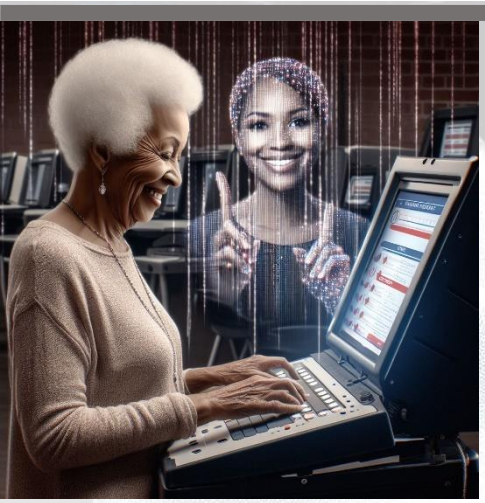
Trust on Electronic Voting Machine



Electronic Voting Machines (EVMs) promise a new era of swift, efficient, and transparent elections. However, they also pose significant security risks that could undermine the democratic process.

This article delves into the opportunities offered by EVMs, while critically examining the potential threats they pose. Join us as we navigate the complex landscape of electronic voting, balancing the promise of innovation with the imperative of security.

Electronic voting machines (EVMs) are devices that allow voters to cast their ballots electronically, without the need for paper ballots or manual counting. EVMs have been widely adopted in many countries, especially in India. EVMs have several advantages, such as faster results, reduced human errors, and improved accessibility. However, EVMs also pose significant risks that could compromise the integrity of the electoral process.

Opportunities of EVMs: EVMs can provide faster results than paper ballots. Another advantage of EVMs is that they can reduce human errors in vote counting. Paper ballots require manual verification and reconciliation by election officials. A third benefit of EVMs is that they can improve accessibility for voters with disabilities or special needs.

Security Risks of EVMs: Despite these advantages, EVMs also face serious security risks that could undermine their reliability and credibility. Some of these risks include:

- **Tampering**: An attacker may tamper with the memory card or software of an EVM during installation or operation. Alternatively, an attacker could insert a malicious device into an EVM during transportation or storage.
- **Hacking**: Similarly, an attacker may hack into the network or system that controls an EVM remotely. Alternatively, an attacker could exploit vulnerabilities in the software or hardware of EVM.
- **Manipulation**: An attacker could bribe or coerce election officials to manipulate an EVM during installation or operation.

Best Practices for Enhancing Security:

To mitigate these security risks, some best practices should be followed by all stakeholders involved in the electoral process.

- **Standardization**: There should be a uniform set of specifications and protocols for designing and testing all types of EVMs used in elections across different states and countries.
- **Certification**: There should be a rigorous process for verifying and validating all components and functions of each individual unit (such as memory card) before deployment.
- **Monitoring**: There should be a continuous system for tracking and auditing all activities Auditability: There should be a reliable method to cross-check all results generated by each unit (such as counting) after deployment. This would ensure accuracy and validity.

EVM has both opportunities and challenges that need to be addressed by following in-depth cyber security risk management.

Sara Malik is a InfoSec professional and volunteer in PakCrypt outreach program.