statistics

	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 data analysis results related to the facial recognition can be presented as follows:
Table 2: Presentation of the facial recognition Authentication Results

Descriptive Statistics ▼

	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 data analysis results related to the RFID card authentication can be presented as follows:
Table 3: Presentation of Results of the Authentication with RFID cards

Descriptive Statistics

	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

The following table provide a comparative analysis of the three methods based on the survey responses.
Table 4: Comparison of Methods

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

The comparative analysis of the three methods show that fingerprint authentication is the most effective and user-friendly method with the highest overall rating of 93,8%. RFID follows closely behind with 92.5%, excelling in performance and ease of use. Facial recognition, while effective, lags behind in terms of user-friendliness and effectiveness with 88.5%. Therefore, for maximum usability and effectiveness, Fingerprint and RFID should be prioritized in biometric-based e-voting systems.

Discussion

Integration

The findings align with prior research advocating for biometric technology in electoral systems, as such technologies have been proven effective in similar contexts to reduce identity-related fraud and enhance voter confidence.

Our findings align with who outlined that RFID can serve as a secondary layer of security, verifying the voter's identity through a unique card, which helps maintain secure access to the voting platform. is sharing the same point of view like us since he argues that the combination of fingerprint, facial recognition, and RFID offers a multi-modal authentication approach, which significantly strengthens security by requiring multiple identity proofs, thus mitigating risks of voter fraud and impersonation [7].

Nagaraj et al. found that fingerprint authentication was particularly user-friendly and efficient, whereas facial recognition, while accurate, faced challenges related to user experience. These findings from show that the Fingerprint is more reliable than the facial recognition. Which implies the fingerprint must be prioritized than the facial recognition. mentioned the e-voting machine presents many disadvantages. Among the inconvenient he mentioned that: "People Vote without confidence by the fact that the voter is ignorant about his vote and Button jamming, cross voting are various other drawbacks in this system." So, our research is solving this problem by the fact that the system provides both the electronic results and the manual results, expressed in the printed ballots which must be counted manually and compared to the results given by the machine [17].

Our findings align with what was mentioned by Borba, Alves, & Nardelli, 2018 that the RFID card authentication is very fast authentication in the context of elections. Biometric systems have previously been adopted in various African nations, contributing positively to election transparency and trustworthiness. The positive perception among Congolese respondents further supports this, suggesting that the DRC is ready for a technological shift to strengthen its electoral processes. mentioned that Nigeria and other countries are facing the serious electoral problems, especially the multiple enrollment and multiple voting [9]. So, our system is not only solving the DR Congo's electoral problems but also any other countries facing the same challenges, including Nigeria.

Implication

The findings have several implications:

- Policy Implications: The DRC government and CENI may consider adopting biometric-based voting systems, as the majority support the implementation and are aware of the benefits. This shift could significantly increase voter confidence and reduce fraudulent practices, promoting fairer elections.
- Operational Changes for CENI: Transitioning to a biometric system with RFID cards necessitates comprehensive training for electoral officers to ensure secure enrollment and voting. Such training could reduce unintentional fraud by improving data accuracy and system familiarity among officers.
- Technical Enhancements: The positive feedback on system usability underscores the need for continuous technical upgrades. The successful implementation of this system would require regular updates to keep up with technological advancements and maintain high security standards.

Limitations

Despite its contributions, the study has several limitations:

- Limited Sample Diversity: The sample may not fully represent the diverse demographic and geographic distribution within the DRC, possibly affecting the generalizability of the findings. Another aspect is that the usability test should include many people containing also less educated people in order to see how easy they could find the system.

- Difficulty of preventing minors to vote: One of the notable limitations of this study is the inability to prevent the enrollment of underage individuals due to the lack of a comprehensive and accessible database containing birth date information for the DRC population. Many respondents expressed concerns that CENI's current system fails to effectively prevent minors from enrolling, which remains a gap in this research. Without access to birth date data, it is challenging to verify age eligibility reliably, leaving a significant area of potential fraud unaddressed.
- Technical Constraints: The usability tests of the biometric system were limited to controlled environments, which may not fully reflect the complexities of a real-world voting environment where technical and logistical challenges are more pronounced.
- The higher cost: the implementation of a such biometric-based system using RFID technology will require much money than the existing system and this can be challenging for the Congolese Government [19-26].

Conclusion and Future studies

In conclusion, this study addressed current challenges in the DRC's electoral system, specifically around issues of fraud and voter integrity, where multiple voting and enrollment have undermined election fairness. Through a survey of Congolese voters, the study highlighted the current inadequacies and the public's preference for secure, biometric-based solutions. Consequently, an enhanced e-voting system using fingerprint and facial recognition with RFID was developed to ensure a secure, one-to-one vote-to-person match. Usability tests confirmed the system's effectiveness, with fingerprint authentication rated as the most user-friendly, followed by RFID and then comes the facial recognition. This study supports adopting bimodal biometric methods and RFID, particularly by prioritizing the fingerprint and RFID, to improve security and voter confidence in DRC elections, promoting a fairer and fraud-free electoral process. Future studies should focus on large-scale pilot testing, developing age-detection algorithms, enhancing public education, and learning from other African countries' experiences.

References

1. Juma Pz (2019) The Issue of The Legitimacy Crisis and Electoral Fraud in the Democratic Republic of Congo, Joseph Kabila Main Player: "from 2001 to the present day". Analysis and Future Perspectives https://www.academia.edu/38942145/LA_PROBL%C3%89MATIQUE_DE_LA_CRISE_DE_L%C3%89GITIMIT%C3%89_ET_LA_FRAUDE_%C3%89LECTORALE_EN_RDC
2. Mavungu ME (2013) Stay in power whatever it takes-fraud and repression in the 2011 elections in the Democratic Republic of Congo. Journal of African Elections 12: 25-50.
3. 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: 1-6.
4. Tadjudine Ali daibacté (2020) Operational and procedural integrity of elections in the Democratic Republic of Congo,Journal of African elections 19.
5. Milolo M (2023) Le numérique dans la gestion du système électoral : l'expérience de la machine à voter dans les scrutins de la présidentielle et des législatives de 2018 en RDC. https://www.researchgate.net/publication/374751440_Le_numerique_dans_la_gestion_du_systeme_electoral_l'experience_de_la_machine_a_voter_dans_les_scrutins_de_la_presidentielle_et_des_legislatives_de_2018_en_RDC
6. Umar BU, Olaniyi OM, Olatunde AB, Isah AA, Haq AK, et al. (2022) A Bi-Factor Biometric Authentication System for Secure Electronic Voting System. Proceedings of the 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development, NIGERCON 2022. https://ieeexplore.ieee.org/document/9803174/authors#authors.
7. Nagaraj P, Muneeswaran V, Ramu B, Pavan CS, Yoganand E, et al. (2022) Voting System using Facial and FingerPrint Authentication. 2022 International Conference on Data Science, Agents and Artificial Intelligence, ICDSAAI 2022, 1: 1-6.
8. Olumide SA, Olutayo KBE Adekunle S (2020) A Review of Electronic Voting Systems: Strategy for a Novel. International Journal of Information Engineering and Electronic Business 12: 19-29. https://doi.org/10.5815/ijieeb.2020.01.03
9. Awotunde JB (2017) Automated voting system using bimodal identification and verification technique. Annals. Computer Science Series. 15th Tome 1st Fasc. – 2017 AUTOMA, XV.
10. Hazzaa FI, Kadry S, Zein OK (2012) Web-Based Voting System Using Fingerprint: Design and Implementation.

International Journal of Computer Applications in Engineering Sciences 2231-4946.
11. Nadar GR, Paulraj R, Rajesh M, Kiruthika SV, Jasmine I (2017) Smart Voting Machine Based on Finger Prints and Face Recognition. International Journal of Engineering Research & Technology (IJERT).
12. Najam S, Shaikh AZ, Naqvi S (2018) A Novel Hybrid Biometric Electronic Voting System: Integrating Finger Print and Face Recognition. Mehran University Research Journal of Engineering and Technology 37: 59-68.
13. Padmavathi J, Jahnavi M, Hemanth M, Rama Rao SV, Sunitha R (2023) A secured hybrid biometric based e-voting system for election process. Industrial Engineering Journal 52: 1-10.
14. Olumide SA, Olutayo KBE Adekunle S (2020) A Review of Electronic Voting Systems: Strategy for a Novel. International Journal of Information Engineering and Electronic Business 12: 19-29. https://doi.org/10.5815/ijieeb.2020.01.03
15. Mansingh BP, Titus J (2020) A secured biometric voting system using RFID linked with the Aadhar database. IEEE ICACCS 24-30.
16. Carter Center, (2024). Final Report General Elections in the Democratic Republic of the Congo. December.
17. Narayana DS, Sarma GS (2022) a Fair and Secure Electronic Voting System Authentication With Biometric Information 13: 212-217.
18. Awotunde JB (2017) Automated voting system using bimodal identification and verification technique. Annals. Computer Science Series. 15th Tome 1st Fasc. – 2017 AUTOMA, XV.
19. Dahl Robert A, Shapiro Ian, Cheibub Jose Antonio (2003) The Democracy Sourcebook. MIT Press. p. 31. ISBN 978-0-262-54147-3.
20. Democracy | Definition, History, Meaning, Types, Examples, & Facts". Britannica. 16 August 2023. Retrieved 17 August 2023.
21. IFES (2019) Elections in the Democratic Republic of the Congo 2018 General Elections. International Foundation for Electoral Systems. https://www.bbc.com/news/world-africa-11108589
22. Kris Berwouts, Filip Reyntjens (2019) The Democratic Republic of Congo: The Great Electoral Robbery and how and why Kabila got away with it 1-6.
23. Møller, Jørgen; Skaaning, Svend-Erik (2013) Regime Types and Democratic Sequencing. Journal of Democracy 24: 142-155.
24. Ramandeep Kaur, Er Himanshi (2015) Face Recognition Using Principal Component Analysis, IEEE International Advance Computing Conference (IACC) 585-589. https://ieeexplore.ieee.org/document/7154774.
25. Ravi Jk, B Raja, Venugopal Kr (2009) Face Recognition Using Principal Component Analysis “, International Journal of Engineering Science and Technology 1: 1-8.
26. Sudeepthi Komatineni, Gowtham Lingala (2020). Secured E-voting System Using Two-factor Biometric Authentication. Fourth International Conference on Computing Methodologies and Communication, IEEE Xplore Part Number 1-4. https://www.scribd.com/document/518138668/5