

# End-to-end verifiable voting for developing countries - what's hard in Lausanne is harder still in Lahore

Hina Binte Haq<sup>1,2</sup>, Syed Taha Ali<sup>2</sup>, and Ronan McDermott<sup>3</sup>

<sup>1</sup> National University of Computer and Emerging Sciences, Islamabad, Pakistan.

`hina.haq@nu.edu.pk`

<sup>2</sup> School of Electrical Engineering and Computer Sciences (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan.

`taha.ali@seecs.edu.pk`

<sup>3</sup> MCDIS `ronan@mcdis`

**Abstract.** In recent years end-to-end verifiable voting (E2EVV) has emerged as a promising new paradigm to conduct evidence-based elections. However, E2EVV systems thus far have primarily been designed for the developed world and the fundamental assumptions underlying the design of these systems do not readily translate to the developing world, and may even act as potential barriers to adoption of these systems. This is unfortunate because developing countries account for 80% of the global population, and given their economic and socio-political dilemmas and their track record of contentious elections, these countries arguably stand to benefit most from this exciting new paradigm. In this paper, we highlight various limitations and challenges in adapting E2EVV systems to these environments, broadly classed across social, political, technical, operational, and human dimensions. We articulate corresponding research questions and identify significant literature gaps in these categories. We also suggest relevant strategies to aid researchers, practitioners, and policymakers in visualizing and exploring solutions that align with the context and unique ground realities in these environments. Our goal is to outline a broader research agenda for the community to successfully adapt E2EVV voting systems to developing countries.

**Keywords:** end-to-end verifiable voting · developing countries

## 1 Introduction

In recent years end-to-end verifiable voting (E2EVV) has emerged as a revolutionary new paradigm to enable secure and transparent elections [8]. E2EVV voting systems preclude implicit trust in administrators, polling staff, and voting machines, and instead make voters themselves active participants in auditing the election and certifying its results - “the Holy Grail for electronic voting” [82]. These systems are backed by expert bodies [55] and have been piloted in numerous small-scale mock elections and pilots [37] [89] [76], some large-scale politically

binding elections - Australia in 2016 [18] and, most notably, nationwide deployment in the Estonian parliamentary elections in 2019 [30]. This technology is also on the cusp of commercialization[17].

As these systems transition to the mainstream, we consider it an opportune moment to revisit gaps in the research literature, particularly with regards to deploying these systems in developing countries - environments which would arguably benefit most from the superior integrity and trust guarantees offered by these systems. E2EVV systems thus far have primarily been designed for the developed world, where it is largely assumed that there is a sufficient infrastructure for elections, voters are largely literate and relatively technically sophisticated, and dispute resolution mechanisms are reliable and effective. These assumptions do not necessarily translate to the developing world and may even act as potential barriers to adoption of E2EVV systems in these countries.

To motivate this study, we consider the fact that the overwhelming majority of the global population - approximately 80% - hails from the developing world [87]. Distrust in democracy and electoral processes runs high in many of these countries [56], and election fraud has resulted in mass protests [48], political deadlock [75], and violence [35]. Some of these countries have introduced electronic voting systems, and, in several, results have proved controversial [22].

We believe that E2EVV systems, with their potential to restore trust and confidence in electoral processes, have a vital role to play in the developing world. In recent years there have even been public calls to explore application of this technology in countries including Brazil [10], Pakistan [40] and India [19].

In this paper, we make the following contributions:

- We contend that certain fundamental assumptions implicit in the design of E2EVV systems developed thus far conflict with ground realities in developing countries. To make these assumptions explicit, we highlight the manifold challenges in adapting E2EVV systems to these environments.
- This reorientation opens up significant new ground. We identify various social, political, technical, operational, and human concerns specific to E2EVV systems in developing countries and frame specific research questions.
- We suggest potential strategies for the way forward based on relevant trends and success stories in developing countries as well as re-purposing solutions from research literature. Our goal is to aid the community to devise solutions that are appropriate to the unique ground realities of the developing world.

There is a considerable body of research on the challenges of deploying election technology in the developing world [38] [5]. To the best of our knowledge, we are the first to focus specifically on adapting *E2EVV systems* to the socio-political realities and infrastructure in these countries. One of our primary contributions is a detailed review of the literature, election experiences, and news reports from the developing world.

We believe this is a critical research gap, addressing which requires close collaboration between researchers, technologists, practitioners, and policymakers. We hope our paper stimulates exciting and impactful new thinking and research and extends the benefits of E2EVV voting systems to the developing world.

## 2 Background and Prior Work

In this section, we briefly describe E2EVV voting systems, we motivate the case for their application in the developing world, and we discuss prior work.

### 2.1 End-to-End Verifiable Voting Systems

E2EVV systems are a promising new class of voting systems which offer voters the benefits of automation, ease of vote-casting and quick reporting of results, along with stringent cryptographic guarantees of voter privacy and correct computation of the tally. Numerous such systems have been proposed over the years for precinct-based and Internet voting [8]. We summarize next the high-level workings of a representative system to convey to the reader a non-technical and intuitive understanding of end-to-end verifiable voting.

On the day of elections, our citizen, say Alice, arrives at a polling station and identifies herself as an eligible voter. She makes her candidate choice on a voting terminal. The machine records and encrypts her vote and issues her a **printed receipt**, bearing a unique serial number and a cryptographic commitment to her vote. This receipt allows her to later verify that her vote has been correctly processed and counted. However, the receipt does not reveal Alice’s choice of candidate and she cannot use it to sell her vote.

However, Alice may suspect the machine is malfunctioning or has been tampered with. In this case, she avails an option to force the machine to reveal the cryptographic parameters it used to encrypt her vote. This step effectively ‘spoils’ her ballot but allows her to double-check that the machine is operating correctly. She can repeat this step several times until she is ready to cast her vote. In the parlance of E2EVV systems, Alice is now confident that **her vote has been cast as intended**.

When polls close, election staff post copies of all receipts online. Alice uses the serial number to navigate to her receipt. If anyone has tampered with her vote, she can detect it by comparing the receipt to the physical copy she holds in her hand, and can file a complaint using her physical receipt as hard evidence. This gives her confidence that **her vote has been recorded as cast**.

E2EVV systems usually employ two key techniques to tally results in a privacy-preserving manner: systems such as Prêt à Voter [71] and Scantegrity [21] rely on mixnets to anonymize and decrypt cast votes which are then added. The other approach, exemplified by STAR-Vote [13], employs homomorphic encryption to aggregate encrypted votes and decrypt only the tally. Both processes offer voters and observers cryptographic proofs of correct operation. Alice can use these proofs to verify that **her vote has been tallied as recorded**.

These three guarantees span all critical steps of the election life-cycle, and empower users to verify the integrity of the process for themselves. By empowering voters to verify the integrity of the process themselves, E2EVV represents a dramatic improvement over traditional ‘black box’ voting machines.

Because of space constraints, we have eschewed technical details and refer the reader to [8] for the same.

## 2.2 Prior Work

There is little work specifically on E2E<sub>EVV</sub> systems and the developing world. Exceptions include E2E<sub>EVV</sub> systems Threeballot, Twin [73] and Aperio [29], which are geared to provide verifiability in “minimally equipped election environments”. These systems are of considerable interest due to their novel paper-based design which precludes any use of technology or cryptography. Unfortunately there has been no effort to adapt or pilot these systems in a developing country. Moreover, they lack the highly desirable benefits of automation such as less spoiled votes, prompt reporting of results, and enfranchisement of marginal communities [79].

There is, however, a considerable body of research on the application and challenges of electronic voting in the developing world which is relevant to our purposes. This includes feasibility studies [51], holistic frameworks [63], cost benefit analyses [58], and adoption studies [9] [5]. Some studies focus on specific topics, such as economic determinants of voter behaviour [57] or technical concerns [7]. There are case studies on e-voting in individual countries [10] [42], and efforts to adapt insightful metrics, such as the E-Voting Readiness Index [50].

This literature contains several findings, which generalize to E2E<sub>EVV</sub> systems and which, as we noted earlier, clash directly with the ground realities in technologically advanced countries. For instance, in the developing world resources and infrastructure for elections is commonly inadequate [51] [63] and countries often face severe financial constraints [10] [51] [58]. Governments may also lack technical, administrative, and operational capacity to conduct elections [51] [10]. Election management bodies often face issues of autonomy [72] [6]. The political environment may be volatile which affects conduct of elections [58]. Corruption and election fraud are systemic and transparency and accountability are lacking [57] [58] [10]. Voters may be suspicious of election technology and acceptance and adoption can be problematic [9] [5] [20].

Any effort to introduce E2E<sub>EVV</sub> systems has to engage with these fundamental ground realities. We explore these themes in more detail in the following sections.

## 3 Motivation

The vast majority of the world’s population, a staggering 80%, live in the developing world [87], covering the landmass of Africa, Latin America, and much of the Middle East and Asia. These include six of the world’s ten most populous countries, namely India, Indonesia, Pakistan, Brazil, Nigeria and Bangladesh [87]. Despite significant variance in size, demography, history, and culture, many of these countries face similar economic and socio-political problems: widespread poverty and inequality, low literacy, poor governance, systemic corruption, and dependence on foreign institutions [86]. Elections are routinely contentious and frequently result in political deadlock, street protests, and violence [56].

For instance, in Pakistan, major rigging allegations in the general elections of 2013 resulted in mass protests and a public sit-in by a major opposition party [68]. Likewise, in 2014, the Bangladesh saw a national strike lasting 85 days

and a violent crackdown on opposition workers. Opposition parties boycotted the election and over half the seats went uncontested [75]. Opposition boycotts, street protests, and civil unrest, also featured recently in Venezuela [44].

Perceptions of rigging can also trigger major political disruptions and take on life-threatening consequences. Allegations of “terrible fraud” were a key justification for the recent military coup in Myanmar, where army officials claim to have identified some 10.5 million irregularities in the voter list used in the last general elections [35]. The violence following the coup resulted in over 700 deaths and more than 3,300 people detained.

Technology has often been introduced, with mixed results, to resolve this issue of trust. Reported improvements in India include a significant decline in electoral fraud, a more competitive electoral process, and increased participation of marginalized groups in society [79]. Automated counting in Philippines corresponded with dramatic reduction in result compilation time. [78].

However, there are frequent discrepancies and irregularities which undermine trust in technology. In 2017, the Supreme Court of Kenya nullified election results citing irregularities in the results transmission system [16]. In Pakistan, in 2018 the results transmission system broke down inexplicably on the night of elections, raising extreme suspicion [84]. In Azerbaijan, introduction of a smartphone app in 2013 to report election results backfired when it released the election results the day before the actual election [14]. In India, numerous incidents were reported in different polls where electronic voting machines ‘malfunctioned’ by recording all votes in favour of the ruling party, no matter which choice the voter made [26]. In 2018, the introduction of untested voting machines in Democratic Republic of Congo was strongly opposed by opposition parties, and thousands of machines were subsequently destroyed in an act of arson [64].

Researchers have sought to explain these “unintended consequences” of election technology in terms of a “fetishization of technology” [22], or a silver bullet [27], which distracts stakeholders from rigorous assessments and stringent checks and balances in the overall ecosystem. This lack of attention can render election processes even more vulnerable than before.

To situate the potential contribution of E2EVV systems, it is helpful to differentiate between electoral efficiency and transparency as two desirable yet distinct outcomes of using election technology [88]. Unfortunately, there is a marked tendency to prioritize efficiency over transparency, and favor a “black box” approach which concentrates trust “away from the many” and into the “hands of the few”. We anticipate that E2EVV systems - by incorporating security and integrity as core design features of the system - can help redress this balance between electoral efficiency and public transparency.

Similar sentiments have recently been voiced in the developing world, namely Brazil [10], Pakistan [43] [39], and India [19], where security professionals, researchers, and civil society organizations have urged election authorities to explore the adoption of E2EVV systems to restore credibility of electoral processes. Indeed, very recently in India, some 11 opposition parties unanimously passed

resolutions affirming that the existing EVMs do not comply with “democracy” principles in that his or her vote is not verifiable [1].

## 4 East is East and West is West: Misplaced Assumptions, Knowledge Gaps, and Other Challenges

As we noted earlier, the design of most E2E<sub>EVV</sub> systems is based on implicit assumptions which hold true for technologically advanced countries and do not necessarily translate easily to developing regions. A key goal in this section is to make these assumptions explicit by describing the challenges and knowledge gaps relevant to these environments. We divide these into four categories: structural constraints, social and political factors, human factors, and technical and operational concerns. We also include issues which are generic to adapting election technology and are well studied, but which may become more pronounced or take on added dimensions for the case of E2E<sub>EVV</sub> systems.

### 4.1 Structural Constraints

**Shoestring Budgets:** Developing countries routinely suffer from severe financial constraints, and, due to large populations, election funding can take on disproportionate dimensions compared to other government priorities, such as poverty alleviation, and healthcare. For instance in 2018 general elections in Pakistan cost 21 billion PKR ( 175 million USD) [45], comparable to the annual allocation for healthcare at 25 billion PKR ( 208 million USD) and almost quarter the education spending at 97 billion PKR ( 808 million USD) [33].

Expensive technology interventions further strain these shoestring budgets. For instance, upgrading voting machines with paper trails in the Indian context cost 32 billion INR ( 492 million USD) [41]. Nationwide deployment of electronic voting machines in Pakistan are estimated to cost 350 billion PKR (2 billion USD), almost three quarters the national GDP [2]. These realities can foster undesirable trends: to quote the UN Secretary General, “techniques and systems that might cause a State, in the conduct of its own elections, to be financially dependent on donors” [22].

There is therefore a pronounced need to develop compact and minimalist E2E<sub>EVV</sub> systems in a low-cost, sustainable manner, along the lines of India’s famous voting machines. Perhaps, existing minimal FPGA-based E2E<sub>EVV</sub> solutions like VoteBox Nano could be adapted for these settings [59]. A modular design approach would further maximize options to recycle components.

The research community can contribute with open-source tools, software packages, libraries, kits, or hardware platforms to facilitate the development of such projects, similar to the ElectionGuard [17] effort or the wide availability of blockchain platforms like Hyperledger or Ethereum.

Another promising direction is to develop E2E<sub>EVV</sub> solutions which integrate with existing voting systems in developing countries. This is the design approach behind Scantegrity [76]. Recently, Mohanti et al. adapted risk limiting audits for

Indian voting machines [52]. **Is it possible to upgrade Indian or Brazilian machines in a similar cost-effective manner for verifiability?**

**Resource and Infrastructure Woes:** Developing countries frequently suffer from resource shortages, including lack of essential equipment, IT systems, labs and storage facilities. Infrastructure problems include lack of utilities especially electricity, telecommunications, and Internet service. Expertise issues include poor access to IT expertise, quality technical support, and shortage of qualified polling staff. There is a dire need for indigenous capacity building and reforms for restructuring of broader management structures.

However there is encouraging evidence that technology can be creatively deployed within these constraints. India and Brazil’s homegrown electronic voting machines are largely considered a success story. The under-banked in sub-Saharan Africa bypassed traditional banking and leap-frogged onto mobile money, accounting for 70% of the global 1 trillion USD mobile money market [62]. Alternatives need to be researched in response to specific challenges encountered in each country.

To consider how infrastructure issues relate to E2E/VV systems, we consider the specific example of the online bulletin board requirement. Whereas Internet access is ubiquitous in the developed world, in developing countries basic cell phone coverage and Internet access can be limited and unreliable due to network faults or traffic congestion. Our question becomes: **what kind of public bulletin board for vote verification could we offer in Asia and Africa where cell phone coverage is unreliable and an estimated 1.3 billion people still use dumb phones [23]?**

The popularity of text-messaging services (like SMS) may offer a way forward. These services have been successfully used in phone-based financial services, voter registration drives, social security programs, and mass vaccination efforts. Researchers have proposed SMS-based primitives including one time pads, return codes and transaction authentication numbers to harden remote voting systems [12] which may potentially be leveraged for a bulletin board service over SMS.

Infrastructure constraints may also be leveraged by malicious actors (e.g. a spoofing attack which misdirects voters to a fake bulletin board [81]).

## 4.2 Social and Political Factors

**Electoral Fraud is Systemic:** It is well documented that developing countries often suffer from poor governance and endemic corruption [61], trends which also manifest in electoral practices. Vote buying, coercion, and suppression are commonplace: the 2013 Afrobarometer survey noted that 48 percent of voters in 33 African countries reported fearing violence during elections, whereas 16 percent reported being offered cash or goods for their vote. In Pakistan, in 2013, a watchdog body reported electoral irregularities at over 21,000 polling stations [31]. In 2017, the Supreme Court of Kenya nullified election results citing irregularities in the results received over the results transmission system [16]. In 2017, in Venezuela, vendor Smartmatic disclosed that general results were “manipulated” and off by a count of at least 1 million [32].

Persistent and systemic security threats in these environments necessitate additional security measures. **But what about attack scenarios caused by deploying E2EVV technology?** Poll workers can collect discarded receipts, voters may sell their receipts or surrender them on intimidation. Malicious parties could then manipulate the corresponding votes without fear of detection.

A potential countermeasure is a verifiable encrypted paper audit trail (VEPAT) which incorporates additional checks performed by independent auditing authorities [69]. These bodies could routinely verify the correspondence between the audit trail and receipts posted on the bulletin board. Solutions allowing voters to delegate the verification process to a trusted party [77] also merit investigation.

Another relevant concern: **how would E2EVV systems fare in environments where polling day security is lax and family voting, impersonation, and collusion are common?** These trends are well-documented in developing countries: a patriarch or another party obtains credentials of multiple legitimate voters and then casts votes on their behalf. Poll workers can cast votes on behalf of absentee voters. It is not surprising that the earliest election technology systems implemented in countries like Ghana, Nigeria, Kenya, DRC, Somaliland, Afghanistan are biometric voter verification systems. Following up on this, **can we integrate biometric checks with E2EVV systems in a binding way to provide enhanced security guarantees of voter identification, presence, and eligibility verifiability? Could these be done in a way that is universally verifiable?**

**The Politics of Perfection:** There is often lack of debate and rigorous analysis of election technology in developing countries. The Venezuelan government has described its electronic voting system as “the most perfect voting system in the world”[49]. The Indian Election Commission reacted angrily to reasonable security analysis of its voting machines [67]. **Can developing countries who see their particular EVM systems as already “perfect” even begin to accept the need to evolve towards evidence-based elections and E2EVV systems? What kind of outreach effort would this entail?**

### 4.3 Human Factors

**Linguistic and Cultural Diversity** Developing countries, marked by their linguistic diversity (dialects may change every few miles) ethnic diversity and varying cultural constructs [85], require localization of both the voting system and accompanying receipts and verification mechanisms, which adds complexity to processes. People are often hesitant to carry out important transactions, especially ones involving finances in an unfamiliar language. Language can potentially act as a barrier to election participation and disenfranchise certain voters [66]. **Can E2EVV systems cope with the sheer scope and scale of linguistic localization needed for many developing countries?**

**What about Mental Models?** Mental models are essential to help foster public understanding of novel technology and customize interventions. Most voters think about a voting system first and foremost in terms of how to vote [4]. Mental models for technology as well as attitudes and perceptions have been known

to vary considerably in developing countries for certain applications [36]. **What would mental models for E2EVV systems look like for voters in developing countries? How would these models vary, given the wide-ranging social and cultural diversity in these regions?**

**Usability - the highest hurdle?** Research points to correlation between low literacy (including digital literacy) and rejected ballots [34]. Extending usability recommendations (for low-literacy voters in traditional electronic voting) to the E2EVV scenario is not trivial. A preliminary study involving Helios, Pret-a-Voter, and Scantegrity II found that it took almost twice as long to cast a vote, a significant number of voters failed to cast votes, and many did not realize their errors [3]. Voting success rates in developing countries will likely be lower. **How will this play out in developing countries with massive populations and already long queues, where voter or poll workers have been known to die of exhaustion [80]. Can E2EVV systems be designed to emphasize usability in low-literacy contexts??**

Moreover, recent testing and ‘live’ applications of E2E systems have resulted not just in consistently low rates of voter verification but even lower rates for those who actually report discrepancies [53]. Chipcase [24] observe that non-literate populations avoid complex functions and this reinforces the assumption that if a step is optional, it will be skipped [28].

**Can we develop technical solutions to simplify or automate the vote verification process in the context of developing countries?** Researchers have proposed solutions to make verifiability universal [54] [70], delegate it, or enable mass verification by bundling multiple receipts for batch verification [15]. Could these be made more usable and practical for low-literacy users? Perhaps we could leverage research on textual key-fingerprint representations [25] and hash visualization [11] for this purpose. Research also shows that motivating messages can persuade voters to verify [60]. **What sort of nudges or incentives could we devise to encourage voter verification in developing countries?**

#### 4.4 Governance and Operational Factors

##### **E-Governance and Digital Transformation:**

Developing countries often lack overarching institutional frameworks for governance, suffer from fragmentation and poor coordination of processes, and low uptake of digital technology. In the context of E2EVV systems, this can manifest in multiple ways. We consider the simple example of effective management of cryptographic credentials, recognized as problematic in trials of E2EVV systems. Logically, this problem will be more pronounced in developing countries.

Moreover, end-to-end verifiability and voter privacy are sensitive to human behaviour in the protocol. Errors in use of cryptography could result in exposure of critical data and undermine the integrity of the whole process. It would be helpful to characterize the set of behaviours under which security can be preserved and also highlight explicit scenarios where it fails [46]. **How can we customize the key management and ceremonies to ensure separation of duties and principles of least privilege?**

**Cybersecurity - Canaries in the Coalmine?** Developing countries lag far behind in terms of capacities and resources for cybersecurity. For E2EVV, therefore, vulnerabilities such as DDoS attacks on bulletin boards become more likely. Attacks on electoral information systems are on the increase and are often conducted by external or state actors with significant resources. The design of E2EVV systems must take this into account. **Can E2EVV systems be designed to be more "tamper-proof" (to use the infosec term) as well as "tamper-evident" (the elections term)?**

**Legal Framework** In case of E2EVV systems, it should be legally binding on election management bodies (EMBs) to issue a receipt to every voter, upload all the receipts on a bulletin board within a stipulated time frame, verifying the results through the software provided to observers, making the software open source, sharing of public cryptographic parameters, conduct of Risk Limiting Audits. without which the security guarantees of E2EVV systems become moot.

As noted in the Brazil experience, “important judicial decisions are not based on scientific research; they are often based on the personal opinions of judges who have no understanding of (election) technology.[10]” Accordingly, for disputes involving technologies, defining the requirements for the admissibility of evidence, training the judiciary to handle the intricacies of E2EVV systems based digital evidence is of utmost importance. Moreover, comprehensive and high quality voter instruction is critical to uptake of a radically new system like E2EVV and typically falls under the auspices of the legal framework ensuring equal access. [8] Transparency and accountability are key to minimizing risk, and risk perception.

Although it is not possible to have a generic, one-size-fits-all set of requirements for E2EVV, we need to avoid the idea that all countries can do completely different things - fundamentally, technical requirements, and regulations, laws, and indeed constitutions, must deliver E2EVV systems that are fully compliant with universal principles.

#### **Toothless or Compromised EMBs and Ineffective Dispute Resolution**

Many EMBs lack the regulatory teeth and political autonomy needed to ensure that incumbent government and political parties do not interfere in their duties, and they often operate under political influence and fear.[83]. The lack of technical skills means there is unreliable implementation of technical protocols.

In developing countries, disputes over elections results often act as triggers for mass protests, violence, political deadlock and animosity, often times bordering civil war. This situation can be exacerbated when judicial mechanisms cannot resolve these disputes in a timely, fair and transparent manner [56].

Another implicit assumption is that evidence of election malfeasance, if available from an E2EVV system, and provided to the authorities, would facilitate interventions by said authorities. There are various examples of EMBs in developing countries ignoring compelling evidence of electoral malfeasance. Moreover, in developing countries it is not uncommon for electoral processes to be politically controlled and for EMBs to be compromised. For instance, in Mozambique in 2014, the regime turned biometric registration into a technique of manipulation, suppressing registration in opposition areas by provisioning inadequate

equipment and under-trained teams. In Kenya, over a million dead citizens were maintained in the voter register in an attempt to rig the polls [47]. Venezuelan election results were internally ‘manipulated’ by at least 1 million votes [32].

In such situations, E2EVV systems, with their rigorous security guarantees, may well be perceived as an existential threat. **In this regard, to what degree could E2EVV systems be corrupted in a compromised ecosystem? Moreover, could E2EVV systems possibly be developed to offer guarantees against a compromised ecosystem? Could solutions be developed to render these ecosystem issues transparent as well?**

**Electoral Integrity Theatre** The security guarantees of E2EVV systems become moot if the verification step is not undertaken, and the system is not auditable. If legislatures in developing countries cannot pass and enforce laws that are sufficiently detailed to address both core and ancillary processes, E2EVV risks becoming nothing more than the electoral equivalent of "security theatre" [74]. To quote Park et al “*Auditability* alone isn’t enough”, and “must be accompanied by *auditing* to be effective. [65]”. **There is therefore a need for public awareness on this issue and devising satisfactory mechanisms, policies, and legislation to enforce electoral integrity checks.**

**Belt and Braces** E2EVV systems need to be made resilient with backup ‘belt and braces’ mechanism. For instance, Star-Vote is a system which incorporates Risk Limiting Audits to an E2EVV system. Risk Limiting Audits have even been devised to cater to on-ground realities in India. It is essential to work in close engagement with existing systems on the ground.

## 5 Conclusion

Despite formidable recent efforts to portray elections management in the United States as dysfunctional and corrupt, the reality in developed countries is of well-resourced EMBs, reliable infrastructure, competent staff, reliable dispute resolution mechanisms, digitally literate voters and empowered civil society and media stakeholders. In contrast, we have outlined systemic problems in most developing countries in most of those aspects. Accordingly, the underlying assumptions of most E2EVV systems mean that implementation of E2EVV in developing countries is an uphill task. Some of the solutions we have discussed thus far even clash with one another. For example, if biometrics need to be introduced to deal with corruption and fraud, that would increase the cost, thereby counteracting efforts to reduce that cost. Significant research with an explicit focus on developing country contexts is needed in order to bridge this gap. Given the potential benefits of E2EVV, we believe this pivot is well justified. We hope our paper is a catalyst in this regard.

## Acknowledgement

This research was supported by the ‘Research for Social Transformation & Advancement’ (RASTA), a Pakistan Institute of Development Economics (PIDE) initiative, through Competitive Grants Programme Award [Grant No. CGP-01-127/2021].

## Bibliography

- [1] Will Fight Against Voting Machine "Misuse", Say 11 Opposition Parties (Sept 2022), <https://www.ndtv.com/india-news/will-fight-against-electronic-voting-machine-evm-misuse-say-11-opposition-parties-3252460>
- [2] Abbasi, A.: EVM-based general polls may cost up to Rs 350 bn. The News International (Dec 2021), <https://www.thenews.com.pk/print/920735-evm-based-general-polls-may-cost-up-to-rs350-bn>
- [3] Acemyan, C.Z., Kortum, P., Byrne, M.D., Wallach, D.S.: Usability of voter verifiable, end-to-end voting systems: Baseline Data for Helios, Prêt à Voter, and Scantegrity {II}. In: 2014 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 14) (2014)
- [4] Acemyan, C.Z., Kortum, P., Byrne, M.D., Wallach, D.S.: Users' mental models for three end-to-end voting systems: Helios, prêt à Voter, and Scantegrity ii. In: International Conference on Human Aspects of Information Security, Privacy, and Trust. pp. 463–474. Springer (2015)
- [5] Agbesi, S.: Adoption of e-voting system to enhance the electoral process in developing countries. In: Evaluating Media Richness in Organizational Learning, pp. 262–273. IGI global (2018)
- [6] Ahmad, S., Abdullah, S., Arshad, R.B.: Issues and challenges of transition to e-voting technology in Nigeria. Public Policy and Administration Research **5**(4), 95–102 (2015)
- [7] Akinyokun, O.N.: Secure voter authentication for poll-site elections in developing countries. Ph.D. thesis, University of Melbourne (2020)
- [8] Ali, S.T., Murray, J.: An overview of end-to-end verifiable voting systems. Real-world electronic voting: Design, analysis and deployment **173** (2016)
- [9] Alomari, M.K.: E-voting adoption in a developing country. Transforming Government: People, Process and Policy (2016)
- [10] Aranha, D.F., van de Graaf, J.: The good, the bad, and the ugly: two decades of e-voting in Brazil. IEEE Security & Privacy **16**(6), 22–30 (2018)
- [11] Azimpourkivi, M., Topkara, U., Carburnar, B.: Human distinguishable visual key fingerprints. In: 29th {USENIX} Security Symposium ({USENIX} Security 20). pp. 2237–2254 (2020)
- [12] Backes, M., Gagné, M., Skoruppa, M.: Using mobile device communication to strengthen e-voting protocols. In: Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society. pp. 237–242 (2013)
- [13] Bell, S., Benaloh, J., Byrne, M.D., DeBeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P.B., Wallach, D.S., et al.: Star-vote: A secure, transparent, auditable, and reliable voting system. In: 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13) (2013)
- [14] Bigg, C., Dilaverli, K.: Official App Releases Azerbaijani Vote Results – A Day Early. Radio Free Europe (Oct 2013), <https://www.rferl.org/a/azerbaijan-election-app-results/25131902.html>
- [15] Bohli, J.M., Henrich, C., Kempka, C., Muller-Quade, J., Rohrich, S.: Enhancing electronic voting machines on the example of bingo voting. IEEE Transactions on Information Forensics and Security **4**(4), 745–750 (2009)

- [16] Burke, J.: Kenyan election annulled after result called before votes counted, says court. *the Guardian* (Sep 2017), <https://www.theguardian.com/world/2017/sep/20/kenyan-election-rerun-not-transparent-supreme-court>
- [17] Burt, T.: New cyberthreats require new ways to protect democracy - Microsoft On The Issues (July 2019), <https://blogs.microsoft.com/on-the-issues/2019/07/17/new-cyberthreats-require-new-ways-to-protect-democracy>
- [18] Burton, C., Culnane, C., Schneider, S.: vvote: Verifiable electronic voting in practice. *IEEE Security & Privacy* **14**(4), 64–73 (2016)
- [19] CCE: CCE Report | Reclaim the Republic (May 2021), <https://www.reclaimtherepublic.co/report>
- [20] Chauhan, S., Jaiswal, M., Kar, A.K.: The acceptance of electronic voting machines in India: a UTAUT approach. *Electronic Government, an International Journal* **14**(3), 255–275 (2018)
- [21] Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A., Vora, P.: Scantegrity: End-to-end voter-verifiable optical-scan voting. *IEEE Security & Privacy* **6**(3), 40–46 (2008)
- [22] Cheeseman, N., Lynch, G., Willis, J.: Digital dilemmas: The unintended consequences of election technology. *Democratization* **25**(8), 1397–1418 (2018)
- [23] Cheney, C.: Want to reach the world’s poorest? Design for dumb phones (Mar 2018), <https://www.devex.com/news/want-to-reach-the-world-s-poorest-design-for-dumb-phones-90993>
- [24] Chipchase, J.: Understanding non-literacy as a barrier to mobile phone communication (2005)
- [25] Dechand, S., Schürmann, D., Busse, K., Acar, Y., Fahl, S., Smith, M.: An empirical study of textual key-fingerprint representations. In: 25th {USENIX} Security Symposium ({USENIX} Security 16). pp. 193–208 (2016)
- [26] Desk, N.H.W.: Why EVMs always ‘malfunction’ in favour of the BJP? *National Herald* (Oct 2019), <https://www.nationalheraldindia.com/india/why-evms-always-malfunction-in-favour-of-the-bjp>
- [27] Electronic voting machines: The promise and perils of a new technology (2011)
- [28] Ellison, C.: Upnp security ceremonies design document for upnp device architecture 1.0. In: UPnP Forum (2003)
- [29] Essex, A., Clark, J., Adams, C.: Aperio: High integrity elections for developing countries. In: *Towards Trustworthy Elections*, pp. 388–401. Springer (2010)
- [30] of Estonia, S.E.O.: General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia, <https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf>
- [31] General Election 2013: FAFEN Observation - Key Findings and Recommendations (Oct 2015), <https://fafen.org/general-election-2013-fafen-observation-key-findings-and-recommendations>
- [32] Faiola, A.: Venezuela election results ‘manipulated’ by at least 1 million votes, polling company says. *Washington Post* (Aug 2017)
- [33] Finance Division, G.o.P.: Federal Budget 2018-2019, Pakistan (2018), [https://www.finance.gov.pk/fb\\_2018\\_19.html](https://www.finance.gov.pk/fb_2018_19.html)
- [34] Fujiwara, T.: Voting technology, political responsiveness, and infant health: Evidence from brazil. *Econometrica* **83**(2), 423–464 (2015)
- [35] Goodman, B.J.: Myanmar coup: Does the army have evidence of voter fraud? *BBC News* (Feb 2021), <https://www.bbc.com/news/55918746>

- [36] Hanel, P.H., Maio, G.R., Soares, A.K., Vione, K.C., de Holanda Coelho, G.L., Gouveia, V.V., Patil, A.C., Kamble, S.V., Manstead, A.S.: Cross-cultural differences and similarities in human value instantiation. *Frontiers in Psychology* **9**, 849 (2018)
- [37] Hao, F., Wang, S., Bag, S., Procter, R., Shahandashti, S.F., Mehrnezhad, M., Toreini, E., Metere, R., Liu, L.Y.: End-to-end verifiable e-voting trial for polling station voting. *IEEE Security & Privacy* **18**(6), 6–13 (2020)
- [38] Hapsara, M., Imran, A., Turner, T.: E-Voting in Developing Countries. In: *Electronic Voting*, pp. 36–55. Springer, Cham, Switzerland (Jan 2017). [https://doi.org/10.1007/978-3-319-52240-1\\_3](https://doi.org/10.1007/978-3-319-52240-1_3)
- [39] Haq, H.B., Ali, S.T.: Electronic voting machines for pakistan: Opportunities, challenges, and the way forward. 1st RASTA Conference (2022), <https://www.pide.org.pk/rasta/wp-content/uploads/Hina-Bint-Haq-Conference-Paper.pdf>
- [40] Haq, H.B., McDermott, R., Ali, S.T.: Pakistan’s Internet Voting Experiment. arXiv preprint arXiv:1907.07765 (2019)
- [41] Rs 3,200 crore granted to EC for EVM paper trail units (2017), <https://economictimes.indiatimes.com/news/politics-and-nation/rs-3200-crore-granted-to-ec-for-evm-paper-trail-units/articleshow/58269901.cms?from=mdr>
- [42] Inuwa, I., Oye, N.: The impact of e-voting in developing countries: focus on Nigeria. *International Journal of Pure and Applied Sciences and Technology* **30**(2), 43 (2015)
- [43] Findings and Assessment Report of Internet Voting Task Force on voting rights of overseas Pakistanis (2018)
- [44] Joe Sterling, F.C., Gillespie, P.: Deadly election day in Venezuela as protesters clash with troops. CNN (July 2017), <https://edition.cnn.com/2017/07/30/americas/venezuela-on-edge-vote/index.html>
- [45] Kiani, K.: The most expensive elections. DAWN (Jul 2018), <https://www.dawn.com/news/1421946>
- [46] Kiayias, A., Zacharias, T., Zhang, B.: Ceremonies for end-to-end verifiable elections. In: *IACR International Workshop on Public Key Cryptography*. pp. 305–334. Springer (2017)
- [47] Kimani, N.: Kenyan poll haunted by the ghosts of voters passed - The Mail & Guardian (Jul 2017), <https://mg.co.za/article/2017-07-14-00-kenyan-poll-haunted-by-the-ghosts-of-voters-passed>
- [48] López, V.: On the frontline of Venezuela’s punishing protests. *The Guardian* (May 2017), <https://www.theguardian.com/world/2017/may/25/venezuela-protests-riots-frontline-caracas-nicolas-maduro>
- [49] Machin-Mastromatteo, J.D.: The most “perfect” voting system in the world. *Information Development* **32**(3), 751–755 (2016)
- [50] Maletić, M., Barać, D., Rakočević, V., Naumović, T., Bjelica, A.: Scaffolding e-voting in developing countries. *Management: Journal of Sustainable Business and Management Solutions in Emerging Economies* **24**(2), 47–62 (2019)
- [51] Maphunye, K.J.: The feasibility of electronic voting technologies in Africa: Selected case examples (2019)
- [52] Mohanty, V., Culnane, C., Stark, P.B., Teague, V.: Auditing Indian elections. In: *International Joint Conference on Electronic Voting*. pp. 150–165. Springer (2019)

- [53] Moher, E., Clark, J., Essex, A.: Diffusion of voter responsibility: Potential failings in E2E voter receipt checking. {USENIX} Journal of Election Technology and Systems ({JETS}) **1**, 1–17 (2014)
- [54] Nandi, M., Popoveniuc, S., Vora, P.L.: Stamp-it: a method for enhancing the universal verifiability of E2E voting systems. In: International Conference on Information Systems Security. pp. 81–95. Springer (2010)
- [55] Securing the vote: Protecting american democracy (2018)
- [56] Norris, P., Frank, R.W., i Coma, F.M.: Contentious elections: From ballots to barricades. Routledge (2015)
- [57] Oganessian, R.: Economic voting in the developing world (2014)
- [58] Okoro, E.: A Cost-Benefit Analysis of Electronic Voting Operations and Capabilities in sub-Saharan Africa
- [59] Oksuzoglu, E., Wallach, D.S.: Votebox nano: A smaller, stronger FPGA-based voting machine (short paper). In: Proceedings of the 2009 USENIX/Accurate Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (2009)
- [60] Olembo, M.M., Renaud, K., Bartsch, S., Volkamer, M.: Voter, what message will motivate you to verify your vote. In: Workshop on Usable Security, USEC (2014)
- [61] Olken, B.A., Pande, R.: Corruption in developing countries. *Annu. Rev. Econ.* **4**(1), 479–509 (2012)
- [62] Onyango, S.: GSMA: 70% of the world’s \$1 trillion mobile money market is in Africa (May 2022), <https://qz.com/africa/2161960/gsma-70-percent-of-the-worlds-1-trillion-mobile-money-market-is-in-africa>
- [63] Osho, L.O., Abdullahi, M.B., Osho, O.: Framework for an e-voting system applicable in developing economies. *International Journal of Information Engineering & Electronic Business* **8**(6) (2016)
- [64] Paravicini, G.: Congo fire destroys thousands of voting machines for presidential election. U.S (Dec 2018), <https://www.reuters.com/article/us-congo-election-fire-idUSKBN1OC0VP>
- [65] Park, S., Specter, M., Narula, N., Rivest, R.L.: Going from bad to worse: from Internet voting to blockchain voting. *Journal of Cybersecurity* **7**(1), tyaa025 (2021)
- [66] Pool, J.: The multilingual election problem. *Journal of Theoretical Politics* **4**(1), 31–52 (1992)
- [67] Rao, G.N.: Democracy at Risk! Citizens for Verifiability, Transparency & Accountability in Elections. Veta (2010), <http://indianevm.com/book.php>
- [68] Reporter, T.N.S.: NA briefed on economic cost of sit-ins. DAWN (Jul 2020), <https://www.dawn.com/news/1569471>
- [69] Ryan, P.Y.: Verified Encrypted Paper Audit Trails. Citeseer (2006)
- [70] Ryan, P.Y.: Prêt à voter with confirmation codes. *EVT/WOTE* **11** (2011)
- [71] Ryan, P.Y., Bismark, D., Heather, J., Schneider, S., Xia, Z.: Prêt à voter: a voter-verifiable voting system. *IEEE transactions on information forensics and security* **4**(4), 662–673 (2009)
- [72] Salimonu, R.I., Osman, W., Shittu, A.J.K., Jimoh, R.: Adoption of e-voting system in Nigeria: A conceptual framework. *International Journal of Applied Information Systems* **5**(5), 8–14 (2013)
- [73] Santin, A.O., Costa, R.G., Maziero, C.A.: A three-ballot-based secure electronic voting system. *IEEE Security & Privacy* **6**(3), 14–21 (2008)
- [74] Schneier, B.: Essays: In Praise of Security Theater - Schneier on Security (May 2021), [https://www.schneier.com/essays/archives/2007/01/in\\_praise\\_of\\_securit.html](https://www.schneier.com/essays/archives/2007/01/in_praise_of_securit.html)

- [75] Shah, A.: Democracy deadlocked in Bangladesh. *Current History* **115**(780), 130 (2016)
- [76] Sherman, A.T., Carback, R., Chaum, D., Clark, J., Essex, A., Herrnson, P.S., Mayberry, T., Popoveniuc, S., Rivest, R.L., Shen, E., et al.: Scantegrity mock election at Takoma Park. In: 4th International Conference on Electronic Voting 2010. Gesellschaft für Informatik eV (2010)
- [77] Simpson, R., Storer, T.: Third-party verifiable voting systems: Addressing motivation and incentives in e-voting. *Journal of information security and applications* **38**, 132–138 (2018)
- [78] Philippine Votes Transmitted in Record Time in Largest Ever Electronic Vote Count (May 2016), <https://www.smartmatic.com/media/article/philippine-votes-transmitted-in-record-time-in-largest-ever-electronic-vote-count/>
- [79] Somanathan, M.: India’s electoral democracy: How EVMs curb electoral fraud. Brookings (May 2019), <https://www.brookings.edu/blog/up-front/2019/04/05/indias-electoral-democracy-how-evms-curb-electoral-fraud>
- [80] The: Voting-made-easy has a cost: Over 400 deaths (May 2021), <https://www.thejakartapost.com/academia/2019/05/07/voting-made-easy-has-a-cost-over-400-deaths.html>
- [81] Tjostheim, T., Peacock, T., Ryan, P.Y.: A case study in system-based analysis: the ThreeBallot voting system and Prêt à Voter. School of Computing Science Technical Report Series (2007)
- [82] Ummelas, O.: World’s Most High-Tech Voting System to Get New Hacking Defenses (2017), <https://www.bloomberg.com/news/articles/2017-07-17/world-s-most-high-tech-voting-system-to-get-new-hacking-defenses>
- [83] Understanding Electoral Violence in Asia (2012)
- [84] Wasim, A.: RTS controversy likely to haunt ECP, Nadra for a long time (Aug 2018), <https://www.dawn.com/news/1424394>
- [85] Weber, S., Davydov, D., et al.: Societal and economic effects of linguistic diversity. *Voprosy Ekonomiki* **11** (2017)
- [86] West, J., Desai, P.: Diverse structures and common characteristics of developing nations. Ingggris: Oxford University p. 39 (2002)
- [87] Population by Country (2021) - Worldometer (May 2021), <https://www.worldometers.info/world-population/population-by-country>
- [88] Yard, M.: Direct Democracy: Progress and Pitfalls of Election Technology. International Foundation for Electoral Systems Washington, DC (2010)
- [89] Zagórski, F., Carback, R.T., Chaum, D., Clark, J., Essex, A., Vora, P.L.: Remotegrity: Design and use of an end-to-end verifiable remote voting system. In: International Conference on Applied Cryptography and Network Security. pp. 441–457. Springer (2013)