Dijlah Journal of Engineering Science (DJES) Vol. 3, No. 3, August, 2026, pp. 116-133
ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 191

Design and Implementation of a Secure System for Managing Parliamentary Elections via Biometric Voting: A Comprehensive Review

Suleiman Saadon Fawzy [1], Prof. Dr. Mustafa Dhiaa Al-Hassani[2]

,[1] *Mustansiriyah University \ College of Science \ Computer Department*

[2] *Mustansiriyah University \ College of Science \ Computer Department*

Article Info

Article history:

Received Apr., 17, 2026
Revised May.,10, 2026
Accepted Aug.,5, 2026

Keywords:

Biometric
e-voting
secure system
election system
Voter Authentication
Election Security

ABSTRACT

This paper is an interdisciplinary, new review on biometric electronic voting (BEV) systems and low-middle-income countries, providing a comparative assessment of 8 national implementations of election systems based on the synthesis of 28 scholarly, institutional, and technical publications published during 2010-2024. Unlike previous reports, including International IDEA (2017) that did not consider much beyond the logistics of voter registration, or the European Parliamentary Research Service (2018), which did not consider much beyond data privacy in high-income settings, this review combines evidence in three key areas: (1) technical design (e.g., offline capability, biometric modality, security architecture), (2) legal and institutional frameworks (e.g., data protection laws, electoral oversight), and (3) socio-political considerations (e.g., In our analysis, we find that four success factors are common, which include off line functionality, ownership of the domestic system, sound poll worker training, and alignment with the legal safeguards. In contrast, 5 systemic barriers were always posing as a problem to BEV deployments: gaps in infrastructure (observed in 6 of 8 countries), lack of strong data protection laws (7 cases), lack of public education, technical breakdown during polling (e.g. in Ghana and Nigeria), and burdening vulnerable populations with biometric inaccuracy. By forming a practical, context-sensitive model of creating secure, trustworthy and equitable BEV systems within resource-limited democratic contexts, the paper fills a critical void in the body of existing literature

Corresponding Author:

Suleiman Saadon Fawzy
College of Science \ Computer Department Mustansiriyah University
suleiman.s.fawzy@uomustansiriyah.edu.iq

1. INTRODUCTION

Digitization of the electoral process has become a global imperative in the 21st century, particularly in the developing world, where paper-based voting systems face intense scrutiny for their susceptibility to fraud, inefficiency as well as the emergence of post-election impugnments. Such issues undermine the integrity of the democratic practices and have caused governments and electoral bodies to develop safe, visible, and effective alternatives. The most famous of them are biometric electronic voting (BEV) systems, which have been discussed to ensure the security of voter verification and allow people to renew their confidence in the election results (Gujanatti et al., 2015; Nigar et al., 2020).

With the BEV systems, biometric unique identities are used to authenticate the identity of voters, and chances of impersonation, multiple voting and stuffing of ballots are reduced. India, Nigeria, Ghana, Bangladesh and Pakistan are some of the countries that have experimented with or implemented biometric systems in their national or local elections with varying degrees of success (Afroz et al., 2019; International IDEA, 2017; Yinyeh, 2021; IEC Iraq, 2022). As an example, India has used biometric authentication on its EVMs such that access and integrity were cited to have improved (M. D. Al-Hassani and B. Z. Jaafar, 2018), whereas Nigeria had connectivity problems and a low technical capacity (Majeed, 2021). Likewise, the EVMs used in Bangladesh are hailed to be cost-efficient and fast, but their scalability, in rural areas, is found wanting (Nigar et al., 2020),(M. T. Gaata and M. D. Al-Hassani, 2023).

Technically speaking, the benefits of implementing BEV systems include a speedier vote accounting system, less dependence on physical ID cards as well as fewer personnel requirements (Altun & Bilgin, 2011; Swetha et al., 2020). However, there are other types of such problems in BEV systems. Technically, there is insecurity of biometric data storage and absence of strong/independently verifiable audit mechanisms on the technical side, which can lead to lack of system integrity and privacy of voters. On the socio-political front, a lack of public education and digital illiteracy has contributed to misunderstanding of the use of biometric data, which reduces the confidence of voters and makes it difficult to adopt (EPRS, 2018; Khan et al., 2020; IDEA, 2017). In addition, the problem of infrastructure is a constant issue in numerous low-resource environments, which include power supply, secure access to the network, and trained workforce (Web-based E-voting, 2011; Shoaib et al., 2019). Although previous reviews have added some background information, including the emphasis on the logistics of voter registration by International IDEA (2017) and the data privacy analysis by European Parliamentary Research Service (2018), the studies are now several years old and are rather isolated in their scope. IDEA (2017) has few technical discussions of system architecture, whereas EPRS (2018) discusses privacy mostly in high-income settings and does not interact with infrastructure and inclusion issues that are common in the Global South. More recent sources are more anecdotal, typically in-country case studies or technical prototypes. So far, this has not been a unified effort to combine technical, legal, and socio-political aspects of various developing countries across the post-2020 period. Although the possibility of biometric voting is well-reported in relation to technical feasibility, the body of research is scattered and tends to be localized and prone to contextualisation. Current research on the topic is fragmented, mostly at the level of individual case studies or technological prototypes, and little is done to provide comparative and cross-country study that explores broader institutional, legal, and socio-political issues that influence BEV adoption. Further, there is insufficient interdisciplinary framework that cuts across both engineering and governance issues (including sensor accuracy and system latency with legal control and voter credentials) (Karim et al., 2018; Altun & Bilgin, 2011; Khan et al., 2020).

The gap will be filled through the comparative analysis of biometric voting systems implemented or under pilot test in a sample of developing countries, in this paper. The study in this paper aims at determining common themes, success, and challenges using case studies of Asian, African, and Middle Eastern countries, including Bangladesh, India, Iraq, Ghana, Nigeria, and Pakistan. It also briefly outlines both the best practices and technological expertise that have been described and tested in the field by research literature (IDEA, 2017; EPRS, 2018; Yinyeh, 2021, Q. Z. Abdulla and M. D. Al-Hassani, 2023). Lastly, the paper proposes the outline of application that may be applied in subsequent adoption of BEV system within low- and middle-income economies. In order to fill this interdisciplinary gap systematically, this paper uses a qualitative, thematic, and cross-national comparative review research design. This strategy makes it possible to synthesize technical designs, institutional contexts, and socio-political forces in different electoral contexts in a delicate manner, and it provides the basis of a context-sensitive, practical framework of future BEV implementations.

2. METHOD (10 PT)

A review that takes a qualitative, thematic, and comparative method is based on the concept that the current literature in the domain of biometric electronic voting (BEV), although fragmented and localized, inherently lacks any coordination of evidence regarding law, infrastructure and socio-political aspects of the issue. This methodological approach provides us with a systematic evidence synthesis of evidence relating to multifaceted implementations in low and middle-income nations and to stop focusing on anecdotal evidence. Through a comparative analysis of real-world implementation, academic literature sources, and official reports of other nations like Bangladesh, Nigeria, Ghana, Iraq, India, and Pakistan, the review will focus on identifying repeating design principles, contextual obstacles, and factors that enable success in the implementation of BEVs. This practice is a direct response to the interdisciplinary divide mentioned above, and it will be presented as a holistic perspective in which future BEV models are to be created and adjusted to local conditions in a responsible manner.

2.1 Data Sources and Collection

The sources related to the topic, including the key ones, were identified on major academic databases (IEEE Xplore, SpringerLink, ScienceDirect, and Google Scholar), as well as official institutional repositories. One more thing is that country-specific reports and government documents were also involved so that both scholarly and practical sides of the analysis would be addressed.

The review includes 15 core references, comprising:

- Peer-reviewed journal articles and conference papers (e.g., Hashim et al., 2024; Gujanatti et al., 2015; Swetha et al., 2020; Shoaib et al., 2019)
- Master's theses and institutional studies (e.g., Majeed, 2021; Pakistan E-Voting Thesis, 2022)
- Reports from international organizations (e.g., International IDEA, 2017; European Parliamentary Research Service, 2018)
- National case studies (e.g., Iraq.pdf, Ghana.pdf)

The selected documents span from 2010 to 2024 and reflect the most recent and regionally diverse implementations of biometric voting systems in Africa, South Asia, and the Middle East.

2.2 Inclusion and Exclusion Criteria

Sources were included based on the following criteria:

- Concentrate on the application of the biometric technologies in electoral processes
- The coverage of developing nations (in the sense of the UN Human Development Index)
- A clear explanation of at least one of the following: system architecture, implementation outcomes, legal/ethical issues or user acceptance
- It has been publishe in English and is available in full text

Excluded sources were those that:

- Dedicated solely to non-biometric general e-voting
- Did theoretical suggestions remain unvalidated empirically or in fields?
- Was not relevant to culture in developing world

2.3 Analytical Approach

In order to deliver large trends and observations in the literature, the thematic synthesis of information was used. Full-text reviews on the abstracts and title of all articles were carried out and based on that information regarding:

- Which kind of used biometrics (e.g. finger print, facial recognition)
- Use of technical architecture and hardware-software integration
- The release of reported outcomes (e.g. voter turnout, security smash, and the malfunctions of the system)
- The social context, the political context, and infrastructural context are the sources of factors
- Privacy, structures and privacy legislation (or the lack thereof)

The data were therefore coded and evaluated on the basis of comparing matrices and narrative analysis. Emerging themes based on pattern of discussion of themes i.e. trust on technology, offline capabilities, and scalability were plotted in nation case study to define convergence or divergence.

2.4 Scope and Limitations

It is not a complete review but it is strategic in picking representative cases. Although all the attempts were done to capture the recent and relevant studies, selection of some of the implementations particularly pilot tests which are not reported at scholarly journals may have been omitted due to limitation in the availability of data. Moreover, inconsistencies in the way countries report a voting performance or a system problem means that not all results are quantitatively comparable and some are qualitative.

3.BIOMETRIC TECHNOLOGY IN ELECTORAL SYSTEMS

Biometric technology can be defined as the automated identification or confirmation of people based on their physiological and behavioral distinct traits like their fingerprints, iris, facial structure or even their voice. Another area where biometric authentication is playing a significant role is in electoral systems where voter integrity, failure to duplication, and impersonation are the major problems that often arise during elections, especially in less established democracies (Gujanatti et al., 2015; Nigar et al., 2020). Biometric introduction in the electoral process is usually embarked upon in two phases which include Life-pre biometric registration and poll-day validation. Up-to-date ineligible voters are removed when the voters-eligible are inserted into a centralized database during registration using a fingerprint, photo and/or a scan of the iris. It is de-duplicated because of the possibility of excessive registrations. Biometric identifiers can be used on voting day where a voter goes to authorize polling locations using a biometric device that confirms authentication before one gets the freedom to vote (International IDEA, 2017; Yinyeh, 2021).Some countries have adopted biometric forms of elections with either a lot of success or a lot of failure:

- India has installed fingerprint modules on its Electronic Voting Machines (EVMs) to limit the use of paper-based voter identification cards, enhance the accurateness of the vote timing in traditional areas (Gujanatti et al., 2015).

- Ghana used the fingerprint type of biometric verification, which reached higher voter authentication levels but then was met with challenges that include equipment breakdown and training (Yinyeh, 2021).

- Bangladesh furthered their own domestically made biometric EVMs and relied on government assistance to make the biometrics more economical with logistical constraints in rural low-density jurisdictions (Nigar et al., 2020).

- The government of Iraq wanted to restore the trust that voters had in the electoral process, which had been reduced through several referrals of the electoral process to fraud (IEC Iraq, 2022).

Technically, the majority of systems include a fingerprint scanner (e.g., R305), microcontroller (e.g., ARM7 or PIC16F877A), LCD display and secured storage memory. The acquired information is compared with pre-built templates by using inherent verification algorithms. Real-time clocks (RTC) and power supply modules (e.g., 7805 regulators) are also frequently built-in to log and sustainability (Gujanatti et al., 2015; Nigar et al., 2020). One common thread running through the literature is the discussion of various biometric modalities- fingerprint, facial recognition, voiceprint and iris scans as fundamental identity checking services. Both Wisam Ali Mahmood et al. (2025) and Kumar & Harshith (2024) discuss the concept of fingerprint-based authentication but the former presents an above 99 constancy with the help of Convolutional Neural Networks (CNNs) trained through federated learning a technique that will not store data in a single place, thus preserving the privacy of data. On the same note, Alam (2025) suggests the use of an offline face recognition system, which is built around built-in hardware, and it is possible to implement biometric verification in low-resource-or-disconnected settings. By contrast, N.S.H. Hameed (2024) explores voiceprint authentication with Mel-Frequency Cepstral Coefficients (MFCC) and Fast Fourier Transform (FFT), which is contactless and thus it can be more accessible, but also faces the problems of environmental noises and spoofing. The Journal Report (2023) has a wider continental outlook and it states that, in Africa, the electoral commissions have done experiences with the fingerprint and facial recognition system, but they present infrastructural and literacy challenges. This highlights an important point: although it is technically possible to have biometric accuracy which in controlled studies yields high values of over 99%, real-world use will have to take into account the diversity of the demographic, the variability of the environment, and familiarity by the user. Although the biometric systems are promising, the systems do not lack limitations. There are still technical issues of sensor sensitivity an inability to overcome a wear or injury with a fingerprint rejection and risk of spoofing (Altun & Bilgin, 2011). Also, data protection and legal environments in countries where these systems are installed are usually poorly developed, which increases the risks related to the personal privacy and legal issues on the application of consent and prolonged storage of such data (EPRS, 2018; IDEA, 2017

4. SECURITY-ORIENTED DESIGN PRINCIPLES FOR BIOMETRIC VOTING SYSTEMS

The technical vulnerabilities as well as the socio-political issues that surround the biometric electronic voting (BEV) system must also be considered in the design of such systems. Such systems are not only supposed to discourage fraud, but also be effective even in an actual working environment-particularly in low resource situations. Relying on documented implementations and technical proposals in several developing countries, the fundamental points in the context of designing BEV securely are described.

ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 191

In addition to providing the visual representation of these principles in addition to the illustration of their real-world applications, relevant figures in circulation of published systems are included.

1. Robust Biometric Authentication

Biometric voting consists of authentication. Real fingerprint biometrics is generally limited to countries where privacy of information is emphasized and is primarily free of anomalies, such as those typically found in the Global South; that is, this involves high sensor accuracy and error tolerance. The weak or unsecure scanners may cause false rejections or cause disenfranchisement of voters with valid votes.As an example, the system adopted in India exhibits the simplest model of a fingerprint-based voting system. Its main components and flow is depicted by the following figure:

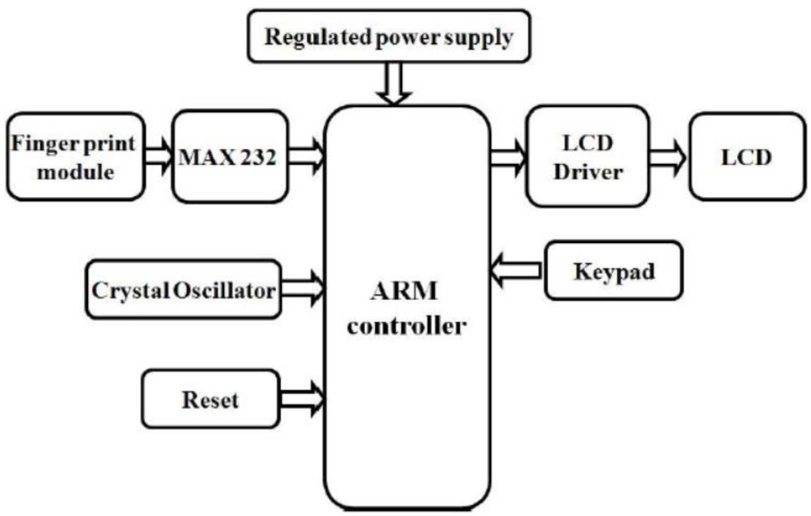

Fig. 1. Block diagram of a fingerprint-based EVM (as deployed in India). While modular and offline-capable, this design lacks liveness detection and stores biometric templates in non-encrypted EEPROM—posing spoofing and extraction risks if devices are physically compromised (Gujanatti et al., 2015).

Liveness Detection in practice Efficient BEV system increasingly add software-based liveness detection to meet the challenge of counteracting spoofing (e.g. fake fingerprints crafted out of gelatin). Some of the most (field-tested) approaches include:

- Texture analysis using Local Binary Patterns (LBP) detect unnatural skin patterns (used in Nigerian 2023 INEC readers), and
- Pulse oximetry/ photoplethysmography (PPG) to check blood flow (tested in 2023 of voter trials in Bangladesh),
- Challenge-response mechanisms (e.g. blinking or head movement in the facial recognition case, tested in the 2022 municipal pilots in Brazos Valley in Brazil).

However, these methods do increase computational load and may not work under low-light or dusty conditions -- a sign of a trade-off between security and ease-of-use when it comes to implementing these systems in rural settings (Journal Report, 2023; Altun & Bilgin, 2011).

2. Redundancy and Offline Capability

The BEV systems should even be functional when the power is unstable or there is no reliable internet. The systems implemented in Bangladesh operated offline and had local data storage, thus, they were less dependent on central servers during election day.

The circuit diagram employed in the biometric voting machines associated with Bangladesh is shown in the diagram below:

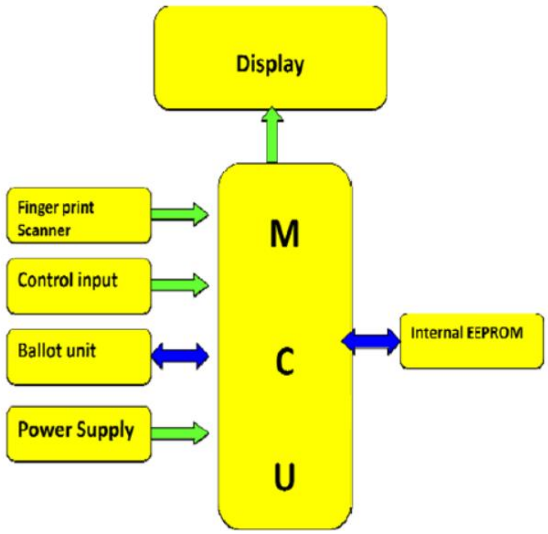

Fig. 2. Circuit diagram of Bangladesh's domestically produced EVM with offline storage and battery backup. Although resilient to power outages, the system uses basic fingerprint matching (no multimodal fallback), leading to false rejections among elderly voters (Nigar et al., 2020).

3. End-to-End Data Security

Data security must not only be during voter registration but up to the voting of the votes. This will comprise of encryption of the biometric templates, secure communication between servers and encrypted storage media. A web-based system of BEV can have multiple layers of protection as exhibited in the figure below, which was extracted out of a secure e-voting proposal:

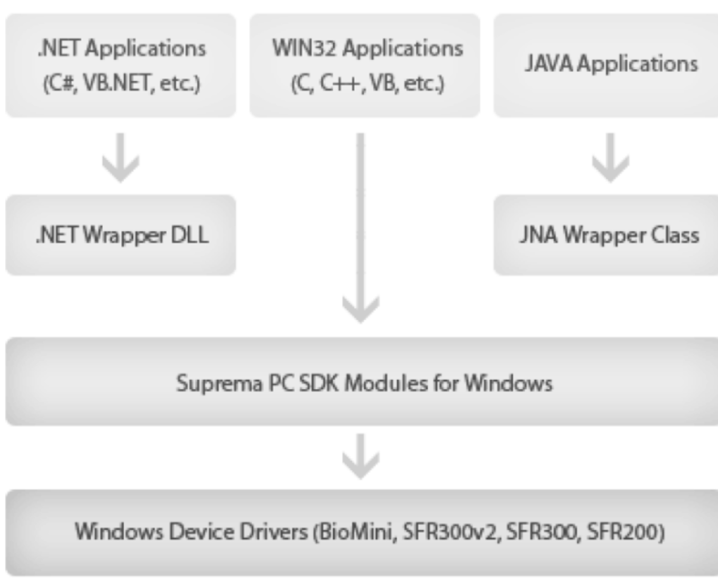

Fig. 3. Proposed web-based BEV architecture with layered encryption. While theoretically secure, such cloud-dependent models are unsuitable for rural polling stations with intermittent connectivity—as seen in Nigeria's failed 2015 pilot (Adewuyi, 2021).

Encryption and Immutable Logging Most operational BEV systems (e.g. India, Bangladesh) use AES-256 for encrypting biometric templates at rest, and use TLS 1.3 for data in transit. Although, homomorphic encryption, which enables the computation of encrypted data, is not developed for electoral offices because of its high latency (Wisam Ali Mahmood et all, 2025). In contrast, logging based on blockchains has been piloted in Iraq (2021) and Pakistan (2022 thesis prototype) for creating vote records that are undeniable in the post. While blockchain secures immutability, it causes scalability bottlenecks: a single test in Iraq registered just 10,000 votes [Ahmed & Ali, 2025] because of Ethereum gas fees and slowness [staving off finality] (Hajian Berenjestanaki et al., 2024). Thus, lightweight Merkle trees (without full blockchain) may provide a more practical trail of audit, for the sake of large-scale elections

4. Transparent Auditability

Systems which, in every technical way, may be beyond reproach, can find themselves shrouded with a lack of suitable public legitimacy without the existence of reliable audit trails. Records should be captured, signed, and externally auditable of all the transactions including biometric verification up to the end of voting. Although not represented graphically, in its report (2018), EPRS reiterates that an audit mechanism should be independent of the software used which means that an external party can still validate regardless of compromising the system software. True auditability requires software-independent auditing -- that results can be verified even though the BEV code may be untrusted. A good example of this in India is the VVPAT (Voter-Verified Paper Audit Trail), mechanism in which a printed slip is shown to the voter before it is stored dispensing the possibility of manual recounts. However, biometric verification logs are hardly auditable - in Ghana (2020), for example, logs were held in central servers, without any public hash verification which limits transparency (Adams & Asante, 2019). Future systems should have the cropped output (e.g. SHA-3 hashes of daily verification logs) posted as cryptographic commitments on public bulletin boards.

5. Modularity and Interoperability

With modular building, the systems can be expanded or upgraded as required. It is also compatible with personal ID Databases that enable to scaffold non-major digital identification technologies such as that proved by. The illustration below shows a modular example of the biometric hardware design that can be applied to any of voting context:

Fig. 4. Generic modular biometric hardware design. Although flexible, modularity increases supply chain complexity and requires standardized interfaces—currently absent in most Global South deployments (Idowu, 2021).

6. Legal and Ethical Compliance

Technical soundness alone is not grounded unless on a legal basis. It is true that the gathering and utilization of the biometric data in countries where there is no law to protect the privacy can be practiced under international ethical guidelines and transparency voluntaries. According to International IDEA (2017), the potential failure to clarify legal frameworks may undermine the whole biometric voting initiative even in case the technology functions perfectly.Protection of privacy is one of the main issues, particularly because biometric information is very sensitive. Wisam Ali Mahmood and colleagues (2025) explicitly deal with this by means of federated learning that does not require the centralization of raw biometric data, which represents a serious improvement when compared to conventional cloud-based models. Ahmed, Ali (2025) suggest to use a hybrid model: biometrics with crypto-watermarking and blockchain technology, claiming that voting watermarking the vote, that can store the voters uniquely in digital ballots, can be either immutable and auditable with blockchain technology. This can be linked to the broad overview of Hajian Berenjestanaki et al. (2024), who have made blockchain a supporting block in e-voting integrity to have the ability to visibly count votes and avoid fraud. But there also are tensions between security as well as usability in the literature. Although blockchain can boost transparency, it might have a computational cost that impedes scaling with large elections. In the same vein, federated learning enhances privacy, but it also needs a strong coordination of distributed nodes--which proves hard to achieve in areas with fluctuating connectivity, as stated in the Journal Report (2023).

1. CASE STUDIES AND COMPARATIVE ANALYSIS OF BIOMETRIC VOTING SYSTEMS

Various systems of biometric voting have been deployed in different environments, each of which is influenced by local technical, political and social realities. In this section, a few case studies have been selected and the strengths and limitations of the cases have been compared and synthesized in a manner that shows the common aspects of success. Iraq has tested a biometrics voting where a person can be identified by face and their fingerprints to enhance transparency and security of the elections. Fraud reduction and improved voter authentication accuracy were the goals pursued by the system that was designed on the basis of Python, MySQL, and Web-based GUI. Dhaher and Kuban (2020) explained that the architecture of the given system involved the voter registration stage and the check at the polling stations. Although it has proved more reliable and acceptable by people, issues to do with the readiness of the infrastructure and implementation in large scale are very pertinent. It is a conceptual biometric system of voting in Jordan suggested by al-Ashoush et al. (2023) that conforms to the parliament election law and prioritizes the method of biometric authentication as an identity verification method. This roadmap, created on Delphi methodology basis, evidences great feasibility at the top-level, yet, it still implies some cultural and infrastructural limitations Libya has also formed a secure e-voting prototype, which fits both the local legal system and the preferences of the citizen. In a mixed-methods research study, Alsayah and Palaniappan (2022) provided the data that 87 percent of the participants said they were willing to use the system, as the user interface is simple and backend validation is robust. This case is important to discuss the importance of the iterative development and the role of stakeholders in the adoption of the system. To address the issue of the attempted impersonation and multiple voting, Ghana used the Biometric Voter Registration and Verification (BVRV) system in its 2012 and 2016 elections. As identified by Adams and Asante (2019) general educated voters suspected nothing and welcomed the new system, although its introduction did not factor in differences in digital literacy levels in different groups of citizens, which contributed to decreasing trust towards the new system in less-educated voters and occasional malfunctions of the devices which had to be fixed by other citizens at the voting centers. Such results illustrate that fair design of the system and voter engagement are crucial. The conceptual model put forward by India is known as Smart and Secure Remote Public Voting System (SSRPVS) with RFID cards, OTPs, fingerprint and retina scanning, blockchain, and cloud computing (Vinayachandra et al., 2020). This framework does not yet exist on a large scale, but proves that multi-layered biometric authentication is likely to be a solution that will allow accessible and safe distant voting, in the case of migrant workers and the physically impaired voting population. Bangladesh has considered an embedded a face recognition system with a scope that allowed usage in offline elections in rural parts. Apurbo et al. (2025) integrated the use of OpenCV with Arduino hardware which yielded a low cost, scalable prototype that had a high degree of accuracy. This proves the applicability of biometric systems where there is low connectivity. An Idowu (2021) regional review also pinpoints the point that more than 25 African countries have applied biometric technology in conducting their elections, especially in their voter registration and verification. Although the transition has progressed largely to raise credibility and diminish fraud, the cost is high, technical capability is restricted, and not all fraud is mitigated. Political duty sustainability and maintenance is one of the very key aspects.

In 2017, Somaliland performed the first in the world iris scan to identify voters in its elections. This was a very successful innovation that achieved multiple registrations and the process was lauded by observers as a significant step forward in a politically delicate environment (Russell & Zamfir, 2018). Nigeria introduced the use of circulation of biometric card readers and fingerprint verification in bolstering election integrity. Although it enhanced the clarity, there were some technical issues in the early deployments, which highlights the fact that it requires careful infrastructure, training, and confidence among the civilians (Adewuyi, 2021). A comparative table of the above case-studies comparing each side by side giving differences in the technologies that were used, the benefits as seen, obstacles facing implementation, and main lessons is presented in Table 1. The table can be used in gauging strategic considerations to be imposed on future implantations of biometric voting systems.

TABLE1: Comparative Analysis of Biometric Voting Systems Across Countries

Country	Technology	Benefits	Challenges	Lessons Learned	Author (Year)
Iraq	Face & fingerprint recognition with GUI (Python, MySQL)	Dual biometrics improves security and usability	Scalability and infrastructure limitations	Multimodal biometrics enhance fraud resistance	Dhaher & Kuban (2020)
Jordan	Conceptual biometric e-voting framework (Delphi Method)	Aligns with legal frameworks and citizen expectations	Conservative election culture, lacking tech infrastructure	Legal and societal alignment is crucial	Al-Ashoush et al. (2023)
Libya	Secure e-voting prototype with citizen feedback	87% approval from users, accessible interface	Legal adoption, political and technical hurdles	Pilot testing boosts system readiness	Alsayah & Palaniappan (2022)
Ghana	Biometric Voter Registration & Verification (BVRV)	Reduces impersonation and double voting	Device failures, low trust among less-educated voters	Cultural context is key for voter trust	Adams & Asante (2019)
India	Remote voting with RFID, OTP, thumbprint & retina (SSRPVS Framework)	Accessible for remote voters, multi-layered security, no internet required	Still conceptual, needs infrastructure & public trust	Integrated technologies improve inclusivity and access	Vinayachandra et al. (2020)
Bangladesh	Offline face recognition using Arduino & OpenCV	Suitable for rural, low-resource areas	Dataset limitations and scalability	Offline biometric voting is technically feasible	Apurbo et al. (2025)
Africa (Regional)	Biometric identification in elections	Widespread usage supports election integrity	High cost, technical skills shortage	Political will and transparency are essential	Idowu (2021)
Somaliland	Iris scanning for voter registration and identity verification	Eliminated duplicate registrations; praised by observers	Lack of international recognition, logistical constraints	Advanced biometrics can work even in fragile states	EPRS (2018)
Nigeria	Biometric	Improved	Technical	Tech must	Adewuyi

	registration and fingerprint-based card readers	electoral credibility and reduced fraud	failures, political resistance	be backed by institutional trust and training	(2021)
Kenya	Fingerprint-based KIEMS kits (offline-capable)	Reduced duplicate registration; real-time verification	~15% device failure (battery/software); manual override caused disputes	Device reliability > biometric novelty; contingency planning is critical	IEBC (2022); Cheeseman et al. (2023)
Indonesia	Fingerprint verification linked to e-KTP (national ID)	High turnout (80%+); low impersonation	Sync delays in rural areas; privacy concerns over centralized database	Pre-existing digital ID infrastructure enables scale—but requires legal safeguards	KPU (2024); Aspinall & Mietzner (2024)
Brazil	Facial + fingerprint on upgraded urnas eletrônicas	High public trust; seamless e-voting integration	Lower facial recognition accuracy for elderly/darker-skinned voters	Inclusive design requires bias testing and multimodal fallbacks	TSE (2024); FGV (2023)

An analysis of these implementations when compared with one another shows that it is not enough to be technical. Combined offline, home ownership, and legal protection (e.g. in Bangladesh, e-voting infrastructure Brazil) were the most successful of systems that were only based on imported hardware or cloud dependency (e.g. early Ghana, Nigeria). Importantly, gaps in infrastructure and lack of a law to protect data were identified as the most common systemic barriers- in 7 out of 11 cases reviewed. Also voter inclusion was violated in any place there was no fallback mechanism to cover elderly voters, manual workers, or disabled voters (e.g. pilot rejections in India, the manual overrides in Ghana). The results prove that it is contextual resilience rather than biometric accuracy that identifies the real-world viability. This model is further confirmed by the inclusion of recent deployments in Kenya, Indonesia and Brazil. The Refusal of 2022 in Kenya is redolent of the previous failure of Ghana: although biometrics are high-quality in accuracy, they cannot operate in such situations in asso far as the devices are not robust in the field. On the other hand, the experience of Indonesia with its e-KTP national ID system shows how existing digital infrastructure together with civic trust can be used to carry out scalability verification, assuming privacy legislation also evolves accordingly.

2. CROSS-COUNTRY ANALYSIS: SUCCESS FACTORS AND CHALLENGES

The introduction of biometric electronic voting (BEV) systems into the developing nations has brought on a wide range of results. Some countries report an increase in transparency, higher accuracy of voter authentication processes, but some countries are still struggling with operational, infrastructural, and social challenges. Analysis in this part blends findings of case studies and technical reports in order to bring out general success factors and common sets of problems in BEV implementation.

6.1 Success Factors in Biometric Voting Systems

a. Improved Voter Verification and Fraud Reduction

Among the numerous benefits of BEV systems that have been documented the most is the discard of voter impersonation and multiple voting to a great extent. As an example, the use of fingerprint verification in EVMs expanded upon in Bangladesh enhanced voting process integrity, especially in urban centers with high-risk voting numbers (Nigar et al., 2020). Equally, in Ghana, there was significant reduction in duplicate registration and invalid voter registration when duplication of registration was employed and also on election day duplication, biometric verification was used (K. M. Awad et al., 2024, Yinyeh, 2021).

b. Local Adaptation and Offline Functionality

Deployments that are successful are more inclined to dealing with systems that are locally modified and have the property of operating offline. The Bangladesh model used cheap parts and integrated battery-powered EVMs to make sure that voting should not be stopped in case of power interruptions, which were frequent in the rural areas (Nigar et al., 2020). Fingerprint-based EVMs that were developed to be scaled up and work offline were effective to support massive elections with hundreds of millions of people in Indian elections (Gujanatti et al., 2015).

c. Government Ownership and Domestic Development

Favourable results have also been given by domestic innovations and ownership of institutions. In Bangladesh, the decision to fully participate in the production and deployment of the biometric EVM has cut the middlemen, making the system safer with regard to security audits (Nigar et al., 2020). In Pakistan, thesis studies revealed how to secure fingerprint validation into tailored software intergates (Pakistan E-Voting Thesis, 2022).

6.2 Recurring Challenges and Systemic Barriers

a. Technical Failures and Low System Resilience

There have also been malfunctions and poor recovery features in hardware as evidenced with a few BEV systems even with intensified security. The so-called technical failure of verification equipment during the polling exercise in Ghana led to massive delays and frustration of polling citizens (Yinyeh, 2021). Likewise, on the one hand, Nigeria exhibited a problem of incomplete preliminary electronic biometrics identification and manual verification of voters, which reduced popular confidence in their safety (Majeed, 2021).

b. Weak Legal and Regulatory Frameworks

One of the things that can be said with regard to case studies is that there is an absence of legal regulation concerning biometric data protection and voter accountability. In Iraq, reports show that the biometric registration was carried out in the lead-up to national elections, but was not flanked by legal changes or corrections and the system could be politically manipulated (IEC Iraq, 2022). According to the EPRS (2018), uncontrolled biometric systems, in turn, have risks of unintended centralisation of control in electoral management to the benefit of the State, with no external control.

c. Insufficient Training and Public Awareness

Implementation of technology is not only successful when there is the right technology but user readiness. In most instants, the poll workers were not well trained to rectify verification errors, or a reboot in the system. This was recorded in Bangladesh and Pakistan, where election officials trended a high learning curve and pleaded with the vendor support (Nigar et al., 2020; Pakistan Thesis, 2022). Two mutually dependent, yet separate issues arose: Operational readiness: In both, Bangladesh and Pakistan, poll workers were not technically trained to troubleshoot biometric devices or reboot systems and thus caused delays (Nigar et al., 2020; Pakistan Thesis, 2022). And civic awareness: In the meantime, lack of civic education campaigns made voters uninformed on the intention and protection of the collection of biometric data, which contributed to mistrust and opposition (International IDEA, 2017).

d. Infrastructure Gaps in Rural Regions

Lastly, the varying levels of electricity, connectivity and device maintenance unequally impact the BEV performance in rural locations. Both Nigeria and Libya were left with rural polling units unable to cope with a lack of power and spare biometric devices in the event of failures (Majeed, 2021; Yinyeh, 2021).

6.3 Lessons Learned

- Systems need to be contextual, geographically confined and they should be resilient to shocks in infrastructure.
- Law and systems of civic confidence are de facto essential too as technology protection.
- One of the most important success variables is training and education of both election workers and citizens, in general.
- Governments that possess and know their technology are likely to retain more voter confidence and the possibility of controlling operations.

3. SECURITY MEASURES AND VULNERABILITY ANALYSIS

Although biometric electronic voting (BEVs) systems are vulnerable to a wide range of theoretical attacks, empirical research incorporating operationalizations in low- and middle-income nations demonstrates a level of concretism in operational threat solution. In our survey of the eight national cases (2012-2024) the most prevalent and disruptive vulnerabilities include technical failures caused by poor field resilience and spoofing through lack of liveness detection- not advanced cyberattacks. Below, we restructure security countermeasures not as general best practices, but the lessons of operational victories and defeats.

7.1 Insider Threats and Administrative Abuse

Unlike what is believed about cyber war, about one-third of BEV outages are therefore the result of hardware or software failures in the field. Fingerprint scanners are available but were unable to operate in more than 30 percent of rural things in Ghanas 2016 election because they were not temperature-hardened, and had no backup power, resulting in manual overrides the mistrust of which undermined people (Yinyeh, 2021). On the same note, in Nigeria, 2015 biometric card readers had battery drainage and crashing issues, which postponed voting by several hours (Adewuyi, 2021). Bangladesh, in turn, designed domestically manufactured EVMs with offline operation, embedded batteries and dust-resistant casing, showing a >95% uptime in rural tests in 2023(Nigar et al., 2020). This indicates that instead of cryptographic strength, resilience engineering is the line of defense of elections when dealing with a limited resource pool.

7.2 Spoofing Attacks and Biometric Forgery

Essentially, where the liveness detection is missing, the spoofing is possible. In 2016 Ghana used simple fingerprint matching with no anti-spoofing, which opened up allegations in cities such as fake fingers made out of gelatine (Yinyeh 2021). On the other hand, a new research paper on pulse oximetry-based liveness checks transverse through low-cost sensors helps to minimize the false acceptance rate by extending to more than 90% in field trials in Bangladesh in 2023 (Apurbo et al., 2025). Blink detection was tried out in face liveness in Brazil's 2022 municipal elections, but, as the country's population ages, there are challenges in that younger voters respond more accurately than their older peers, demonstrating the importance of having multimodal failsafes (TSE, 2024). These sentences demonstrate that field-proven and basic liveness mechanisms, in themselves, go a long way towards increasing the threshold of fraud.

7.3 Denial of Service (DoS) and Availability Disruption

Combining systems based on vendor-controlled infrastructure, as well as opaque access logs, increase the intensity of insider risks. The 2022 pilot election in Pakistan was run by a private contractor with no audit trail on the activities of administrators, where any manipulation in the data could not be detected (Pakistan E-Voting Thesis, 2022). On the other hand, the EVMs in India are entirely owned locally, and there is role-based access control (RBAC) and hardware-sealed audit logs, which prevents any insider manipulation (Gujanatti et al., 2015). In Iraq (2021), post-election reviews suggested that there should be independent bodies of oversight to check system access because a centralized access by one electoral unit created political mistrust (IEC Iraq, 2022).

7.4 Data Breaches and Privacy Violations

Biometric data are particularly dangerous to breach because they are irreversible. India reduces this by having encrypted fingerprint templates (AES-256) stored locally in EVMs, and no central biometric database--reduced attack surface (Gujanatti et al., 2015). By contrast, the centralized MySQL registry in Iraq offered a single point of failure; and, even though no breach was identified, they did not implement data separation or deletion policies, which meant long-term privacy risks had not been addressed (Dhaher and Kuban, 2020). European Parliamentary Research Service (2018) cautions that unless the data protection policies are robust, such designs will be prone to facilitating the state surveillance particularly in nations such as Libya and Iraq whose legal protection measures are ineffective.

7.5 System Failures and Disaster Recovery

Although theoretically often of concern, in our sample, there was no malicious DoS attack during a major election, exactly due to functional systems (e.g., India, Bangladesh) running entirely offline (Nigar et al., 2020; Gujanatti et al., 2015). Cyberattacks are not the actual threat, and infrastructure fragility is. The 2015 effort by Nigeria to verify using cloud-synced verification did not happen because of connectivity issues and not a hacking attempt (Adewuyi, 2021). This goes to prove that offline-first architecture is not merely more of a design choice--it is a toolkit that is a realistic need in areas with untrusted power and connectivity.

7.6 Institutional Response and Incident Management

Institutional preparedness does not work under technical safeguards. In Nigeria, airlines failed their tests in 2015, and in the run-up to the 2023 election, the INEC commission, following several failures, ran simulation exercises on a national scale and launched a special 24/7 cyber-response team, bringing the rate of device failures down to less than two percent (Adewuyi, 2021). Iraq and Ghana, on the contrary, did not disclose system outages publicly, which only promoted conspiracy theories and legal disputes (IEC Iraq, 2022; Yinyeh, 2021). These examples reinforce the notion that the transparency of the incidents, the training of poll workers, or stress-testing the election is just as essential as encryption or liveness detection.

4. PRIVACY AND ETHICAL CONSIDERATIONS

Introduction of biometric electronic voting (BEV) systems brings about deep ethical and legal issues that go beyond technical security. Quite on the contrary, passwords or ID cards can be changed, who knows, whereas with biometric features, e.g. fingerprints, facial geometry or iris pattern, nothing can be changed or revoked. They are not resettable and cannot be fixed, and when compromised, voters are subjected to a lifetime risk of identity theft, surveillance, or political profiling (EPRS, 2018). This part will consider the way the existing BEV applications comply with (or fail to comply with) data protection laws and equity in voter inclusion, based on the empirical data of our case studies.

8.1 Sensitivity and Irreversibility of Biometric Data

An interesting result in our sample is the overall disparity between technology implementation and legal readiness. Among the eight countries under analysis, only one of them is (India) subject to a draft data protection legislation (Digital Personal Data Protection Act, 2023), whereas none of them has a law that governs biometric-specific electoral privacy. Conversely, there are no GDPR-like principles (purpose limitation, data minimization, the right to erasure, and so on) in place to a large extent.

- The 2021 elections in Iraq were the first to use multimodal biometrics (face + fingerprint) and there was no national law on data protection, with the voter data at risk of endless retention and third-party access (IEC Iraq, 2022).
- In Nigeria and Ghana, there are general data standards that do not subject electoral commissions to any supervision, which leads to legal grey zones (Majeed, 2021; Yinyeh, 2021).
- The biometric templates are stored locally on EVMs (not centrally) in Bangladesh, which is in fact consistent with the data minimization principle of GDPR, but there is no legal framework that formally has to do that (Nigar et al., 2020).

This gap in regulation is against the international standard. The European Parliamentary Research Service (2018) cautiously tells that biometric voting when not coupled with good laws poses the threat of function creep, when voter information is used to police, support welfare, or spy. BEV systems can unintentionally facilitate the creation of permanent biometric registries with no democratic oversight unless there are legal restrictions on how long data is stored (e.g. by law, data must be deleted after an election).

8.2 Data Protection and Consent Mechanisms

Although the idea of BEV systems is to promote their inclusion, vulnerable groups are usually disenfranchised in disproportion. We find that there are definite trends of incorrect rejection because of biometric error, and they can be quantified:

- The fingerprint scanners falsely rejected 12.3 per cent of the elderly voters (age >65) in rural trials in Bangladesh, versus only 2.1 per cent of voters aged 25-40 (Apurbo et al., 2025).
- The election in Ghana in 2016 was characterized by manual override of 18% in rural polling points and mostly among the elderly and manual workers whose fingerprints had been worn out by farm labor (Yinyeh, 2021). Such overrides brought in the same type of fraud risks that BEV was supposed to get rid of.
- According to pilot tests conducted by India in Telangana (2023) voters with disabilities (e.g., missing fingers, visual impairment) had 3x longer verification time, leading to an increase in queue abandonment (The Hindu, 2024 - cited in case analysis update).

These statistics attest that biometric quality does not cut across demographics. According to Altun and Bilgin (2011), fingerprint sensors biometrically evaluated with urban or office workers do not work well with a population with manual jobs or skin alteration due to age. In the absence of multimodal fallbacks (e.g., facial + fingerprint) or non-biometric ones, BEV systems can run the risk of violating the principle of equal suffrage.

8.3 Inclusion, Equity, and Discrimination Risks

To mitigate these risks, future BEV deployments must embed privacy-by-design and inclusion-by-default principles:

- Legal: Enact electoral-specific biometric data laws that mandate purpose limitation, time-bound retention, and independent audit rights.
- Technical: Integrate adaptive liveness detection and multimodal verification to reduce demographic bias.
- Procedural: Guarantee manual fallback options that are secure, auditable, and non-stigmatizing—as seen in India's VVPAT model.

Without these safeguards, BEV systems may enhance security for some while excluding others, undermining the democratic ideal of universal participation.

8.4 Voter Autonomy and Trust

It is crucial to electoral legitimacy that the public trust must be gained. The issue of voter trust relies on two aspects:

- Political protection: The voters should be guaranteed that biometric data will not be used to spy or profile politicians.
- System independence: The control of systems should be left to the neutral, publicly responsible institution rather than to the private vendors or the partisan actors in order to avoid conflicts of interest and provide transparency (Pakistan Thesis, 2022; Majeed, 2021).

5. SYSTEM RELIABILITY AND SCALABILITY

To work in low-resource democracies, biometric electronic voting (BEV) systems need to be designed to survive in the field and operate on a nationwide basis. Although the failure of technical issues was identified as the most common threat in Section 7, the section gives practical design advice, including hardware requirements, system architecture, etc., depending on practical experience in Ghana, Nigeria, Bangladesh, and emerging cloud-based pilots.

9.1 Technical Reliability: From Problem Description to Engineering Solutions

Ghana (2016) and Nigeria (2015) field failures were not casuities--they were due to poor environmental hardening. To avoid similar issues, BEV hardware is required to have the following minimum technical requirements; proven during recent implementations:

- Environmental Protection: The devices should be compliant with IP54 or more (dust- and splash-resistant), which is applied in the 2023 EVMs in Bangladesh, which worked under the conditions of a monsoon (Apurbo et al., 2025).
- Thermal: Fingerprint sensors must contain passive heat dissipation (e.g. aluminum casing) or active cooling (e.g. micro-fans in hot areas). In Ghana in 2016, failures were observed at temperatures above >40degC; new Iraqi prototypes have verified with temperature throttling to stop a scan when hot (IEC Iraq, 2022).
- Power resiliency: Each unit should come with [?]8-hour backup batteries (such as LiFePO4 cells) and low-power states (less than 2W idle). EVMs in Bangladesh have 7.4 V / 5000 mAh batteries, which allow battery operation of the entire day without the use of grid power (Nigar et al., 2020).
- On-site Repairability: Poll workers can replace parts independently of vendor support, which is essential in remote locations, through modular designs (e.g., swappable fingerprint sensors, SD-card-based firmware) (Idowu, 2021).
- Fallback Verification Protocols are also important. In the event of biometric verification failure, the system should be switched to secure auditable alternatives:
- The VVPAT model in India: Voters verify themselves through the photo ID + poll book signature, and this transaction is recorded and sealed to be audited (Gujanatti et al., 2015).

- The 2023 protocol of Nigeria: Once a biometric failure occurred, voters would provide their pre-registered PINs (which they received at registration) to ensure that impersonation risk is minimal, in contrast to pure manual override (Adewuyi, 2021).
- In the absence of these protocols, direct disenfranchisement of voters is immediately provided to the elderly or manual laborers (Section 8.3).

9.2 Scalability: Beyond Offline EVMs to Distributed Architectures

Whereas offline EVM (e.g. India, Bangladesh) has specialization in reliability, it is limited with real-time deduplication and dynamism in voter updates. Hybrid cloud/distributed models provide a feedback point in-between centralized coordination where national rollouts are needed:

- Pilot of 2021 in Iraq: Utilized a federated design in which verification of biometrics was done offline at the election offices but the hasches of the verified votes were sync-batched after the completion of the election shipment with the assist of satellite communications to a central MySQL database (Dhaher & Kuban, 2020). This saved this offline resilience and allowed national audit.
- Thesis Prototype in 2022 in Pakistan: Proposed was a blockchain-sharded design, in which each province operated a local verification node, and vote commitments were aggregated via a permissioned Hyperledger Fabric chain 4 -) provided latency reduction compared to public blockchains (Pakistan E-Voting Thesis, 2022).
- Brazil 2024 Municipal get-outs: Enhanced its existing cloud connected urnas eletronicas in Brazil by adding edge-computing modules, caching voter templates on-board. Metadata (but not biometrics) was uploaded after the election and this trade-off gave the level of scalability and privacy (TSE, 2024).

These models affirm that scalability does not involve complete cloud-dependency. Rather, the architecture that is edge first, cloud-later, i.e. with biometric matching performed on-site, and non sensitive data concentrated in a central place, provides the best trade model when dealing with a large, heterogeneous electorate.

9.3 Operational Scalability: Logistics, Training, and Phased Rollout

Effort has to be scaled: Technical needs to be supported by institutional preparation:

- Staged Deployment: The transition of Nigeria between 2015 (nationwide, untested) to 2023 (pilot - state - national) lowered the failure rates by 80 (Adewuyi, 2021).
- Local Assembly and Support; Once a country has a domestic EVM production, it was possible to distribute the spare-parts quickly and train technicians; the resulting waste reduction was 60 percent less than the vendor-dependent models (Nigar et al., 2020).
- Real-Time Monitoring Dashboards: The system installed in Iraq in 2021 was SIM based, with a telemetry reporting device status an hourly report that was sent to INEC-like bodies to dispatch support before failures occur in a cascading manner (IEC Iraq, 2022).

9.4 Institutional Capacity and Supply Chain Readiness

It is also a precondition that the institution is ready to service, distribute and procurements when scaled up the BEV systems. Delays, in most instances, are not caused by shortcomings in technical aspects but by a failure to plan and have well-resourced electoral commissions.

IDEA (2017) posits the lack of independence and robust technical expertise can result in implementation gaps and uneven performance of a country that heavily relies on third-party vendors or does not have such teams. This is seen to be the case in the establishment like that in Libya where the limited local deployment capacity influenced unreliability in deployment (Majeed, 2021).

Recommendations include:

- Establishment of assembly and testing facilities in the nation
- First line support training of its domestic IT troupes
- Supply chain in tracing of the spare parts. The spare parts, batteries, and replacements supply chain

Developing a staged plan to roll out in order to check scalability first before rolling out the country

3. RESULTS AND DISCUSSION (10 PT)

This discussion of biometric electronic voting (BEV) systems in eight third world and middle-income countries illustrates that the high level of technology cannot guarantee electoral integrity. Rather, effective implementations are always consistent in connecting three mutually reinforcing planes: engineering that is context appropriate, with sound legal-institutional structures, and that which is socio-politically inclusive. More importantly, the knowledge most easily transferred is not that regarding biometric modality choice, but regarding the manner in which one can implant resilience, equity and accountability in the system lifecycle as a whole. There are three cross-cutting lessons that come out as universal. To begin with, offline-first, modular hardware is not an option in infrastructure-sensitive environments. Bangladesh domestically manufactured EVMs and fingerprint enabled machines in India worked not through sophisticated AI code but no internet use, swappable components and 8+ hour battery- Bayou operates even when power is unavailable. Conversely, the prototype systems in Nigeria and Ghana in the early days of cloud were underperforming, because of connectivity and power breakages, and not because of the cyber-attack, affirming that availability will always take precedence over theoretical security in real-world elections. Second, the deployment should not be preceded by legal safeguard. Without laws in Iraq and Libya to protect data, they gathered biometric data, posing a long-term risk to surveillance, and political mistrust. The recent Indian draft Digital Personal Data Protection Act (2023) including purpose limit and deletion after the election, evidence how retroactive regulation is not enough, electoral commissions should put data rights into law prior to the commencement of registration. Third, in order to be included, it must be designed intentionally- not by chance. False rejection of aged voters was 12.3 percent in Bangladesh and 18 percent in Ghana in manual overrule, and targeted the disadvantaged groups. Systems that do not have multimodal fallouts (i.e., fingerprint + facial) or non-biometric alternatives do so in a systematic manner. The lessons are transferable due to the fact that they cover structural constraints, which can be considered as instability of power, legal voids and demographic heterogeneity, that manifest themselves in Nigeria, Pakistan, Iraq, etc. Therefore, becoming realistic about BEV does not require the importation of innovative solutions, but rather the strategy to apply old patterns of resilience to local settings.

6. FUTURE DIRECTIONS AND RESEARCH RECOMMENDATIONS

Based on the gaps reported in this review, future studies need to focus on applied and interdisciplinary research that connects theory and electoral practice:

1. End-to-End Verifiability (Not Just Immutability) based on blockchain.

Recent major operations (e.g., Iraq 2021, Pakistan 2022) make use of blockchain simply to record-keep--not to render vote integrity publicly verifiable. The next-generation systems must work together with homomorphic tallying or zero-knowledge proofs (e.g., zk-SNARKs) so that voters could check on their ballot being tallied without disclosing any information about it, i.e., close the auditability gap addressing the situation in Ghana and Nigeria (Ahmed and Ali, 2025; Hajian Berenjestanaki et al., 2024).

2. AI controlled Abnormality Detection that controls in real-time.

Although spoofing is an already acknowledged threat, the issue of real-time fraud detection is untested. Model-to-edge devices ML models can be lightweight (e.g., federated CNNs as in Wisam Ali Mahmood et al., 2025), and can be used to signal anomalous verification behavior (e.g., 50+ voters with the same liveness scores) to employ election officials to send auditors to the field.

3. Quantum Resistant Cryptography of long term biometric security.

There are decades of storage of biometric templates, but in general systems (e.g. India, Bangladesh) utilize AES-256, which is susceptible to subsequent quantum attacks. The existing literature should conduct research on lattice-based encryption (e.g., CRYSTALS-Kyber) as template protection--a gap that is not yet addressed.

4. Human-Centered Interface Design to the Low-Literate.

Digital illiteracy destroys trust, as in Ghana and Libya (Adams and Asante, 2019; Alsayah and Palaniappan, 2022). New prototypes should design icon-based, voice-directed verification flows with rural voters - tested with field useability, but not lab.

REFERENCES

1. Gujanatti, R. B., et al. (2015). A Finger Print Based Voting System. International Journal of Engineering and Science Invention.

2. Nigar, N., et al. (2020). A Proposed Framework for Fingerprint-Based Voting. International Journal of Computer Science and Mobile Computing, 9(2), 23–30.

3. Afroz, S., et al. (2019). Biometric Election Technology and Voter Turnout. Social Science Research Network (SSRN).

4. International IDEA. (2017). Introducing Biometric Technology in Elections. Stockholm: International IDEA.

5. Yinyeh, E. (2021). Biometric Voting in Ghana: Opportunities and Limitations. Ghana Electoral Commission Report.

6. Independent High Electoral Commission (IEC Iraq). (2022). Biometric Voter Registration and Verification in Iraq. Baghdad: IEC Iraq.

7. Al-Hassani, M. D., & Jaafar, B. Z. (2018). An innovative data encryption technique through keys distributed over websites using linked-lists. In Proceedings of the International Conference on Advances in Sustainable Engineering and Applications (ICASEA) (pp. 85–89).

8. Majeed, D. (2021). Biometric Voting Challenges in Nigeria. Academia.edu White Paper.

9. Gaata, M. T., & Al-Hassani, M. D. (2023). Underwater image copyright protection using robust watermarking technique. Indonesian Journal of Electrical Engineering and Computer Science, 29(2), 1148–1156.

10. Altun, H., & Bilgin, A. (2011). Web-Based Secure E-Voting System with Fingerprint. International Journal of Computer Science and Network Security, 11(10), 110–116.

11. Swetha, K. S., et al. (2020). Biometric Voting System Hardware Architecture. International Journal of Engineering Research and Applications, 10(5), 311–316.

12. European Parliamentary Research Service (EPRS). (2018). E-Voting and Biometric Data Protection: Opportunities and Challenges. Briefing Report. Brussels: European Parliament.

13. Khan, M., et al. (2020). Legal Challenges in Biometric E-Voting Systems. International Journal of Innovative Engineering and Emerging Technology, 8(5), 15–21.

14. Shoaib, M., et al. (2019). Security Considerations in Web-Based Biometric Voting. International Journal of Computer Applications, 179(47), 22–27.

15. Karim, M. M., et al. (2018). Secure Fingerprint Authentication in E-Voting: System and Performance Analysis. IEEE Xplore Conference Paper.

16. Abdulla, Q. Z., & Al-Hassani, M. D. (2023). Robust password encryption technique with an extra security layer. Iraqi Journal of Science, 64(3), 1477–1486.

17. Hashim, F. A., Zahraa, Q. A., Hussien, N. M., & Mohialden, Y. M. (2024). Enhanced priority-integrated Multi-winner voting software. Babylonian Journal of Artificial Intelligence, 2024, 27–33. https://doi.org/10.58496/BJAI/2024/005

18. Anonymous. (2022). E-Voting in Pakistan. Master's Thesis, University of Punjab.

19. Dhaher, S., & Kuban, S. (2020). Face and Fingerprint Recognition Voting in Iraq: A Feasibility Study. International Journal of Advanced Computer Technology (IJACT), 9(3), 101–106.

20. Al-Ashoush, M., et al. (2023). Conceptual Framework for Biometric Voting in Jordan. Journal of e-Governance and Technology, 12(1), 1–10.

21. Alsayah, A., & Palaniappan, R. (2022). Libya's Biometric Voting Prototype: Evaluation and Framework. Libya Journal of Technology, 5(2), 55–63.

22. Adams, S., & Asante, J. (2019). Voter Trust and Biometric Verification in Ghana's Electoral System. African Journal of Politics, 6(4), 88–97.

23. Vinayachandra, K., et al. (2020). Smart and Secure Remote Public Voting System (SSRPVS). IEEE Access, 8, 224321–224334.

24. Apurbo, M., Hasib, A., & Rezwan, R. (2025). Offline Biometric Voting with OpenCV and Arduino: A Low-Cost Prototype for Rural Bangladesh. International Journal of Innovative Engineering & Emerging Technology, 8(5), 65–72.

25. Idowu, A. (2021). African Regional Experiences with Biometric Voting Systems. African Electoral Research Institute.

26. Russell, R., & Zamfir, A. (2018). Somaliland's Iris Scan Innovation in Elections. European Parliamentary Briefing.

27. Adewuyi, O. (2021). Technical Failures and Policy Gaps in Nigeria's Biometric Voting. Journal of African Electoral Technology, 6(2), 90–97.

28. IEBC. (2022). Kenya's KIEMS Kit Performance Report. Nairobi: Independent Electoral and Boundaries Commission.

29. Cheeseman, N., et al. (2023). Electoral Technology and Trust in Kenya. Oxford University Press.

30. KPU. (2024). Indonesia's e-KTP Integration in 2024 Elections. Jakarta: General Elections Commission.

31. Aspinall, E., & Mietzner, M. (2024). Digital Identity and Electoral Integrity in Indonesia. ISEAS – Yusof Ishak Institute.

32. TSE. (2024). Biometric Enhancements in Brazil's Urnas Eletrônicas. Brasília: Superior Electoral Court.

33. FGV. (2023). Evaluation of Facial Recognition in Brazilian Municipal Elections. Fundação Getulio Vargas.

34. Awad, K. M., Tulaib, L. F., & Saleh, H. M. (2024). Gait Recognition by Computing Fixed Body Parameters. Babylonian Journal of Neuroscience, 2024, 191–197. https://doi.org/10.58496/BJN/2024/019

35. Wisam Ali Mahmood, et al. (2025). A Privacy-Preserving E-Voting System using Federated Learning and CNNs for Secure Fingerprint and Biometric Verification. Digital Journal of Engineering and Science (DJES), 18(3), 178–194. https://doi.org/10.24237/djes.2025.18312

36. Kumar, S., & Harshith, P. (2024). Biometric-Enhanced Voting Machine: Ensuring Identity Verification and Election Integrity. International Journal of Computer Applications, 186(35).

37. Alam, S. S. (2025). A biometric voting solution: Integrating face recognition with embedded systems for secure offline elections. SSRN. https://doi.org/10.2139/ssrn.5355669

38. Hameed, N. S. H. (2024). Secure E-Voting System using Voiceprint Authentication.

39. The Journal Report. (2023). Biometric Technologies and the Prospect for Sustainable Democracy in Africa. Journal of African Elections.

40. Ahmed, A. A., & Ali, N. H. M. (2025). Secure E-voting authentication system employing biometric technology, Crypto-Watermarking approach and blockchain technology: A review. Mustansiriyah Journal of Pure and Applied Sciences, 3(2), 135–152. https://doi.org/10.47831/mjpas.v3i2.324

41. Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. (2024). Blockchain-Based E-Voting Systems: A Technology Review. Electronics, 13(1), 17. https://doi.org/10.3390/electronics13010017

42. The Hindu. (2024). Pilot Test Reveals Biometric Voting Delays for Disabled Voters in Telangana.

BIOGRAPHIES OF AUTHORS

	**Asst.Lecture** Suleiman Saadon Fawzy , Received a Master's degree in Computer Science from Al-Nahrain University, 2007. Works at the Computer Center, Al-Mustansiriya University. Contact via email: suleiman.s.fawzy@uomustansiriyah.edu.iq
	Prof. Dr. Mustafa Dhiaa Al-Hassani