ELECTRONIC VOTING MACHINES FOR PAKISTAN: OPPORTUNITIES, CHALLENGES, AND THE WAY FORWARD

Hina Binte Haq, Syed Taha Ali
(CGP #01-127)

RASTA CONFERENCE
Monday 28th & Tuesday 29th March 2022
PC Bhurban, Murree

This document is unedited author's version submitted to RASTA.

RESEARCH FOR SOCIAL TRANSFORMATION & ADVANCEMENT
Pakistan Institute of Development Economics
Islamabad

ABSTRACT

This paper is an attempt to structure the ongoing debate around Electronic Voting Machines (EVMs) and election technology in Pakistan and ground the discourse in research, international best practices, and expert guidelines. EVMs have been used in different countries since the 1960s and have proved highly controversial. A concerning trend has emerged over the last two decades in those various developed countries, including Ireland, the Netherlands, and Germany, have phased out or terminated their EVM deployments over concerns of voter privacy and election integrity. At the same time, deployment of EVMs in developing countries, such as India, Brazil, Venezuela, and Philippines, has yielded mixed results. There is therefore an urgent need to decipher this trend such that we may maximize the gains of these technologies and avoid mistakes made by other countries.

Moreover, revolutionary new technologies have emerged in recent years which enable citizens and observers to verify and audit election results. Technologies such as *end-to-end verifiable voting* and *risk limiting audits* are being developed and piloted in the West, but there is as such, little recognition of the unique challenges in adapting these methodologies in developing countries like Pakistan. There is a need to make these technologies accessible to election stakeholders and to precisely identify the critical research gaps and challenges we need to address in Pakistan. This paper draws together these complementary lines of inquiry and provides a comprehensive vision for election technology in Pakistan

We also present recommendations to address these challenges at every stage. The accompanying roadmap spells out these recommendations in the form of concrete detailed steps that stakeholders need to take. This paper provides a framework for such efforts andis supported by a detailed roadmap which describes the key steps that stakeholders need to take to successfully deploy EVMs and election technology in Pakistan.

PREFACE

We believe introduction of election technology is a viable and very promising option for restoring trust and credibility to our elections. However, this move must not be done in haste: adapting election technology to our unique ground realities in a secure,reliable, and cost-effective manner requires great care, effort, and deliberation on thepart of stakeholders and considerable work on building a supporting ecosystem for the technology. Moreover, we must be cognizant of the key lesson from our prior experiences with election technology: we lack fundamental expertise in this domain and there are critical knowledge gaps in our discourse and strategy. We believe it is vital that we recognize and confront these shortcomings squarely.

This initiative started as an academic research project but has now broadened into an outreach effort thanks to the financial support of the PIDE RASTA grants initiative. We are thankful to the RAC members and project mentors for their constructive feedback which has considerably broadened thescope of our investigation and made it more relevant to the ongoing discourse on Electronic Voting Machines in Pakistan.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

BVM	Biometric Voting Machines
CERT	Computer Emergency Response Team
CNIC	Computerized National Identity Cards
CCE	Citizens' Commission on Elections
DRE	Direct Recording Electronic
DRE-VVPAT	Direct Recording Electronic-Voter Verified Paper Trail
E2E-V	End-to-End Verifiable
ECP	Election Commission of Pakistan
EMB	Election Management Body
EVM	Electronic Voting Machines
IDEA	Institute for Democratic and Electoral AssistanceI
FES	International Foundation for Electoral Systems
IVTF	Internet Voting Task Force
NA	National Assembly
NADRA	National Database Registration Authority
NDI	National Democratic Institute
PCER	Parliamentary Committee on Electoral Reforms
PCOS	Precinct Count Optical Scanning
R&D	Research and Development
RLA	Risk Limiting Audits
RTS	Results Transmission System
RMS	Results Management System
VVPAT	Voter Verified Paper Audit Trail

INTRODUCTION

Elections in Pakistan suffer from poor execution, persistent rigging and fraud, and a pronounced lack of transparency. Polls are routinely contentious and frequently result in political deadlock, street protests, and violence. Such instances undermine citizens' confidence in elected leaders and negatively impact civic participation and trust in democracy (FAFEN, 2018).

Major rigging allegations in the general elections of 2013 resulted in mass protests and a public sit- in by a major opposition party. Lasting over four months, this was the longest protest in Pakistan's history, and caused estimated losses of over USD 5 million (Hussain, 2020). Election watchdog bodyFAFEN reported electoral illegalities and irregularities at over 21,000 polling stations in General Election 2013 (FAFEN, 2013). Almost a decade on, nothing much has changed. In recent by-polls in Daska, 20 election presiding officers were abducted, and the Election Commission of Pakistan (ECP)declared the poll results null and void (Ebrahim, 2021). *Appendix A* gives a quick summary of how General Elections in Pakistan have routinely been contentious. It also gives a brief overview of the key irregularities reported.

In this context, the government's recent push for electoral reforms is a welcome step to restore citizen confidence and trust in elections. Election technology, such as electronic voting machines (EVMs), result transmission system (RTS), and Internet voting have documented benefits at curbingfraud. However, these technologies are prone to fail and may even result in disastrous election day outcomes if deployed without careful research and homework.

The international experience has documented considerable benefits to using EVMs: EVMs dramatically reduce the time and manual effort required for vote tabulation and result reporting andsignificantly mitigate certain types of electoral fraud. EVMs also provide accurate counts by eliminating spoiled ballots. Certain countries document that adoption of EVMs improve voter turnout, empower marginalized communities to vote, reduce electoral expenses, and may even correlate with improved governance.

The disadvantages are also considerable: EVMs are closed systems, prone to malfunction, and can be easily hacked. Whereas EVMs counter certain types of electoral fraud, they may open the door to newand more dangerous attacks. Voters might find EVMs difficult to use. EVMs can be very costly and cannecessitate further significant costs in infrastructure and logistics.

We have significant examples of countries including the Netherlands, Ireland, Kenya, Venezuela, and Russia, where election technology deployments undertaken in haste proved controversial, and in some cases were aborted or failed outright. Our own experience with developing a homegrown Internet voting solution for overseas Pakistani in 2018 illustrates this point. An expert audit commissioned by the Supreme Court of Pakistan identified critical vulnerabilities in every major component of this system (Internet Voting Taskforce, 2018), re-endorsed by Minsait which also undertook an audit of the same system in 2021 (Minsait, 2021). Likewise, the mysterious failure of the result transmission system during the general elections of 2018 cast a cloud of suspicion on the election results (Thomas & Khuhro, 2018).

Critics have repeatedly noted that our own mainstream discussions on election technology lacks essential depth and rigor (Gul, 2021) (Express Tribune Editorial, 2021) (Dawn Editorial, 2021) and ``add little value to the general populace's understanding' (Bari & Muhammad, 2021).' Prior

reportshave also emphasized our lack of critical expertise regarding election technology and urged stakeholders to invest in this domain to prevent such incidents in the future. Deploying election technology is a large-scale exercise which will likely cost several tens of billions of rupees and we cannot afford to make decisions without high quality research, clear thinking, and rigorous debate.

Our primary contribution in this paper is to structure the debate around EVMs and ground it in verifiable facts and international best practices, to effectively "separate the wheat from thechaff". We address fundamental questions: What are the pros and cons of EVMs? Should we deploy EVMs in Pakistan? What are the key challenges we can expect? How do we address these challenges? In this paper, we argue that these negatives of EVMs can be effectively mitigated using a two-pronged approach:

- by adapting state-of-the-art technologies, such as End-to-End Verifiable (E2E-V) voting and Risk Limiting Audits (RLAs) which are specifically designed to audit EVMs and ensure the integrity of their results. There is, unfortunately, yet very little awareness of these technologies and their revolutionary potential in our electoral reforms discourse in Pakistan.

- by exercising due diligence, applying international best practices, strengthening the overall elections ecosystem, developing procedural mechanisms and appropriate checks and balances at every stage. Unfortunately, there is no global standard or formula for deploying EVMs, and each country must carefully adapt these machines to their own unique ground realities and build a supporting ecosystem.

Our second contribution, therefore, is to provide election stakeholders essential insight into new election technologies and to demystify their workings. We provide a detailed layman- oriented description in this report.

Third, we provide a framework within which to develop, trial, and deploy EVMs in Pakistan. We explicitly spell out the technological, human, and sociopolitical challenges we expect and present concrete recommendations to address them. This section of the report is supplemented by a roadmap document which details key steps we need to undertake to successfully introduce EVMs in Pakistan.

Similar feasibility reports and studies have been commissioned numerous times in other countries (e.g. Estonia (General Framework of Electronic Voting and Implementation Thereof at National Elections in Estonia, 2019), Finland (Vaalit, n.d.), NAS (Committee on Science, Technology, and Law et al., 2018) Norway (Ministry of Local Government and Regional Development, 2006), but to the bestof our knowledge, we are the first to conduct a technology-focused study, specifically for a developing country. Developing countries present unique challenges to election technology which are rarely recognized and remain to be comprehensively addressed in elections policy or in the research literature. We believe this document will also be useful and informative to other developing countries considering electronic voting machines.

We are optimistic that this study will clarify the debate around EVMs, provide stakeholders with actionable information to start this national project, and contribute to public confidence in election technology in Pakistan.

1.1 Background

The Road to Electronic Voting Machines

In its earliest consideration of the subject, in 2009, the Election Commission of Pakistan (ECP) commissioned a study to assess the feasibility of Electronic Voting Machines (EVMs). The subsequent report recommended that "use of electronic voting and counting technologies be pursued further, although a final decision on the national adoption of these technologies will remain pending" (Election Commission of Pakistan, 2010). In 2011 the ECP evinced interest in Indian EVMs and evenrequested for a demonstration (India Times, 2011), but later relinquished the idea as any such association may prove controversial. ECP also asked interested vendors to manufacture the EVM according to certain approved specifications. Other interested parties such as academic institutions (COMSATS) and vendors (TIP, KRL, NIE, Smartmatic, and Indra) were also invited to demonstrate their models of EVMs. In 2012, the EVM presented by COMSATS was given a field test in a few pollingstations in by-elections in Multan (Jafri, 2012).

In 2014, ECP announced its intention of shifting to EVMs in a couple of years. It also presented demonstrations of EVM prototypes to political parties and representatives of the media at an event organized for this purpose. A demonstration was staged for the Parliamentary Committee on Electoral Reforms (PCER) which remained ambivalent on the use of EVMs and asked the ECP to come up with concrete and secure proposals for the same. (Correspondent, 2014).

In 2015, ECP held a field test of the Biometric Voting Machines (BVM) EVMs during bye-elections in NA-19, Haripur. The machines verified only 46% of the 15,723 votes cast through BVMs. The reported reasons for failed verifications were unavailability of fingerprints in the NADRA database, invalid or blocked CNICs, and fingerprint detrition (Sadaqat, 2015).

After the promulgation of the Election Act, 2017, an EVM pilot was conducted in NA-4 bye-elections.ECP officials said more than 100 electronic machines would be used in more than 100 polling boothsof 35 polling stations (Imran & Bari, 2017), however details of the pilot are not available publicly. Further ECP made efforts to acquire EVMs Electronic Voting Machines from Smartmatic that ran up to a few thousand dollars per unit (Correspondent, 2017).

The PTI also had another longstanding demand to enfranchise the diaspora, for which it had submitted multiple petitions. (Bhatti et al., 2018) Consequently, an Internet Voting (IV) System was developed by NADRA (on orders of the Supreme Court in early 2018), for overseas Pakistanis, in 10 weeks, at a cost of Rs. 150 million (Bhatti, 2018). This system was not deployed in General Elections,2018 due to security apprehensions highlighted by the IVTF (Internet Voting Taskforce, 2018) constituted by the Supreme Court to undertake an audit of the iVote system. The system was later piloted in the October 2018 bye-elections in 35 constituencies. Another pilot was conducted in December 2018, bye-elections in 1 constituency. The overseas votes of both the pilots were incorporated in the final tally. The elections had a very low overseas voter turnout of around 1% withonly 7,538 votes cast in both the bye-elections. This deployment cost approximately Rs. 95 million. (Election Commission of Pakistan, 2018). EVMs pilot project report was presented in the National Assembly (NA) and Senate in January 2019. Their discussion in parliament however remained pending for 2 years. In 2021, directed by the PM, the Ministry of IT (MoIT) hired Minsait as consultant to audit the Internet voting system. The Spanish firm reiterated IVTFs concerns and said the internet

voting system does not meet international standards and the recommendations of the IVTF have notbeen incorporated in any manner (Minsait, 2021).

The issue of electoral reform resurfaced in late 2020, when the PTI government expressed their intention to introduce Electronic Voting "to ensure free and fair elections". The coming months saw hostility between the government and the ECP, specifically in the aftermath of the senate elections, 2021. President Arif Alvi promulgated an ordinance to amend Section 94 ad Section 103 of the Elections Act 2017, without extensive consultation with the opposition and the ECP. This amendment directs the ECP to enfranchise the overseas Pakistanis as well as begin the procurement to conduct General elections using EVMs (Naqvi & Lodhi, 2021). The opposition disagreed with this decision, citing that technology will only be used to manipulate and rig the elections, with the premise that the staged failure of the Results Transmission System (RTS) in 2018 was also done to manipulate election results (Chaudhry, 2021).

Among the technology related concerns of the ECP is the premature Internet Voting provision for overseas Pakistanis and binding ECP to procure EVMs without determining if these will prove useful in combating rigging. The ECP also fears the proposed amendments such as the proposed role of NADRA in preparing electoral rolls will dilute its constitutional powers and shift them to NADRA which is part of the federal government and not an independent body like the ECP (Correspondent, 2021). The ECP has since formed a technical committee to evaluate the proposal of EVMs on technical, legal, and financial aspects (Khan et al., 2021).

1.2 Literature Review

There is a considerable body of research on the application and challenges of electronic voting technology in the developing world which is relevant to our purposes. This includes feasibility studies (Maphunye & Kealeboga J, 2019) holistic frameworks (Osho et al., 2016) cost benefit analyses(Okoro & Ephraim, 2016) and adoption studies (Alomari & Mohammad Kamel, 2016), (Agbesi & Samuel, 2018). Some studies focus on specific topics, such as economic determinants of voter behavior (Oganesyan & Rafael, 2014) or technical concerns (Jillbert et al., 2003) (Akinyokun & Olukayode Nicholas, 2020). There are case studies on e-voting in individual countries (Aranha et al.,2018) (Herstatt et al., 2014) (Inuwa et al., 2015) and efforts to adapt insightful metrics, such as the E-Voting Readiness Index, to the developing world (Aljarrah et al., 2016) (Maleti et al., 2019).

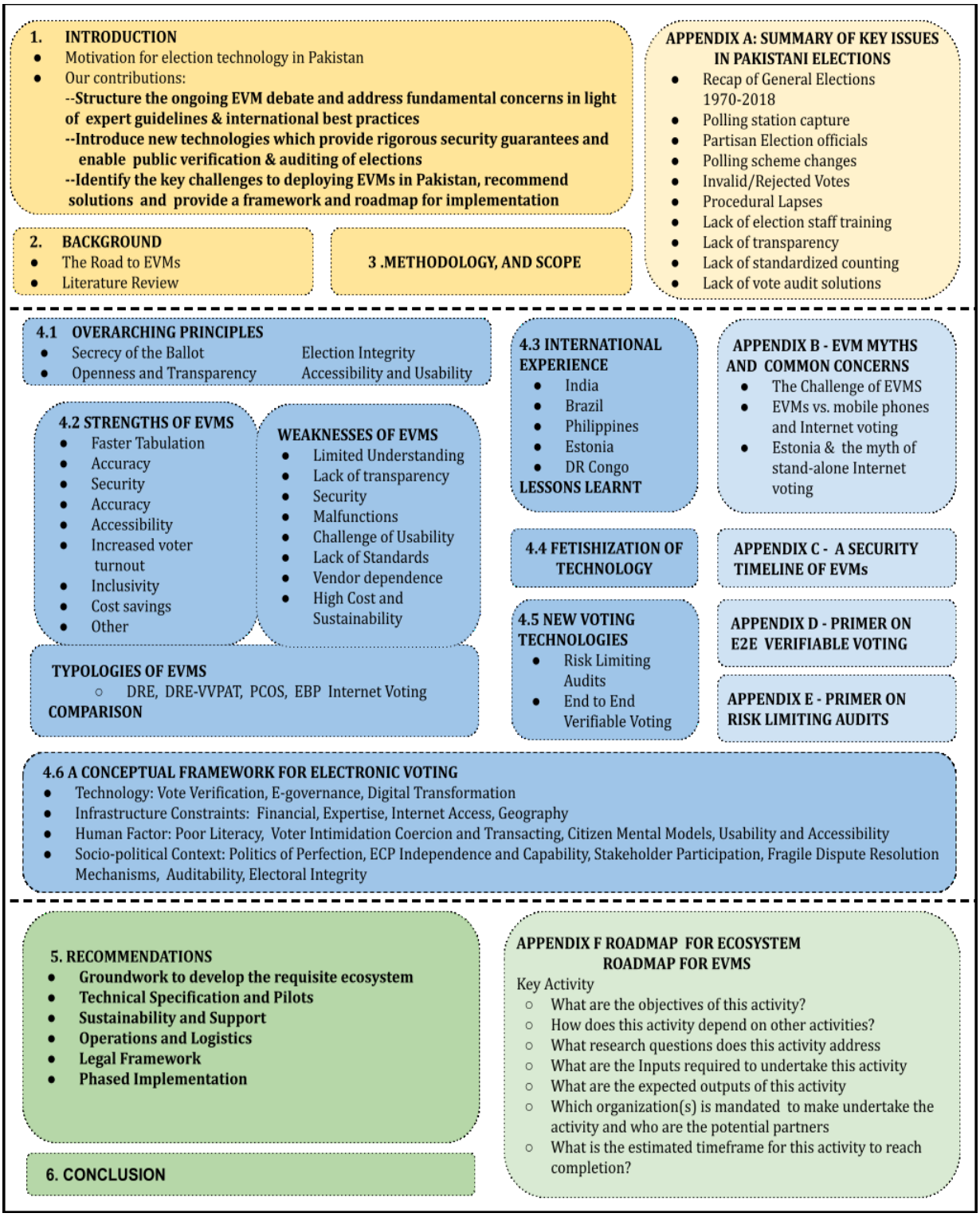
Other work produced by indigenous researchers (Arooj et al., 2016) (Solehria et al. 2011) (Khan et al. 2011) (Khawaja et al. 2016) (Ghaffar et al. 2017) attempts to approach the subject, but there is lack of an in-depth study.

There is also a wealth of supplementary material for practitioners (Reynolds et al., 2008) (Goldsmith et al., 2013). Internationally, there are numerous studies, recommendations and handbooks providing general guidelines, introducing best practices and standards in the context of E-Voting These include reports by the National Academy of Sciences (National Academies of Sciences & Engineering, and Medicine and others, 2018), Council of Europe (Council of Europe, 2016), International Idea (Introducing Electronic Voting: Essential Considerations, 2011), Carter Center (Center & Carter, 2012) , Ace Project (ACE, 2020) etc. However, there is a lack of any work that focuses on the unique social, economic, and political predicament in Pakistan. We explore these themes in more detail in the following sections.

METHODOLOGY, SCOPE AND LIMITATIONS

This paper follows the structure depicted in Fig.1. The findings are divided into six main sections, each supplemented with appendices of relevant material.

Figure 1: Structure of the paper



First, we define the overarching principles that should govern the initiative to shift to EVMs.

In the second part we note documented strengths and negatives of EVMs and present a comparativesummary of common EVM models deployed in developing countries.

Third, we present case studies of countries such as India, Brazil, and Philippines, followed by the lessons to learn from these deployments.

Fourth, we highlight common pitfalls, explaining the phenomenon of "fetishization of technology"andhow it distracts stakeholders from rigorous assessments and stringent checks and balances in the overall ecosystem, rendering election processes even more vulnerable than they were without technology.

Fifth, we describe the novel concept of public verifiability and how risk-limiting audits, and verifiable voting can mitigate outstanding security concerns regarding EVMs and ensure trust in poll results.

Sixth, we present a holistic framework to identify the challenges to address as we move towards EVMs. Our national discourse to date has focused primarily on EVM units, and there is unfortunately, very little recognition of the enormous task of building a supporting ecosystem for EVMs. This ecosystem is critical to the success of the overall project and the effort and costs involved in setting it up can easily dwarf that of procuring the EVMs themselves.

We also present recommendations to address these challenges at every stage. The accompanying roadmap spells out these recommendations in the form of concrete detailed steps that stakeholdersneed to take. The roadmap lists key activities, including research assessments, pilot studies, hackathons, and demos and suggests timelines, references, resources at every step and highlights dependencies and concerns. We also identify critical research gaps to be addressed.

There is very little existing research in this domain and this section highlights our novel research contribution. To compile data for this section, our team studied election technology deployments in India, Brazil, Philippines, and various African countries. We initiated conversations with key stakeholders in Pakistan, including the ECP, the Ministry of Science and Technology, NADRA, the Ministry of IT & Telecommunications, and the National Institute of Electronics. We interacted with international EVM vendors including Smartmatic, Dominion, Indra, and Miru and participated in demos of their machines. We consulted international election technology experts and academics working in this domain. And we participated in seminar programs organized by civil society, election activists, and field workers in India.

Here we also specify the limitations of our study. Our paper is essentially a position paper which advocates the use of cutting-edge election technologies in Pakistan, demonstrates their security properties, and describes the way forward. We do not claim to answer all questions regarding EVMs. Instead, we envision our contribution as the first and foundational step towards a culture of researchto support election technology in Pakistan.

There are considerable research concerns that still need to be addressed - which we describe in the following sections and in the roadmap - questions pertaining to EVM design, feature specifications, user interface, usability studies, procedures and protocols, legal issues, costing analysis, and concerns related to ecosystem and infrastructure. Most of this work is unique to Pakistan and it has never been done before.

FINDINGS AND DISCUSSION

3.1 Overarching Principles

Here we define the overarching principles that should guide the deployment of Electronic Voting Machines in Pakistan. For successful deployment, it needs to be ensured that the following principlesare not forgone:

Secrecy of the Ballot: A transition to an Electronic Voting system should not compromise ballot secrecy. The right to a secret ballot is etched in the Universal Declaration of Human Rights (Article 226), and Elections Act, 2017 (Section 94) (Elections Act, 2017).

Election Integrity: The new system should entail stringent checks and balances that ensure that election integrity is not compromised. Auditability measures need to be integrated into the election procedures such as public ceremonies, EVM inventory, functioning and log audits, cryptographic checks for verifiability, paper trails to name a few.

Openness and Transparency: Engaging stakeholders at every step of the decision-making process is necessary. The ECP needs to maintain transparency in all their undertakings. A key feature is to democratize the debate around EVMs, as the US civil rights icon, Bayard Rustin, stated, “If we desire a society that is democratic, then democracy must become a means as well as an end.” (Making Real thePromises of Democracy, 2020)

Accessibility and Usability: The upgraded election process should be a service to citizens: It should increase transparency, as well as accessibility and usability for voters. Thus far, there has been no study that indicates how the voter experience in Pakistan could be altered with the introduction of Electronic Voting Machines. Pilots offer a good opportunity to collect data for such studies. Given thelingual diversity within Pakistan and the low literacy rate, it is important to develop a system that does not discourage or hinder voters from voting due to their linguistic background or low literacy. Accessibility extends the concept of usability to differently abled citizens. Special provisions need tobe made for such voters, which ensures ballot secrecy and election integrity.

Sustainability refers to practical concerns and costs of deploying EVMs. Pakistan is a developing country and efforts should be made to emulate the model of India and Bangladesh, which chose to invest in indigenous expertise and developed low-cost machines suited to their environments. Moreover, EVMs should be usable for at least three to four election cycles, which necessitates that the technology be broadly aligned with future trends and new innovations.

It is important to develop an appreciation among the stakeholder of these properties and the different requirements they entail in an Electronic Voting system. Researchers have identified that some of these properties have an inherent conflict with other properties. For the avid reader we discuss this in detail in Appendix B.

Conventional Electronic Voting Machines: Strengths and Weaknesses

Electronic voting encompasses any system in which the casting of a vote, the recording of a vote or the tallying of the votes is done through electronic means. These processes may further be aided by information and communication infrastructure for the transmission and dissemination of results.

EVMs are gaining popularity in developing nations. While India, Brazil and Philippines boast a country wide deployment that is now at least a decade old in each of these countries, Namibia has recently become the first African nation to transition to EVMs. Paraguay, Panama, Bangladesh, and Mexico have all begun to experiment with electronic voting machines.

This section discusses documented pros and cons of EVMs. The strengths of electronic voting mainlydeal with electoral efficiency and improved security due to reduced human intervention:

1. **Faster Tabulation and Reporting of Results:** EVMs provide a dramatic reduction in time taken required for vote counting and result tabulation. In the Philippines, in recent elections,two-thirds of the election results were counted and transmitted within 2 hours after polls closed (Manila & The Philippines, 2016). Automation also eliminates much of the manual effort required to count votes. In Indonesia, in the 2019 polls, in the laborious vote counting process over five hundred and fifty poll workers passed away due to exhaustion and thousands more were hospitalized (Endy Bayuni, 2019). This has propelled Indonesia to consider Electronic Voting Machines for future Elections. EVMs can play a significant role in such an environment to reduce human effort.

2. **Accuracy** EVMs provide more reliable and accurate tabulation of results by eliminating human error in recording and counting votes. Spoilt ballot papers can considerably skew the outcome of an election. In General Elections 2018, the number of spoiled votes exceeded the margin of victory in over 30 constituencies (*FAFEN General Election Observation 2018 Result Assessment and Analysis*, 2018). Researchers document that human error in hand counts can be up to 2 percent (Ruth & Hodges, 2012). Such procedural and counting errors in the 2018 general elections led the ECP to order a recount in 70 constituencies (*FAFEN General ElectionObservation 2018 Result Assessment and Analysis*, 2018).

3. **Security:** Conducting the typical paper-based election exercise involves a lot of human resources to the order of hundreds of thousands of workers. These workers are to be trustedto not manipulate the results. EVMs take away the power from the polling station officials, by automating the process of recording the votes and counting the votes, reducing polling station fraud significantly. In India electronic voting has set about a marked reduction in election related corruption and fraud, especially in areas with high political volatility, where re-polling and recounts were routine due to allegations of rigging (Debnath et al., 2017). Thefaster tabulation process also significantly reduces the time window within which rigging can be undertaken.

4. **Accessibility:** Electronic Voting Machines offer new opportunities to provide voters multilingual support at the press of a button. EVMs can also be designed with increased

accessibility options, including audio aids, Braille support, and other technologies for peoplewith disabilities.

5. **Increased Voter Turnout:** In certain cases, the introduction of EVMs has been reported to increase voter interest and participation. For instance, the Philippines witnessed a historic voter turnout, where 81% of the registered voters cast a vote in 2016 when electronic votingwas adopted (Kagawaran, 2022). This has been linked to increased user satisfaction and better overall user experience, which leads to increased voter trust and confidence.

6. **Inclusivity** Studies on elections in India report that EVMs empower women, scheduled castesand other marginalized communities to cast their votes and participate in the political process (Somanathan & Madhavan, 2019) (Debnath et al., 2017).

7. **Cost Savings:** Although initial transition to EVMs requires huge capital investment, studies from Estonia and Brazil indicate that operational costs of elections decline considerably in the long run due to decreased human resource requirement, not requiring to print ballot papers to name a few. Moreover, countries such as India have devised effective strategies which include developing very low-cost hardware-based machines and by staggering national elections over a longer timeframe to reduce operational costs.

8. **Other Positive Indicators:** Introduction of EVMs has also evidenced certain positive social indicators. The introduction of EVMs in some regions correlates with improved governance and increased electoral competitiveness. This pattern is highlighted in research which indicates competitive electoral races In Brazil infant healthcare outcomes noticeably improved because of the cost savings due to EVMs (Fujiwara & Thomas, 2015). In India, electronic voting correlated with improved overall supply of electricity and a decline in crime in some regions. (Debnath et al., 2017)

   Despite demonstrated benefits, EVMs have several disadvantages, which have resulted in several technologically advanced countries, including Germany, Ireland, and the Netherlands discontinuing their EVM deployments.

9. **Limited Understanding for Public** The ability to understand the inner working of EVMs requires technical knowledge which is only possessed by a small fraction of the electorate. Itwas due to this reason that the German Supreme Court ruled the use of EVMs as unconstitutional, requiring that *"essential steps of the voting and of the ascertainment of the result can be examined reliably and without any specialist knowledge of the subject".* (The Wire,2021)

10. **Lack of Transparency** Arguably the most problematic aspect of popular EVM types is that they are technically black boxes which do not give stakeholders transparency into their inner workings, limited audit, and forensic capabilities. This is unfortunately due to the inherent tension which exists between voter privacy and election integrity (Orcutt, 2016). Individual ballots must be anonymized to safeguard voter privacy, and this leaves them vulnerable to rigging and manipulation within the EVM. A recent report by the Citizens' Commission on Elections, an Indian civil society organization, comprising contributions by international

authorities in elections security, concluded that the Indian EVMs, due to lack of transparency
in their present form, are "*near-fatal for electoral democracy*" (CCE, 2021).

11. **Security** While EVMs are known to reduce polling station frauds, they also create new vectors for rigging elections. EVMs are unfortunately very easy to hack and present an opportunity for large-scale manipulation of election results without leaving any physical trace. Almost every EVM that has been analyzed has been successfully compromised by researchers to leaksensitive vote information and alter vote counts, including various machines certified and used in the US, Brazil, Netherlands, and India.

    The premier hacking symposium DEFCON runs an annual election technology hackathon called the Voting Village. In the 2020 Voting Village event, over a hundred certified electronicvoting machines were hacked. The organizers of the event noted in their report: "As disturbing as this outcome is, we note that it is at this point an unsurprising result." (Newman, 2019)

12. **Prone to Malfunction**: EVMs occasionally suffer serious technical difficulties due to extremeweather conditions and unexplained circumstances, which can frustrate voters and delay results. In the 2018 midterm elections in the US, ballot tabulators could not read ballots due to humidity in North Carolina and Alabama (NBC News, 2018). In New York City, election officials stated that rain had wet the ballots and caused scanning machines to jam. In India, 3- 10% of voting machines are known to fail mock polls held prior to field deployment (POONAM AGARWAL, 2019). In polls in 2018, the Election Commission of India had to provision 15 percent extra EVMs during polls to compensate for faults because of extreme heat, light, and dust. (CCE, 2021)

13. **Challenge of Usability:** EVMs may be challenging to use in developing countries like Pakistan. Usability is also a complex topic and there are several facets to consider: for instance, usability generally correlates with computer literacy and technical skills within citizenry, the scope and effectiveness of voter education and outreach efforts and is typicallyassisted by piecemeal and gradual deployment strategies (ODIHR, 2013). The physical designand the voting protocol of EVMs must be adapted to cater to voters. A wide range of factors must be carefully considered, including legibility of text on the machines, the time it takes tocast a vote, how the machine deals with unintentional undervotes, etc. Adapting EVMs to theunique ground realities of a developing country like ours will likely require considerable research and pilot testing.

14. **Lack of Standards and Certifications:** There are no clear and authoritative standards or certifications for EVMs as there are for various other technologies. The reason for this is thatEVMs are a complex phenomenon which must be adapted to the unique ground realities of every society. A whole host of socio-political, cultural, logistical, and financial considerationscome into play. Attempts to transplant election technology on a large scale without rigoroushomework are quite likely to fail and incur heavy political and financial costs, as observed inIreland (Wrong, 2013) and Kenya (Melia & Byrne, 2012).

15. **Vendor Dependency and lock-in** Lack of self-sufficiency in election technology have been known to create situations where national election management bodies became dependent

    on vendors or technologies, with a possible risk of compromising electoral processes.

Moreover, EVMs typically contain electronic, or software components sourced from differentcountries, and this dependency can pose potential security risks to elections.

16. **High Costs and Sustainability Concerns**: Many developing countries lack the resources forexpensive EMV deployment and often depend on international donors for financial assistance and engage international consultants to provide technical expertise. This situation can be costly, its sustainability is questionable in the long run, thereby preventing countries from developing indigenous capacity. Moreover, EVMs manufactured in foreign countries or containing vital parts sourced from such countries raise important issues about security and trustworthiness of these machines and concerns about foreign interference. Such concerns have recently been raised in the US by the three largest EVM vendors, Dominion Voting Systems, Hart InterCivic and Election Systems & Software, who have sought explicit guidancefrom the Department of Homeland Security and supporting legislation, regarding their dependency on components manufactured by companies based in or having links with Chinaand Russia (Ross, 2020) (Alexa Corse, 2019).
17. **Wholesale Rigging** Indeed, manipulating scales is extremely difficult with paper ballots, as each attack is geographically limited. Influencing, modifying, or destroying a considerable number of votes requires significant resources, time, and money, and is likely to generate witnesses and tangible proof. In comparison, the electronic voting process is completely opaque to the typical voter, more error-prone than many believe, and much, far morevulnerable to undetectable large-scale attacks.

Typologies of Electronic Voting Machines

In this section, we describe the electronic voting options available. We briefly describe each system and share the experiences of developing countries with the system, including the country's process of implementation, successes with the system, and main challenges that arose.

As paper ballots were blamed for persistent fraud the turn of the century saw the adoption of voting machines. The US was the first to use mechanical lever voting machines back in 1890. By the 1960s they were used by more than half of the US voting population. The 60s saw the first use of the machine-readable Optical scan or mark sense voting systems by which votes are recorded by meansof marks made on the ballot card. The system uses a light beam to scan the marked paper ballots and tally the results. Another popular technology in the 60s was punch card systems, in which voters marked their vote by using a punch device to punch a hole in the ballot card. Tabulation was later done by a computerized counting machine. The increasing sophistication of computer technology saw the first electronic voting system delivered for the Utah State Legislature in 1970. (*Electronic Voting | US House of Representatives: History, Art & Archives*, 2022)

Since then, technology has advanced, and various types of electronic voting machines have been developed. In this section we give an overview of the different types of voting machines being used around the world, along with details about where they are deployed and estimated costs. We followit by brief case studies.

Precinct Count Optical Scanning (PCOS) Machines: In Precinct Count Optical Scanning (PCOS) Machines, voters cast their votes on ballot papers that are specifically designed to be input to the

PCOS machine. These ballot papers can be marked using pens or electronic markers. The marked papers are fed to the Optical Mark Recognition (OMR) based device, which scans each ballot and counts the votes for each candidate. This technology is similar to that used to mark standardized tests. The marked ballots are generally counted at the precinct where they were cast, however they can be gathered at a centralized counting location. The Philippines has a country-wide deployment of PCOS systems, where each PCOS Machine it procures from Smartmatic, has an estimated price of around 1600 USD. (Gotinga, 2015)

Direct Recording Electronic (DRE) Voting Machines: DRE machines use a screen as an output device which shows the potential candidates. This screen display is accompanied by buttons and/ora touch panel, which are used as an input device as well, used to cast votes. The machine directly records these cast votes in its memory. DRE Voting Machines do not produce a physical print out of the vote; therefore, the voter has no guarantee that their vote was recorded as cast. The machine may transmit individual votes or vote totals. The saved voting data can be transmitted via the internet, the detachable memory components or through printed ballot paper. These are the primary machines used in Brazil. The cost of each machine is estimated to be approximately USD 700. (Jokura,2021)

Direct Recording Electronic with Voter Verified Paper Audit Trail (DRE-VVPAT) Voting Machines: These machines have a screen or a display which shows the potential candidates to the voters. This display is accompanied by buttons and/or a touch panel, which are used as an input device used to cast votes. The machine directly records these cast votes in its memory. DRE-VVPAT Voting machines also produce a physical print out of the vote. This paper trail, formally called VVPAT, is meant to serve as physical proof of the votes that have been cast. The voter can view the Voter Verified Paper Audit Trail (VVPAT) to make sure the vote was cast as intended and put it in a sealedballot box. DRE-VVPATs are used extensively in the USA and nationwide in India for national level elections. DRE-VVPATs used in India cost USD 660 approximately. (Press Trust India, 2014)

Electronic Ballot Printers The voter marks his choice using a button on the machine itself, which produces a token, or a paper print out of the vote. This printed ballot is then placed in a ballot box either automatically by the voting machine or manually by the voter. At the end of polling, all the tokens/ballots are manually counted. This option is being explored by Bangladesh, where it is expected to cost USD 2,400 per machine. (Irani, 2018)

Remote Internet Voting This system entails using the Internet to relay the vote to a centralized tallying server. The voters vote in an unsupervised environment such as home or public computers and devices, voting kiosks set up for this purpose. Due to infrastructural, financial, literacy, and societal challenges, no developing country has implemented internet voting. Currently, Estonia is theonly country in the world that uses Internet Voting for politically binding national level elections. (e- Estonia, 2017)

Comparison

In this section we offer a comparison of the strengths and weaknesses of various electronic voting machines. There is no such thing as a perfect electronic voting system. The following table summarizes the common strengths and weaknesses of several electronic voting methods in comparison to paper-based alternatives. An improvement over the paper-based system is

indicated by 'Yes' while the impairment of a function is indicated by 'No'. If the function or property remains unaffected it is indicated by 'Not affected'. While if the outcome is dependent on the specifications of the model of EVM it is represented by 'Maybe'.

Table 1: Comparison of EVM Typologies

Comparison Metrics, with paper-based votingas baseline	**PCOS**	**DRE**	**DRE-VVPAT**	**ElectronicBallot Printers**	**Remote Internet Voting**
Counting and Tabulation Speed Increased	Yes	Yes	Yes	Yes	Yes
Improved Accuracy of Results	Yes	Yes	Yes	Yes	Yes
Flexibility to adapt to various electoral systems	Yes	Yes	Yes	Yes	Yes
Simplification of Ballot Paper Design	No	Maybe	Maybe	Maybe	Maybe
Increased Ease of Access to System	No	Maybe	Maybe	Maybe	Yes
Increased Voter Turnout	Not affected	Not affected	Not affected	Not affected	Yes
Accessible to Mobile Voters	No	No	No	No	Yes
Usability	No	No	No	No	Maybe
Reduction in Polling Station Fraud	Yes	Yes	Yes	Yes	Not affected
Greater accessibility	No	Maybe	Maybe	Maybe	Yes
Multi-language support	No	Yes	Yes	Yes	Yes
Elimination of Rejected/ Spoilt Ballots	Yes	Yes	Yes	Yes	Yes
Reduced Voter Coercion/ Buying	Not affected	Not affected	Not affected	Not affected	No
Increases Openness and Transparency	Maybe	No	Maybe	Maybe	No
Easily understood by non-technical people	Maybe	No	Maybe	Maybe	No
Maintains Secrecy of the vote	Maybe	Maybe	Maybe	Maybe	No
Hard to hack/manipulate system for outsiders	Maybe	Maybe	Maybe	Maybe	No
Hard to hack/manipulate system for insiders	No	No	No	No	No
Costs of introduction and maintenance	No	No	No	No	Yes
Infrastructure/environmental requirements	No	No	No	No	Maybe
Do e-voting standards exist	No	No	No	No	No
Possibility of meaningful recount and audit	Yes	No	Yes	Yes	No
Independence from Vendor	No	No	No	No	No
IT security requirements easy to achieve	No	No	No	No	No
Software Independence	No	No	No	No	No
Machine malfunctions are rare	No	No	No	No	No

International Experience with Voting Technology

India: DRE with VVPAT

India first introduced EVMS in 1982 in 50 polling stations – suspending its use two years later whenthe Supreme Court specified the need to amend the Representation of People Act. Through 1988 to 1992, the foundational institutional structures and legislations were established to make the use of EVMs in elections a reality. In the subsequent years, the technology was tested with the first pilot implemented in the state assembly elections in 1998 in a few constituencies. Thereafter, the ECI conducted a phased implementation of the EVMs in subsequent assembly elections. By 2003, all by- elections and state elections were held using EVMs, and a nation-wide roll-out followed in the 2004 general elections. (*History of EVM*, 2022)

In 2011, the prototype of the EVM & VVPAT system was demonstrated and the 1st field trial was conducted. Based on the trial, the system was reviewed and revised in 2012 and a second field trial was conducted. Finally in 2013, the design was approved, and legal amendments were passed to enable the use of VVPAT with EVMS. The deployment of the VVPAT was conducted in phases as well,with the nation-wide roll-out in Parliamentary general elections of 2019.

Due to the phased introduction of EVMs, researchers were able to establish clear linkages between the introduction of EVMs and the decline in election related corruption and fraud, the enfranchising of the marginalized segments of the society, and a more competitive electoral process (Debnath et. al, 2017).

Importance of local context

Ballot stuffing, among other election fraud, had been endemic in Indian elections. The Indian EVMs were designed to add a barrier to "stuffing" the EVM, by allowing only 5 votes to be processed per minute.

What makes it a success?

- Government support for election technology and public confidence in ECI as an independentbody has been foundational in the journey to make election technology a success in India.

- Despite criticism and lawsuits challenging e-voting in India, there has not been any substantial proof of the failure of EVMs to provide free and fair elections, and the problems are often overshadowed by the prevailing perception that benefits are far greater. The VVPATtechnology has alleviated concerns surrounding the potential for fraud and manipulation.

- ECI is intentional in its communication with voters and voter education mechanisms, which has also been crucial in improving voter acceptance of the new technology.

- To address infrastructural challenges, election management challenges, cost limitations, andensure efficient use of its EVMs, ECI conducts elections in multiple phases across the constituencies.

Challenges

So far, cybersecurity has not been given primary importance by the ECI and Indian voters alike. Thepremise is that the EVMs are stand-alone machines without any network connectivity such as the Internet. Likewise, in recent years, citizen bodies and the electorate have stressed that the voter registration system needs to be updated to make it more transparent. Recently, the civil society has also urged the uptake of state-of-the-art technology such as E2E-V voting and RLA (CCE, 2021) to increase transparency.

Brazil: DRE

Timeline

The TSE (Tribunal Superior Electoral) began the computerization of Electoral Justice in 1986, starting with electronic registration of voters. Like the case of India, Brazil's strategy for the implementation of electronic voting span over multiple years, starting with civic information as well as usability and feasibility studies in 1986. This was followed by a decade of efforts involving capacity building within the TSE. Trials of electronic voting machines in the Brazilian environment began in 1996, which involved various quality control exercises and multiple revisions to the system, followed by the nationwide roll-out in 2002. (*The History of Electronic Voting — Superior Electoral Court*, 2022)

Public Security Tests and Pre-election Audits

The Brazilian Superior Electoral Court (TSE), the EMB of Brazil, has complete ownership of the source code used in the EVMs. Legally, the TSE is required to make the final source code available to the political parties and the Brazilian Bar Association (OAB), at least 120 days before an election for inspection and audit. There have been some indigenous researchers that have attempted to conduct somewhat of an independent audit since 2001. Further, the OAB also outsourced the audit of the source codes in 2004. However, due to the limited capacity of the OAB and political parties, the stakeholders were unable to effectively examine the technology in subsequent years.

Following a petition in the Brazilian supreme court, which raised the concern that the public cannotvet the EVMs and its source code, the TSE has organized hackathons, commonly known as "The PublicSecurity Tests (TPS)". These events are restricted and only the researchers that are approved by the TSE can assess the system, find, and report vulnerabilities and recommend improvements. The needfor these events arose after two political parties filed an appeal before the Court of Justice regardingthe impossibility of verification of the security system of e-voting. The TPS is conducted in phases, starting a year before the elections. In the first round, researchers and experts find and report issues in the source code. Thereafter, the TSE has six months to resolve the issues identified by the expertsin the EVM. Regarding the recommendations from the inspection phase, it is at the discretion of the TSE whether it is willing to incorporate them in the current election cycle. After revisions to the system, if any, the researchers are invited to re-test the system. (Silva, 2020)

The TSE also authorizes another audit procedure by the name of "parallel vote." Two EVMs are randomly selected in each state a day before the election and checked to see if they produce the same results. However, some experts have criticized the parallel vote as they claim it is possible to manipulate the system between the parallel vote and election day. (*Introducing Electronic*

Voting: Essential Considerations, 2011)

What makes it a success?

- The voting system has consistently improved over Brazil's election cycles through Public Security Tests (TPS) – most notably in terms of the source code running on the machines. TheTSE has been intentional in its effort to constantly improve the voting system, which may bethe reason for the success of the Brazilian e-voting experience.

- The procurement process legally followed by the TSE centralized the development of electoral hardware and software. The software is designed and developed internally by the TSE, while it sends its team to the hardware production facility to oversee manufacturing. Inaddition to the EVM itself, for which the TSE solicits bids as per its own specification of the security architecture, election-related apps are also developed by their in-house teams.

Challenges

The biggest issue with the Brazilian mode of EVM is the lack of a paper-trail or VVPAT. This restrictsany kind of auditing and recounting activity. Consequently, candidates are unable to successfully challenge any election results. In the cases where the election results have been challenged and called to a comprehensive audit, the TSE demands over USD 1 million to fund the recount.

Further, the TSE has, in some election cycles, not made the final version of the EVMs available for audit by OAB, political parties, and experts. Due to the continued lack of a) TSE's transparency, and b) a stakeholder consensus on auditing mechanisms, future election results will be subject to furthercontention.

Philippines – PCOS

Timeline

The Commission on Elections (COMELEC) initiated discussions to automate the election process in the Philippines in 1992, and the first nationwide use of voting technology was in 2010. The lengthy transition from manual to automated elections entailed multiple revisions to the legislation through deliberations, and a structured and inclusive process. Although some provisions had been questioned to be ambiguous, most stakeholders found there to be a solid legal foundation for conducting automated elections.

However, the COMELEC faced a multitude of implementation challenges in the decade before its firstnationwide rollout. While COMELEC was authorized to implement the automated process in the 1998 elections, due to the lack of preparation, time, and funding, it was only used in 4 constituencies. Further, in 2001, the COMELEC's negligence in addressing civic education required for the new election process led to the unintended disenfranchisement of nearly 3 – 6 million voters. (Filipinas Heritage Library, 2021)

First nationwide roll-out: The Aftermath – the need for capacity building

Although the technology was tested, shortly before election day in the 2010 Elections, 75,000 PCOS machines were found to be incorrectly configured. COMELEC assigned resources on a large

scale to address this problem, extending till the end of election day (International IDEA 2011: 22).

Election day itself posed challenges for the voters. To curb costs, COMELEC had reduced the numberof polling stations by 75%, resulting in overcrowding and long waiting times for the voters. (*Carter Center Limited Mission to the May 2010 Elections in the Philippines*, 2010)

In its first nationwide use of voting technology in 2010, electoral protests, and complaints, unexpectedly, increased. Compared to the previous years, the defeated candidates filed more cases to the COMELEC. The complaints encompassed issues such as inaccuracy in vote counting, misreading of ballots by the optical-scan machines, errors in transmission and consolidation of results, faulty rejection of ballots, non-implementation of security measures, manipulation of optical- scan machines and/or compact flash cards. However, due to insufficient and inadequate evidence orprocedural inconsistencies, many cases were dismissed. Party observers lacked the adequate technical skills for observing the technology and hence, did not have the knowledge to identify the evidence needed to support their claims. These events also highlight the importance of courts having the technical capacity to effectively rule on technology-related cases. (National Democratic Institute, 2022)

Additionally, the results of the random manual audit were also unavailable weeks after the election,casting further mistrust in COMELEC and the technology. Similar problems occurred in the 2013 elections, after which VVPAT technology was introduced. However, COMELEC purchased new PCOS machines for this purpose, since the previously acquired machines were incompatible with VVPAT. (*Introducing Electronic Voting: Essential Considerations*, 2011)

Post-election Audit Process

The Poll Automation Law in the Philippines stipulates that "there shall be a random manual audit in one precinct per congressional district randomly chosen by the Commission on Elections (Comelec)". After the 2019 Philippines Elections, the Random Manual Audit (RMA) Committee reported a 99- percent accuracy rate between the results of the manual audit and the Automated Elections System (AES). The manual audit was conducted on 711 out of the 715 clustered precincts. While the Comelec declared the election a success, the AES Watch (election watchdog organization) declared it the "worst" as their experts suggested that the precinct sample size should be raised from 700 to 2,500 for real accuracy, which the RMA Committee failed to do. (Patinio, 2019)

What makes it a success?

- Transparency as a key factor in the acceptance of results: In the 2016 elections, the source code was audited for over seven months by political parties, authorities, and election watchdogs. It was also certified by an independent US-based company. Field monitors (technical staff documenting election day system issues) were also recruited by COMELEC onelection day and the media was granted full access to the documentation.

- Audit mechanisms: The 2016 elections generated one of the largest paper-audit trails, with nearly 43 million voter-marked ballots and its corresponding voter receipts. The Random Manual Audit confirmed the election results with 99.8 percent accuracy.

Estonia - Internet Voting

Timeline

Discussions surrounding internet voting in Estonia began in 2001, followed by legislation enabling the effective use of the technology. In 2003, the National Electoral Committee (NEC) locally contracted a firm to develop their electronic voting system that used smart cards and electronic signatures. This was followed by trials of the system in a consultative referendum in the capital city of Tallinn in 2004.

The Estonian solution has been the most technologically advanced, and trusted internet voting solution, and has been used as one of the voting channels since 2005. While mail-in and on-site paperballots are also available during elections, Estonia has observed an increase in the use of the internet voting system. In addition to ensuring a secure, secret, and transparent vote, the i-voting solution has also proven to be cost-efficient, inclusive, and convenient.

Since the introduction of i-voting in Estonia, voter participation has risen continuously. The 2019 Parliamentary Elections saw online participation increase by 40% compared to the same elections in2015. (*World's Most Hi-Tech Voting System Raises Cyber Defences*, 2019)

What makes it a success?

Estonia's e-governance, infrastructure, and public trust: Estonia has been developing its digital infrastructure since the 1990s and has provided e-government services since 1999. The government also developed and issued electronic resident identification cards in 2001, and deployed internet voting in 2005. Given NEC's technological capacity, expertise, transparency and compliance with election principles, public trust in the internet voting technology is naturally high.

Democratic Republic of Congo: Electronic Ballot Paper

Timeline

The Congolese Electoral Commission (CENI) adopted the Electronic Ballot Printer (EBP) technology in the 2018 national and concurrent elections, with the goal of reducing fraud and manipulation. CENI acquired three machines for public demonstration and information dissemination in 2017, and two of the three machines experienced issues post-demonstrations. (Ross & Lewis, 2018)

The CENI faced immense opposition to the decision of adopting the EBP for the 2018 elections, on both the national and international front, for all the right reasons (Clooney & Prendergast, 2022). TheEBP machines have been problematic since their demonstration. DRC also lacked the required infrastructure since most remote areas have power supply issues. Literacy rate of the electorate is also low. The voters also discovered that CENI did not have the technical capacity to understand and inspect the software, source code and database, which intensified opposition. This led to the arson of a storage facility of the EBP machines 10 days before the elections. (Paravicini, 2018)

Reasons for failure

CENI pursued to implement this technology in a short time frame, with little consideration to the legal framework and public acceptance. The implementation was rushed, and public perception mismanaged, which led to increased conflicts in the country.

Lessons Learnt

- Planning and implementation should not be rushed, and time should be built in the pre- election phase for systems review, revisions, and retesting. From its decision to deploy election technology to its first use in elections, DR Congo took only a year to acquire, test, andreview the technology, and to build the ecosystem supporting it. It is evident that their EMB failed to do so effectively. ECP should plan for a timed and phased implementation to realizebenefits and limitations of the system.

- Thorough legislation and regulation are required to enable the use of EVMs. In most countries, it has taken years of careful, thorough, and constant revision of legislation, following trials and retrials of technology, well in advance for a nationwide transition to electronic technologies.

- Invest in capacity building efforts. The example of the electoral complaints filed by political parties in 2010 Philippines elections is quite relevant to highlighting the capacity voids that can be created in the adoption of election technology. The required expertise and skills at every level and function of the ECP needs to be identified and assessed, and a comprehensiverecruitment and training plan needs to be developed.

  The TSE practices can also be reviewed to generate options for capacity development. Aside from the localized training, the TSE regularly invests in its staff through providing international training and following IFES training guidelines.

- Technological specifications for EVMs should account for the ability to accommodate anticipated future technologies: COMELEC had purchased the PCOS machines in 2010 for EUR 120 million (International IDEA 2020: 46). However, the purchased machines were not

  compatible with the VVPAT technology that was required post 2016 elections, rendering them useless post 2016. An investment of such immense scale needs to be well-thought and the timelessness of the technology needs to be addressed in the planning phase.

- Since the Estonian government had a highly developed digital infrastructure for its public services prior to the introduction of election technology, the electorate had built an inherenttrust in the NEC's abilities to implement it. Learning from Estonia's experience, ECP needs todigitize its internal processes, at the least, to reflect upon the electorate that it has the expertise to oversee the deployment of EVMs in future elections.

- Stakeholder acceptance is crucial for election results acceptance. The experiences in DR Congo and Kenya reflect that an understanding of the technology is essential for

stakeholder acceptance of the technology, which is essential in establishing the legitimacy of the electionprocesses.

- Transparency measures between the EMBs, political parties, and the electorate need to be established in law and regulation for building trust and understanding the system.

- Voter information and education mechanisms are needed as per the local needs: A major factor in the EVM acceptance in India has been the exposure to the technology ECI has provided to the electorate. As part of its civic education efforts, ECI also took prototypes of EVMs to be demonstrated to the public, and dummy EVMs to be tested by the public.

- While costs are an important consideration, it is important not to compromise on the systemquality and requirements to appease the budget. In 2019, new regulations required COMELEC to procure the system and logistics at the lowest bid, which compromised the quality and compatibility of the acquired technology with the existing systems.

3.2 Fetishization of Technology

Most election management organizations (EMBs) now utilize some form of technology to try to improve election operations. From basic office tools and websites to complex biometric voter registration databases, voting systems, electronic voting, and internet voting.

Technology has often been introduced as a panacea to this issue of trust. Several countries, includingBrazil, India, Namibia, Nigeria, and Venezuela, have adopted electronic voting machines, and the Philippines and Mongolia have deployed automated counting systems. Other countries including Argentina, Kenya, Bangladesh, Indonesia, Pakistan, Panama, Ghana, Kyrgyzstan, and Kazakhstan have begun experimenting with technology.

The results from the international experience are mixed. Reported improvements in India include a significant decline in electoral fraud in some regions, a more competitive electoral process, and increased participation of marginalized groups in society (Somanathan & Madhavan, 2019) (Debnath et al., 2017,). Automated counting in the Philippines corresponded with record turnouts of over 81%(Team & Web Development, 2021) and dramatic reduction in time taken to compile and finalize election results (Manila & The Philippines, 2016).

However, there are frequent irregularities which undermine trust in technology. In 2017, the Supreme Court of Kenya nullified election results citing irregularities in the results transmission

system (Burke, 2017). Similar concerns were raised by opposition leaders in Pakistan in 2018 when the results transmission system broke down inexplicably on election night (Wasim & Saadat, 2018). In Azerbaijan, the introduction of a smartphone app in 2013 to report election results backfired whenit released the election results the day before the actual election (Bigg, 2013).

There has also been a backlash against voting machines. In India, numerous incidents were

reportedin different polls where machines recorded votes in favor of the ruling party, no matter which choicethe voter made (Sinha, 2019). 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 (Paravicini, 2018).

Researchers have sought to explain these "unintended consequences" of election technology in termsof a "fetishization of technology" (Cheeseman et al., 2018), or a silver bullet (DR, 2011), which distracts stakeholders from rigorous assessments and stringent checks and balances in the overall ecosystem (Barkan & Joel D, 2013). Paradoxically this lack of attention can render election processes even more vulnerable than before.

To situate the potential contribution of E2E-V voting systems, it is helpful to differentiate between electoral efficiency (speed, accuracy, and elimination of 'rejected votes') and electoral transparency as two desirable yet distinct outcomes of using election technology (Yard & Michael, 2010). Unfortunately, in most deployments of election technology, 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 E2E-V voting systems - by incorporatingsecurity and integrity as core design features of the system - can potentially redress the balance between electoral transparency and efficiency.

Similar sentiments have also recently been voiced in the developing world, namely Brazil (Aranha etal., 2018), Pakistan (IVTF Report, 2018), and India (CCE, 2021), where security professionals, researchers, and civil society organizations have urged election authorities to explore the adoption of E2E-V voting systems in elections to enable transparency and restore credibility of electoral processes.

New Election Technologies

End-to-end Verifiability

Conventional electronic voting machines are black boxes, and they lack the transparency that is the cornerstone of an effective voting solution. **End to End Verifiable (E2E-V)** voting Systems are a promising new paradigm in the world of electronic voting that provide voters strong cryptographic guarantees that the vote was **cast as intended**, **recorded as cast,** and **tallied as cast**. Every individual can rigorously audit every essential step of the election process, with a smartphone and internet connection available to them. It makes the entire election life cycle auditable by third parties, the voters, and the election administration alike, and provides strong cryptographic security guarantees each step of the way. The voter does not have to blindly trust the voting system, polling officers, or election authorities regarding the integrity of the election. If there is any malfeasance or rigging, it will be exposed by the protocol itself.

This is a revolutionary remodeling of the conventional voting machines, the inner workings of whichare largely opaque to voters. It has often been touted as the de facto holy grail of electronic voting (e-Estonia, 2017). Various pilots have also been conducted UK (Hao et al., 2020) and are now being deployed in binding political elections on a small scale (for instance, in intra-party elections in Israel, in mayoral elections in Maryland, US (Zagorski et al., 2013), in state elections in Victoria, Australia (Burton et al., 2016), and at the county level in gubernatorial elections in Texas (Acemyan et al., 2014). Estonia also deploys a E2E-Voting system for its nationwide parliamentary elections, the first deployment being in 2019 (e-Estonia, 2019).

These systems have also gained trust and recognition from the National Academy of Sciences (The National Academy of Sciences, 2018), international researchers, experts, industry, and technologists(Inspector General, 2021). Recently, E2E-V voting has garnered immense interest by technology giants and various large scale commercialization efforts are underway. Among these is Microsoft's partnership with Smartmatic, a leading vendor for election technology. Hart InterCivic, Dominion, and others are also set to trial E2E-V voting systems.

India's Election Commission, in partnership with IIT-Madras, has been conducting extensive research on E2E-V voting. Plans for pilots are underway and there is an increased awareness within the public about the radical benefits E2E-V voting Systems offers. A pilot was intended for last year's municipal elections in Hyderabad. Additionally, public awareness is high. As the report from the Citizen Commission of India explains, conventional electronic voting machines have "defects that appear to be near-fatal to electoral democracy." and further in favor of E2E-V voting systems "Wouldn't it makesense if elections embodied democratic ideas as well? Why not create a system that allows individualcitizens to independently verify and audit elections – to ensure that the votes they cast genuinely count?"

All of this can be achieved without compromising ballot secrecy. No voter can demonstrate to a third party which candidate they chose to vote for. We provide a primer on E2E-V voting technology in Appendix D.

Risk Limiting Audits

Election procedures and controls implemented throughout the election life cycle are meant to guardagainst undetected human error, intentional malfeasance, and voting system malfunctions that maycause harm to the integrity of the election outcome. Another such critical component of a transparent election is a risk-reducing Post-Election Audit. Post-election audits, as the name suggests, occur after the voting period ends and before certifying the results of an election.

Post-election audits are statistical tests that reduce the risk of an erroneous election outcome. They help identify anomalous tallies and give election officials to make amends before the elections results are certified. Post-election audits are public ceremonies, to which invitation is extended to the public, civil society, and media. Such public ceremonies can also be live streamed. They are a very effective measure to increase voter and stakeholder confidence in the outcome of elections and raise the perception of electoral integrity. The process is summarized in Figure 2.

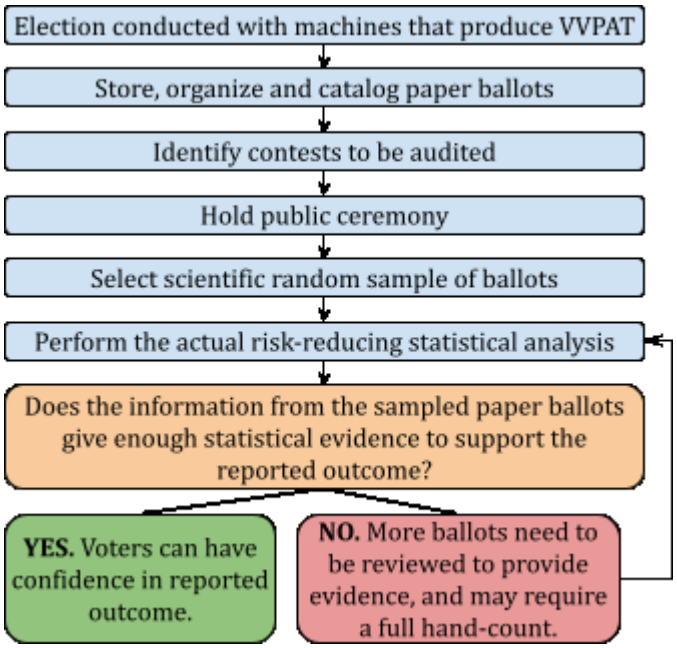
The idea is to build trust in systems that have become less transparent as they are more mechanized. In 2012, a municipal election in Palm Beach County, Florida conducted a post-election audit. The audit identified a discrepancy in the reported results and the audit-based results. This led to the identification of a bug in the election management software which was attributing voters to the wrong candidate. The results were consequently officially corrected.

Risk Limiting Audits begin with a small number of randomly selected ballots. They continue to scrutinize an increasing number of ballots, selected at random. This step is repeated until there is enough statistical evidence that a manual counting of all the votes cast, will not change the outcome.(IFES, 2021).

Risk-limiting audits are more time- and cost-efficient than hand-count audits. By the end of this there is either a quantifiable level of confidence that the election outcome is correct or quantifiable evidence of an error that can then be corrected by way of a full hand count.

Risk-limiting audits have been recommended by numerous international bodies such as the Senate Select Committee on Intelligence (Brennan Center Quick Take, 2018) and the National Academies ofSciences (National Academies of Sciences & Engineering, and Medicine, 2018,), American Statistical Association (ALEXANDRIA & , VA (PRWEB), 2010), Brennan Center for Justice (Howard & Rosenzweig, 2021), among others. In *Appendix E* we walk the reader through Risk Limiting Audits byan example.

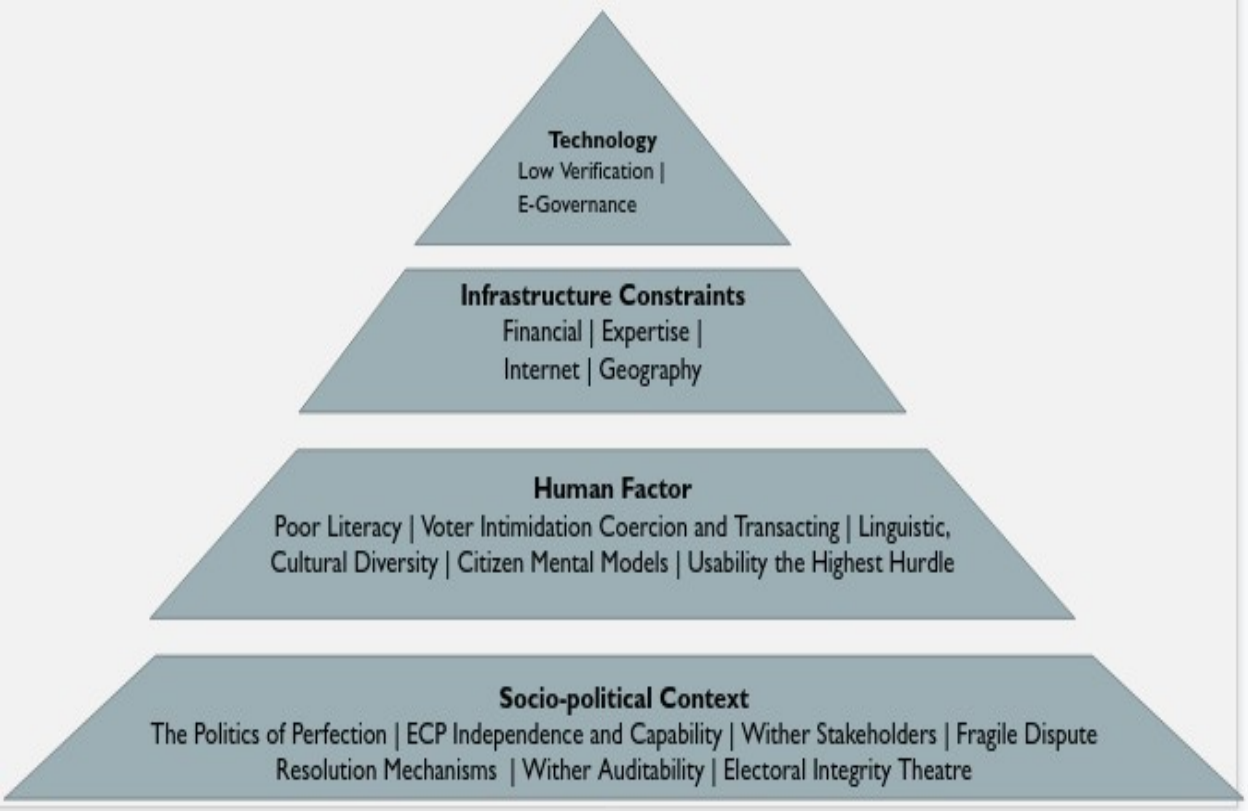
Figure 2: Risk Limiting Audits



3.3 A Conceptual Framework for Election Technology

Literature suggests that "A voting system is only as good as the public believes it to be." (McGaley etal., 2003). The perception of fraud can be just as detrimental to the credibility of an election as actualfraud itself. Researchers have described the Perceptions of Electoral Integrity around the world. Pakistan ranks 118th with a low PEI Index of 47 points (Norris et al., 2019). The goal of E2E-V votingis to provide transparency to the voters which in turn will improve voter trust, electoral integrity, and its perception thereof. We define the challenges along the lines of the pyramid of trust that we propose to help understand the distinct factors that contribute to building trust in electoral systems.

Figure 3: Conceptual Framework for Election Technology



Technology

E-Governance and Digital Transformation: E-voting is a cornerstone of E-Governance. Pakistan is at a nascent stage of E-governance and digital transformation, with traditional methods of service delivery dominant especially in the public sector. Estonia began its online voting initiatives only after widespread use and gradual growth of pre-existing services in areas like social security, taxation, and property registration. As of now over 99% public services can be performed online. Through these measures Estonia in a year saves over 1400 years of human effort. (e-Estonia, 2017) The success of Estonia's Internet Voting system is also attributed to the extensive and pervasive digital infrastructure that supports it.

The ECP needs to develop a Cybersecurity strategy and undertake rigorous cyber hygiene exercises within all its departments. It needs to bring itself at par with the international standards with regards to cyber security. A step towards this is to obtain ISO-27001 certification. EMB's are

increasingly becoming the target for Cyber threats. Hackers and crime gangs have been targeting EMBs worldwide with a 3-fold increase in attacks since 2015. One such incident involves a ransomware attack on the Caribbean EMB, which had to pay ransom in bitcoins to gain access to its data (Commonwealth Secretariat, 2020). A Computer Emergency and Response Team (CERT) should be established withinthe ECP to handle any untoward incident.

Low Verifiability Rates The provision in E2E-V voting Systems that permits every participant in thevote to check and verify their vote is revolutionary. However, there is a dire need to motivate votersto exercise this option. So far, in all the pilots and deployments it has been observed that the rate of verification is very low. An even lower percentage of people identify and report differences in their vote and the one cast by the machine (Moher et al.,2014). Chipcase (Chipchase & Jan, 2005) observedthat non-literate populations dodge complex functions and this reinforces the assumption that if a step is optional, it will be skipped (Ellison & Carl, 2003).

Infrastructure Constraints

Financial Estimates suggest the cost to shift to traditional EVMs to be around Rs 1 trillion (Brecorder, 2021). Cost calculation must occur early in the process so that stakeholders fully grasp the criteria on which they are making their judgments. Although E2E-V voting may offer greater financial gain in the long run over many electoral cycles, the upfront investment related to system development, security procedures, testing, promotion, voter education campaigns, and so on is significant. Anotherapproach could be to start with traditional EVMs and then using the Scantegrity approach, implement E2E-V voting on top of existing DRE-VVPAT machines. This can be done easily through modularity inthe EVM design. Such modularity will increase the lifetime of the EVMs and make sure they do not have to be scrapped.

Utilities There is a lack of utilities provision such as electricity, telecommunications, and robust broadband Internet service. The internet penetration is 54%. Even where such capacities are available in Pakistan, they are primarily concentrated in urban centers (almost ⅔ of all internet users are based in urban centers), with negative implications for widespread deployment of the E2E-V voting systems which require a bulletin board to ensure individual and universal verifiability. I

Transport and Geography A significant operational challenge, rarely recognized in existing studies,is that geographic terrains are diverse, from mountains to deserts, the distances are great - far flungpolling stations, sometimes only accessible by foot, thus the machines need to be rugged, weather resistant, sealed from insect infestation and capable of lengthy periods operating on battery power. In some countries, there might even be a delay - between the casting (and recording) of a ballot, the return of the equipment to a location with connectivity, and the votes being centralized - before verification is even possible. How these delays create opportunity for malfeasance needs to be studied.

Human Factor

Voter Intimidation Coercion and Transacting Voters in the developing world are more likely to cast votes based on sects, castes, tribe, biradaries and political affiliations, while those in the developed world based on a thorough, logical, and comparative analysis of the contesting politicians (Bossuroy & Thomas, 2007). Pakistan is no exception. Accordingly, E2E-V voting

awareness campaigns must ensure that voters understand and appreciate that the receipt does not reveal theirvote, in order not to exacerbate an already serious problem.

Linguistic, Cultural Diversity Pakistan is marked by their linguistic diversity (dialects may changeevery few miles) (Weber et al., 2017), ethnic diversity and varying cultural constructs (Alesina et al., 2003) requires the need for localization of both the voting system and the accompanying receipts and verification mechanisms.

Citizen Mental Models There is a need to educate the voters on the paradigm of E2E-V voting. It hasbeen reported in literature that voters' perception about a voting system is based on how-to-vote procedures (Acemyan et al., 2015). It is necessary to formulate mental models for E2E-V voting to help all stakeholders including voters, election officials and judiciary to foster an understanding of this novel paradigm, as unverified assumptions may hinder stakeholder acceptance (Zollinger et al., 2019). Citizen awareness programs through various media, public demonstrations, operating phonehelplines and awareness sessions etc. should be undertaken. These can be targeted to help remove mismatch, impart clarity to voters in their pre-existing mental models and overcome cognitive barriers (Kshetri & Nir, 2007).

Usability the Highest Hurdle E2E-V voting systems are weak from a usability perspective (Acemyan et al., 2018) and they have been known to confuse voters (Schneider et al., 2011) (Acemyan et al., 2014) even in the developed world. In E2E-V voting systems, usability considerations include a voter's ability to cast their vote effectively and, more crucially, their ability to complete the verification procedure. Extending low literacy HCI recommendations (for voters in traditional electronic voting), to the E2E-V voting scenario is not trivial. A preliminary assessment of prominentE2E-V voting solutions discovered that voting took about twice as long with each system, and a huge proportion of the voters failed to independently use the systems to cast their vote with each of the systems, many of whom were unaware of the error they made (Acemyan et al., 2014).

Several technical alternatives, such as simplifying security features or improving voting systems to ease individual vote verification, have been proposed (Nandi et al., 2010) (Ryan & Peter YA, 2011) (Dechand et al., 2016) (Perrig et al., 1999) (Olembo et al., 2013) (Azimpourkivi et al., 2020). It is necessary to study how these can be adapted for Pakistan.

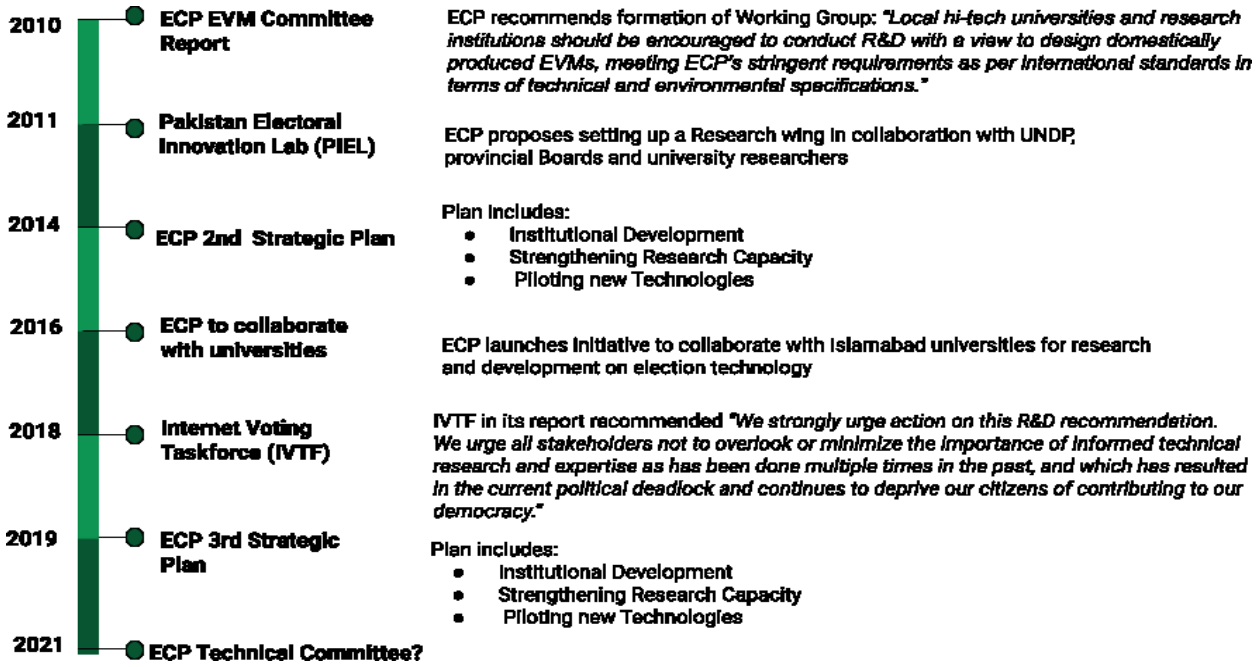
Social and Political Factors

A supportive sociopolitical environment considerably aids in the deployment of e-voting and can even temporarily mask initial implementation difficulties. In this section we explore how Pakistan's volatile socio-political setting puts it at risk of an unfavorable outcome of the deployment of Electronic Voting Machines.

ECP Independence and Capability According to an IFES report "Challenges with the ECP's full exercise of its mandate had implications for the integrity of elements of the election process." (IFES, 2014) The introduction of E2EV- Voting in such a scenario may result in increased doubts over electoral integrity. It is vital to maintain the ECP's central role in addressing the deployment of any contemporary IT solutions for the election process, as it is the only organization tasked with administering them. It is important that ECP is provided with the autonomy and regulatory teeth it requires for this huge undertaking and not operate under political influence and fear.

The ECP also needs to undergo major restructuring and reforms at all levels in its institution. This will require a dedicated long term multidisciplinary effort, for which constituting a Research & Development cell is the first step. Under the umbrella of the R&D Cell a long-term research and development agenda should be formulated. In countries with a reputation for electoral innovation, such as Estonia, Brazil, India, and Australia, election management bodies typically partner with leading universities to undertake research. This point has been raised numerous times in expert reports and official proceedings over the last decade. The ECP itself has tried to initiate steps in this direction. Unfortunately, none of these efforts have been fully pursued.

Figure 4: Over the last decade numerous expert reports and official proceedings have asked the ECP to set up a dedicated research unit



Legal Framework: A restructuring of the legal framework is also required with the introduction ofelectronic voting systems. It is necessary to ensure the confidentiality of the vote is maintained and identity data is disassociated. The legal framework should provide for ample auditing of the electionoutcomes as well as the processes that lead to those outcomes. It also needs to specify the course of action in case a discrepancy in results arises during audits or some irregularities in the process are discovered. The election authority must ensure that technology has undergone certification. The lawneeds to identify those institutions that can provide certifications, how long the certification period will be, and the requirements for the certification. Legal provisions regarding the logistics such as transport and storage of EVMs and resident data need to be provided, such as the time period for retaining data, how data is deleted, how it is backed up and what to do in case of data loss. If voter identification is done through biometric data of voters, then the law needs to bring data under the umbrella of a data protection act. Whether the source code of the EVMs and associated technology will be made open source or not needs to be spelled out in the law. This will also dictate the level of access and information that is available to stakeholders for scrutiny.

There needs to be a thorough analysis of what audit reports and forensic investigation data can

be collected from the Electronic Voting System. In case the election results are challenged in court, what kind of evidence is admissible in court needs to be assessed apriori. In case of E2E-V Voting, it should be binding on ECP 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 E2E-V voting systems become moot. The election day integrity measures, procedures also need to be updated in accordancewith the new electronic system.

Fragile Dispute Resolution Mechanisms: In Pakistan, disputes over election results often act as triggers for mass protests, violence, political deadlock and animosity, often bordering civil war. Following the 2013 elections, PTI chairman Imran Khan ordered an investigation into electoral improprieties in 4 constituencies. However, it took a sit-in of over four months to institute a Judicial Commission that discovered over forty flaws in the handling of election results. IFES summarizes "fordecades, the executive branch has manipulated the election law to increase its control over the process and there has been resistance from a range of sectors to reforming the current framework. The legal framework is also mostly silent or unclear about the processes by which complainants filegrievances and the ECP investigates and rules on these complaints. The lack of specificity leads to inefficiencies, limited transparency, an increased chance of malpractice and great confusion. More could be done by the ECP to remedy the legal vacuum or to take on the responsibility of adjudication." (IFES, 2014)

It is necessary to ensure that the introduction of electronic voting does not exacerbate dispute resolution problems. Similar incidents are common in developing countries. For instance, in Kenya, the lack of awareness among many individuals and observers about how digital processes truly function made it incredibly difficult to distinguish between false and credible assertions. (Cheesemanet al., 2018). Similarly in Brazil researchers have noted that, "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." (Aranha et al., 2018). Accordingly, for disputes involving technologies, defining the requirements for the admissibility of evidence, training the judiciary to handle the intricacies of electronic voting systems based digital evidence is of utmost importance.

Electoral Integrity Theater: The security guarantees of E2E-V voting systems become moot if the verification step is not undertaken, and the system is not auditable. If legislatures in developing countries cannot draft and pass laws that are sufficiently detailed to address both core and ancillaryprocesses (such as risk limiting audits and electoral dispute resolution), E2E-V voting risks becoming nothing more than the electoral equivalent of "security theater" (Schneier & Bruce, 2021). To quote Park et al “Auditability alone isn’t enough”, and ``must be accompanied by auditing to be effective”. (Park et al., 2021). Without auditability, paper trails are “ornamental”.

The Politics of Perfection: Many electronic voting efforts in developing nations have been launchedwithout a solid research base or a strategic plan in place first (Hapsara et al., 2017). Despitedeveloping countries taking the lead in E-voting deployments there is little discussion and dialogue about E2E-V voting systems. Venezuelan government calls its voting system “the most perfect voting system in the world” (Machin-Mastromatteo & Juan D, 2016), while India's EMB angrily reacted to reasonable analysis of its EVM (G.V.L. N. Rao, 2010). Similarly, in August

2021, the Minister for Science and Technology, reiterated that The Electronic Voting Machine developed by MoST cannot be hacked. Can developing countries who see their EVM systems as "perfect" even begin to accept the need to evolve towards E2E-V voting and evidence-based elections?

Wither Stakeholders: The majority stakeholders have strong opinions regarding electronic voting. There is a dire need to involve these stakeholders from the outset, which is the opportune time to letthe stakeholders express their concerns, as well as ensure their concerns are addressed in the process of introducing electronic voting.

RECOMMENDATIONS

In this section we formulate actionable recommendations based on our findings. The recommendations are accompanied by a roadmap in Appendix F that may serve as a guide in the implementation of these recommendations.

5.1 Groundwork to Develop the Requisite Ecosystem

1. **We recommend the ECP constitute a Steering Committee, which will serve as a structured body to provide leadership, governance, and oversight for this endeavor.** The next logical step is to establish a research division within ECP to provide high quality research inputs for technological, legal and policy decisions. The ECP needs to undertake a gap analysis to identify the limitations in its capacity that may hinder the project from achieving its objectives. An action plan should be developed to bridge these gaps.
2. **We recommend ECP solicit stakeholder input at the early stage of the project to develop trust in the voting system**. The ECP should seek to engage and consult stakeholderssuch as political representatives, civil society, activists, and technologists, and seek their inputs at every stage of the deployment process. At every step the ECP needs to maintain transparency in its conduct. This can be achieved by setting up active working groups and organizing outreach efforts, such as public calls for comments and organizing seminars, invited talks, demos, and hackathons. The ECP should also actively conduct knowledge mobilization and build linkages between itself and research bodies, private sector project partners, and international EMBs.
3. **We recommend the ECP assess the readiness of the country to transition to EVMs.** This needs to be assessed specifically from a technological and infrastructure perspective. For instance, the readiness to indigenously manufacture EVMs. Critical national infrastructure like election technology should not be outsourced. Critical EVM hardware and software components should be manufactured within Pakistan to give ECP greater oversight and control over the process. Countries much like our own, including Brazil, India, and Bangladesh, have successfully innovated EVMs as per their own needs within their own limited resources.
4. **We recommend the ECP devise a Digital Transformation Strategy to modernize ECP and its systems to the point where they can successfully launch and manage large-scale EVM deployments.** This would involve upgrading internal systems, digitizing existing processes, host dedicated data centers, developing policies and processes to support the newinfrastructure and safeguards against technology failures.
5. **We recommend the ECP on an urgent basis develop a Cybersecurity Strategy to counter attacks on its IT infrastructure.** It should identify and work towards implementing international information security standards such as ISO/IEC 27001. ECP should also undertake periodic and comprehensive risk assessment audits. It should also prepare for any untoward incident either by developing inhouse capacity for cybersecurity emergency response and recovery or seek active assistance from national cybersecurity agencies and specialist bodies.
6. **We recommend ECP pay special consideration to measures to foster social support and trust.** This includes targeted strategies such as media strategy, active voter

engagement strategy, strategy for public oversight, strategy to fight disinformation, technologist involvement strategy, effective communication plans for election day and post-elections processes like audits, election petitions, and dispute resolution.

7. **We recommend ECP define baseline security requirements for EVMs.** This study, referred to as a threat model, should precisely define the security issues and vulnerabilities on the ground that we expect to address using EVMs.
8. **We recommend ECP conduct an analysis of the suitability of popular EVM types for usein Pakistan.** Given the different characteristics and benefits of each type of EVM, it is important to assess how each performs on ground in Pakistan. We recommend that ECP procure multiple units of each EVM type and pilot them. It is important to know which EVM type and interface our citizens find easiest to use and is most conducive to enfranchising them. This will be an extensive exercise examining a range of factors, including security, usability, costs, logistics, storage, and handling requirements.
9. **We recommend ECP research and devise voter verification strategies, like multi-fingerauthentication, computer vision solutions, tokens, and smart cards.** ECP's earlier pilot of Biometric Verification Machines noted a significant failure rate of 54%. This was due to scanning issues, environmental or lighting conditions, and poor quality of fingerprints due toinjuries, or calluses due to intensive manual labor.
10. **We recommend ECP undertake multiple large-scale pilots in a mix of urban and rural areas to ensure a representative cross-section of the electorate is covered.** ECP may commence large scale procurement and nation-wide deployment after a sufficient number ofsuccessful pilots.

5.2 Sustainability and Support

11. **We recommend ECP develop a comprehensive strategy for supporting technologies such as Result Transmission System (RTS).** Procedures must be devised to transfer the results from the EVMs in a safe, secure, and timely manner. The RTS should be rigorously stress tested and be piloted alongside EVMs multiple times to identify potential integration issues.
12. **We recommend ECP develop sustainability strategies for EVMs and supporting technologies.** As a developing country, it is vital that we seek out cost-effective options and utilize our resources effectively. We should try to "future-proof" our EVMs, such that they have a lifetime of at least 2 to 3 election cycles.
13. **We recommend ECP develop comprehensive standards and testing and certification protocols for EVMs.** These processes must be designed with a view to giving stakeholders greater transparency into the state of the machines.
14. **We recommend ECP organize hackathons for EVMs and solicit feedback from the international and local election technology community to identify vulnerabilities and provide stakeholders with greater transparency.** We recommend ECP engage third partytechnical experts and consultants at periodic intervals to analyze the security properties of EVMs.

5.3 Operations and Logistics

We recommend ECP develop comprehensive storage and transport facilities and protocols for EVMs. EVMs will likely require fleets of customized trucks or large vehicles totransport EVMs between storage sites and polling booths on election day. For this purpose, ECP should develop detailed standards and SOPs to store and transport EVMs, as devised in countries like India and Brazil. We recommend ECP devise stringent protocols for accessing,handling, and maintenance of EVMs that can be rigorously monitored and policed.

5.4 Legal Framework

We recommend ECP identify the issues with the current legislation, and introduce legislation to support EVMs:

a. Voting laws should not be so specific that they hinder innovation, nor should they be so generic that they leave room for lingering litigation.

b. The law should provide for conducting pilots for Risk Limiting Audits and End-to-end Verifiable Voting.

c. Also included in law should have provisions for technology trials and certifications, identifying authorized certifying institutions and establishing the certification standards.

d. There should be laws that mandate the pre-audit and post-audit of EVMs and supporting equipment. Election laws will need to specify requirements and standards for auditing mechanisms.

e. The law should provide for efficient dispute resolution under the new voting modality.

f. The law should provide for what constitutes admissible evidence in court

g. The law should specify rules for source code access.

h. The law should update procedural checks according to the updated voting mechanism.

i. The law should specify which Data protection law does voter data fall into and what recourseis required in case of breach.

j. The law should specify procedures and access to observers and political party representatives.

5.5 Phased Implementation

Planning and implementation should not be rushed, and time should be built in the pre-election phase for systems review, revisions, and retesting. From its decision to deploy election technology to its first use in elections, DR Congo took only a year to acquire, test, andreview the technology, and to build the ecosystem supporting it. It is evident that their EMB failed to do so effectively. ECP should plan for a timed and phased implementation to realize benefits and limitations of the system. The timeline as recommended by international experts and their guidelines should be respected. As an NDI report notes: *"The timeframe for consideration and possible adoption of electronic voting and counting technologies is an issue that needs to be carefully considered. It is easy to underestimate the time that proper consideration and implementation can take, even for a pilot project. A full assessment of electoral requirements; availability of technologies; and identifying benefits and challenges of using such technologies can take many months. Once suitable technologies are identified, they must be procured – ideally and initially on a small scale – for a pilot. When pilots are held, a fulland thorough evaluation of the process must be*

conducted before any plans or decisions are made for further implementation." (National Democratic Institute, 2013).

CONCLUSION

We started out by defining the context of electoral issues in Pakistan. We then delineate our finding that any shift towards electronic voting machines should be guided by the overarching principles of secrecy of the ballot, electoral integrity, openness and transparency, accessibility and usability, and sustainability.

In the second part we note documented strengths of EVMs such as faster tabulation with greater aaccuracy, reduction in polling station fraud, increased voter turnout and accessibility, inclusivity, and long-term cost savings. On the flip side, we also discussed the potential weaknesses such as lack of transparency and limited Understanding for the voters,information security concerns, malfunctions, usability, lack of standardization, sustainability, and high initial costs. We present a comparative summary of common EVM models deployed namely PCOS, DRE, DRE-VVPAT, EBP and Remote Internet Voting.

We then presented case studies from India, Brazil, Philippines, Congo and Estonia, followed by the lessons to learn from these deployments: avoid rushed implementation, undertake phased implementation, ensure timely regulatory and legislative support, invest in capacity building efforts, anticipate and leave room for future improvements, do not undermine the importance of a supporting digital infrastructure, build stakeholder acceptance and transparency measures, engage in rigorous voter education and acceptance efforts, and lastly, do not compromise quality to appease the budget.

We highlighted common pitfalls, explaining the phenomenon of "fetishization of technology" and howit distracts stakeholders from rigorous assessments and stringent checks and balances in the overall ecosystem, rendering election processes even more vulnerable than they were without technology. We described the novel concept of public verifiability and how risk-limiting audits, and verifiable voting can mitigate outstanding security concerns regarding EVMs and ensure trust in poll results.

We presented a holistic framework to identify the technical and human factors, socio-political, challenges and infrastructure constraints to address as we move towards EVMs. Our national discourse to date has focused primarily on EVM units, and there is unfortunately, very little recognition of the enormous task of building a supporting ecosystem for EVMs. This ecosystem is critical to the success of the overall project and the effort and costs involved in setting it up can easily dwarf that of procuring the EVMs themselves. There is very little existing research in this domain, and we believe it is the first comprehensive document of its kind on the EVM discourse in Pakistan.

We also present recommendations to address these challenges at every stage. The accompanying roadmap spells out these recommendations in the form of concrete detailed steps that stakeholdersneed to take. The roadmap lists key activities, including research assessments, pilot studies, hackathons, and demos and suggests timelines, references, resources at every step and highlights dependencies and concerns. We also identify critical research gaps to be addressed. The ECP in collaboration needs to ensure the synergy of people, processes, and technology. It should evaluate, manage, and mitigate risks at every stage. There should be a steady progression towards adopting election technology propelled by careful research and deliberation, so that

unfavorable outcomes can be avoided. However,

"We must not ... make the mistake of placing our faith in technical solutions to political problems. When opposition parties and donors invest in the transformative power of new scientific advances, they often overlook the fact that even the most advanced forms of election technology rely on humanprogramming and management. And there is nothing about digital technology that means that thosewho use it are likely to be any more trustworthy or fair." (Cheeseman et al., 2018). As John Githongo, Kenya's former anti-corruption tsar, has put it: "You cannot digitize integrity". (Cheeseman et al., 2018).

REFERENCES

ACE. (2020). ACE. Retrieved from https://aceproject.org/ace-en/focus/e- voting/introducing-electronic- voting -considerations/default

Acemyan, Claudia Z, Kortum, Philip, Byrne, Michael D, Wallach, & Dan S. (2014). Usability of Voter Verifiable, End-to-end Voting Systems: Baseline Data for Helios, Pret a Voter, and Scantegrity II. In *014 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 14)*.

Acemyan, Claudia Z, Kortum, Philip, Byrne, Michael D, Wallach, & Dan S. (2015).

Users' mental models for three end-to-end voting systems: Helios, Pret a Voter, andScantegrity II. *International Conference on Human Aspects of Information Security, Privacy, and Trust*, 463--474.

Acemyan, Claudia Ziegler, Kortum, Philip, Byrne, Michael D, Wallach, & Dan S. (2018). Summative usability assessments of STAR-Vote: A cryptographically secure e2e voting system that has been empirically proven to be easy to use. *Human factors*.

Agbesi, & Samuel. (2018). Adoption of E-Voting System to Enhance the Electoral Process in Developing Countries. In *Evaluating Media Richness in Organizational Learning* (262--273). IGI global.

Akinyokun, & Olukayode Nicholas. (2020). Secure voter authentication for poll-siteelections in developing countries.

Alan Fowler. (2000, January 1). Civil Society, NGDOs and Social Development: Changing the Rules of the Game | Publications | UNRISD. *United Nations Research Institute for Social Development*. https://www.unrisd.org/unrisd/website/document.nsf/0/f553495f06f98dce80256b5e005c9ddc/

Alesina, Alberto, Devleeschauwer, Arnaud, Easterly, William, Kurlat, Sergio, Wacziarg, & Romain. (2003). Fractionalization. *Journal of Economic growth*, *8*, 155--194.

Alexa Corse. (2019, December 16). Voting-Machine Parts Made by Foreign SuppliersStir Security Concerns. *Wall Street Journal*. https://www.wsj.com/articles/voting- machine-parts-made-by-foreign-suppliers-stir-security-concerns-11576494003

ALEXANDRIA, &, VA (PRWEB). (2010, April 26). *American Statistical Association Recommends Risk-Limiting Audits of Federal and Statewide Elections.*

Ali, S. T., & Murray, J. (2016). An overview of end-to-end verifiable voting systems,*Real-World Electronic Voting*.

Aljarrah, Emran, Elrehail, Hamzah, Aababneh, & Bashar. (2016). E-voting in Jordan:Assessing readiness and developing a system. *Computers in Human Behavior*, *63*, 860--867.

Alomari, & Mohammad Kamel. (2016). E-voting adoption in a developing country.

Transforming Government: People, Process and Policy.

Aranha, Diego F, van de Graaf, & Jeroen. (2018). The good, the bad, and the ugly: twodecades of e-voting in Brazil. *IEEE Security \& Privacy*, *16*, 22--30.

Aranha, Diego F, van de Graaf, & Jeroen. (2018). The good, the bad, and the ugly: twodecades of e-voting in Brazil. *IEEE Security \& Privacy*, *16*, 22--30.

Arlo. (2022). Risk Limiting Audits with Arlo. VotingWorks. https://www.voting.works/risk-limiting-audits

Arooj, Ansif, Riaz, & Mohsin. (2016). Electronic voting with biometric verification offline and

hybrid EVMs solution. In *2016 Sixth International Conference on Innovative Computing Technology (INTECH)* (332--337). IEEE.

Azimpourkivi, Mozhgan, Topkara, Umut, Carbunar, & Bogdan. (2020). Human Distinguishable Visual Key Fingerprints. In *29th USENIX Security Symposium USENIXSecurity 20* (2237--2254).

Bari, S., & Muhammad, K. (2021, October 12). Electronic Voting Machines: Politicians, NGOs, TV Anchors & ECP. *Global Village Space*. https://www.globalvillagespace.com/electronic-voting-machines-politicians-ngos- tv-anchors-ecp/

Barkan, & Joel D. (2013). Kenya's 2013 Elections: Technology Is Not Democracy.

Journal of Democracy, *24*, 156--165.

BBC News. (2019, April 19). India voter 'chops off finger' after voting for wrongparty. *BBC*. https://www.bbc.com/news/world-asia-india-47986377

Bhatti, H. (2018). NADRA to develop Internet voting system for expats. *Pakistan Today*. https://www.pakistantoday.com.pk/2018/01/25/nadra-to-develop- internet-voting-system-for-expats-report

Bhatti, H., Sattar, N., & Bari, F. (2018, January 5). SC accepts 16 petitions regardingoverseas Pakistanis' voting rights. *Dawn*. https://www.dawn.com/news/1380952

Bigg, C. (2013, October 9). Official App Releases Azerbaijani Vote Results -- A DayEarly. *Radio Free Europe*. https://www.rferl.org/a/azerbaijan-election-app- results/25131902.html

Bossuroy, & Thomas. (2007). Voting in an African democracy: does only ethnicityrule. *EHESS, Paris School of Economics, DIAL, mimeo*.

Brecorder. (2021, March 21). Digital voting no feasible option: ex-ECP official.

Business Recorder. https://www.brecorder.com/news/40075960

Brennan Center Quick Take. (2018). *Senate Intelligence Committee's Election Security Recommendations. Brennan Center for Justice.* https://www.brennancenter.org/our-work/analysis-opinion/brennan-center-quick-take-senate-intelligence-committees-election.

Burke, J. (2017, September 20). Kenyan election annulled after result called beforevotes counted, says court. *The Guardian*. https://www.theguardian.com/world/2017/sep/20/kenyan-election-rerun-not- transparent-supreme-court

Burton, Craig and Culnane, Chris and Schneider, & Steve. (2016). vvote: Verifiableelectronic voting in practice. *IEEE Security \& Privacy*, *14*, 64--73.

Carter Center Limited Mission to the May 2010 Elections in the Philippines. (2010,June 11). The Carter Center.

https://www.cartercenter.org/resources/pdfs/news/peace_publications/election_reports/philippines-may%202010-elections-finalrpt.pdf

CCE. (2021, May). *CCE Report {$\vert$} Reclaim the Republic*. https://www.reclaimtherepublic.co/report

Center, & Carter. (2012). The Carter Center Handbook on Observing Electronic Voting. *January. Atlanta, GA: Carter Center*. https://www. cartercenter. org/resources/pdfs/peace/democracy/des/Carter-Center-E_voting-Handbook. pdf

Chaudhry, A. (2021, May 9). Ordinance issued for procurement of e-votingmachines. *Dawn*. https://www.dawn.com/news/1622847

Cheeseman, Nic, Lynch, Gabrielle, Willis, & Justin. (2018). Digital dilemmas: The unintended

consequences of election technology. *Democratization*, *25*, 1397--1418.

Chipchase, & Jan. (2005). Understanding non-literacy as a barrier to mobile phone communication. *Retrieved September 16*.

Clooney, G., & Prendergast, J. (2022). *Electronic Voting Technology DRC*. The Sentry. https://thesentry.org/reports/electronic-voting-technology-drc/

Committee on Science, Technology, and Law, Committee on the Future of Voting: Accessible, Reliable, Verifiable Technology, Policy and Global Affairs, Division on Engineering and Physical Sciences, Computer Science and Telecommunications Board, & National Academies of Sciences, Engineering, and Medicine. (2018).

Securing the Vote: Protecting American Democracy. National Academies Press.

Commonwealth Secretariat. (2020). *Cybersecurity for Elections: A CommonwealthGuide on Best Practice*. Commonwealth Secretariat.

Correspondent. (2014, November 17). Parliamentary panel ambivalent overuse of EVMs for polling. *The Express Tribune*. https://tribune.com.pk/story/792551/parliamentary-panel-ambivalent-over-use- of-evms-for-polling

Correspondent. (2021, June 19). ECP expresses reservations over election amendment bill. *The Express Tribune*. https://tribune.com.pk/story/2306094/ecp- expresses-reservations-over-election-amendment-bill

Correspondent, O. (2017, March 11). *ECP places order for 150 voting machines*. *The Express Tribune*. https://tribune.com.pk/story/1352315/ecp-places-order-150- voting-machines

Council of Europe. (2016). *Using International Election Standards: Council of EuropeHandbook for Civil Society Organisations*. Council of Europe Publishing.

Dawn Editorial. (2021, May 21). *Debating poll reform* - Newspaper - DAWN.COM.

Dawn. https://www.dawn.com/news/1624823

Debnath, Sisir, Kapoor, Mudit, Ravi, & Shamika. (2017). The impact of electronic voting machines on electoral frauds, democracy, and development. *Democracy, andDevelopment (March 16, 2017)*.

Dechand, Sergej, Schurmann, Dominik, Busse, Karoline, Acar, Yasemin and Fahl, &Sascha and Smith, Matthew. (2016). An empirical study of textual key-fingerprint

representations. In *Proceedings of The25th USENIX Security Symposium*. USENIXAssociation.

DR. (2011). *Electronic Voting Machines: The Promise and Perils of a New Technology*. https://democracy-reporting.org/wp-content/uploads/2016/02/dri_briefing_paper_11_-

_electronic_voting_machines.pdf}, publisher= {Democracy ReportingInternational

Ebrahim, Z. T. (2021, February 21). ECP goes public on attempted rigging in by-election. *Dawn*. https://www.dawn.com/news/1608489

e-Estonia. (2017, July 20). World's most hi-tech voting system raises cyber defences.*e-Estonia*. https://e-estonia.com/worlds-most-hi-tech-voting-system-raises-cyber- defences/

e-Estonia. (2017, September 25). Estonia's i-voting: more secure, more popular. *e- Estonia*. https://e-estonia.com/estonias-i-voting-more-popular-more-secure/

Election Commission of Pakistan. (2010, September 7). *Election Commission of Pakistan:Final Report on the use of EVMs*. ACE Electoral Knowledge Network —. https://aceproject.org/ero-en/regions/asia/PK/pakistan-final-report-of-the-

committee-on-the-use

Election Commission of Pakistan. (2018). *ECP Report on I-Voting Trial*. https://ecp.gov.pk/documents/ivotingreport.pdf

Elections Act. (2017, October 2). *ISLAMABAD, MONDAY, OCTOBER 2, 2017, PART I*

Acts, Ordinances, President's Orders and Regulations NATIONAL ASSEMBLY SECRETARIAT. Election Commission of Pakistan. Retrieved February 16, 2022, from https://www.ecp.gov.pk/Documents/laws2017/Election%20Act%202017.pdf

ELECTORAL ROLLS. (2021). ECP. *ECP - Election Commission of Pakistan*. https://www.ecp.gov.pk/frmGenericPage.aspx?PageID=3047

Electronic Voting | US House of Representatives: History, Art & Archives. (2022).History House Gov. Retrieved February 18, 2022, from https://history.house.gov/Exhibitions-and-Publications/Electronic- Technology/Electronic-Voting/

Ellison, & Carl. (2003). UPnP Security Ceremonies Design Document for UPnPDevice Architecture 1.0. In *UPnP Forum*.

Endy Bayuni. (2019, May 7). *Voting-made-easy has a cost: Over 400 deaths*. The Jakarta Post. Retrieved February 8, 2022, from https://www.thejakartapost.com/academia/2019/05/07/voting-made-easy-has-a- cost-over-400-deaths.html

Express Tribune Editorial. (2021, September 23). Electoral reforms. *The Express Tribune*. https://tribune.com.pk/story/2321416/electoral-reforms

FAFEN. (2013). *General Election 2013, FAFEN Observation*. FAFEN. https://fafen.org/wp-content/uploads/2014/12/Key-Findings-May13.pdf

FAFEN. (2018). General Election Observation, 2018. *Free and Fair Election Network*. https://fafen.org/wp-content/uploads/2019/04/FAFEN-2018-General-Election-Result-Analysis-Report-Pakistan-Complete.pdf

FAFEN General Election Observation 2018 Result Assessment and Analysis. (2018). FAFEN. Retrieved February 8, 2022, from https://fafen.org/fafen-general-election-observation-2018-result-assessment-and-analysis/

Filipinas Heritage Library. (2021, May 10). *A History of Automated Elections in the Philippines*. Filipinas Heritage Library. https://www.filipinaslibrary.org.ph/articles/a-history-of-automated-elections-in- the-philippines/

Fujiwara, & Thomas. (2015). Voting technology, political responsiveness, and infant health: Evidence from Brazil. *Econometrica*, *83*, 423--464.

General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia. (2019). https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf

Ghaffar, Abdul, Azhar, & Tashfeen M. (2017). The Key to Triumphant Practices of

Technology in Elections: It's Time to Reboot Electoral Process in Pakistan. *Journal ofManagement and Research*, *4*, 1--17.

Goldsmith, Ben, Ruthrauff, & Holly. (2013). *Implementing and overseeing electronicvoting and counting technologies*. International Foundation for Electoral Systems.

Gotinga, J. (2015, August 14). *Comelec to lease 94,000 new machines for 2016 elections*. CNN Philippines. Retrieved February 18, 2022, from https://cnnphilippines.com/news/2015/08/13/Comelec-decision-lease-94K-new-machines.html

Gul, A. (2021). *Electoral Voting Machines, PIDE Webinar Brief*. Pakistan Institute of Development Economics. https://pide.org.pk/research/electoral-voting-machines

G.V.L. N. Rao. (2010). *Democracy at Risk!Citizens for Verifiability,Transparency \&Accountability in Elections*. Veta. http://indianevm.com/book.php

Hao, Feng and Wang, Shen and Bag, Samiran and Procter, Rob and Shahandashti,Siamak F and Mehrnezhad, Maryam and Toreini, Ehsan and Metere, Roberto andLiu, & Lana YJ. (2020). End-to-End Verifiable E-Voting Trial for Polling Station Voting. *IEEE Security \& Privacy*, *18*, 6--13.

Hapsara, Manik and Imran, Ahmed, and Turner, & Timothy. (2017). E-Voting in Developing Countries. In *Electronic Voting* (36--55). Springer. 10.1007/978-3-319-52240-1_3

Herstatt, Maximilian, Herstatt, & Cornelius. (2014). India's Electronic VotingMachines (EVMs): Social construction of a" frugal" innovation.

The History of Electronic Voting — Superior Electoral Court. (2022). SuperiorElectoral Court. https://english.tse.jus.br/news/the-history-of-voting

History of EVM. (2022). Election Commission of India. Retrieved February 18, 2022, from https://eci.gov.in/voter/history-of-evm/

Howard, E., & Rosenzweig, P. (2021, February 1). Risk-Limiting Audits in Arizona.*Brennan Center for Justice*. https://www.brennancenter.org/our-work/research- reports/risk-limiting-audits-arizona

Hussain, Z. (2020, July 17). NA briefed on economic cost of sit-ins. *Dawn*. https://www.dawn.com/news/1569471

IFES. (2014, June 19). Pakistan Electoral Integrity Assessment | IFES. *TheInternational Foundation for Electoral Systems*. https://www.ifes.org/news/pakistan-electoral-integrity-assessment

IFES. (2021, March 2). Risk-Limiting Audits: A Guide for Global Use. *The International Foundation for Electoral Systems*. https://www.ifes.org/publications/risk-limiting-audits-guide-global-use

Imran, N., & Bari, F. (2017, October 20). E-voting machines to be used in NA-4 by-elections. *Dawn*. https://www.dawn.com/news/1365009

Imran Khan on Twitter. (2021). Imran Khan on Twitter. In *Imran Khan on Twitter*.Twitter. https://twitter.com/ImranKhanPTI/status/1388431468259680256

India Times. (2011). Pakistan Election Commission interested in Indian EVMs. https://economictimes.indiatimes.com/news/politics-and-nation/pak-ec- interested-in-indian-evms/articleshow/7342874.cms?from=mdr

Inspector General. (2021, March 29). *Evaluation of Department of Defense Voting Assistance Programs for Calendar Year 2020*. https://media.defense.gov/2021/Mar/31/2002611446/-1/-1/1/DODIG-2021-066_REDACTED.PDF

Internet Voting Taskforce. (2018). *Findings and Assessment Report of Internet VotingTask Force on Voting Rights of Overseas Pakistanis*. https://www.ecp.gov.pk/ivoting/IVTF/Report/Executive/Version/1.5/Final.pdf

Introducing Electronic Voting: Essential Considerations. (2011). International Institute for Democracy and Electoral Assistance (International IDEA).

Inuwa, Ibrahim, Oye, & ND. (2015). The impact of e-voting in developing countries:focus on Nigeria. *International Journal of Pure and Applied Sciences and Technology*,*30*, 43.

Irani, B. (2018, May 13). *EC to buy 2535 new EVMs at four times the cost of previous models*. Dhaka Tribune. Retrieved February 18, 2022, from https://archive.dhakatribune.com/bangladesh/2018/05/13/ec-to-buy-2-535-new-evms-at-four-times-the-cost-of-previous-models

IVTF Report. (2018). *Findings and Assessment Report of Internet Voting Task Force on Voting Rights of Overseas Pakistanis*. https://www.ecp.gov.pk/ivoting/IVTF\%20Report\%20Executive\%20Version\%201.5\%20Final.pdf

Jafri, O. (2012, April 26). PP-194 seat: PPP's Usman Bhatti squeezes in a win by 400votes. *The Express Tribune*. https://tribune.com.pk/story/370403/pp-194-seat-ppp%E2%80%99s-usman-bhatti-squeezes-in-a-win-by-400-votes

Jillbert, Julius, Musaruddin, & Mustarum. (2003). ONLINE VOTING FOR E- DEMOCRACY IN DEVELOPING COUNTRIES: IS IT POSSIBLE?

Jokura, T. (2021). *Brazil's electronic voting machine comes of age*. Revista Pesquisa Fapesp. https://revistapesquisa.fapesp.br/en/brazils-electronic-voting-machine- comes-of-age/

Kagawaran. (2022). *Historical data on overseas voter registration and voter turnout*. DFA. https://dfa.gov.ph/historical-data-on-overseas-voter-registration-and-voter-turnout

Khan, Muhammad Qasim, Mehmood, Feroz, Khan, Dawood, Hussain, & Walayat. (2011). Barriers to implement E-voting system in Pakistan. *Journal of Applied andEmerging Sciences*, *2*, pp131--135.

Khan, I. A., Imran, N., & Bari, F. (2014, November 14). Electronic voting machines can be manipulated more easily: ECP. *Dawn*. https://www.dawn.com/news/1144417

Khan, I. A., Naqvi, J., & Lodhi, M. (2021, November 24). ECP forms three panels toenforce EVM legislation. *Dawn*. https://www.dawn.com/news/1659858

Khawaja, Asma Shakir, Hasan, & Jamal. (2016). Implementing biomatric voting system in Pakistan: an anaytical review. *Journal of the Research Society of Pakistan*,*53*.

Kreigler, J. (2011, October 26). *Direct Democracy:* The International Foundation for Electoral Systems. Retrieved February 16, 2022, from https://www.ifes.org/sites/default/files/20111026_direct_democracy_progress_and_pitfalls_election_technology_yard_0.pdf

Kshetri, & Nir. (2007). Barriers to e-commerce and competitive business models indeveloping countries: A case study. *Electronic commerce research and applications*,*6*.

Kuenzi, R. (2019, August 2). These are the arguments that sank e-voting in Switzerland. *SwissInfo*. https://www.swissinfo.ch/eng/e-voting_these-are-the- arguments-that-sank-e-voting-in-switzerland/45136608

Lindeman, M., & Stark, P. B. (2012). A Gentle Introduction to Risk Limiting Audits.*IEEE Security & Privacy*. https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

Lindeman, M., Stark, P. B., & Yates, V. S. (2012). *BRAVO: Ballot-polling Risk-limitingAudits to Verify Outcomes*. USENIX. https://www.usenix.org/conference/evtwote12/workshop-program/presentation/lindeman

Machin-Mastromatteo, & Juan D. (2016). The most “perfect” voting system in the

world. *Information Development*, *32*, 751--755.

Making real the promises of democracy. (2020, October 8). American Friends ServiceCommittee. Retrieved February 16, 2022, from https://www.afsc.org/newsroom/making-real-promises-democracy

Maleti, Marija, Bara, Du, Rako, evi, Vuk, Naumovi, Tamara, Bjelica, & Artur. (2019).Scaffolding e-voting in developing countries. *Management: Journal of Sustainable Business and Management Solutions in Emerging Economies*, *24*, 47--62.

Manila, & The Philippines. (2016, May). *Philippine Votes Transmitted in Record Timein Largest Ever Electronic Vote Count*. Smartmatic. https://www.smartmatic.com/media/article/philippine-votes-transmitted-in- record-time-in-largest-ever-electronic-vote-count/

Maphunye, & Kealeboga J. (2019). The feasibility of electronic voting technologies in Africa: Selected case examples.

McGaley, Margaret, Gibson, & J Paul. (2003). E-voting: a safety critical system. *NUIMaynooth, Computer Science Department, Tech. Rep. NUIM-CS-TR-2003-02*.

Melia, P., & Byrne, L. (2012, June 29). €54m voting machines scrapped for €9 each.*Independent.ie*. https://www.independent.ie/irish-news/54m-voting-machines- scrapped-for-9-each-26870212.html

Microsoft SEAL. (2022). *Microsoft SEAL: Fast and Easy-to-Use HomomorphicEncryption Library*. Microsoft. Retrieved February 17, 2022, from https://www.microsoft.com/en-us/research/project/microsoft-seal/

Ministry of Local Government and Regional Development. (2006). *Electronic Voting, Challenges and Opportunities*. https://www.regjeringen.no/globalassets/upload/kilde/krd/red/2006/0087/ddd/ pdfv/298587-evalg_rapport_engelsk201106.pdf

Minsait. (2021). *Consultancy for the analysis, design and implementation of Internet voting for overseas Pakistanis, Audit Report*. https://www.ecp.gov.pk/documents/reports/Final%20report%20by%20Minsait% 20Final.pdf

Moher, Ester, Clark, Jeremy, Essex, & Aleksander. (2014). Diffusion of voter responsibility: Potential failings in E2E voter receipt checking. *USENIX Journal ofElection Technology and Systems (JETS)*, *1*, 1--17.

Morgan, S. (2021).

Nandi, Mridul, Popoveniuc, Stefan, Vora, & Poorvi L. (2010). Stamp-it: a method forenhancing the universal verifiability of e2e voting systems. In *International Conference on Information Systems Security* (81--95).

Naqvi, J., & Lodhi, M. (2021, May 9). Ordinance issued for procurement of e-votingmachines. *Dawn*. https://www.dawn.com/news/1622847

National Academies of Sciences, & Engineering, and Medicine and others. (2018).

Securing the Vote: Protecting American Democracy.

National Democratic Institute. (2013, December 17). *Timeframe for considerationand adoption*. National Democratic Institute. Retrieved February 18, 2022, from https://www.ndi.org/e-voting-guide/timeframe

National Democratic Institute. (2022). *Challenges and Recounts: Political Parties and the Complaints Process in the Philippines*. National Democratic Institute.

https://www.ndi.org/e-voting-guide/examples/challenges-and-recounts- philippines

NBC News. (2018, November 6). Voters face malfunctioning machines and long linesat polls. *NBC News*. https://www.nbcnews.com/politics/elections/midterms-2018- voters-face-malfunctioning-machines-long-lines-polls-across-n932156

Newman, L. H. (2019, September 26). Some Voting Machines Still Have Decade-Old Vulnerabilities. *WIRED*. https://www.wired.com/story/voting-village-results- hacking-decade-old-bugs/

Norris, Pippa, Max, & Gromping. (2019). Electoral Integrity Worldwide. *Sydney: TheElectoral Integrity Project*.

ODIHR. (2013). SCE Office for Democratic Institutions and Human Rights. In

Handbook for the Observation of New Voting Technologies. ODIHR. Oganesyan, & Rafael. (2014). Economic Voting in the Developing World.

Okoro, & Ephraim. (2016). A Cost-Benefit Analysis of Electronic Voting Operations and Capabilities in sub-Saharan Africa.

Olembo, Maina M and Kilian, Timo and Stockhardt, Simon and Hulsing, Andreas andVolkamer, & Melanie. (2013). Developing and Testing a Visual Hash Scheme. In *EISMC* (91--100).

Olembo, M Maina, Renaud, Karen, Bartsch, Volkamer, Steffen, & Melanie. (2014). Voter, what message will motivate you to verify your vote. In *Workshop on UsableSecurity, USEC*.

Orcutt, M. (2016, August 18). Internet Voting Leaves Out a Cornerstone of Democracy: The Secret Ballot. *MIT Technology Review*. https://www.technologyreview.com/2016/08/18/107858/internet-voting-leaves- out-a-cornerstone-of-democracy-the-secret-ballot/

Osho, Lauretta O, Abdullahi, Muhammad B, & Oluwafemi. (2016). Framework for anE-Voting System Applicable in Developing Economies. *International Journal of Information Engineering \& Electronic Business*, *8*, 6.

Osho, Lauretta O, Abdullahi, Muhammad B and Osho, & Oluwafemi. (n.d.).International Journal of Information Engineering \& Electronic Business.

Paravicini, G. (2018, December 13). Congo fire destroys thousands of voting machines for presidential election. *Reuters*. https://www.reuters.com/article/us-congo-election-fire-idUSKBN1OC0VP

Paravicini, G. (2018, December 13). *Congo fire destroys thousands of voting machines for presidential election*. Reuters. Retrieved February 18, 2022, from https://www.reuters.com/article/us-congo-election-fire-idUSKBN1OC0VP

Park, Sunoo and Specter, Michael and Narula, Neha and Rivest, & Ronald L. (2021).Going from bad to worse: from internet voting to blockchain voting. *Journal of Cybersecurity*, *7*, tyaa025.

Patinio, F. (2019, June 6). *Manual audit reports 99% accuracy rate of May 13 polls*.Philippine News Agency. Retrieved February 18, 2022, from https://www.pna.gov.ph/articles/1071703

Perrig, Adrian, Song, & Dawn. (1999). Hash visualization: A new technique toimprove real-world security. In *International Workshop on Cryptographic Techniques and E-Commerce* (Vol. 25).

POONAM AGARWAL. (2019, February 2). EVM Hacking Row: EC's 2 Sets of Data in MP Election 2018 Show Discrepancies in the Vote Count. *The Quint*. https://www.thequint.com/news/india/evm-hacking-tampering-malfunction-mp-election-2018-discrepancies-vote-count

Pressing the button for European elections: verifiable e-voting and public attitudes toward internet voting in Greece. (2014). In R. Krimmer & M. Volkamer (Eds.), *2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE) : 28-31October 2014 : Lochau/Bregenz, Austria : IEEE Proceedings EVOTE2014*. IEEE.

Press Trust India. (2014). *Electronics Corp, Bharat Electronics get EVM contracts | Business News*. The Indian Express. https://indianexpress.com/article/business/companies/electronics-

corp-bharat- electronics-get-evm-contracts/

Reynolds, Andrew, Reilly, Ben, Ellis, & Andrew. (2008). *Electoral system design: The new international IDEA handbook*. International Institute for Democracy and Electoral Assistance.

Ross, A., & Lewis, D. (2018, March 9). *In Congo, voting machines raise suspicionsamong president's foes*. Reuters. Retrieved February 18, 2022, from https://www.reuters.com/article/us-congo-election-idUSKCN1GL13W

Ross, M. (2020, January 9). Chinese Technology in Voting Machines Seen as Emerging Threat. *Bloomberg Law*. https://news.bloomberglaw.com/privacy-and- data-security/chinese-technology-in-voting-machines-seen-as-emerging-threat

Ruth, D., & Hodges, A. (2012). *Post-Election Auditing: Effects of Election Procedure and Ballot Type on Manual Counting Accuracy, Efficiency and Auditor Satisfaction and Confidence*. https://news2.rice.edu/2012/02/02/hand-counts-of-votes-may-cause- errors-says-new-rice-u-study/

Ryan, & Peter YA. (2011). Pret a Voter with Confirmation Codes. *EVT/WOTE*, *11*.

Saadat, S. (2018, August 4). 'Stamped' ballot papers recovered from garbage dump,this time in Peshawar. *Dawn*. https://www.dawn.com/news/1424749

Sadaqat, M. (2015, July 16). NA-19, Haripur: Biometric system in the offing for by-polls. *The Express Tribune*. https://tribune.com.pk/story/921528/na-19-haripur- biometric-system-in-the-offing-for-by-polls

Schneider, Steve, Llewellyn, Morgan, Culnane, Chris, Heather, James, Srinivasan, Sriramkrishnan, Xia, & Zhe. (2011). Focus group views on Pret a Voter 1.0. In *2011International Workshop on Requirements Engineering for Electronic Voting Systems*(56--65).

Schneier, & Bruce. (2021, May). *Essays: In Praise of Security Theater - Schneier on Security*. https://www.schneier.com/essays/archives/2007/01/in/_praise/_of/_securit.html

Silva, R. (2020). *The public security test of Brazilian e-Voting system: the challenges inpre-electoral observation*.

https://www.researchgate.net/publication/345439719_The_public_security_test_of

_Brazilian_e-Voting_system_the_challenges_in_pre-electoral_observation

Sinha, R. (2019, October 22). Why EVMs always 'malfunction' in favour of the BJP? *National Herald*. https://www.nationalheraldindia.com/india/why-evms-always-malfunction-in-favour-of-the-bjp

Solehria, Salman Faiz, Jadoon, & Sultanullah. (2011). Cost effective online voting system for Pakistan. *International Journal of Electrical \& Computer Sciences*, *11*, 39--47.

Somanathan, & Madhavan. (2019, May). India's electoral democracy: How EVMscurb electoral fraud. *Brookings*. https://www.brookings.edu/blog/up- front/2019/04/05/indias-electoral-democracy-how-evms-curb-electoral-fraud

Team, & Web Development. (2021, April). Official COMELEC Website: Commissionon Elections. In *COMELEC*. https://comelec.gov.ph/?r=2016NLE/Statistics/VotersTurnout2016NL

The National Academy of Sciences. (2018). *SECURING THE VOTE Protecting American Democracy*. https://www.nap.edu/resource/25120/Securing%20the%20Vote%20ReportHighlights.pdf

The NBC News. (2020, September 11). With election cybersecurity experts in shortsupply, some states call in the National Guard. *NBC News*. https://www.nbcnews.com/tech/security/election-cybersecurity-experts-short-

supply-some-states-call-national-guard-n1238893

The Parliament of Victoria. (2016). Inquiry into Electronic Voting. In *The Parliamentof Victoria*. https://www.parliament.vic.gov.au/file_uploads/EMC_Inquiry_into_electronic_votin g_HDMYyfRd.p

The Wire. (2021, March 15). ECI's Conduct of 2019 Elections Raises 'Grave Doubts'About Its Fairness: Citizens' Report. *The Wire*. https://thewire.in/rights/election- commission-bjp-polls-fairness-citizens-commission-on-elections-report

Thomas, M., & Khuhro, Z. (2018, August 28). RTS failure - Newspaper - DAWN.COM.

Dawn. https://www.dawn.com/news/1429434

Thomas, M., & Khuhro, Z. (2021, March 15). Govt asks ECP members to resign after'losing confidence of the people'. *Dawn*. https://www.dawn.com/news/1612691/govt-asks-ecp-members-to-resign-after- losing-confidence-of-the-people

Tjostheim, T and Peacock, Thea, Ryan, & Peter YA. (2007). A case study in system- based analysis: the ThreeBallot voting system and Pret a Vote. *School of ComputingScience Technical Report Series*.

U.S. Department of Homeland Security. (2017, January 6). Statement by Secretary Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector. *Homeland Security*. https://www.dhs.gov/news/2017/01/06/statement- secretary-johnson-designation-election-infrastructure-critical

Vaalit. (n.d.). *Electronic Voting in Finland, The Electronic Voting Experiment*. https://vaalit.fi/en/electronic-voting1

Wasim, A., & Khan, R. (2018, August 2). RTS controversy likely to haunt ECP, Nadrafor a long time. *Dawn*. https://www.dawn.com/news/1424394

Wasim, A., & Saadat, S. (2018, August 2). RTS controversy likely to haunt ECP, Nadrafor a long time. *Dawn*. https://www.dawn.com/news/1424394

Weber, Shlomo, Davydov, Denis, & others. (2017). Societal and economic effects oflinguistic diversity. *VOPROSY ECONOMIKI*, *11*.

World's most hi-tech voting system raises cyber defences. (2019). e-Estonia. https://e-estonia.com/worlds-most-hi-tech-voting-system-raises-cyber-defences/

Wrong, M. (2013, March 7). In Kenya's High-Tech Election, Almost Everything ThatCould Have Gone Wrong Did. *Latitude*. https://latitude.blogs.nytimes.com/2013/03/07/in-kenyas-high-tech-election- almost-everything-that-could-have-gone-wrong-did/

Yard, & Michael. (2010). *Direct Democracy: Progress and Pitfalls of Election Technology*. International Foundation for Electoral Systems Washington, DC.

Zagorski, Filip and Carback, Richard T and Chaum, David and Clark, Jeremy and Essex, Aleksander, and Vora, & Poorvi L. (2013). Remotegrity: Design and use of anend-to-end verifiable remote voting system. In *International Conference on AppliedCryptography and Network Security* (441--457). Springer.

Zollinger, Marie-Laure, Distler, Verena, Roenne, Peter, Ryan, Peter, Lallemand, Carine, Koenig, & Vincent. (2019). User experience design for e-voting: How mentalmodels align with security mechanisms. *Electronic Voting*.

APPENDIX A

Summary and Recap of Key Issues in General Elections

Pakistan with its 200 million citizens ranks 6th in the world in regard to population. It has an electorate of 118 million voters (ELECTORAL ROLLS, 2021). However, elections here are routinely contentious and frequently result in political deadlock, street protests, and violence.

Prior to 1970, Pakistan had no national direct elections. Unfortunately, in the aftermath of the first ever general elections in 1970, the political situation escalated into a civil war that led to the creation of East Pakistan. Democracy returned to the country in 1972, with Zulfiqar Ali Bhutto instated as Prime Minister (PM). General elections were held again in 1977, with Pakistan's People Party (PPP) winning handily. However, accusations of rigging by the opposing Pakistan National Alliance (PNA) resulted in turmoil and violent protests, leading to Martial Law under General Zia-ul-Haq, which lasted over a decade. Thereafter PPP and PMLN took turns to form government in 1988, 1990,1993,1997 but none could complete its turn. Martial law returned in 1999 under General Musharraf. The next general elections happened in 2008 when the PPP formed the government. But keeping its tradition of electoral violence, in the run up to the elections Benazir Bhutto was assassinated in a political rally. After obtaining majority of seats in the elections, the PML (N) formed the governmentin 2013. This was the country's first transfer from one civilian government to another, and it was animportant step forward for democracy. However, major rigging allegations in the general elections of 2013 resulted in mass protests and a public sit-in by the PTI. Lasting over four months, this was the longest protest in Pakistan's history, causing estimated losses of over Rs 1.5 billion (Imran & Bari, 2020). Following the 2018 elections when PTI came into power, the failure of the RTS (automated results management system) led to widespread accusations of fraud and irregularity by the opposition, making the General Elections 2018 controversial. (Wasim & Khan, 2018).

In the 11 General elections Pakistan has conducted since independence, hundreds of lives have been lost as incidents of election related violence, gun, and bomb attacks, sparked by the perennial mistrust in the credibility of elections, routinely mar the election discourse.

Systemic corruption and procedural inefficiencies run rife in the electoral system. And the current paper-based elections present with the perfect means to exploit these systemic issues. According toFAFEN's report, election malpractices and major election day irregularities include:

- Partisan election officials campaigning for a certain party or candidate.
- Polling station capture by unauthorized individuals
- Voters trying to cast multiple votes or ineligible parties trying to cast votes.
- The percentage of spoiled/rejected votes far exceed the normal range of 2 to 3 percent, andoften greater than the margin of victory.
- The lack of publicly official documents from all polling stations on ECP website.
- Last minute changes in polling schemes.
- Preventing or restricting observers from observation.
- Unofficial breaks in voting as well as extension in polling hours.
- Lapses in following procedures such as failure to seal ballot boxes.

- Lack of basic training of the election staff regarding how to correctly fill critical forms.
- Lack of transparent and standardized counting procedures.
- Lack of vote audit solutions and lack of robust dispute resolution mechanisms.
- Violence, Voter intimidation, bribery and coercion, barring women from voting.
- Minimal security deployment outside polling stations.

APPENDIX B

EVM Myths and Common Concerns

The Challenge of Using Electronic Voting Machines EVMs are a unique case. The fundamental requirement of the secrecy of the ballot, means that the identity of the voter needs to be stripped off from the vote itself. This severely limits auditing and accounting activities. Most other IT systems rely on rigorous logging of events and an audit trail to track and monitor any transactions and activities performed. We discuss this in detail in Appendix B. Until recently, separating the voter's identity from the cast vote meant that there was no way to ascertain if the vote was indeed counted in the final tallyas cast by the voter. Consequently, voting systems have relied on indirect proofs through paper trailsand strict procedural checks and balances. Without such procedures incorporated with the introductions of EVMs, the process could be rendered more vulnerable than it was in paper-based systems. The fundamental difficulty in designing EVMs is to reconcile the conflicting requirements of process openness and vote secrecy. As we discuss in our paper, new election technologies such as End-to-End verifiable voting resolve this dilemma.

The most striking example of this is the friction between ballot secrecy and election integrity. The name of the voter is stripped from the vote, to ensure ballot secrecy. However, this same act makes it very difficult to track the vote and ensure that it has not been modified. Similarly, stakeholders can inadvertently take electoral efficiency to mean electoral transparency. Michael Yard of IFES notes: "*This is not to say the efficiency in elections is, in itself, a bad thing; on the contrary, it is only when efficiency comes into conflict with transparency that it becomes undemocratic.*" (Kreigler, 2011) A narrow focus on efficiency can result in deployment of "*black box*" components that "*lead to more efficient development and employment*", but these risks transferring power "*away from the many*" into the "*hands of the few*" (Cheeseman et al., 2018)

As a baseline, to justify the use of EVMs for elections in Pakistan, we should identify a system that, at the very minimum, provides significant advantages over paper-based elections. These advantages could be in terms of superior security, greater transparency, reduced election costs, simplified logistics, etc. These benefits need to be documented and spelled out explicitly in rigorous cost-benefit analyses. In the absence of a rigorous assessment, the introduction of technology "*may create significant opportunities for corruption that (among other things) vitiate their potential impact... precisely because new technology tends to deflect attention away from more 'traditional' strategies, the failure of digital checks and balances often renders an electoral process even more vulnerable to rigging than it was before".* (Cheeseman et al., 2018)

Banking vs Voting - Election Security is Unique

One of the most frequently asked questions in the debate around Internet voting, is that in a world where online banking and commerce applications are pervasive, why can citizens not vote online? This question raises a valid point, as if we can trust the internet with our monetary transactions, then why not our vote? Banking and E-commerce applications are critical in nature and organizations go to great lengths to secure them. Regardless, cybercrime related to such breaches amounts to a staggering $ 6 trillion annually and is expected to rise to $10 trillion by 2025 (Morgan, 2021). Such breaches have been accepted as the cost of doing business, a stance which is unacceptable when it comes to elections and democracy.

Furthermore, the techniques that are used to secure our monetary transactions cannot be extended to Internet voting. For instance, maintaining thorough records and fine-grained audit trails of every transaction is routine in financial institutions. However, maintaining any such information such as the vote and the identity of the voter are in direct violation of the principle of the secret ballot. Similarly, financial institutions have recovery protocols such as reversing transactions, blocking stolen cards, compensating customers etc. However, in the case of Internet Voting and elections there is no way to undo a miscast vote or compensate a voter. The nature of elections is also far more sensitive than a financial transaction. Therefore, the USA classifies election infrastructure as critical national infrastructure. The incidence of election tampering raises serious questions over national sovereignty and seriously impacts citizen confidence.

When the voting ritual is taken out of the polling station to an unsupervised environment many newconcerns about the integrity of an election are raised. In addition to above, these also include the possible violation of the vote secrecy, voter coercion and buying, possible disenfranchisement of voters due to the digital divide to name a few.

Estonia and the Myth of Stand-alone Internet Voting

To allay a few of the concerns listed above and to diminish their impact, Internet voting can be run in parallel to paper based or internet voting systems giving the voters the choice to cast their vote. This is true for Estonia, the only nation to deploy remote Internet-based voting on a national scale. However, it provides internet voting as an alternate channel and voters may cast their vote using thepaper-based system in the polling station. Voters may cast multiple votes and the paper-based vote would override the internet-based vote. This is done to ensure if a voter has been coerced to vote a certain way, he / she can still salvage their vote.

APPENDIX C

Security Timeline of Electronic Voting Machines

2003 – Diebold hack: In early 2003, activists found a version of Diebold's software on an unprotected server, where anyone could download it. This server was used by Diebold employees toupdate software on its machines. In addition to this security breach, the code, itself, had many security flaws. Researchers evaluated the penetrability of this software aided by the voting machinesource code that was available on the Internet. In their findings, they reported multiple vulnerabilities and deemed the system as unreliable and subject to abuse.

2004 – Voter Verified Paper Trails: In 2004, Nevada became the first US state to require all electronic voting machines used for federal elections to produce voter-verified paper trails and it became the first state in the U.S. to produce a paper trail of electronic ballots.

2005 - The Commission on Federal Election Reform recommends DREs to include VVPAT (Voter Verified Paper Audit Trails): The Commission on Federal Election Reform releases the report "Building Confidence in U.S. Elections", which makes the recommendation to include VVPAT for increasing trust in elections and improving election administration.

2005 – Black Box Voting, demonstrates hackability of the Electronic Voting Systems (Hursti hack) When invited by the Leon County Supervisor of Elections, Black Box Voting, an election watchdog, set up a demonstration of the Diebold machines. Computer security experts, Harri Hurstiand Herbert Thompson, were able to compromise the central vote tabulator of the Diebold machinesand alter the results of a mock election without any evidence of interference. During the attempt, Hursti discovered that Diebold's machines allowed negative votes, and changed the votes using onlya memory card - producing a "one-step hack" that could alter the central tabulator as well as the voting machine results to produce matched results.

2006 – Black Box Voting Highlights Electronic Voting Machines "Backdoors" Black Box Voting, in collaboration with Harri Hursti performed another penetration attempt on Diebold voting machines in Utah. Hursti found backdoor channels which make it possible for malicious software to be installed as early as the machines are manufactured.

2010 - National Database on Voting System Failures and Vulnerabilities Issued This report highlighted that even though electronic voting machine failures have been documented time and again, no concrete step has been taken to improve the security of the electronic voting machines. The report attributed this partly to the lack of legislation in this regard, as vendors are not legally obligated to report security vulnerabilities and past breaches to the election authorities.

2012- Voting Machine Malfunctions in 2012 Presidential Election In Pennsylvania, at least two electronic voting machines were recorded switching votes from Obama to Romney. According to thefounder of the watchdog group Verified Voting, this appeared to be a classic case of "vote-flipping", which in most cases is a result of improperly calibrated machines. Additionally, the elections were also rife with long waiting times with machine breakdowns in Virginia, causing 3–5-hour long lines leading to extended polling hours. Machine malfunctions were also reported in Georgia, South Carolina, Ohio, Colorado, and Wisconsin.

2013- NYC returns to Lever machines The NY State Legislature in 2013 authorized the return to the lever machines for the primary and any ensuing runoff. These lever machines were acquired in

the 1960s, and they replaced the $95 million electronic voting system because of the chaos that ensued in the 2012 election, as described above.

2017 – US Department of Homeland Security categorizes elections as "critical infrastructure" Prior to the USA, 2016 federal election, the information technology infrastructure of several state level and local election management bodies became victims of cyberattacks (purportedly of Russianorigin). As a result, in January 2017, the Department of Homeland Security (DHS) declared the election infrastructure as part of the nation's critical infrastructure. Under the designation, the DHS provides assistance, on a priority basis, that election officials can request for to reduce both cyber and physical risk to their election systems.

2018- National Academy of Sciences Report calls for Verifiable Voting and Risk Limiting Audits According to the 2018 National Academies of Sciences, Engineering and Medicines report, thecurrent state of election technology fails to guarantee vote secrecy, security, and verifiability. It suggested that the voting machines that do not provide a VVPAT should not be certified to be used inany future elections. The report also recommended the states to start trialing E2E-V voting systems and to mandate Risk-Limiting Audits prior to the certification of election results.

2018 -Internet Voting Task Force report calls for Verifiable Voting in Pakistan IVTF report urges election authorities to explore the adoption of E2E-V voting systems in elections to enable transparency and restore credibility of electoral processes, specifically in the context of Internet Voting for Overseas Pakistanis.

2018 – Estonia commits to Verifiable Voting Estonia expresses its resolve to deploy Verifiable Voting in the next nationwide elections.

2018 – Annual DEFCON Voting Village This event has gained recognition for being the only publicforum in the USA where hackers get unrestricted access to voting machines to discover vulnerabilities in the equipment. In 2018, the Voting Village made available over 30 electronic voting machines, most of which are still deployed for elections in the USA. According to the event's report, the participants were able to effectively breach the machines within minutes, revealing the inherent vulnerabilities in the electoral system and raising awareness about election security issues.

2019 – Estonia deploys Verifiable Voting in national elections Estonia becomes the first and only country in the world to deploy nationwide Internet Voting. It also became the first nationwide deployment of verifiable voting for binding national level elections.

2019- Microsoft partners with Galois to develop open-source E2E-V Voting software In 2019, Microsoft, in partnership with Galois, announced ElectionGuard, an open-source collection of modules that can be integrated to form an election system based on E2E-V Voting, and support risk-limiting audits that help assure the accuracy of elections.

2020 – Risk Limiting Audits implemented in multiple states in the U.S. In the U.S., a small community of practitioners has worked to convince legislators and administrators to adopt the

practice in several states. According to recent figures, more than 60 pilot RLAs have been conductedin the U.S.A. While around 8 U.S. states have made the use of RLAs mandatory. In 2020, 15 U.S. states implemented RLAs post-elections, with Virginia, Atlanta, Pennsylvania, confirming the results of the elections with the successful execution of their statewide Risk-Limiting Audit. The audit in Virginia confirmed the results of the presidential election and senate race with over 99% confidence.

2021-CCE report on Indian elections, calls for Verifiable Voting and Risk Limiting Audits Citizens' Commission on Elections (CCE) Report on Indian elections declared that DRE-VVPAT votingmachines currently deployed in India are not verifiable. Hence, they do not fulfill the requirements of free and fair elections. Additionally, even though VVPAT is installed in every EVM, yet the votes are not audited before declaring the results, exposing the elections to serious fraud. It emphasized the importance of RLA and E2E-V Voting to demonstrate the validity of election results and to increase trust in the democratic processes.

2021 – Microsoft announces Verifiable Voting partnership with Galois, Dominion, Smartmatic,Hart InterCivic, Clear Ballot In June 2021, Hart InterCivic and Microsoft entered a partnership to integrate ElectionGuard software into Hart's Verity voting systems, making it the first major voting machine manufacturer in the U.S. to provide end-to-end verifiability to voters.

Table 2: A Security TimeLine of EVMs

2003	Diebold Hack
2004	Voter Verified Paper Trail compulsory in NEVADA
2005	The Commission on Federal Election Reform recommends DREs to include VVPAT
2005	Black Box Voting demonstrates "Hursti Hack"
2006	Black Box Voting exhibits Electronic Voting Machines' "Backdoors"
2010	National Database on Voting System Failures and Vulnerabilities Issued
2012	Numerous Voting Machines Malfunction in Presidential Election
2013	NYC returns to Lever machines
2017	US Department of Homeland Security categorizes election infrastructure as "criticalinfrastructure"
2018	National Academy of Sciences Report calls for E2E-V Voting and Risk Limiting Audits
2018	Internet Voting Task Force report calls for E2E-V Voting in Pakistan
2018	Estonia commits to E2E-V Voting
2018	Annual DEFCON Voting Village, hackers compromise all machines
2019	Estonia deploys E2E-V Voting in national elections
2019	Microsoft partners with Galois to develop open-source E2E-V Voting software
2020	Risk Limiting Audits implemented in multiple states in the U.S.
2021	CCE report on Indian elections, calls for E2E-V Voting and Risk Limiting Audits

2021	Microsoft announces E2E-V Voting partnership with Galois, Dominion, Smartmatic, HartInterCivic, Clear Ballot

APPENDIX D

Primer on End-to-End Verifiable Voting

This section presents a primer on E2E-V Voting systems (Ali & Murray, 2016) intended for a non-technical audience. We motivate the case for their application in Pakistan. The explanation is intended to eschew the technical concepts and present them in a way that is understood by the non-technical audience. We purposely omit cryptography heavy descriptions and processes and try to convey the intuition and rationale behind the design of End-to-End Verifiable (E2E-V) voting systems. E2E-V Voting Systems are a promising new paradigm in the world of voting systems that provides voters strong cryptographic guarantees that their vote was **cast as intended**, was **recorded as cast,**and **tallied as cast** (Ali & Murray, 2016). Three guarantees it provides are

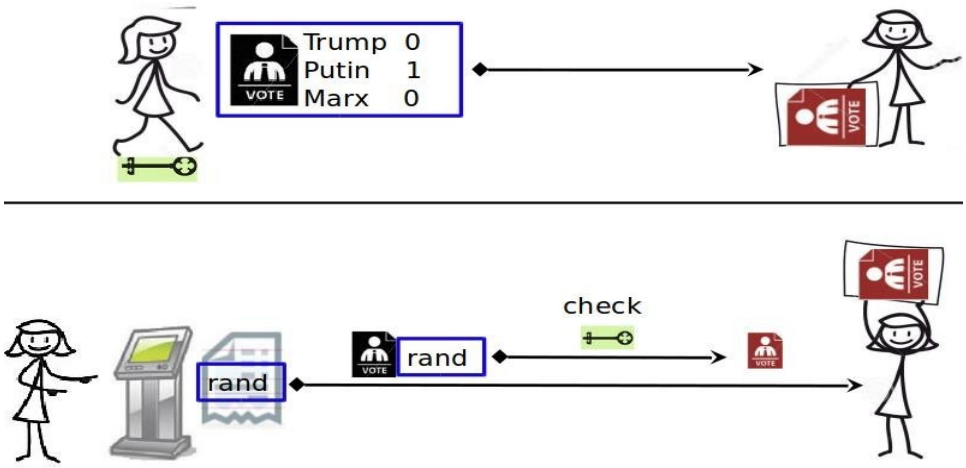
- Individual verifiability, which empowers any voter to confirm and verify that the votes castby them are correctly included in the set of votes cast.
- Universal verifiability, which empowers any voter to check and endorse that all the votes inthe ballot box have been counted with fidelity
- Additionally, Eligibility Verifiability guarantees provided by this class of voting systems helpvoters verify that all votes cast were cast by registered voters indeed.

We walk the read through what an experience with E2E-V Voting would look like:

The voter, Ali, visits the polling stations on the day of the election and presents identification information to help authenticate himself as an eligible voter. At the polling booth, Ali marks the option for his candidate by either through a touch or pressing of a button on the voting machine. Themachine records and encrypts his vote and provides him with a paper trail, just like a traditional EVM, but with one notable difference: it also prints and provides him with a receipt to take home, a small slip bearing a unique serial number and a verification code consisting of a string of random- looking characters, a cryptographic commitment to his vote. This receipt allows him to later ascertain that the vote cast by him has been accurately processed and included in the tally. However, the receipt does not reveal Ali's choice of candidate and he cannot use it to sell his vote or be coerced into votingfor a particular candidate.

However, Ali may suspect the machine is malfunctioning or has been tampered with. In this case, heavails an option to force the machine to reveal the cryptographic parameters it used to encrypt his vote. This step effectively “spoils” his ballot but allows him to double-check that the machine is operating correctly. He can repeat this step several times until he is ready to cast his vote. In the parlance of E2E-V voting systems, Ali is now confident that **his vote has been cast as intended**.

Figure 5 E2E-V Voting: Cast as Intended

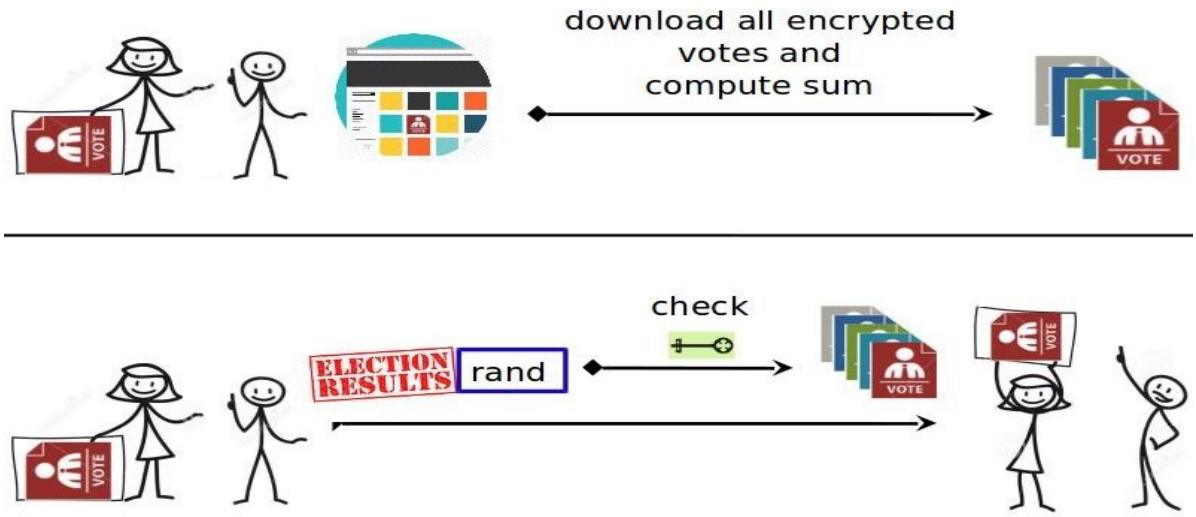


After the polls close, election officials upload copies of all receipts to the election website. Ali navigates to his receipt using the serial number. If anyone has tampered with his vote, he can detectit by comparing the receipt to the physical copy he holds in his hand and can file a complaint using his physical receipt as hard evidence. This gives his confidence that "**his vote has been recorded ascast"**. Statistical analyses indicate that if a mere fraction of voters were to check their votes in this way, they would detect any attempt at large scale vote tampering with very high likelihood.

Figure 6 E2E-Verifiable Voting: Recorded as Cast

E2E-V voting systems usually employ two key techniques to tally results in a privacy-preserving manner: systems such as Pret 'a Voter and Scantegrity rely on mixnets to anonymize and decrypt cast votes which are then added. This approach, exemplified by STAR-Vote, employs homomorphic encryption to aggregate encrypted votes and decrypt only the tally. Both processes offer voters and observers cryptographic or mathematical proofs of correct operation. Ali can use these proofs to verify that ***"his vote has been tallied as recorded".***

Figure 7 E2E-V Voting: Tallied as Cast



Cryptographic primitives that enable this are sophisticated but not incomprehensible. Patriotic citizens with programming skills could spend sometime writing this software—essentially, independent audits. QR codes, smartphone apps, and mobile SMS services may simplify this processconsiderably. These E2E-V Voting or simply "verifiable voting" technologies are being developed foruse with electronic voting machines and online voting.

End-to-End voting system prototype may be developed using the open-source SEAL Library by Microsoft (Microsoft SEAL, 2022).

APPENDIX E

Primer on Risk Limiting Audits

If the initial count of votes is produced by EVMs, then Risk Limiting Audits can be deployed to increase the confidence in the results produced. A risk-limiting audit initially takes a small number of ballots, which humans count and check against the initial outcome. If discrepancy is found the sample of ballots is increased until there is statistical proof that the initial outcome was correct. Otherwise, the wrongly reported outcome is rectified. However, a prerequisite for an effective risk- limiting audit is a VVPAT (Voter Verified Paper Audit Trail), as the tally produced by the machine will be checked against this VVPAT to ensure that the outcome correctly reflects the voters' choice.

There are many methods to conduct Risk Limiting Audits each catering to specific needs of differentelectoral systems. We describe a simple "ballot-level risk-limiting comparison audit" that is compatible with the electoral system in Pakistan. In a ballot-level comparison audit, polling staff count a randomly drawn sample of ballots. Any discrepancy between the EVM reported percentage and the audit percentage will lead to another round of audit with a larger randomly drawn sample of ballots. This continues until there is convincing proof that a manual count of all the votes will lead to the same outcome as was originally reported. We walk through an example adapted from seminal work by Lindeman et al (Lindeman & Stark, 2012). We begin with defining some relevant terminology.

Ballots Cast, b, refers to the turn out in terms of the total votes cast in an electoral race.

Margin of Victory, MoV, refers to the difference in votes between the victor and the losing candidate.A separate Margin of Victory may be calculated between the winner and each of the losing candidates.

Diluted Margin, m refers to the smallest reported margin of victory as a proportion of the totalnumber of votes cast.

Risk Limit, r, refers to the greatest probability/chance that a wrong outcome is not detected.

Random Sample, n, of ballots is drawn to comply with the statistical notion of randomness.

Outcome refers to the winners and not the actual vote totals. A wrong outcome therefore implies theinitially reported outcome conflicts with the outcome of a full count during the audit.

Additionally, when manual counts are conducted there could be two types of errors:

An **understatement** is the total number of votes by which the audit results report less votes for thewinner**.** This means that the reported margin of victory is smaller than the actual margin of victory between the winner and every loser. Identification of understatements benefits the already reportedwinner and solidifies his victory.

An **overstatement** is the total number of votes by which the audit results report more votes for the winner. This means the margin of victory is inflated between the winner and one or more losing candidates.

2-vote overstatement, o2 is an event when the ballot cast in favor of a losing candidate is attributed to the reported winner; **1-vote overstatement, o1** is an event when the ballot cast in favor of one losing candidate is attributed to another losing candidate; **1-vote understatement, u1** occurs when the minimum number of candidates in the race are three and a vote for the winning candidate is

attributed to a losing candidate; **2-vote understatement, u2** is an event when the electoral race is between two candidates and the ballot cast in favor of the reported winner is attributed to the losingcandidate.

The audit begins in full public view. The polling officials draw a random sample of VVPAT, based on the margin of victory. These are manually reviewed to identify any conflict with the outcome reported by the EVM and the actual outcome. The Risk Limit needs to be defined in the legal framework. For our example, we set the Risk Limit to 10%. Suppose the audit has inspected a sample of **n** ballots. The audit can stop when

$$n \geq \frac{4.8 + 1.4(o_1 + 5o_2 - 0.6u_1 - 4.4u_2)}{m}. \qquad (1)$$

Both overstatements and understatements being errors alter the requirement for further ballots to be drawn. As an understatement adds to the votes of the winners it means less additional ballots need to be drawn. The opposite happens with an overstatement which attributes a winner for one ofthe losing candidates to the winning candidate, and the number of additional ballots to be drawn increases. However, the increase and decrease are not by equal amounts, as is evident from their coefficients in Equation 1 above. The increase is greater than the decrease.

Let us suppose that in an election race there were 10,000 ballots cast. According to the results reported by the EVM the winner obtained 4,000 votes while the first runner-up obtained 3,500.

For this contest, the Margin of Victory, MoV= 4,000-3,500 = 500 votes.

The Diluted Margin = (4000 − 3500)/10000 = 5%

We sample single ballots incrementally. Here, the polling audit staff will randomly select a ballot outof the ballot box and manually ascertain if the results reported by the EVM is in line with that of the drawn ballot. If there is only one error in the first 80 votes and this error is a 1-vote understatementthen, u1 = 1 and o1, u2, and o2 are all zero. At this point, the condition in equation one is satisfied:

$$80 \geq \frac{4.8 - 1.4 \times 0.6 \times 1}{5\%}. \qquad (2)$$

There is no need to draw further ballots. However, a repeat of the audit can be undertaken with a more stringent risk limit. The confidence in the outcome is greater if less errors are found as compared to if many, but equal numbers of overstatements and understatements are found. If a

lot of errors are being reported then it is at the discretion of the auditor to terminate the audit and beginan exhaustive manual count of all the ballots cast in the electoral race.

Arlo (Arlo, 2022), Bravo (Lindeman et al., 2012) are a couple of the open-source and free software tohelp conduct these audits cheaply and quickly, in the hope of increased adoption by EMB's worldwide.

APPENDIX F

Roadmap

In this section, we outline the actions required to implement the recommendations we have suggested. The first step to developing this roadmap was assessment and analysis of the existing systems and information, studying international best practices. The roadmap interventions are drawn from the gaps and barriers we have identified during our study. We recommend interventionfor the Ecosystem, R&D Cell and for the EVM exercise are given under separate roadmaps below. A nationwide EVM deployment is a complex endeavor, and we highlight activities that must not be skipped on this journey. The purpose of this roadmap is to help achieve full scale EVM deployment by General Elections, 2028.

There is limited groundwork towards achieving a country-wide deployment of EVMs. The capacity of the institutions mandated to undertake this task is sub-optimal. Similarly, government and infrastructure support are lacking. This document aims to support this process. Our engagement assumptions include a buy-in of all relevant stakeholders, adequate availability, and allocation of resources.

Table 3: Roadmap: Ecosystems for EVMs in Pakistan

Roadmap: Ecosystem for EVMs in Pakistan								
Key Steps	**Document / Activity**	**Objective(s)**	**Dependencies**	**High-Level Goals / Issues to be Addressed**	**Requirement(s)& Input(s)**	**Output(s)**	**ECP's partners**	**Timeline / Duration * ****
1	***Establish Steering Committee***	Set up a structured body to provide leadership, governance, and oversight for this project	-	Define primary goals for this project Translated these goals into actionable activities Define key milestones Precisely define key human, financial, infrastructure, and technical resources for this project Identify stakeholders, their roles, and inputs	*Stakeholder consultation necessary for this step* Seminars and round- table discussions with stakeholders to define composition and terms of reference (ToRs) forthis body	An empowered and representative Steering Committee which includes members from various stakeholder bodies	Politicalparties CivilSociety Academia	0-1 month (1 month)
2	***R&D Cell***	Establish Research division within ECP to provide high quality research inputs for policy decisions		Setting up R&D Division: Structure the division Initiate hiring process Set up dedicated officespace	*Stakeholder consultation necessary for this step* Potentially study other such dedicated efforts	R&D Cell should issue detailed Activities roadmap for the year ahead	Academia Donorbodies Technical bodies, e.g.,	1-2 months (1 month)
	Stakeholder Consultation and Outreach	To achieve stakeholder consensus on deployment of election technology		Procure and setup essential equipment Staff orientation and Training	in Estonia, United States, Brazil, etc.		IT boards, NADRA, etc.	

3			[1] [2]	Structure the mainstreamdiscourse Secure essential inputs from stakeholders regarding benefits, objections, concerns regarding EVMs Inform stakeholdersregarding international Practices Demo and pilot newtechnologies for stakeholders Advance the debate on EVMs Set up working groupsand subcommittees with stakeholder representatives to draft policy proposals		A wide-ranging and structured forum for consultation with stakeholders with a detailed activities program	Politicalparties Civilsociety Academia Donorbodies	3-4 months (1 month)
4	**Capacity Building**	Develop capacity within ECP to successfully deploy election technology	[1]	What is the current capacity of the ECP and election- associated institutions vis-à-vis electronic election administration? Identify critical gaps within ECP which need tobe addressed 3. Develop an action plan toaddress these gaps 4. Set up a specialized project	Qualifications/training/capacity requirements for typeof e-voting system Current structure and capacity limitations of ECP in light of the capacity requirements for every stage of technology deployment 3. Study	Recruitment and development of Project Management Team Communication expert/team Technical Specialists 4. Implementation specialists/team 5. Training Specialists 6. Legal experts	This process should be driven by a dedicated project management division overseen by the Steering Committee	3 months onwards (ongoing)

				management unit to address these gaps	international practices in capacity building through literature review and/or collaborative learning groups withother EMBs	7.Evaluation Commission (with security expert, election expert, andlocal authority) 8. Training/Skillsand Needs Assessment 9. Identify existing training or courses (local/international) 10. Action plan with timelines		
5	**E-Voting Readiness Strategy**	To assess the ecosystem gaps (social, political, technical and legal requirements) to introduce EVMs in Pakistan	[1] [2] [3]	1. Define precise requirements needed to shift to EVMs. Researchers have devised various metrics to guage suitabilityto introduce electronic voting. However, these metrics are primarily applicable to developed countries with far less voters. We need to adapt these for Pakistan. 2. Where do we	*Extensive consultation with stakeholders* .1. Examine similar models devised for EU countries, Netherlands, UK, Russia, etc. 2. Examine attemps to devise similar models in Kenya, Indonesia, Jordan, etc. 3. Examine international election technology	A report detailing specific metrics which need work to introduce electronic voting technology successfully in Pakistan. This will include social, political, technical, and legal determinants.	Stakeholders, including political parties, civil society, and academia	3-4 months (1month)

				stand in terms of these requirements? 3. What actions need to be taken to achieve this shift?	experiences and failures in the developing world			
6	**A Digital Transformation Strategy for ECP**	To modernize ECP and its systems to the point where they can successfully launch and manage large-scale EVM deployments	[1] [2] [3]	1. To upgrade ECP's internal systems 2. To improve existing processes within ECP to support EVMs 3. To develop new supporting infrastructure and policies to support EVMs 4. To develop safeguards against technology failures observed in the past (RTS/RMS) 5. To set up dedicated digital resources within ECP, e.g., datacenters	Survey strategies employed in Brazil, Estonia, India, Australia, etc.	A detailed plan for digital transformation within ECP with milestones and timelines	Help may be sought from government technical bodies, e.g., IT boards, NADRA, etc.	3-5 Months (3 months)

7	**A Cybersecurity Strategy for ECP**	To secure elections infrastructure within Pakistan in line with international standards	[1] [2] [3] [4] [6]	To identify international standards for elections systems 2. To incorporate transparency checks To develop appropriate incident response and mitigation strategies To determine relevant organizational-level security certifications	*This document directly depends on the Digital Transformation Strategy* Survey strategies employed in Brazil, Estonia, India, Australia, etc.	A detailed plan for cybersecurity readiness within ECP with milestones and timelines	1. Ministryof IT&T 2. Ministryof Science and Technology Privatesector cybersecurit 1. y firms	6-7 months (2months)
8	**Public Engagement**	1. Increase the public's trust in elections and educate the voter about election processes and election security 2. Provide oversight and control to the Pakistani society (experts, Civil Society Organizations, activists, voters) to foster social support and trust	[1] [2] [3] [4] [5]	Media strategy for publicengagement Active voter engagementstrategy Strategy for public oversight . Social involvementstrategies to target disinformation 5. Technologist involvement strategies audit source code and system vulnerabilities, hackathons 6. Voter engagement strategies, to improve transparency on	. A public survey canbe administered to identify the perceptionof electronic voting and ECP's capacity, to identify trustworthy sources of information for different segments of the society, and modes of information consumption . Comparative analysis of international experience regarding measures taken to a) ensure the e-voting system is transparent	Voters have adequate knowledge of how the overall system works 2. Voters comfortable with how to vote 2. Voters understand reason for adoption of the technology and the security measures undertaken to ensure integrity 3. Appropriate response to media or other stakeholders'	CSOs, NGOs, and media experts	4 months onwards (ongoing)

				election day (e.g., inviting public tobe poll workers) 7. Effective communicationplan on election day (e.g., live election portal) 8. Communication strategyfor transparency in post-elections processes like audits, election petitions, and dispute resolution	and b) determine outreach and education strategies that can be implemented within multiple target groups (e.g, senior voters, disabled voters, women, rural, urban, etc.)	narrative of the election technology Voter's knowledge of capacity building and other efforts undertaken by the ECP to ensure successful implementation		

Table 4: Roadmap: R&D Cell

Roadmap: R&D Cell								
Key Steps	**Document / Activity**	**Objective(s)**	**Dependencies**	**High-Level Goals / Issues to be Addressed**	***Requirement(s)* & Input(s)**	**Output(s)**	**ECP's partners**	**Timeline* ****
1	**Building Linkages and Knowledge Mobilization**	To develop a strong research culture to providecritical support for the election's ecosystem in Pakistan		. To identify and build linkages between research bodies and project partners to address knowledge gaps in Pakistan 2. To conduct symposiums, seminars, and outreach efforts n technology andpolicy 3. To conduct hackathons and demos of election technology To build internationallinkages 5. To foster indigenous expertise in election technology, policy, law, etc.	*The R&D Cell should ideally have an Advisory Board comprising local and international experts to advise on these matters* Launch research grants programs Organize seminars and symposiums . Undertake observationtrips to observe foreign elections	1. High quality research to inform elections policy and address local problems 2. Tech transfer efforts	1. Donor bodies: UNDP, IFES, etc. 2. Research partners – PIDE, HEC, NCCS, MoST, etc. 3. Research-intensive universities 4. Foreign election management bodies	2 months

Table 5: Roadmap: Electronic Voting Machines for Pakistan

Roadmap: Electronic Voting Machines for Pakistan								
Key Steps	**Document / Activity**	**Objective(s)**	**Dependencies**	**High-Level Goals / Issues to be Addressed**	***Requirement(s)* & Input(s)**	**Output(s)**	**ECP's Partners**	**Timeline / Duration * ****
1	**Threat Model for Electronic Voting Machines in Pakistan**	Precisely define baseline security requirements for EVMs in Pakistan	-	1. Describe the ecosystem of Pakistan's voting system - list key actors, processes, and data units 2. Describe current threats to the existing voting system 3.What are the key procedural and process inefficiencies and shortcomings? 4. Differentiate between procedural and technological resolutions to these threats 5. What is the feasibility of using EVMs in Pakistan? 6. Is electronic voting at least as reliable and secure as paper-based elections? 7. Is it in compliance with the fundamental principles of elections? 8. Do the benefits of EVMs outweigh the drawbacks? 9. Does the cost benefit	*Stakeholder consensus is essential for thisreport* 1. An investigation of failures and irregularities in General Elections of2013 and 2018 2. Threat models forsimilar environments, e.g., India/ Bangladesh/ African countries	Study clearly defines the threat model and inefficiencies in the electoral system in Pakistan that willbe addressed by EVMs There also needs to be concrete remedial procedures suggested for each of these issues, along witha holistic perspective specifying how they have been	1. Academia 2. Donor bodies 3. Technical bodies, e.g., IT boards, NADRA, etc.	2-4 months(3 months)

				analysis indicate a favorable outcome?				
2	**Vulnerability Analysis of MoST EVM**	To undertake a rigorous security analysisof the prototype EVMs developedby MosT	[1]	Detailed analysis of prototype machines developed by MoST considering: security properties international best practices suitability for Pakistan cost-benefit analysis 1. It would be instructive to pilot this EVM in small-scale elections, if possible, to assess usability and logistics.	1. Detailed specifications document 2. Details of manufacturing and supply chain	Study gives a complete pictureof pros and cons of MoST EVM handled in other countries	Academia . Donor bodies 3. Technical bodies, e.g., IT boards, NADRA, etc.	5-6 months (2 months)
3	**Vulnerability Analysis of Smartmatic**	To undertake a rigorous security analysisof the EVMs acquired from Smartmatic	[1]	Detailed analysis of EVMs acquired by Smartmatic Security properties International best practices Suitability for Pakistan Cost-benefit analysis 5. It would be instructive to pilot this EVM in small-scale elections, if possible, to assess usability and logistics.	1. Detailed specifications document 2. Details of manufacturing and supply chain	Study gives a complete pictureof pros and cons of Smartmatic EVMs	1. Academia 2. Donor bodies 3. Technical bodies, e.g., IT boards, NADRA, etc.	5-6 months(2 months)

4	**Comparative Analysis of Popular EVM Models for Pakistan**	Detailed comparison of 3 popular EVM types across various metrics to judge suitability for local deployment	[1]	Three popular EVM models for developing countries (India-button-press, Brazil-keypad, Iraq/Philippines-scanning) 1. Investigate security properties and vulnerabilities for each model. 2. Investigate on-ground operational requirements for each EVM model (transport, storage, handling, configuration, maintenance, etc.) 3. Conduct pilots for each model to measure usability. Pilots should be conducted in non-political elections (e.g., organizational polls, trade bodies, bar associations, etc.) Care must be taken to ensure statistically significant results. 4. Formulate dispute-resolution strategies for each model Investigate legal frameworkfor each model 6. Detailed cost-benefit analysis for each model (including overall costs for logistics, handling, manpower)	*The availability of prototypes of each of the machines* 1. Specifications documents for each EVM type Security analyses from research literature 3. Reports from existing pilots and deployments	Study gives stakeholders a comprehensive picture on pros and cons of each EVM type as well costing figures Existing pilot studies and reports prepared inhouse by ECP are typically not of high quality, they lack rigorous security and statistical analysis. It is highly recommended they partner witha research organization for this exercise or train their staff in the required skills.	1. Academia 2. Donor bodies 3. Technical bodies, e.g., IT boards, NADRA, etc.	7-8 months(2 months)

5	**Deployment Study for E2E-V Voting in Pakistan**	Investigate and adapt verifiable voting for local deployment	[1] [2] [3] [4]	1. Pilot EVMs with verifiable voting in non-political settings (bar association polls, chambers of commerce, etc.) 2. Investigate on-ground operational requirements . Studies to investigate citizen mental models for verifiable voting systems 4. Formulate dispute-resolution strategies Investigate legal framework 6. Trial different technical options for bulletin board -e.g., Internet-based bulletin board, SMS service, etc. 7. Trial different code visualization options - e.g., alphanumeric text, images, emojis, etc.	*elopment of a prototype* 1. Develop or procure EVMs with verifiable voting capability specifically for this exercise 2. Prior research work on verifiable voting trials, measuring verifiability rates, and mental models can help with developing a template for this exercise, but care must be taken to adapt for our own ground realities, e.g., language, culture, etc.	Study to examine feasibility of verifiable voting in a local setting, as well as measure verifiability rates, and check how citizens understand this technology and derive mental models	1. Academia 2. Donor bodies 3. Technical bodies, e.g., IT boards, NADRA, etc.	6-11 months(6 months)

6	**Deployment Study for Risk Limiting Audits in Pakistan**	Investigate and adapt RLAs for local deployment	[1] [2] [3] [4]	1. Pilot RLAs in existing polls (by-elections, LG polls, etc.) - multiple pilots for different RLA methodologies 2. Investigate on-ground operational requirements Studies to investigate c itizenmental models for RLAs 5. Formulate dispute-resolution strategies Investigate legal framework	*Personnel will haveto be trained to run RLAs and E2E-V Voting systems*. 1. RLA based research literature 2. RLA schemes proposed for Indian EVMs	1. Document that serves as a guide for RLA inclusion in the electoral framework Practical guideon how to conduct RLA	1. Academia	6-11 Months (6 months)
7	**Voter Verification Mechanisms**	Feasibility study of various options (biometrics, smart cards, CV techniques)	[1] [2] [3] [4]	What are the false acceptance and false rejection rates of each of the voter verification technologies? How do these vary for the population of Pakistan? What is the relative cost of each of the options for voter	1. Specifications documents for each voter verification mechanism Security analyses from research literature 3. Reports from existing pilots and deployments . There is extensive literature that explores access controls such as biometrics, smart cards, tokens etc	Study gives stakeholders a comprehensive picture on pros and cons of each voter verification mechanism as well costing figures	1. Academia 2. Donor bodies 3. Technical bodies, e.g., IT boards, NADRA, etc.	6-8 months(3 months)

8	**EVMs in Pakistan: Specifications and Requirements**	Define technical and functional specifications and processes for EVMs to be deployed in Pakistan	[1] [2] [3] [4] [5] [6] [7]	phase describes theproposed EVM 1. Map security properties of 2. EVM to threat model [1] Describe detailed technical and functional specifications of proposed EVM 3. Describe workflow and processes for deployment and elections Describe workflow and processes for storage, maintenance, and handling Describe security checksand audit processes 6. Include measures to incorporate future technology (e.g., citizen smart cards) 7. Describe RLA and verification processes Propose dispute resolution strategies Propose changes to legal Framework	Stakeholder consensus is essential for this Report 1. [1] [2] [3] [4] 2. Research Literature	First iteration on technical Specifications Including functional requirements, non-functional requirements hardware and software requirements This documentation must be of high quality and conform to appropriate international standards for technical documentation	1.research-intensive organizations (e.g., universities) 2. technical organizations with small-scale manufacturing capability (e.g., NIE)	12-13 months(2 months)

9	**Prototype EVM**	Develop prototype EVM	[1] [2] [3] [4] [5] [6] [7] [8]	Develop prototype EVM forpilot purposes and also address further questions: Derive precise costingfigures for manufacturing/procuring EVMs Document production supply chain and procurement/manufacturing processes Are there security threats inthe supply chain? 3. Can the EVM design be modified to further improve security and/or reduce costs thout impactingfunctionality? Devise adequate Quality Assurance checks and Processes	[1] [2] [3] [4] Research Literature	Report evaluating the prototype and whether the goals were met or not	1. research-intensive organizations (e.g., universities) 2. technical organizations with small-scale manufacturing capability (e.g. NIE)	14-16 nths(3 months)
10	**Pilot Studies**	Conduct multiple pilots using new EVMs	[1] [2] [3] [4] [5] [6] [7] [8] [9]	Pilot the proposed EVM innon-political and political settings: Collect feedback on usability 2. Record performance of these machines in the field . Observe process flow and procedures with a view to proposing improvements . Modify EVMs or processes in response to feedback from 1, 2, 3 Undertake multiple pilots inrural and urban areas to derive statistically significant	*Stakeholders must be regularly briefed about the outcomes of these trials, ideally at every iteration.* The pilot must be evaluated on multiple dimensions such as technical, social, legal, usability, process efficiency. For this formal observation	Series of pilot processes to fine-tune EVM design and workflow and operational procedures for the field	-	16-18 nths(3 months)

				results which reflect Pakistan's diverse population.	of the pilots is necessary, so that by the end there is enough data to decide on the outcome			
11	**Feedback and Improvement**	Incorporate changes to rectify the issues identifiedin the EVMs in the first pilot before going into production	[1] [2] [3] [4] [5] [6] [7] [8] [9] [10]	1. What were the limitations and weaknesses evident in the electronic voting machine and associated processes? What was the end users thatis the voters perspective?	Survey consisting of diverse stakeholders, public call for comments, engaging with academia, media and collecting as much feedback as possible	A document that defines the changes that need to be made in the EVM to overcome the issues faced in the first pilot	1. research-intensive organizations (e.g., universities) 2. technical organizations with small-scale manufacturing capability (e.g., NIE)	18-19 nths(2 months)
12	**Second Round of Pilots**	To iron out any remaining issues after the first round of improvements made according to the feedback received	[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11]	1. What are the remaining limitations, weaknesses in the system? 2. Do we need to go for another round of change in specifications? 3. What are the outstanding challenges that can be left for the next iteration	*Stakeholders must be regularly briefed about the outcomes of these trials, ideally at every iteration* 1. The result of first pilot, the documents detailing the changes made, further observation from second pilot	Series of pilot processes to fine-tune EVM design and workflow and operational procedures for the field		20-21 nths(2 months)

13	**Second roundof feedback and Improvement**	Incorporate changes to rectify the issues identifiedin the EVMs in the second pilot before going into production	[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12]	1. What were the limitations and weaknesses evident in the electronic voting machine and associated processes? What was the end users thatis the voters perspective?	Survey consisting of diverse stakeholders, public call for comments, engaging with academia, media and collecting as much feedback as possible	A document that defines the changes that need to be made in the EVM to overcome the issues faced in the first pilot	1. research-intensive organizations (e.g., universities) 2. technical organizations with small-scale manufacturing capability (e.g., NIE)	22-23 nths(2 months)
14	**Hackathons Source code review**	To gain public trust Identify security loopholes	[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13]	Has the EVM been subjected to scrutiny by public, technologists, international experts?	EVM prototype	Possibility of EVM being hacked and new security issues and bugs identified	Media, Election Observer Groups	16-17 months20-21 months(2 monthseach)
15	**Election System Certification**	Election System Verification	[1] to [14]	Under what parameters were the Security Claims Validation, Testing Rules Determination, and System Audit, Compliance and Certification performed?	nalized Electronic Voting Machine	Approval of statutory body that machine is fit to be deployed	-	22-24 nths(3 months)

16	**Procurement**	Tendering and Production	[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15]	Has the tendering process occurred according to rulesand regulations? How to avoid vendor dependence and lock in? Should there be a single vendor or multiple vendors? What are the evaluation parameters to vet the vendor? How to vet the supply chain of the vendor? How do we ensure production in stipulated time? Who will perform the quality checking? Who will perform a third party audit? Does the ECP send its technical team to the vendor to oversee the manufacturing process? What happens if the vendor fails to deliver the machines in the stipulated time?	Call for Tender	Delivery of EVMs	Vendor	24-42 onths(18 months)
17	**System Integration**	To ensure the different components (RTS, RMS, Voter Verification,ECP Management Portal) of the	[1] [2] [3] [4] [5] [6] [7]	Are the difference components of the ecosystem compatible with each other? Does the system work together as a whole without technical glitches? Have some mock elections	RTS, RMS, EVMs, Voter Verification Module, ECP Election Management Portal, Voter Rolls	End-to-End running electronic voting system	1. research-intensive organizations (e.g., universities) 2. technical organizations	24-26 onths(3 months) scale manufacturing capability (e.g., NIE)

		election systems function together seamlessly and satisfy the design properties and characteristics of the system	[8] [9] [10] [11] [12] [13] [14] [15]	been conducted to simulate an election day exercise? Are the interfaces of a component of a system inconflict with another? does the integration of a system create any new security loopholes?			with small-	
18	**Infrastructure, Operations and Logistics**	To ensure adequate infrastructure, logistics, and operational support is available to make the EVM deployment a success	[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15]	How have internal regulations been changed to cater to EVMs? What are the methods to ensure inventory control of EVMs? How is it ensured that machines remain functional, are not tampered? What are the protocols for movement and transport of EVMs? What training programs are to be undertaken for the Election officials? What are the long-term goalsin terms of improving infrastructure and communication support? Has the ownership, roles and responsibilities been defined?	A comprehensive and holistic guide to the electoral lifecycle with the introduction of EVMs that details when they will be procured, stored, and used.	A handbook of policies, procedures, guidelines, and internal regulations by which election officials can operate and be held accountable	Law Enforcement Agencies	24-29 nths(6 months)

				what measures have been taken for the physical security of assets? Are there adequate disaster management and recovery protocols in place?				
19	**Updating Legal Framework**	Identify and Outline: 1. the enabling legislative amendments 2. key elements of regulations governing the details the e-voting system	[1] [2] [3] [4]	Identify legislative, regulatory and procedural elements pertaining to the electoral system, including, but not limited to: - Authority for elections authorities to create procedures for electronic voting - Physical aspects of the electronic voting system - Provisions for trials, pilots, and certification - Audit requirements before and after election Provisions for scrutineers - Means of authenticating/ identifying voter - Procedural requirements on election day(vote invalidity, vote count, etc.) - Dispute resolution mechanisms and training of judiciary	*Stakeholder consensus is necessary* Analyze and define the allowances and limitations of the current legislation and regulation with respect to electronic voting 2. What aspects need to be defined in the legislative and regulatory environment that will ensure validity of the election results 3. Comparative study of e-voting elements in enabling legislationand regulations in other countries	Effective Legal Framework to oversee Electronic VotingMachines based elections	Election Law Experts, Election Observation Bodies	22 months onwards (ongoing)

				Anti-corruption legislation for electoral staff Defining Admissible evidence - Access to source code - Data governance, ownership, security, storage and retention - Transparency - Electronic voting offences and related law enforcement - Communication with stakeholders Provisions and protocols for election observation				
20	**Monitoring, Evaluation, and Innovation**	Continue efforts to resolve residual issues To ensure continued electoral innovation and avoid stagnation	[1] to [19]	What are the unresolved issues? What is the latest research in terms of technology that needs to be studies to be able to incorporate in the system	The feedback from real election deployments, voters, media, election observersand judiciary	Upgraded system based on the feedback received	1. Academia 2. Donor bodies 3. Technical bodies, e.g., IT boards, NADRA, etc.	30 months onwards
*Many of these activities are independent of each other and may be undertaken in parallel as denoted in the timeline. **This depends on the availability of qualified personnel in the R&D wing, as well as the resources and facilities available. ***Pilots are subject to scheduling of Bye-elections								