**Electronic voting security**

**[Major General Syed Ali Hamid](https://nation.com.pk/Columnist/major-general-syed-ali-hamid)**

June 12, 2021

Voting is an important part of our political landscape but while most people are galvanised to participate in elections, they don’t have faith in the voting system. The integrity of elections is questioned from voter registration to submission and everything in between, particularly by those who lose.

Introducing technology in the election process has many advantages. The casting of votes becomes far easier, encouraging people to participate. The results appear within a couple of hours which enhances the confidence of the candidates and the voters in the process and results. This in turn reduces incidents of post-election violence. In the long-term it reduces organisational and implementation costs significantly and compared to traditional paper voting, increases the efficiency of election management. While most people recognise and appreciate these advantages, they find it difficult to accept the fact that it is also a lot more secure than manual voting.

[WHO advises keeping masks on after vaccination](https://nation.com.pk/11-Jun-2021/who-advises-keeping-masks-on-after-vaccination)

The security of paper-based manual balloting with a manual count is extremely low. The fact that there are just single copies of each paper ballot makes them extremely vulnerable. Paper ballots can be destroyed, tampered with, manipulated, intercepted, lost, forged, or fraudulently pre-marked. Ballot boxes can be lost or stuffed with fraudulent votes. Every step from voting to counting to final tally, and everywhere else in between are subject to human error, malicious or otherwise. Yet there are many politicians and analysts who are not willing to allow the introduction of a well-designed, special-purpose system that reduces the possibility of results tampering and eliminates fraud. They question its security, secrecy and safety. This article considers critical aspects of e-voting—security and auditing of voting machines, identification of voters, risk-limiting audit and creating a paper trail.

The logistics and warehousing involved in automated elections can be a complex undertaking. However, it is miniscule compared to the scale of logistics and warehouses routinely handled by project managers of large mail-order companies like Amazon and Ali Baba and manufacturing giants like Toyota. Election commissions worldwide store EVMs and election paraphernalia under lock and key, with armed security, surveillance cameras and access control. It would be next to impossible for unauthorised persons to access the machines and any tampering can be easily detected in the pre-election audits.

[Israeli police detain 3 Palestinians in Jerusalem](https://nation.com.pk/11-Jun-2021/israeli-police-detain-3-palestinians-in-jerusalem)

Biometric voter authentication (BVA) deters fraud by preventing people from attempting to vote multiple times, but NADRA admits that at best it can recognise fingerprints of 82 percent voters. The anti e-voting lobby in Pakistan cite this as one of the weaknesses of the system. They don’t realise that voter authentication is a completely distinct and separate process from e-voting. Voter authentication can still be performed in the traditional method, even while e-voting proceeds independently and with all the attendant benefits.

In fact, to protect the secrecy of the vote, any connection between the voter’s identity and the vote cast is avoided. A secret vote is the essential integrity safeguard because it enables voters to cast their ballot with full independence. A well-designed e-voting system further ensures secrecy by completely randomising the votes cast and uses sophisticated algorithms to ensure that votes are never stored in sequence. There is so much that technology allows that can never be achieved by a manual system and yet the uneducated are bent on creating suspicion of e-voting.

[Greek premier shoots down 2-state solution for Cyprus](https://nation.com.pk/11-Jun-2021/greek-premier-shoots-down-2-state-solution-for-cyprus)

A well-designed tamper-proof and tamper-evident system allows for risk-limiting audits that guarantee the legitimacy of results. A risk-limiting audit (RLA) checks a random sample of voter-verifiable paper ballots, giving strong evidence to support the reported election results. The audit stops as soon as it finds strong evidence that the reported outcome was correct. If the reported outcome was wrong because ballots were miscounted, it triggers a full recount that corrects the outcome before the election results are certified.

Unlike manual systems, a well-designed e-voting system produces multiple copies of every data point both in electronic and paper-based forms, creating a very rich audit trail that cannot be circumvented. It also ensures that data is never lost, modified or destroyed. Audit trails give all stakeholders in the election the possibility to verify that the results reflect the will of the voters.

As a best practice, well-designed voting systems furnish physical proof of all votes cast, in case a recount is needed. A printed paper ballot is now a mandatory component of automated election systems as it facilitates the most common audit performed after closing the polling centres on election day: comparing vote receipts against tally reports. With paper trails, post event audits can also be carried out upon request from any of the parties involved.

[State Election Commission to ensure free, fair polls in AJK: Sardar Masood](https://nation.com.pk/11-Jun-2021/election-commission-to-ensure-free-fair-polls-in-ajk-sardar-masood)

Finally, the e-voting solution to be implemented has to be proven in multiple countries with different geographies and idiosyncrasy; and the company deploying the technology must have diverse experiences deploying voting technologies on a massive scale, as elections are unique projects. Its nature is fundamentally different from any other technology project: Implementation happens on one day, it is nationwide, a large portion of the population uses the technology within 8 or so hours on a predetermined day, the project cannot be postponed, deployment means a massive logistical operation and coordination, and implementation mistakes could have drastic negative consequences for the entire country.

In the vast majority of countries that are discussing the implementation of an e-voting solution, the entire discussion evolves only around the voting machine equipment itself. Neglected is the question how this hardware should be deployed in ten or hundred thousands of polling locations on a single day without failure. Every IT student at the end of year-one will probably be able to put together a system that records votes electronically and gives the total of the voting result. The difference between a solution that works in a meeting room and a system that is trusted, immune to attacks and is working in a predetermined timeframe nationwide is, however fundamental. Ignoring the deployment aspect of electronic voting during initial discussions is another reason why implementation projects fail when election modernisation is run on significant scale.

[US' Blinken discusses cooperation with Chinese diplomat on COVID origins](https://nation.com.pk/11-Jun-2021/us-blinken-discusses-cooperation-with-chinese-diplomat-on-covid-origins)

A well-designed automated election system should be both tamper-proof and tamper evident. When an automated election system lends itself to detailed scrutiny of its software source code at all levels, as well as its security mechanisms for data storage and transmission, it succeeds in providing ample guarantees that will foster the confidence of both election authorities and voting public alike.