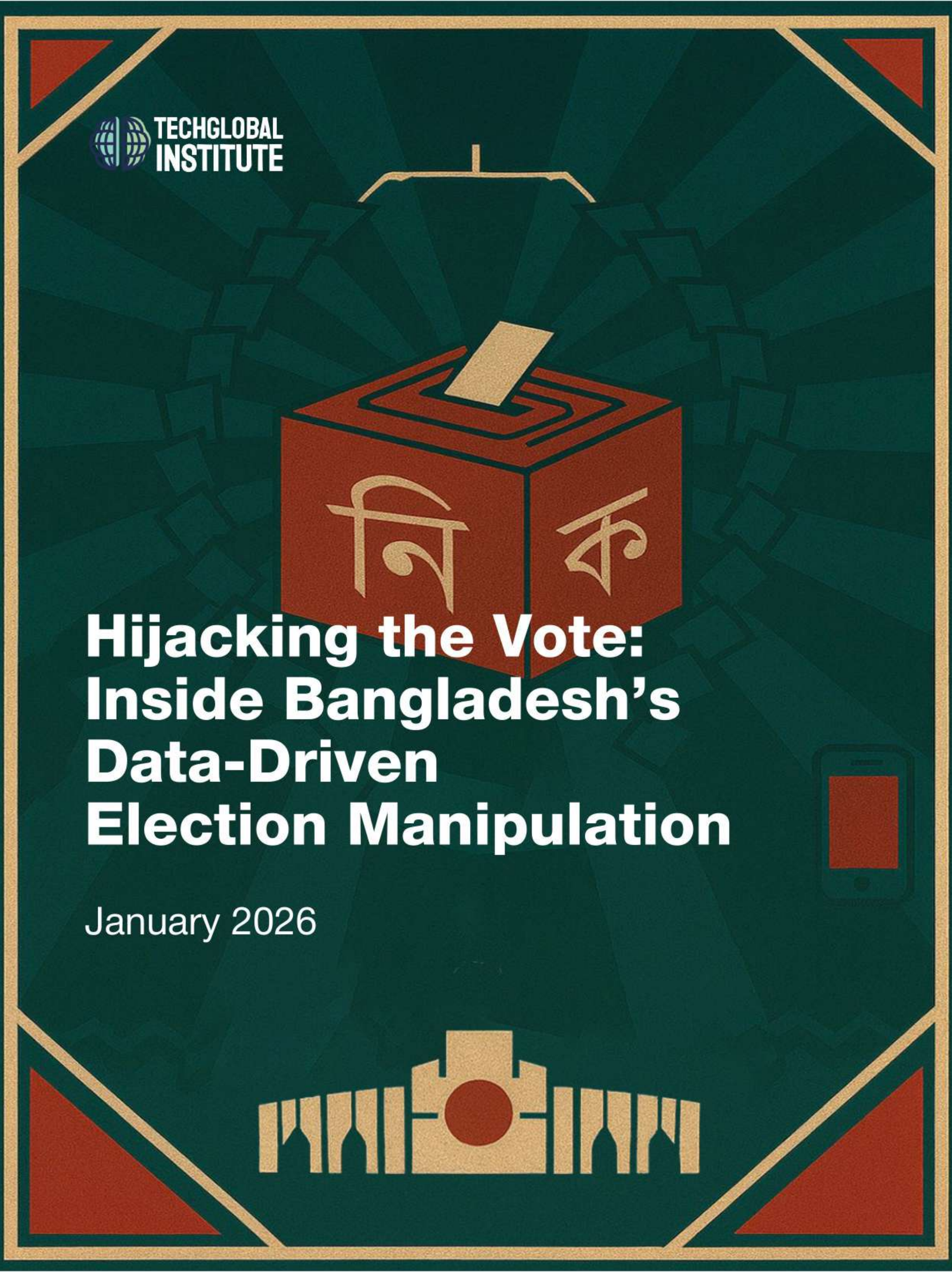
TECHGLOBAL INSTITUTE



Hijacking the Vote: Inside Bangladesh's Data-Driven Election Manipulation

January 2026

Hijacking the Vote: Inside Bangladesh's Data-Driven Election Manipulation

Shahzeb Mahmood, Kalim Ahmed
Zarif Faiaz, Apon Das, Fowzia Afroz

TECHGLOBAL
INSTITUTE

1. INTRODUCTION

This policy brief examines how Bangladesh’s electoral integrity is increasingly shaped and strained by the growing centrality of digital infrastructure across the electoral lifecycle. Drawing on a decade-long electoral and institutional context, statistical analysis of the 2024 parliamentary elections, and documented governance gaps, it contextualises the electoral landscape under previous administrations and identifies recurring anomaly patterns that point to systemic vulnerabilities and coordinated manipulation risks. While the brief does not seek to establish direct causality between these vulnerabilities and specific electoral outcomes, it maps how weaknesses in national identity systems, postal voting workflows, centralised results management platforms, and election-related surveillance create structural fault lines that may be exploited to influence outcomes while preserving the procedural and arithmetic consistency of officially reported results. Its objective is not to relitigate past elections, but to provide the Bangladesh Election Commission (BEC) with concrete, actionable recommendations to strengthen transparency, accountability, and public confidence in upcoming and future elections by addressing these risks at their structural and technological roots.

2. OVERVIEW OF BANGLADESH ELECTION PROCESS AND LANDSCAPE

2.1. ELECTORAL PROCESS

Bangladesh’s parliamentary elections, and their “superintendence, direction and control,” are vested in the BEC under the Constitution and a suite of statutes, including the *Representation of the People Order, 1972*, the *Election Commission Secretariat Act, 2009*, and related legislative and policy frameworks. Under this mandate, the BEC is responsible for preparing electoral rolls and conducting polls for 300 directly elected seats under a first-past-the-post system, along with 50 reserved seats for women allocated to parties in proportion to their parliamentary representation.

Formally, the election process follows a defined sequence. Generally, voter registration begins six to twelve months before polling through household data collection and verification, followed by biometric enrolment at registration centres and de-duplication against the national identity database. Draft electoral rolls are published for public scrutiny and objection before final rolls are prepared, printed, and distributed to polling stations. In the months leading up to polling, the election schedule is announced, and electoral logistics — including candidate nominations, allocation of symbols, publication of final candidate lists, appointment of electoral officers, issuance of directives, and security coordination — are completed within prescribed timelines.

On polling day, stations open in the morning, electoral officers display ballot boxes as empty and sealed in the presence of candidates, their agents, and observers, and voting proceeds through voter identification, application of indelible ink, ballot issuance, and secret marking. After polls close, ballots are counted at the polling station, results are recorded on prescribed forms, and all materials are sealed and transported under escort for constituency-level aggregation, followed by national consolidation and gazette notification by the BEC.

However, throughout this lifecycle — from voter registration and roll preparation to polling, aggregation, and declaration — digital infrastructure has become integral to how elections are administered, monitored, and concluded. This concentration of digital dependence means that weaknesses in system design, access control, or oversight at any single node can cascade across multiple stages of the process, transforming isolated technical or administrative failures into systemic risks to transparency, accountability, and electoral integrity.

2.2. ELECTORAL CAPTURE BY POLITICAL ACTORS

Electoral capture is rarely the result of a single act of ballot fraud; rather, it is a cumulative and continuous process through which institutions tasked with administering and arbitrating elections are gradually repurposed to entrench incumbency. In Bangladesh, while earlier political crises shaped the broader institutional landscape, the last widely recognised credible national election occurred in 2008, and the most consequential manifestations of electoral capture have emerged ahead of the 2014 elections, when formal electoral procedures increasingly diverged from substantive competition and credibility.

Following the removal of the caretaker government framework in 2011, the institutional separation between the incumbent executive and the constitutionally mandated election administration weakened significantly. This shift culminated in the 2014 parliamentary elections, which were boycotted by the principal opposition, the Bangladesh Nationalist Party, and resulted in more than half of parliamentary seats being filled uncontested, with the Bangladesh Awami League winning 232 of the 300 seats. While the BEC reported turnout of around 40%, independent estimates suggested substantially lower participation, ranging between 20% and 30%, and major international observers declined to observe the polls. The 2014 election marked a transition from competitive elections with institutional safeguards to elections conducted under conditions of limited contestation, a trajectory that was further consolidated in the 2018 elections.

Ahead of the 2018 elections, opposition parties faced widespread, systemic repression, including mass arrests through broadly framed "ghost cases" and other criminal lawsuits, raids on campaign offices, and restrictions on media and online speech under the digital security law. Although official turnout was reported at approximately 80%, the actual turnout was significantly lower. Multiple independent assessments documented widespread irregularities, including allegations of ballot marking the night before the polling day across a majority of surveyed constituencies — earning the election the moniker "midnight elections," reflecting a widespread perception that outcomes were effectively determined before voters arrived at polling stations.

By the 2024 elections, the outcome was widely perceived as a foregone conclusion for most voters. Once again boycotted by the principal opposition following a sustained crackdown on political activity, including targeted internet shutdowns during opposition rallies, the polls featured a proliferation of "independent" candidates widely understood to be aligned with the ruling party — commonly referred to as "dummy candidates" — in an attempt to give the appearance of competition without genuine contestation. Voter turnout reporting itself became a point of controversy, with official figures revised upward from approximately 28% at around 3:00 PM to 40% within two hours on election day without clear explanation.

Election Year	Managing Government	Major Opposition Status	Official Turnout	Outcome (Seats)	Assessment Summary
2008	Caretaker	Participated	~87% — undisputed	- Bangladesh Awami League and allies: 263 - Bangladesh Nationalist Party and allies: 33	Free and fair (EU, C'wealth sent delegation)
2014	Partisan, under Bangladesh Awami League	Boycotted	~40% — disputed	- Bangladesh Awami League and allies: 234 (153 uncontested)	Not credible (EU and C'wealth, did not send delegations)
2018	Partisan, under Bangladesh Awami League	Participated	~80% — disputed	- Bangladesh Awami League and allies: 288 - Bangladesh Nationalist Party: 6	Rigged ("Midnight Election," EU and C'wealth, did not send delegations)
2024	Partisan, under Bangladesh Awami League	Boycotted	~41% — disputed	- Bangladesh Awami League and allies: 222 - Independent: 62	Not free and fair (EU and C'wealth, did not send delegations)

STATISTICAL ANOMALIES IN 2024 NATIONAL ELECTIONS

As demonstrated above, Bangladesh's 2024 parliamentary election took place under unusual political conditions: the principal opposition boycotted the election, leaving many constituencies with little genuine competition. In that context, very large winning margins for ruling-party candidates are not, by themselves, surprising. The analytical task, therefore, is not to treat landslides as evidence of manipulation, but to identify combinations of patterns that remain difficult to explain even under the dynamics of a boycott.

Across 150 constituencies that were analysed, the dataset was arithmetically "clean," meaning, when we examined whether the numbers added up correctly — for example, whether the total votes cast equals the sum of valid votes plus rejected votes — we found little to no arithmetic errors. This is a significant finding, as it indicates that even if manipulation occurred, it was done systematically and carefully, not hastily or sloppily. However, whilst the arithmetic checked out on paper, we discovered three specific patterns that appeared repeatedly across polling centres that are difficult to explain as natural consequences of a boycotted election.

PATTERN 1: THE PARADOX OF LOW TURNOUT, HIGH REJECTIONS, AND LANDSLIDE VICTORIES

Consider a polling centre where very few people showed up to vote (low turnout). Of those who did vote, an unusually large number of ballots were rejected as invalid, either because they were improperly marked, damaged, or otherwise deemed unusable; and of the small pool of valid ballots that remained after these rejections, nearly all of them went to a single candidate. This is unusual for a number of reasons.

First, consider low turnout. A low voter turnout in a boycotted election is not, in itself, anomalous or surprising, as many citizens may reasonably choose not to participate when the main opposition is absent; in such circumstances, low turnout can reflect political disengagement rather than procedural failure. Second, consider rejected ballots. In any manual paper ballot system, some ballots will inevitably be rejected. Voters make mistakes: the ballots are marked incorrectly, the papers are damaged, or the mark is unclear. According to international election administration standards, the global average rejection rate is around 3%, and anything between 3% and 5% is regarded as exceeding acceptable administrative thresholds. A rejection rate significantly above this level begins to strain credulity, as it suggests either widespread voter confusion, unusually strict enforcement of ballot validity rules, or something else entirely.

Combining these two factors, that is, low voter turnout with a very high rejection rate, results in an extremely small pool of valid votes. Within this pattern, we observe that this small pool of valid votes is then captured almost entirely — sometimes exceeding 98% — by a single candidate.

A concrete illustration comes from Noakhali-1 (Ulupara Govt Primary School, Centre 82): the turnout was only 19.87% (874 of 4,398 registered voters), yet 29.06% (254 of ballots) cast were rejected. Of the 620 valid votes that remained, 98.23% (609 votes) went to the winning candidate. Contextualised in comparative context, 29.06% rejection rate is nearly ten times higher than the global average. It means that nearly one in every three ballots cast at this centre was invalidated; and of the 620 ballots that were deemed valid, all but 11 went in favour of a single candidate representing the Bangladesh Awami League.

To understand how unusual this is even within the constituency itself, we can compare Centre 82 to all the other polling centres in Noakhali-1. When we do this using a standard statistical measure (called a z-score, which measures how far a data point is from the average), Centre 82 stands out as an extreme outlier — so far outside the normal range that it is statistically improbable to occur by chance.

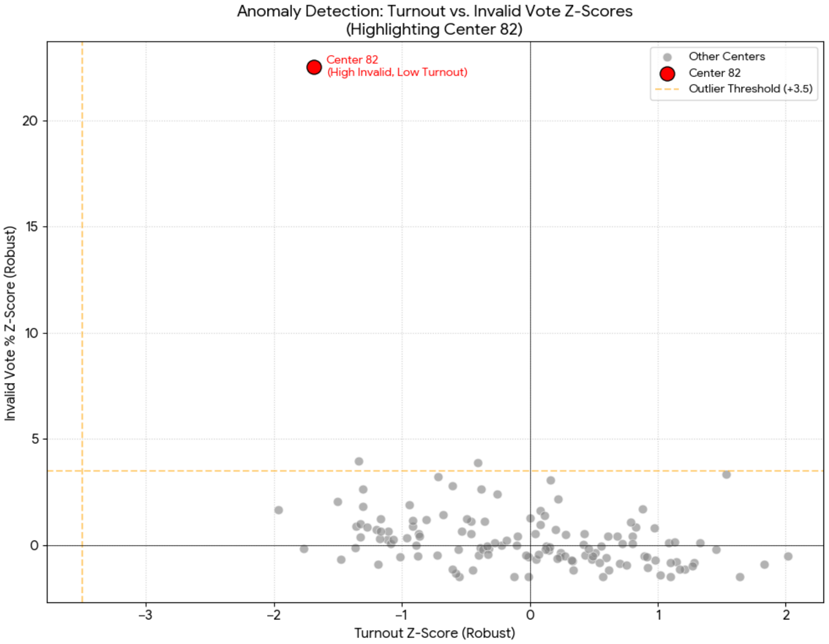


Figure 1. Robust Z-score outlier map for turnout and invalid votes (highlighting Centre 82). Each point is a polling centre plotted by robust turnout Z-score (x-axis) and robust invalid-vote % Z-score (y-axis). The dashed lines mark the outlier threshold (±3.5 robust SD). Centre 82 (red) stands out as an extremely high-invalid outlier while also exhibiting below-average turnout, consistent with the "low turnout + high invalids" anomaly pattern.

Across the 150 constituencies examined in depth, at least 17 polling centres were identified as exhibiting this same pattern: low turnout, exceptionally high rejection rates, and near-total dominance by a single candidate. In 16 of these 17 centres, the winning candidate was from the Bangladesh Awami League. Meanwhile, the seventeenth case involved Narayanganj-5, a constituency where the Bangladesh Awami League did not field a candidate, leaving the seat to its coalition partner, the Jatiya Party. At one centre in this constituency (Madanpur Rahmaniya High School, Centre 168), the rejection rate reached 59.3% — meaning that 668 out of 1,127 ballots cast were rejected, effectively meaning that nearly six out of every ten ballots were invalidated.

PATTERN 2: THE UNIFORMITY PROBLEM

Some constituencies in Bangladesh are genuine long-standing political strongholds. For example, in Gopalganj-2, the Bangladesh Awami League has routinely won more than 90% of the vote for decades. Sheikh Fazlul Karim Selim, the winning candidate, is a cousin of former Prime Minister Sheikh Hasina Wazed and has held the seat across multiple elections since 1980. In such constituencies, lopsided results are the norm, not the exception, and they likely reflect entrenched political dominance rather than electoral manipulation. The more analytically relevant question, therefore, is whether voting patterns across individual polling centres within a constituency display internal consistency and plausibility.

This pattern involves polling centres where both turnout and the winner's vote share are simultaneously at extreme levels (often high 80s to 90+%) while the winner's vote share is near-perfect (99+%), repeated across multiple centres. In a normal election, even within a stronghold constituency, some variation across polling centres is expected: some centres might have high turnout and high winner dominance, whilst others might have moderate turnout and moderate dominance, and still others might have low turnout and low dominance. The results would ordinarily be distributed across a range of combinations rather than tightly clustered.

What raises analytical questions is the repeated concentration of results in the extreme upper-right corner of this distribution — that is, multiple polling centres all showing both very high turnout and near-total winner dominance at the same time. This configuration is sometimes referred to in election forensics literature as a "Russian tail" pattern, reflecting its repeated observation in contexts where electoral manipulation has been credibly alleged.

The key insight is that in a genuinely boycotted election, high winning percentages for the ruling party are plausible across the board. However, those high percentages would ordinarily appear across polling centres with low, medium, and high turnout alike. What is more difficult to explain is why the highest winning percentages would appear specifically and preferentially at the centres with the highest turnout. This suggests that unusually high turnout is not randomly distributed but disproportionately concentrated in centres delivering near-total victories, an outcome that departs from expectations of natural voter behaviour.

For instance, Sherpur-1 has historically been a stronghold of the Bangladesh Awami League, with the incumbent candidate, Md. Atiur Rahman Atik, having won five consecutive terms and served as a parliamentary whip. On paper, this constituency should produce predictable, lopsided results favouring the Bangladesh Awami League. However, in the 2024 election in Sherpur-1, a credible independent challenger emerged from within the ruling party itself — Md. Sanuar Hossain Sanu, the district general secretary of the Bangladesh Awami League — introducing an intra-party split. Under such conditions, even in a stronghold, when there is a credible challenger from within the ruling party itself, one would normally expect some dilution of vote shares or at least measurable variation across polling centres. Some centres would be expected to favour the incumbent, while others might lean towards the challenger; and even in the incumbent’s strongest areas the results would likely remain lopsided but not uniformly or identically so across centres. However, the analysis found remarkable uniformity at the extremes, with 32 centres in the constituency exhibiting a “stuffing-like” signature, characterised by the joint appearance of very high turnout and near-total winner dominance.

By contrast, in Gopalganj-2, the long-standing stronghold of the Bangladesh Awami League, results across centres show high winner percentages, consistent with structural political dominance, without a distinct clustering at voter turnout extremes. However, in Sherpur-1, the results show a different pattern: some heterogeneity across most centres, alongside a distinct subset of centres that cluster in the extreme upper-right corner of the distribution, characterised by simultaneously very high turnout and near-perfect winner dominance.

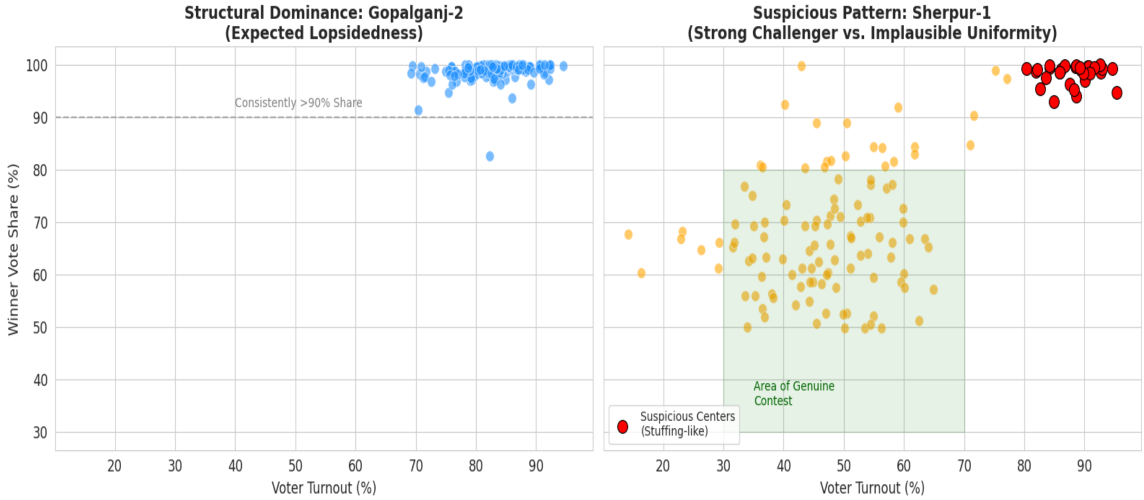


Figure 2. Gopalganj-2 exhibits uniformly lopsided centre results, consistent with structural dominance. Sherpur-1 exhibits heterogeneous centre results but also a distinct high-turnout, near-100% winner-share cluster (highlighted), a pattern commonly treated as an anomaly indicator.

PATTERN 3: THE ZERO INVALIDS PROBLEM

Across more than 1,000 polling centres, the official results reported zero rejected or invalid ballots, implying that every ballot cast was marked correctly, deemed valid, and included in the final tally. While not impossible at the level of an individual polling centre, this outcome is statistically improbable when observed at such scale.

In a manual, paper-based ballot system, it is virtually inevitable that some ballots will be rejected. Voters may mark ballots incorrectly — by selecting more than one option, making ambiguous marks, or failing to follow instructions — while some ballots may be smudged, defaced, intentionally spoiled, or damaged in ways that render them unusable. Some voters, intentionally or unintentionally, spoil their ballots as a form of protest. As documented by the ACE Electoral Knowledge Network, such human and procedural factors produce a natural error rate in paper-based elections, with rejection levels varying by ballot design, voter guidance, and counting rules.

Accordingly, a single polling centre reporting zero invalid ballots among several hundred votes may be unusual but plausible. However, when more than 1,000 centres report zero invalid ballots simultaneously, the result departs markedly from expected patterns in large-scale manual elections, indicating a systemic anomaly rather than isolated variation.

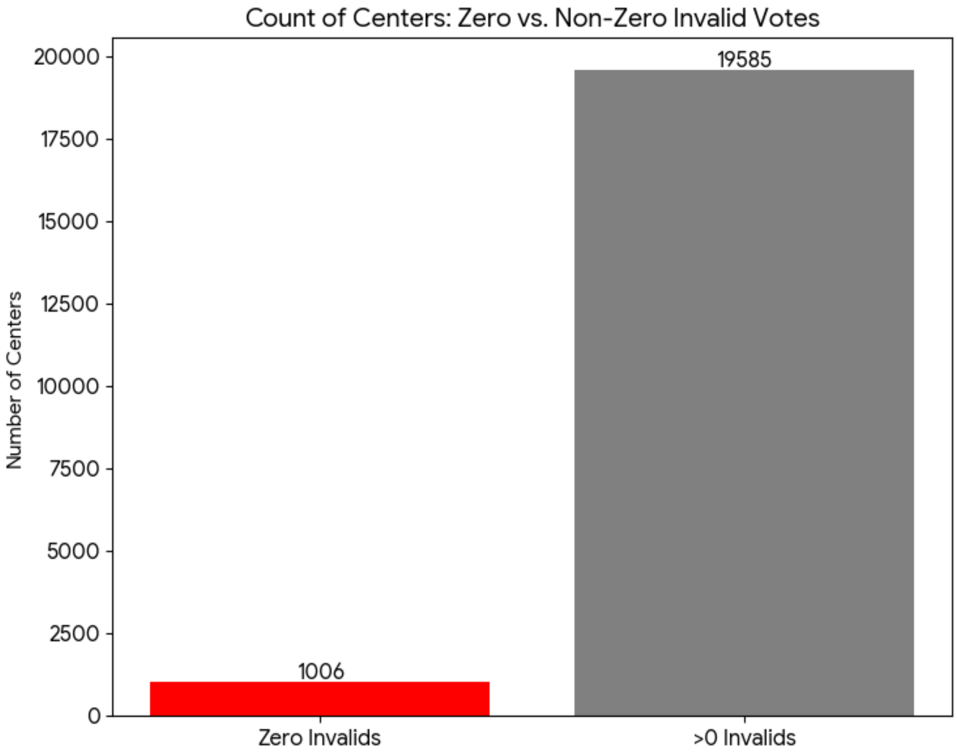


Figure 3. Count of centres reporting zero versus non-zero invalid votes.

Collectively, these statistical anomalies appear clustered and patterned, rather than randomly distributed. When mapped, the composite Risk Score used to prioritise deeper analysis shows that high-risk constituencies are dispersed across the country rather than concentrated in a single region. The recurrence of the same centre-level signatures – extreme invalid rates at low turnout, clusters of high turnouts with near-total winner dominance, and spikes of zero invalid ballots – suggests behaviours that may be systematic rather than incidental.

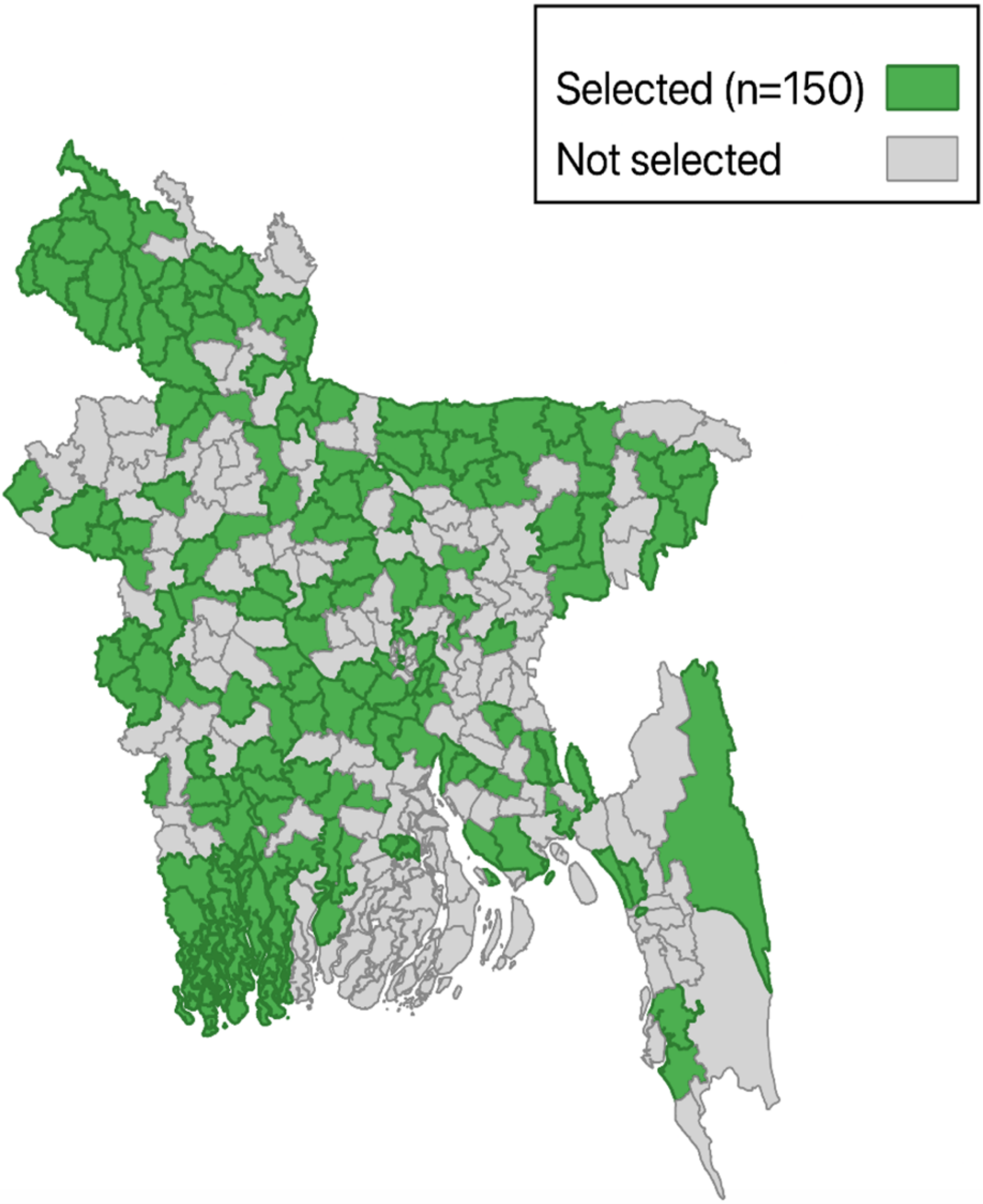


Figure 4. Geographic distribution of the 150 constituencies prioritised for deep-dive analysis. The map reveals no obvious regional bias; anomalies appear in both traditional strongholds and swing districts, suggesting systematic rather than localised manipulation.

Why these patterns, taken together, point to systemic coordination is best understood by considering that any one of them, if observed in isolation, could plausibly be attributed to localised factors, such as unusually strict ballot validation in one district, exceptionally mobilised party machinery in another, or uneven training of election officials elsewhere. What is observed here, however, is not a single anomaly but the repeated appearance of three distinct patterns across multiple constituencies and regions, each systematically favouring the same political outcome. This convergence is more consistent with coordinated practices applied across administrative units than with isolated errors or ad hoc manipulation.

Additionally, while the reported results remain arithmetically coherent — that is, the totals reconcile and internal calculations balance — they simultaneously defy statistical plausibility. This combination suggests that the figures were not the product of random error, but of processes attentive to maintaining numerical consistency. The internal logic holds because it was preserved, indicating deliberate construction rather than accidental distortion: the totals balance because they were made to balance. Taken together, these features point to outcomes engineered to appear procedurally sound while delivering a predetermined result, a conclusion further reinforced by the parallel use of "dummy candidates" to maintain a façade of electoral competition.

3. HOW DIGITAL ELECTORAL INFRASTRUCTURE CREATES SYSTEMIC INTEGRITY RISKS

The findings in the previous section do not, on their own, identify the precise points in the electoral process at which irregularities may have arisen; rather, they point to statistical inconsistencies and patterns suggestive of systemic vulnerabilities and coordinated manipulation risks. Moreover, most returns in the released dataset reconcile arithmetically, indicating that any vulnerabilities may plausibly lie in later stages of the results pipeline — aggregation, transcription, digitisation, or publication — rather than in centre-level bookkeeping alone. This is not to suggest that risks are confined to later stages, as they may very well extend to earlier stages of the electoral process, such as during voter registration and voter roll preparation; the examples cited are illustrative, not exhaustive. As such, electoral integrity cannot be assessed solely on the basis of polling-day procedures and that scrutiny must extend to the systems governing the election process end-to-end.

Digital technologies now underpin multiple stages of Bangladesh's electoral process, from voter registration and roll preparation to overseas voting and results aggregation. While these systems are often presented as tools to enhance efficiency, inclusion, and transparency, their increasing centrality has also introduced structural risks that are not always visible at the level of polling-day procedures. When core electoral functions are mediated through centralised digital infrastructures, particularly those linked to centralised identity, voting, and results management systems, weaknesses in governance, access control, and oversight can be transmitted across the electoral cycle. This section therefore examines how such systemic vulnerabilities, rather than isolated technical failures, create conditions conducive to manipulation and, in doing so, undermine confidence in electoral outcomes.

3.1. SYSTEMIC VULNERABILITIES IN THE NATIONAL IDENTITY INFRASTRUCTURE, AND RISKS TO VOTER ROLLS' INTEGRITY

One of the earliest and most consequential points of vulnerability to systemic manipulation lies at the voter registration and voter roll preparation stage, which is structurally dependent on the national identity database. As voter eligibility is derived almost entirely from this digital infrastructure, weaknesses within the identity system are directly transmitted into the electoral process.

Critical flaws in system architecture, access controls, and oversight, combined with entrenched corruption, enables both citizens and non-citizens to obtain fraudulent national identity credentials. Documented cases illustrate how individuals, acting in collusion with state officials who had privileged access to identity servers, were able to generate multiple false identities by circumventing biometric safeguards, including by "either [using] a finger reversely or the toe to give impressions of fingerprints" during enrollment. In parallel, criminal syndicates involving corrupt officials and intermediaries operate organised rackets producing counterfeit identity documents, including smart national identity cards, for non-citizen refugees and individuals with criminal records. Once fraudulent identities are embedded within the national identity database, they become exceedingly difficult for electoral authorities to detect and remove, creating enduring fault lines within the electoral system that can be exploited by bad actors to influence voter rolls and, ultimately, electoral outcomes. This challenge is compounded by the scale and time constraints of voter roll preparation in a country of approximately 170 million people, which requires the verification and updating of records for an estimated 127.7 million registered voters within short timelines. As a result, the voter roll preparation process becomes a largely extractive exercise from an upstream database whose integrity cannot be independently or meaningfully verified by election administrators.

A now-canonical manifestation of these systemic weaknesses is the repeated reporting of votes cast in the names of deceased citizens in previous national elections. While the election authority has announced the removal of approximately 2.1 million deceased individuals from the voter list, there remains limited transparency regarding how this process was undertaken, whether it was insulated from manipulation, and the integrity of the underlying death registration data maintained by the civil registration authority.

Death registration, an essential but often overlooked component of identity lifecycle management, exhibits several structural, institutional, and policy deficiencies. First, an investigative report demonstrates how fictitious identities can be created by local authorities and subsequently registered as deceased with relative ease. One recorded incident shows patently implausible death entries, including the registration of an 18-year-old mother with 19 children as deceased, despite records showing a child born weeks after her reported death, and multiple family members incorrectly registered as dead while many of them are alive — all done under pressure to meet registration targets. Second, reliance on death registration data to cleanse voter rolls is inherently incomplete, as a significant proportion of deaths, particularly in rural and marginalised areas, often remains unregistered with the Office of the Registrar General, Birth and Death Registration. Third, the removal of deceased voters from electoral rolls is largely static rather than dynamic; individuals who die after finalisation of the roll but before election day are not excluded due to the absence of real-time data synchronisation. Collectively, these gaps create persistent inaccuracies that undermine confidence in the voter list as a living and current register of eligible voters.

Another critical vulnerability in the national identity infrastructure, and its direct spillover effects on voter rolls integrity, arises from the breadth of access granted by the BEC to third parties. Around 180 state and non-state institutions have access to the database for identity verification and allied purposes, while external vendors are contracted to construct and maintain the system.

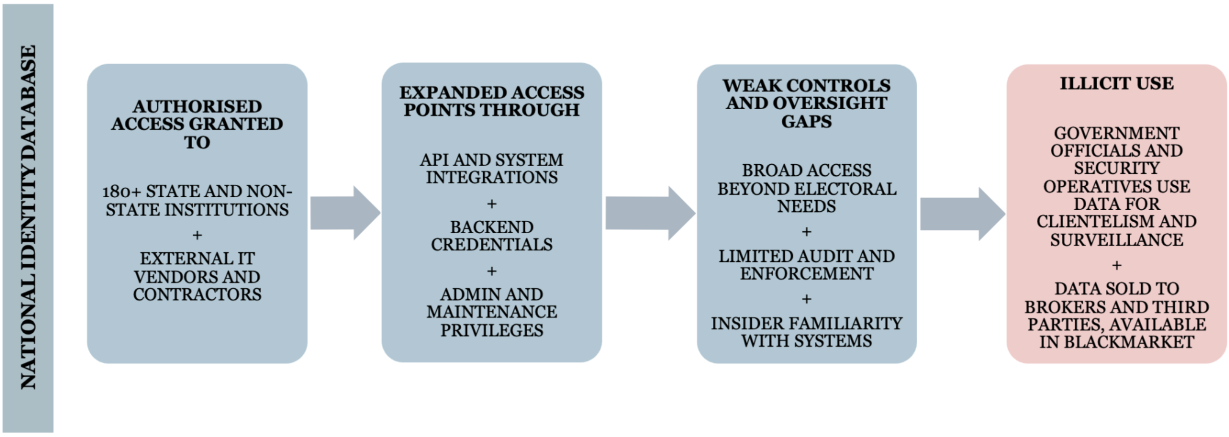

NATIONAL IDENTITY DATABASE
AUTHORISED ACCESS GRANTED TO
180+ STATE AND NON-STATE INSTITUTIONS
+
EXTERNAL IT VENDORS AND CONTRACTORS
EXPANDED ACCESS POINTS THROUGH
API AND SYSTEM INTEGRATIONS
+
BACKEND CREDENTIALS
+
ADMIN AND MAINTENANCE PRIVILEGES
WEAK CONTROLS AND OVERSIGHT GAPS
BROAD ACCESS BEYOND ELECTORAL NEEDS
+
LIMITED AUDIT AND ENFORCEMENT
+
INSIDER FAMILIARITY WITH SYSTEMS
ILLICIT USE
GOVERNMENT OFFICIALS AND SECURITY OPERATIVES USE DATA FOR CLIENTELISM AND SURVEILLANCE
+
DATA SOLD TO BROKERS AND THIRD PARTIES, AVAILABLE IN BLACKMARKET

Figure 5. Expanded, multi-institutional access to the national identity database creates a chain of vulnerability: authorised access granted to numerous state, non-state, and vendor entities multiplies access points; weak controls and oversight allow this access to persist beyond legitimate electoral needs; and, in turn, these conditions enable unauthorised downstream uses of citizens' personal data, including clientelism, data brokerage, and surveillance by government officials, security apparatuses, and private actors.

One interviewee observed that such expansive access, in the absence of robust access controls, audit trails, and accountability mechanisms, significantly heightens the risk of misuse. On the contrary, these risks are further amplified by the fragmented and weakly governed nature of identity data management, including the existence of an illicit market for identity data, fuelled by repeated breaches of government-linked servers, as well as government officials and security operatives selling personally identifiable information — often with insider assistance from employees of the BEC. Illustratively, the interviewee suggested that in an electorally volatile or closely contested constituency (such as Sherpur-1 constituency elaborated above), a well-connected candidate could exploit this inter-agency access to identify non-resident voters through migration or expatriate databases maintained by the Department of Immigration and Passports, the Ministry of Expatriates Welfare and Overseas Employment, and/or Ministry of Labour and Employment, and facilitate proxy voting or otherwise influence voter participation; or draw on records maintained by the Office of the Registrar General, Birth and Death Registration to identify deceased but still-listed voters whose continued presence on the voter rolls could be leveraged to distort electoral outcomes. Even where such actions are not systematically undertaken, the mere plausibility of such exploitation signals a significant vulnerability in the electoral ecosystem, a concern implicitly reflected in the BEC's own warning against the collection of voters' national identity numbers and phone data "under the guise of campaigning," which points to an awareness of how parallel datasets could be assembled and misused.

During the preparation and verification of voter rolls itself, electoral administration relies on a multi-layered digital workflow that links distributed, field-level data collection and local servers to centralised national identity databases maintained by the BEC. While this process is intended to update the voter list, it also introduces multiple digital handover points at which voter information (including photographs, fingerprints, and signatures) is transmitted, reviewed, and synchronised across systems by data entry operators and database managers exercising discretionary administrative authority at different levels. Absent strong access controls, transparent audit mechanisms, and independent oversight, these transition points create structural vulnerabilities within the national identity infrastructure, allowing inaccuracies, delays, or discretionary interventions at any stage of data integration to be absorbed into the final voter rolls.

Overall, these risks reflect systemic vulnerabilities embedded within the national identity infrastructure arising from a convergence of structural factors: the absence of meaningful accountability mechanisms within identity creation, verification, and access management systems; excessive discretionary power vested in individual officials; low-quality enrollment and verification processes; unresolved fault lines arising from the transition from paper-based identity documents to biometric and microchip-embedded smart card systems; fragmented institutional mandates governing identity, civil registration, and electoral administration; and weak enforcement of identity fraud and data protection laws. When such vulnerabilities are transmitted downstream into voter registration and roll preparation processes, they systematically undermine the reliability of the voter rolls as an authoritative register of eligible voters. Collectively, these conditions erode confidence in electoral administration and call into question the integrity of elections that rely so heavily on a digital identity infrastructure without commensurate legal, technical, and institutional safeguards.

RECOMMENDATION 1: Tighten access controls on the voter identity database and make all access traceable. The BEC should review who has access to the national identity database and temporarily suspend API access for approximately 180 non-essential third-party institutions and vendors whose functions are not directly related to electoral administration. For entities that require continued access, the BEC should enforce a strict “need-to-know” protocol, limiting queries to identity verification only, rather than returning full demographic data, addresses, or other attributes that could enable voter profiling, canvassing, or proxy voting. All access should be limited to specific, named officials, with automatic logs recording who accessed or modified data, when, and for what purpose. After the conclusion of the 2026 national elections, the BEC should publish a consolidated report detailing which entities had access during the electoral period (including during voter registration and voter roll preparation), the legal basis for that access, and high-level statistics on data queries and bulk operations, to strengthen transparency and accountability.

RECOMMENDATION 2: Actively and continuously clean voter lists instead of relying on static databases. Rather than updating voter lists only once using existing databases months before the election, the BEC should introduce a short, final verification period approximately two weeks before polling that combines automated checks for duplicate, deceased, and overseas voters with targeted field verification. This process should require cross-checking national identity records with civil registration and aviation exit records.

RECOMMENDATION 3: Undertake a targeted post-election audit of the national identity and voter roll pipeline. The BEC should commission an independent, time-bound audit focused on how national identity records were accessed and integrated into the voter registration and voter roll preparation, prioritising constituencies with abnormal roll changes, duplicate biometrics, or high numbers of deceased or ineligible voters. The audit should combine forensic review of system access logs with limited field verification and publicly release aggregate findings and corrective actions to prevent recurrence.

3.2. SYSTEMIC VULNERABILITIES IN THE NATIONAL IDENTITY INFRASTRUCTURE, AND ITS SPILLOVER EFFECT ON *POSTAL VOTE BD*

While the decision to extend overseas postal voting to 13 million non-resident Bangladeshi citizens represents an important expansion of the franchise, the effectiveness and credibility of *Postal Vote BD* are structurally contingent on the same national identity infrastructure that underpins voter registration and roll preparation. Officially launched on November 18, 2025, with the registration window closed at midnight on January 5, 2026, the initiative enabled expatriate voters across 120 countries to cast nearly 60% of mailed ballots (~405,164) as of late January 2026. However, as voter eligibility, identity verification, and record matching for postal voting rely on the national identity and passport databases maintained by the BEC, any weaknesses embedded within these systems are directly transmitted into the postal voting workflow. *Postal Vote BD,* therefore, does not operate in isolation; it inherits the institutional, technical, and governance vulnerabilities that already affect the integrity of domestic electoral processes.

From a practical standpoint, this reliance creates compounded risks. *Postal Vote BD* requires expatriate voters to submit additional personal information (such as overseas contact details, addresses, and biometric confirmations) that are linked to their existing identity records. This scale expands the volume and sensitivity of data circulating through an ecosystem characterised by fragmented oversight, broad access privileges, and limited enforcement of data-protection obligations. Evidence of how privileged access within this ecosystem can be abused is not merely theoretical: an investigation by the Criminal Investigation Department into the illicit sale of national identity records alleged that election office-linked personnel sold over 365,000 NID records for approximately BDT 110 million. Such findings underscore how authorised access to identity databases can be monetised and repurposed beyond lawful uses. In this context, the expansion of the franchise increases the number of identity-verification touchpoints, each of which may function as a potential interception point where insiders could extract credentials, facilitate proxy registrations, or selectively exclude diaspora applicants.

Crucially, these risks do not stem from the concept of postal voting itself, but from the structural conditions under which it is being implemented. According to the BEC, returned ballots will be processed using barcode machines and QR code scanning, digitally stored on laptops, and subsequently placed in ballot boxes. In the absence of robust safeguards, transparent audit mechanisms, and enforceable limits on data access and use, *Postal Vote BD* risks amplifying pre-existing weaknesses rather than mitigating them. This has implications not only for the security of expatriate voters' personal information, but also for confidence in the integrity of postal ballots as a legitimate extension of the electoral process. Without addressing the systemic vulnerabilities of the national identity infrastructure on which it depends, the expansion of postal voting may inadvertently deepen existing trust deficits instead of strengthening democratic participation.

RECOMMENDATION 4: Ring-fence Postal Vote BD data and enforce strict purpose limitation. The BEC should segregate *Postal Vote BD* data from the broader national identity ecosystem, restrict access to a small, designated unit, and limit use strictly to voter verification and ballot administration, with all access logged and preserved. Aggregate access and usage statistics should be disclosed post-election to strengthen accountability and deter misuse, without disclosing personally identifiable information. Additionally, postal ballot data should not be repurposed or shared with other agencies except under court order.

RECOMMENDATION 5: Establish a transparent and auditable chain of custody for postal ballots. The BEC should, in future elections, replace laptop-based opaque processing with an end-to-end auditable workflow that issues verifiable digital receipts, separates identity verification from ballot handling, and conducts decryption and counting in an observer-accessible facility with random (~5% sample) manual cross-checks with the original metadata of the "Digital Receipt". This workflow should be underpinned by basic public-key cryptography, ensuring ballots are encrypted at submission, decrypted only after polls close by authorised officers, and accompanied by cryptographically signed digital receipts that allow post-election verification without compromising ballot secrecy.

3.3. CENTRALISED DIGITAL ACCESSIBILITY AND AGGREGATION SYSTEMS, AND RISKS TO RESULTS TRANSPARENCY

Centralised digital control over election result accessibility and aggregation constitutes a critical but under-scrutinised dimension of electoral integrity. In both recent and forthcoming elections, the BEC has relied on a suite of digital tools to manage information flows across the electoral lifecycle, including a voter-facing application as well as field-level reporting and backend result management systems. While these tools are presented as efficiency-enhancing and transparency-supporting mechanisms, their architecture concentrates informational authority within a small number of centrally managed systems and administrators. Specifically, three digital systems were identified as consequential for election result accessibility and aggregation.

First, the polling-centre data, including constituency-level turnout figures, vote counts, and candidate and party information, are processed and aggregated through proprietary software environments via a voter-facing mobile application known as *Smart Election Management BD*, through which the information will reportedly be shared with the public at regular intervals to ensure credibility and transparency in the national elections. However, it remains unclear what safeguards exist against alteration or selective reporting, especially in constituencies like Noakhali-1 and Sherpur-1 described above. As such, this layered mediation of electoral information introduces early-stage integrity risks, as primary polling-station data is digitised and disseminated through systems that are not fully observable or independently verifiable. Without publicly accessible safeguards embedded in the application — such as mandatory reconciliation with signed polling-station forms, open access to capture protocols, or disclosure of transmission logs and error reports — candidates, observers, and the public are unable to assess whether reported figures accurately reflect analogue polling-station records at each stage of transmission and aggregation.

Second, similar concerns arise with respect to কপোত (KOPOT), a centrally administered digital platform operating on closed networks that was reportedly used during the 2024 national elections for direct reporting by election officials to transmit centre-wise voting data to BEC headquarters at two-hour intervals. This dashboard reportedly showed that the nationwide turnout figures stood at approximately 28% at the close of polling and remained unchanged for several hours thereafter, before being revised to "more or less 40%" within a short interval, without any public explanation for this significant fluctuation. Such unexplained revisions, when mediated through opaque digital systems, risk reinforcing perceptions that electoral outcomes are shaped by administrative discretion rather than verifiable polling-station records, thereby weakening public confidence in the integrity of the process. Additionally, for certain constituencies in remote or hard-to-access areas, such as hill tract districts or coastal regions, results are reportedly authorised to be transmitted informally to BEC through WhatsApp. The use of such ad hoc communication channels creates a parallel reporting pathway that operates outside formal systems, audit trails, and verification protocols. This further complicates result integrity by introducing unofficial data flows that are difficult to authenticate, reconcile with official records, or scrutinise in the event of disputes.

Finally, the BEC employs a result management system that centralises result entry, aggregation, approval, and dissemination within a closed digital infrastructure controlled by a limited set of authorised users, including system administrators and election officials. While the system is presented as improving efficiency, by automating aggregation, generating result sheets, and enabling real-time monitoring, it also concentrates significant discretionary power over electoral outcomes within centrally managed software environments. The process appears to entail substantial manual involvement, including ballot scanning, data entry, error detection and resolution, and consolidation of results, all conducted within a centrally controlled network. In an environment characterised by limited external oversight or real-time access for candidates and observers, these design features create structural conditions in which errors, delays, or discretionary interventions may be difficult to detect or contest by external actors. As a result, even where individual polling-station records remain intact, confidence in election results depends less on visible reconciliation with paper records and more on trust in the integrity of the digital infrastructure itself, raising legitimate questions about verifiability and public confidence in announced outcomes.

All three systems share key attributes: in the absence of publicly auditable logs, parallel verification channels, or legally mandated disclosure of system design and access protocols, centralisation creates a structural asymmetry between those who generate electoral data and those who control its consolidation and release. As a result, even where no overt interference occurs, the opacity and concentration of digital control over results management can weaken confidence in electoral outcomes and render disputes difficult to resolve through evidence-based scrutiny.

RECOMMENDATION 6: Mandate polling-station-level reconciliation and public audit trails for all digital result reporting. The BEC should require that all digitally reported turnout figures and results — whether transmitted via *Smart Election Management BD*, *KOPOT*, or other tools — be reconciled with signed polling-station result forms, with each such form scanned and uploaded into the relevant results access, reporting, and management systems, alongside time-stamped transmission logs and error reports. Digitised figures should be displayed alongside the original scanned image, and any subsequent corrections should be preserved as visible revisions with mandatory explanatory notes. Unofficial channels such as WhatsApp should be explicitly prohibited for result transmission, except as a last-resort contingency pursuant to a mandatory court order and subject to post-hoc audit.

RECOMMENDATION 7: Open results aggregation to structured external scrutiny. The BEC should provide candidates and their agents, accredited observers, journalists, and other stakeholders with real-time or near-real-time read-only access to constituency-level aggregation dashboards and post-election access to system logs showing when, how, and by whom results were entered, modified, or approved (to mitigate the risks of reprisal, system logs should record unique user-level identifiers without publicly disclosing personal identities — such resolution should occur only if a legal challenge is filed, and then only under court supervision). This would reduce discretionary opacity in centrally managed systems and allow disputes over discrepancies or revisions to be resolved through evidence rather than administrative assertion. In addition, the

BEC should publish a consolidated post-election report summarising aggregation timelines, revisions made, access patterns, and any system anomalies identified during results processing.

RECOMMENDATION 8: Implement automated statistical triggers and real-time transparency safeguards in results aggregation systems. The BEC should configure *KOPOT* and related aggregation software to automatically flag and temporarily quarantine polling-centre results exhibiting statistical anomalies — such as turnout above 90% or zero invalid ballots — for secondary enhanced manual review. In cases of turnout revisions or data updates, the BEC should be required to publish time-stamped server logs identifying when and from which nodes revised data were received, and provide candidates and their agents, accredited observers, journalists, and other stakeholders with read-only access to aggregation dashboards to independently monitor data inflows in real time. All flagged anomalies, revisions, and corrective actions should be documented and published in a consolidated post-election report to enable independent review and institutional learning.

3.4. DEPLOYMENT OF CCTV AND BODY-WORN CAMERAS, AND THEIR INTEGRITY AND PRIVACY RISKS

Across over 42,000 polling centres, the planned deployment of body-worn cameras and CCTV, in the absence of clearly legislated safeguards and a coherent policy framework, introduces a significant expansion of surveillance into the electoral process, with direct implications for ballot secrecy, voter confidence, and the neutrality of the polling environment. While framed as measures to enhance security and transparency, and while such deployment could in principle mitigate risks of electoral malpractice of the nature described above, the use of continuous visual recording during voting risks adversely affecting the conditions under which citizens exercise their franchise, particularly in politically sensitive or closely contested constituencies. The BEC has not issued binding protocols on camera placement, footage capture, retention periods, access controls, or permissible secondary uses of recordings. Moreover, footage generated at polling stations is likely to be stored and managed within centrally controlled digital systems linked to executive authorities. An absence of such safeguards creates a heightened risk that cameras may capture voter behaviour, interactions within polling centres, or other sensitive visual data, undermining the principle that voting must be secret and unobserved — especially in an environment where security apparatuses have been credibly linked to the acquisition and heightened use of surveillance technologies and spywares during past election periods.

Without immutable audit trails, independent oversight of access logs, or clear chain-of-custody requirements, surveillance footage can be selectively accessed, withheld, edited, or repurposed without detection. The lack of defined penalties for disabling cameras or misusing recordings further weakens accountability and risks reducing these technologies to performative gestures rather than effective safeguards against electoral malpractice. Within a broader context of weak data-protection enforcement and limited institutional oversight, the large-scale collection and retention of election-related video data carries risks of post-election misuse, including voter profiling, intimidation, or selective targeting.

RECOMMENDATION 9: Establish binding safeguards governing the use of CCTV and body-worn cameras in polling centres. The BEC should issue legally binding directives governing the deployment and placement of CCTV and body-worn cameras, explicitly prohibiting coverage of voting booths and ballot-marking areas, and setting clear limits on footage capture, strict retention periods, and narrowly defined purposes for use, with a requirement to delete footages following the resolution of electoral disputes within existing statutorily-defined timelines. Body-worn cameras on security personnel should operate on a "trigger-only" basis, activated solely during disturbances rather than continuous recording, to minimise the creation of surveillance records of peaceful voters. Access to footage should be restricted to a small, designated unit within the BEC, subject to written authorisation and comprehensive access logs, and any sharing with security or other agencies should be prohibited except pursuant to a specific court order.

RECOMMENDATION 10: Introduce independent oversight, auditability, and enforceable accountability for election-related surveillance footage. The BEC should mandate immutable, tamper-evident audit trails for all access, viewing, copying, or deletion of polling-station CCTV and body-worn camera footage, with every action logged, time-stamped, and attributable to specific authorised officials whose access automatically expires after polling day. An independent oversight mechanism, such as a multi-stakeholder audit panel or accredited observer access, should be established to review compliance, while clear penalties must apply for disabling cameras without justification or misusing recordings. Where footage from a polling centre is missing or corrupted during a disputed period, a rebuttable presumption of irregularity should apply, shifting the burden to the presiding electoral officer to demonstrate that the vote was unaffected, failing which a re-poll may be triggered; the BEC should also publish a post-election summary report detailing access, retention, and use of surveillance footage to strengthen accountability and public confidence.