ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(c) Jan – Feb 2026

Original Research Article

DIGITAL SYNERGY IN GOVERNANCE : A GOV-TECH STARTUP MODEL FOR HUMAN-CENTRIC, SUSTAINABLE, AND TRANSPARENT ELECTORAL SYSTEM THROUGH LAVIS

** Mr Akshay Mishra & ** Mrs Priti Sawale*

** Student, ** Asst Professor & Head, Department of Political Science, B.K. Birla College (Empowered Autonomous Status), Kalyan.*

Abstract:

As digital technology becomes more common in government, there is a growing demand for Civic-tech solutions that can actually fix real-world problems. This paper looks at the Layered Authentication and Voting Integrity System (LAVIS), a new B2G (Business to Government) Gov-tech startup model designed to create a highly secure, offline-first electoral process. Finding the right balance between human- centric design and sustainable innovation, LAVIS uses a five-step authentication process: a physical KYC check, temporary RFID smart cards, live facial recognition, biometric scanning, and a deactivated cryptographic QR audit trail. Because the system tries to eliminate current gaps and loopholes. Offline database structure segregated into state, constituency, and booth levels (SDB - CDB - PBD) , it essentially neutralizes remote cyber threats and mass data tampering. This study explores the technical viability of LAVIS and ensures it is legally compliance . Ultimately, it shows how digitally synergized startups can eliminate voter impersonation, cut long-term costs, and help restore public faith in the democratic process.

Keywords : *B2G Startup, Gov- Tech Model , electoral integrity, biometric authentication, multi-factor voter verification, offline-first database architecture, digital governance, electoral transparency*

Introduction:

While governments worldwide are quickly adopting digital tools to cut red tape and improve public services, our election systems--the very bedrock of democracy--are surprisingly stuck in the past. Even with the widespread use of electronic voting machines (EVMs), we still rely heavily on polling officers to manually verify physical IDs. This outdated, manual step leaves a massive window open for human error, administrative bias, and fraud. It directly leads to duplicate identities across state lines, exhaustingly long lines at the booths, and constant allegations of vote tampering that severely damage public trust in the democratic process.

The solution lies in "Digital Synergy"—the concept of seamlessly weaving different technologies together so they are far more effective as a whole than they are on their own. But when it comes to elections, you can not just blindly throw new tech at the problem. It has to strictly follow the law, respect voter privacy, and guarantee access for everyone.

This is exactly what this paper explores through the Layered Authentication and Voting Integrity System (LAVIS). LAVIS is a futuristic Gov-Tech startup model that breaks down old, isolated government silos by

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(c) Jan – Feb 2026

Original Research Article

connecting data, authentication, and auditing into one unified platform. By focusing on "humanity -centric" innovation, LAVIS automates the verification process to protect voter dignity, ensure marginalized groups aren't excluded, and ultimately enforce the true democratic promise of "one person, one vote."

Statement of Problem:

Traditional voting systems are structurally broken, sparking a massive crisis of trust in modern democracies. Plagued by identity fraud and unreliable manual checks, these systems routinely shut out migrant and overseas voters. We saw this firsthand in India with recent "vote chori" (vote theft) allegations, where Bihar's Special Intensive Revision (SIR) exposed over 14.35 lakh suspect duplicate entries.

On election day, these back-end data failures cause pure chaos. Manual ID checks take 8 to 10 minutes per voter, which creates massive lines, kills turnout, and exhausts the drafted school teachers running the booths—leaving the process highly vulnerable to innocent mistakes and deliberate tampering. To make matters worse, without a cryptographically secure audit trail, we can not mathematically prove the final tally without violating ballot secrecy.

Unsurprisingly, public faith is tanking. Recent CSDS Lokniti surveys show a sharp drop in trust toward the Election Commission over the last five years. Because our current machines lack multi-layered biometric security, it's dangerously easy for losing candidates to spin narratives of digital tampering.

Significance of the Study :

This study stands out because it delivers a ready-to-deploy product that bridges the frustrating gap between the advanced tech we use daily (like Face ID for banking) and our outdated election systems. It proves a startup can successfully blend heavy-duty cyber- security with a human-centric design, ensuring that high-tech upgrades actively protect vulnerable and elderly voters instead of leaving them behind.

On the business side, LAVIS tackles the immense financial and environmental waste of traditional voting—such as mountains of paper and the massive logistical nightmare of deploying temporary staff. By offering a reusable Gov- Tech infrastructure, it drastically cuts these recurring costs and delivers a strong ROI for the government. Finally, it provides a clear legal blueprint under Article 324 of the Indian Constitution, showing exactly how private startups can drive agile innovation without ever overstepping the state's sovereign control over elections.

The core problem we face is the desperate need for a unified platform that securely and biologically ties a real voter to their ballot, while guaranteeing speed, total transparency, and universal access.

Limitation of the Study:

Here are the key limitations and challenges LAVIS would face specifically from the perspective of operating as a Gov- Tech startup:

1. **Procurement and Bureaucratic Delays:** The public sector is well-known for having very slow and cumbersome procurement processes. Startups have a very hard time surviving the "rhythm mismatch" between their need for rapid, agile deployment and the necessarily slow, conservative pace of government administration.

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(c) Jan – Feb 2026

Original Research Article

2. **Conceptual Framework Limitation:** The LAVIS system is currently a proposed conceptual model without a real-world pilot implementation, which limits the ability to fully assess practical deployment challenges and actual operational performance.
3. **Limited Survey Sample Size:** The primary data evaluating public trust and usability relies on a relatively small survey group of 86 respondents, which may not entirely represent broader demographic and geographic diversity.
4. **High Initial Capital Costs for Hardware:** Since LAVIS is a hardware solution that requires physical infrastructure (RFID smart cards, biometric scanners, and localized PBD hard drives), it is also subject to the classic problems of a hardware startup. Unlike software solutions, hardware startups require much more initial capital investment, longer times to develop prototypes, and are at great risk of financial ruin if large product volumes have to undergo expensive redesigns or retrofits.
5. **Trust and Legal Barriers:** While the system is designed to stay within constitutional limits, it is a huge challenge to persuade statutory authorities (such as the Election Commission) and the public at large to trust a private startup's proprietary hardware solution with the democratic process.

Objective of the Study:

Specifically, the study aims to rigorously assess the proposed system against seven core operational objectives outlined in the original LAVIS architectural design.

1. **Achieve Zero Impersonation:** To see if the five-factor authentication sequence (KYC, RFID cards, facial recognition, and biometric) actually eliminates the statistical probability of duplicate voting.
2. **Establish an Unbreakable Audit Chain:** To analyze how the system generates a cryptographic QR code to maintain a secure chain of custody from the booth to the final tally.
3. **Ensure Universal Voter Access:** To make sure the biometric options are inclusive for manual laborers and the elderly. Additionally, because the local Polling Booth Database (PBD) hardware is compact and low-maintenance, we want to evaluate its potential deployment in remote villages or Indian Embassies to easily facilitate NRI voting.
4. **Promote Dynamic Economic Efficiency:** To investigate how replacing manual processes with reusable Gov- Tech hardware cuts down on workforce burdens and recurring election costs for the government.
5. **Restore Public Trust:** To determine if taking human error out of verification and proving outcomes mathematically can help rebuild faith in the Election Commission.
6. **Maintain Absolute Ballot Secrecy:** To look at the data sanitization protocols (like auto-deleting live photos) to ensure voter privacy is strictly protected.
7. **Guarantee Offline-First Stability:** To review the compartmentalized database setup to ensure the system is completely immune to remote internet hacks and network outages on voting day.

Hypothesis of the Project:

Based on the proposed LAVIS architecture and current electoral vulnerabilities, this study operates on the following hypotheses:

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(c) Jan – Feb 2026

Original Research Article

H1: Using a multi-layered, five-factor authentication framework will drop the statistical probability of voter impersonation to near zero.

H2: An "offline-first" database hierarchy that is physically separated from the internet will effectively neutralize remote hacking and mass data manipulation during the election

H3: Generating a deactivated Cryptographic QR Audit Trail will allow court to mathematically verify election disputes without ever compromising the secrecy of the individual ballot.

H4: A Gov- Tech startup can provide this authentication infrastructure while strictly complying with Article 324 of the Constitution by keeping a hard boundary between identity verification and actual election management.

Review of Literature:

Over the last twenty years, election security has evolved from simply digitizing paper ballots to building tough, multi-layered hardware defenses. We learned early on that combining smart cards and fingerprint scanners drastically cuts down on fake votes, and that wiring these biometric sensors directly into voting machines completely eliminates human interference (Maiya et al., 2018).

However, because centralized cloud databases are highly vulnerable to hackers, experts warn that we must also protect voter privacy with mathematically bulletproof audit trails to truly earn public trust (Marky et al., 2024). This is exactly why the latest research heavily backs layered models like LAVIS, which securely combine RFID tokens, live biometric, and heavy cryptography (Chowdhury et al., 2025). The best part is that real-world tests show these dual-step checks—like pairing a face scan with a second form of authentication—actually boost voter trust and satisfaction past 90% without making the voting process frustrating to use (Egocheaga et al., 2024).

Research Methodology:

This study uses a mixed approach, combining a technical systems evaluation, a doctrinal legal analysis, and primary survey data.

First, we conducted a granular architectural review of the LAVIS functional design, tracking the flow of data from the initial voter registration all the way to the generation of the final cryptographic audit trail. Second, we benchmarked this architecture against traditional manual setups and existing e-voting models.

To ground the research in real-world feasibility, we incorporated primary survey data from 86 respondents to gauge public demand and trust in biometric voting. We also ran a detailed cost-comparison analysis to measure the socio-economic impact and financial sustainability of deploying the hardware. Finally, we applied a strict legal review to ensure the system could realistically operate under Article 324 of the Indian Constitution and the Digital Personal Data Protection Act of 2023, Representation of People Act 1951.

1. *Proposed Method Workflow of Five-Factor Verification*

The proposed system introduces a five-step verification process to make voting more secure while keeping the existing voting system intact.

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(c) Jan – Feb 2026

Original Research Article

Step 1: KYC and Biometric Registration (1st Verification)

Around 6–12 months before elections, voters complete KYC to receive a Smart Voter ID. Existing voters use their old voter ID as a **Special Reference Number (SRN)** linking their identity to fingerprint and iris data. Biometric details are first sent to a secure cloud for sorting and duplicate detection, then stored offline in the **Standing Database (SDB)**. Time and location records prevent fake mass registrations. New voters receive a fresh SRN, and voters aged 18–21 provide extra age proof to prevent underage registration.

Step 2: Smart RFID Voter ID (2nd Verification)

After KYC, voters receive an RFID- enabled Smart Voter ID containing the SRN. The card activates only on election day in the voter's constituency and automatically deactivates afterward to prevent cloning or misuse.

Step 3: Face Recognition (3rd Verification)

At the polling station, tapping the Smart ID retrieves voter details from the **Polling Booth Database (PBD)**. A live photo is matched with the stored image, and the captured image is deleted immediately after verification to protect privacy.

Step 4: Biometric Verification and Voting Access (4th Verification)

The voter completes fingerprint or iris verification using data stored in the PBD. Only after successful face and biometric verification is the voting machine enabled, ensuring unauthorized access is prevented.

Step 5: Cryptographic QR Audit Trail (5th Verification)

After voting, authentication-linked vote data is securely stored in an encrypted booth-level folder and converted into a cryptographic QR record. This remains locked unless legally authorized for verification or recount without re-election**.**

+ Voters receive an SMS confirming successful vote casting.

The Workflow:

The process starts 6 to 12 months before voting day. Citizens link their existing Voter IDs to their biometric, which are saved as compressed files. Next, they are issued a Smart Voter ID card that remains dead and deactivated until the morning of the election, which stops data thieves from skimming the cards.

On election day, the voter taps the card at the booth. The local machine rapidly checks their face against the stored photo and then requires a fingerprint or iris scan. The major shift here is that the biometric scanner talks directly to the EVM. It bypasses the human polling officer entirely. Finally, as the vote is cast, the system silently generates a heavily encrypted, deactivated QR code that legally ties the voter to their ballot—but only a court can ever unlock it if fraud is suspected because its too secret even for Electoral authority.

2. ***Database Architecture and Workflow***

- **Cloud Server:** Handles online KYC data with time and location metadata for sorting and duplicate detection, protected by a firewall. After verification, only essential voter details are sent to the offline SDB and Smart ID printing unit. Internet is needed only up to this stage.

ISSN: P-2455-0515
E- 2394-8450

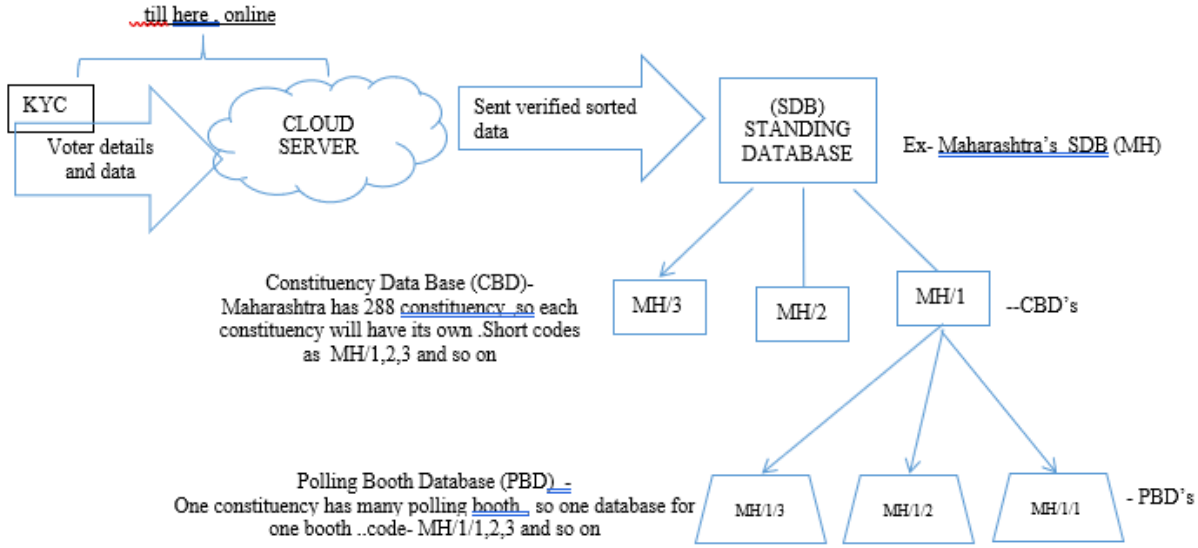
Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(c) Jan – Feb 2026

Original Research Article

- **SDB:** The main offline state database storing all voters on secure disks, performing biometric de-duplication and stopping new entries 10–15 days before elections. Backup systems and security algorithms reduce hacking risk unless physically tampered.
- **CDB:** After cutoff, the SDB divides voter data constituency-wise into CDB segments that function independently during elections while remaining internal SDB compartments.
- **PBD:** Each CDB further splits data booth-wise (500–2000 voters). Compact storage devices are sent one day before polling, acting as the primary offline verification database, supported by backup storage and encrypted QR audit folders.
- **Workflow & Transparency:** Data moves from cloud verification to SDB sorting, then to CDB and PBD for offline polling. Encrypted audit copies are stored at higher levels, and booth-level result publication strengthens public verification and transparency



Data Analysis and Interpretation:

1. Primary Survey Analysis and Interpretation

When we surveyed 86 respondents about the LAVIS prototype, the market demand for better technology was obvious:

61.6% of people strongly believed that voting fraud currently happens in India.

A massive 76.7% said biometric verification would be highly useful, with 72.1% calling it the absolute most secure method available (vastly beating out traditional ballot boxes and standalone EVMs).

Ultimately, 67.4% explicitly wanted a biometric system like LAVIS to completely replace the current setup, citing the elimination of bogus voting and increased transparency as their main reasons.

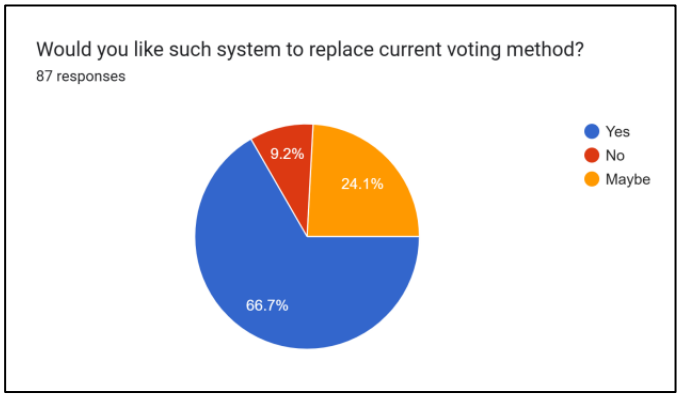
ISSN: P-2455-0515
E- 2394-8450

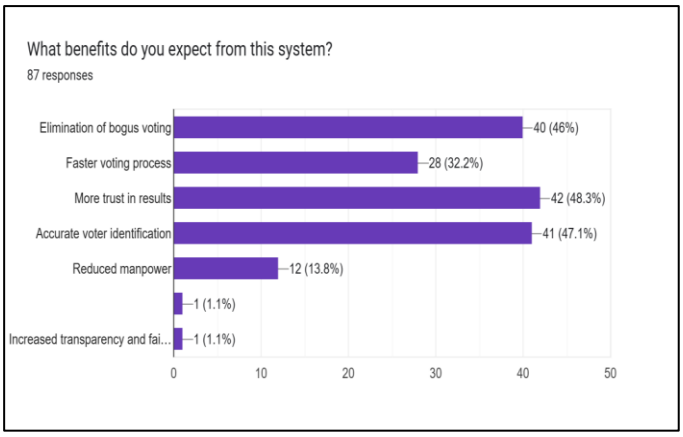
Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(c) Jan – Feb 2026

Original Research Article





2. Unit Economics & Financial Sustainability:

LAVIS involves an upfront cost of about ₹17,000–₹28,500 per polling station for devices and RFID cards, but it sharply reduces manpower expenses. Traditional stations spend ₹45,000–₹50,000 on multiple officers, whereas LAVIS needs only one Presiding Officer and one technical assistant, costing ₹15,000–₹18,000. Across nearly 10 lakh stations, this could save ₹27,000–₹35,000 crore annually, meaning the system recovers its cost within one or two election cycles.

3. Legal Go-To-Market Strategy:

Article 324 gives full election control to the constitutional electoral authority, so private firms cannot run elections. LAVIS stays within limits by acting only as a technology vendor. It does not frame policy, conduct voting, or declare results—it simply provides biometric verification and secure audit support for official use.

Overall Interpretation:

The findings suggest strong public demand for a more secure voting process, with most respondents supporting biometric verification and showing willingness to adopt a system like LAVIS to reduce fraud and improve transparency. Despite moderate initial costs, the system is financially viable due to major savings in manpower, allowing recovery within one or two election cycles. Importantly, LAVIS remains legally compliant by acting only as a technology support tool for identity verification and audit transparency, while election authority stays fully with the constitutional body.

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(c) Jan – Feb 2026

Original Research Article

Challenges:

Despite it is rigorous design, the massive transition to LAVIS presents profound operational challenges:

1. **Biometric Failures:** Studies on large systems show that manual laborers and elderly voters often have worn-down fingerprints, leading to high "False Rejection Rates."
2. **Lost Hardware:** Handing out millions of RFID cards guarantees that thousands will be lost, stolen, or damaged right before election day.
3. **Catastrophic Breakdowns:** Because the PBDs rely on physical hard drives, they can be dropped, damaged in transit, or suffer mechanical failures, which would immediately halt voting at that booth.
4. **Bureaucratic Resistance:** The public sector is notoriously slow to adopt new technologies, and introducing proprietary startup hardware into the democratic process will inevitably face intense political scrutiny.
5. **Dual Registration in Different States:**
   A voter may attempt to obtain multiple voter registrations in different states to enable cross-state impersonation.

Remedies:

To ensure absolute long-term viability, the following rigorous fallback protocols and remedies must be permanently implemented

1. **Multi-Modal Options:** To fix the fingerprint issue, the system mandates that every booth has an iris scanner. Iris patterns do not wear down from manual labor, giving voters a seamless backup option.
2. **The Help-desk Override:** If a voter loses their card or all biometric fail, they are sent to the "LAVIS Help-desk." The Presiding Officer can manually verify their identity against the master electoral roll. Once cleared, the officer generates a single-use, time-bound electronic token to temporarily unlock the EVM so the citizen can still vote.
3. **On-Site Redundancy:** To prevent a broken hard drive from ruining the day, a perfectly cloned backup copy of the PBD disk is legally required to be dispatched to every single polling station.
4. **Open Source Transparency:** To overcome political resistance, the core cryptographic algorithms used by the startup must be open-source and regularly audited by state cyber-security teams to prove there is no hidden bias in the code.
5. **Inter State Sorting of SDB**
   After the cutoff period, state SDBs can use a secure shared cloud platform for inter-state biometric matching. Any duplicate registrations detected can be removed or flagged for verification, and the process can be completed within a few hours, Even track of migration of voters and of place of data can be assessed on automation.

Conclusion:

The strength of any democracy depends on how fair and trustworthy it is voting process is. Today, with rising concerns about impersonation, human error, and public distrust, it’s clear that traditional systems need a serious

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(c) Jan – Feb 2026

Original Research Article

upgrade. The Layered Authentication and Voting Integrity System (LAVIS) presents a practical and realistic solution designed for modern governance.

LAVIS introduces a structured five-step authentication process that reduces mistakes and minimizes bias in voter verification. it is offline-first database design protects the system from cyber- attacks and technical failures, making it more secure and reliable. At the same time, it is cryptographic QR-based audit trail allows election results to be verified mathematically—without ever revealing how an individual voted.

Most importantly, LAVIS proves that strong security, cost efficiency, and voter-friendly design can work together. As a forward-looking Gov-Tech model aligned with Article 324, it offers a way to reduce fraud, cut administrative costs, and most crucially, restore public confidence in the democratic process.

References:

1. *Chowdhury, M. T., Tanim, S. A., Shrestha, T. E., Hossain, M. F., & Bhuyan, M. H. (2025). Enhancing electoral integrity: A multi-layered approach to electronic voting security using Arduino and biometric authentication. Lecture Notes in Networks and Systems, 1299, 643–654. Springer. https://doi.org/10.1007/978-981-96-3358-6_47*
2. *Egocheaga, J., Angulo, W., & Salas, C. (2024). VOTUM: Secure and transparent e-voting system. In Proceedings of 9th International Congress on Information and Communication Technology - ICICT 2024 (pp. 89–99). Springer. https://doi.org/10.1007/978-981-97-4581-4_8*
3. *El Emary, I. M. M., Brzozowska, A., & Maśloch, P. (Eds.). (2025). Digital synergy: Innovative approaches of management in ICT era. CRC Press. https://doi.org/10.1201/9781003440406*
4. *Maiya, K. G., Vineesha, T., Veena, G., & Sujay, S. N. (2018). Secured electronic voting system using biometrics. International Journal of Engineering Research & Technology (IJERT), 6(13). https://doi.org/10.17577/IJERTCONV6IS13110*
5. *Marky, K., et al. (2024). Hybrid online voting systems. Proceedings of the IEEE Symposium on Security and Privacy.*
6. *Reddy, J., Nikhil, S., Sathisha, C., Karur, S. A., & Sidramappa. (2016). Centralized voting system using smart card and biometric. International Journal of Engineering Research & Technology (IJERT), 4(21).*

Cite This Article:

Mr. Mishra A. & Mrs. Sawale P. (2026). *Digital Synergy in Governance : A Gov-Tech Startup Model for Human-Centric, Sustainable, and Transparent Electoral System through Lavis* **In Educreator Research Journal: Vol. XIII (Issue I),** pp. 183–191