e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

HOW RISKY ELECTRONIC VOTING

Manisha Kumari*1, Amanjot Kaur*2

*1Department Of Computer Science And Engineering Mimit, Malout (PB), India.

*2Asst. Prof., Department Of Computer Science And Engineering Mimit, Malout (PB), India.

ABSTRACT

Elections are conducted almost exclusively using electronic voting machines developed over past two decennium by a pair of government-owned companies. These devices, called in India as EVMs, have been glorified for the simple design case of use constancy but recently they have also been blamed following current reports of election irregularities.in this paper I present how risky digital voting. I want to say that some time digital or electronic voting risky. In this voting system there many types of risk management factor like risk of spreading false information, risk of compromised votes, high cost of replacing voting machines. We describe the machine's conspiracy and effort in detail, and we estimate its safety measure in view of applicable election procedure. We conduct that however the machine's purity and least software protected computing base, they are unprotected to serious attack that can modify election results and offend the isolation of the ballot. Electronic voting has spread throughout the U.S. and the world without enough attention to accuracy, certainty. Today's E-voting system use private code and dealers have often affirm the privacy of this code when self-sustaining reviews of verified systems were needed. In order to supply self-sufficient judgment of the voting systems verified for us in California, assistant of state Debra Bowen launched a top-to-bottom reviews of those e-voting system. The outcomes that exhibited systems looked not to designed with safety in mind. The conspiracy and execution avoid basic exposure in all three dealer systems. The outcomes of the top to bottom review give an chance to switch the authoritative procedure to make it productive. This case study carries important lessons for elections and for electronic voting security.

Keywords: Electronic Voting, Risky**,** Security, Voting Machine.

I. INTRODUCTION

Electronic voting is also called e-voting. It is voting that utilize electronics means to either support or take care of heaving and calculating votes. E-voting may utilise free electronic voting machines or computers fixed to the internet depending on the specific execution. The degree of computerization might be limited to naming a paper ballot or may be overall system of vote input, vote reporting, data transportation to helper and tabulation of election outcomes. A notable e-voting system must represent most of the task while observing with a set of levels authorized by administrative bodies, and must also be able to deal successfully with powerful needs connected with accuracy, security, privacy integrity, auditability, swiftness, accessibility, cost-effectiveness, ecological sustainability and scalability. Electronic voting system may include optical scanner voting systems, punched card contained direct recording election voting systems it can engage transportation of election and votes via telephones, personal computer networks too. When we will know about electronic voting. This is important to know what we are referring to. There are main two kinds of voting systems.

1.1 E-voting: E-voting takes place at central polling locations, with observe overlooking the process. The difference between e-voting and paper voting the e-voting using technology and the paper voting does not use technology. E-voting uses technologies which are following

- **Ballot casting:** E-voting system can use technology for recording the vote itself. It can include straight casting electronic voting machines that we have touchscreen or other interfaces that voters can record their tickets on.
- **Tabulation:** A paper- based voting system also be considered e-voting if machines are used in counting process.
- **Transmission:** this can also be considered e-voting if paper -based votes are use alongside human counting, but the results are sent via the cyberspace or more networks.

1.2 I-voting: I-voting also called remote e-voting, uses the internet to allow people to vote from essentially anywhere. it could be done with smart phones computers and other devices. I-voting has the most appeal, because voters don't have to leave their home to vote.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

II. WE WANT FROM VOTING SYSTEM

A useful voting system requires to balance a range of key features. Security is definitely one of the top critical factors, because we want to prevent any self -interested parties from being able to manipulate the result. We want to make sure that the counted votes are authentic too. This still need to be balance out with other requirements. The other properties that require to be considered in voting system are:

- **Accuracy:** we want the final vote count to represent the choice of the people accurately.
- **Verifiability:** this is prime to be capable to scan the correctness of the vote and control weather elections have been modified with. If any exploitation is establish a new election may be counted.
- **Anonymity:** The need for anonymity is complex in voting because we don't want anonymity in all aspects.
- **Accessibility:** it needs to talk all voters into account. This would be great to allow everyone to vote from the comfort of their own homes to make the process easier.
- **Speed:** This is the best if we can receive the results in a relatively short period of time.
- **Cost-effectiveness:** we should have the most secure and accurate system in the world, but if it costs 10 times GDP of nation to implement.

2.1 Perceptions vs. Reality:

- Voters feels that
- Vote was counted
- Vote was private
- Nobody can vote repeatedly
- Nobody can alter others votes
- People trust that the machine works correctly
- These all have to do with voters

2.2 Ugly failure modes:

Ballot stuffing

- Absentee votes from deceased voters
- 100% of votes in Oregon are mail-in post-election ballot tampering
- Froud behavior by elect ion officials.

2.3 Obvious flaws:

- Indication to voter that vote is recorded?

No paper to drop in ballot box

- Why should you trust that the computer wok?

No-voter visible evidence

2.4 Voting machine hacked:

Can a straight reporting digital voting system employee throw the election?

- Is this technically feasible?
  - **Yes**
- Should there be any type of evidence?
  - Probably not
- Accuracy and logic tests?
  - Easily faked

III. CYBER SECURITY REASON

- Election security cannot be guaranteed: In digital voting there would be far too many Vulnerable points in the voting chain- the application itself, operating system your Phone and servers your date will travel along to their final destination for tabulation
- Internet voting increases cyber security risk: National voting via the world wide web expands the opportunity for an raider to engage in damaging disruption and denial-of-service attacks.
- No computer or system is 100% "un hackable" : he complexity of the systems, computers, and applications that would be required for online voting contain bugs and errors that can be leveraged. This complexity and

need for corresponding cyber security protection are growing faster than the methods to keep up with them.

- Election hacking may go undetected: Cyber security experts can eventually, detect e-commerce errors and fraud. The ability to track and audit online elections would be exceeding difficult without an auditable information trail that couldn't be falsely manipulated.
- Identity verification may be impossible: To have proper election security, we would require an impenetrable identity verification system.

IV. CONCLUSION

The most significant risk is related to voters' confidence and the possibility of losing it. It is possible of losing it. It is feasible to shake voters' faith in the voting system even without any actual technical capabilities, since harm can be done just by spreading false information. When votes may be expressly counted and recounted, it is to remove any suspicions of manipulation of the election outcomes, at least. The electoral organization should have the means to identify harmful activities, prevent them and obtain the evidence required to bring criminal charges or to prove that the election outcome is no manipulation has taken place. This is highly doubtful that that these problems may be remedied by simple upgrades to the existing EVMs. Merely making the attacks we have demonstrated more difficult will not fix the fundamental problem: EVMs do not provide transparency, so votes and election formals have no reason to be sure that the machine are behaving honestly.

V. REFERENCES

[1] http://avirubin.com/vote/
[2] http://www.verifiedvoting.org/
[3] http://www.blackboxvoting,org
[4] http://indianevm.com/book.php
[5] http://www.unicef.org/infobycountry/india_statistics.html