iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** II **Month of publication:** February 2023

DOI: https://doi.org/10.22214/ijraset.2023.49128

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue II Feb 2023- Available at www.ijraset.com

The Risks of Remote Voting

Mayank Gupta[1], Manish Kumar[2], Devendra Pratap Sharma[3], Dr. Raj Kumar[4]
[1, 2, 3]*Department of Computer Applications Manav Rachna International Institute of Research & Studies Faridabad, Haryana*
[4]*Associate Professor, Department of Computer Applications Manav Rachna International Institute of Research & Studies Faridabad, Haryana*

Abstract: This paper discusses the risk of remote voting. Furthermore, it investigates claims that "voting via the Internet" or "voting on the blockchain" will enhance ballot safety and finds them insufficient and dishonest. While current election techniques are extremely reliable, Digital and blockchain based voting could dramatically increase the likelihood of undiscovered electoral mishaps.[4]
Keywords: Adversary, proxy, vulnerability, intruders, unanimity, patrons

I. INTRODUCTION

The Internet and computer systems have provided several perks, including improved productivity, dependability, extensibility, and simplicity in many facets of everyday life. People are asking, "Why can't I vote online?" Online voting appears to be appealingly straightforward: a few clicks on a smartphone and you can vote without disrupting your schedule, missing work, or standing in line. However, there is a fundamental issue with electronic voting. Online electoral systems are subject to major failures: cyberattacks on a grander scale, that are more difficult to spot and that are more straightforward to carry out than equivalent attacks on paper-ballot voting systems.[7] Moreover, considering the current level of internet protection and the high risks associated with electoral campaigns, online electronic voting machines will remain susceptible in the nottoo-distant ahead. While convenience and expediency are vital components of democratic systems, they must also be calibrated and strengthened with security.
Whenever one of these goals is undermined, an election system becomes ineffective.[4][11]

II. REMOTE VOTING

It refers to any voting method that allows people to vote remotely from a location other than the polling station designated to their district. This may be done both internationally and domestically.
It includes both electronic and nonelectronic voting techniques. There are two types of voting systems: electronic and non-electronic. Remote and Polling Booth are also options.

A. Voting Through Electronic Means

1) Voting in Polling Booths: The government instals electronic voting equipment at polling stations.
2) Remote Voting: We may vote through E-mail, SMS, the Internet, and other means from anywhere in the globe.

B. Voting via Paper Ballot

1) *Traditional Ballot Paper Voting:* Traditional Ballot Paper voting is utilised at polling places.
2) *Remote Voting:* We can vote from anywhere in the globe via Telegram, Proxy, Mobile Ballot Box, and so on.[1]

C. Risks Related to Remote Voting

There are several potential issues with remote voting.
1) Cyberattacks have the potential to distort and postpone outcomes.
2) A vote's and voter's secrecy might be jeopardised.
3) There is a chance that a single person will vote several times.
4) Vote buying is a possibility.
5) Voters can vote in an unsupervised setting, however this may interfere with their privacy.
6) Influence or meddling with voters.
7) If a voter elects to vote by proxy. As a result, a proxy can modify their vote.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue II Feb 2023- Available at www.ijraset.com

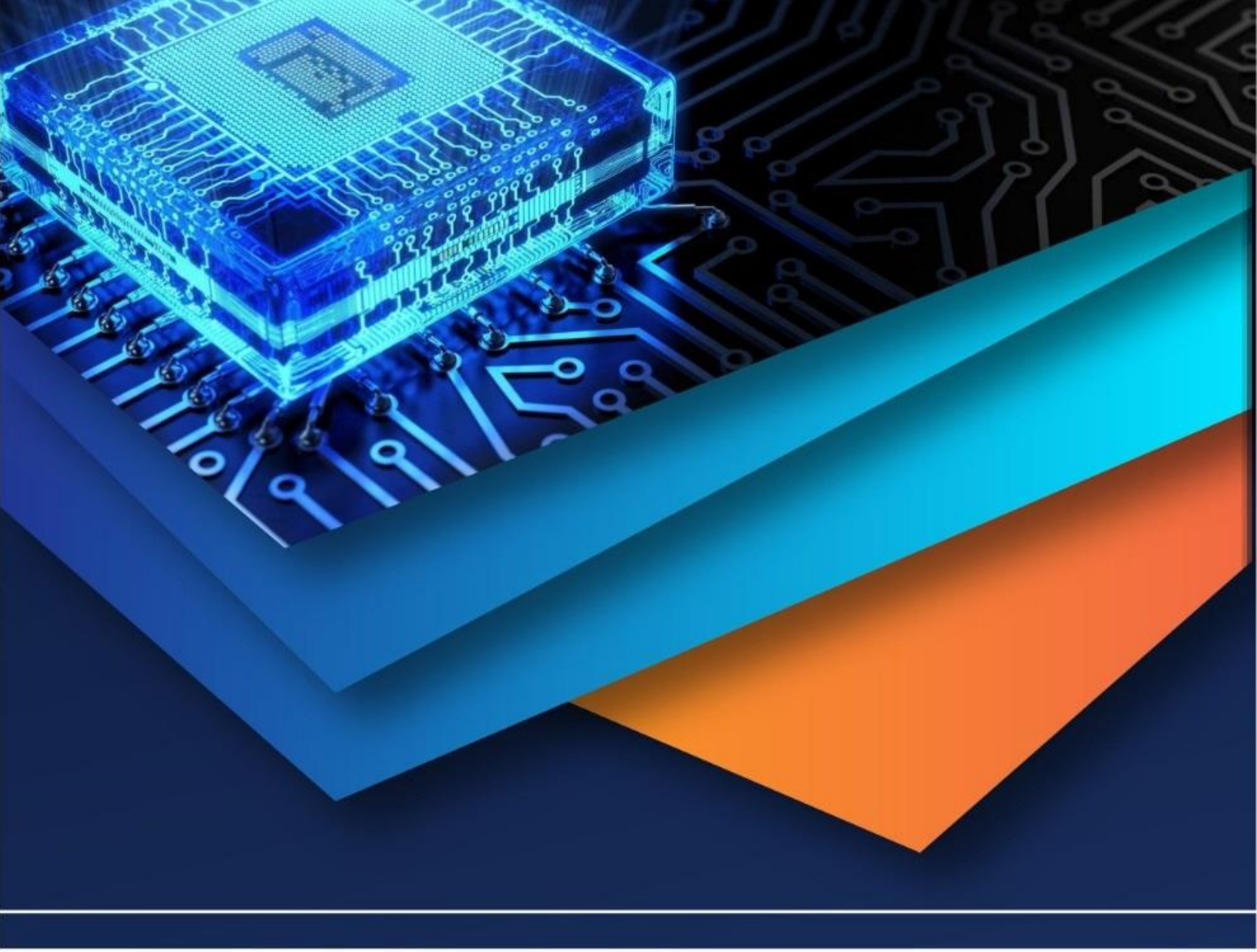
To address these concerns, the Indian Election Commission is experimenting with Blockchain technology. However, as we all know, new technology brings with it new issues. The implementation process is more complicated. Many security researchers and analysts are focusing on finding weaknesses in this technology. Remote voting is possible using software created by the government. Researchers must test the programme in every possible circumstance before releasing it to the public for remote voting. The government should also engage a private testing outfit, although there is a considerable danger of code leaking. As we all know, hackers may use DDOS (Distributed Denial of Service) attacks to render a server inaccessible for a set amount of time. The Election Committee should next construct voter verification and identity hardware in order to verify each and every voter.

It is critical to have facial recognition, voter identification systems, fingerprint verification systems, and, most significantly, the capacity to vote using the Aadhar card. As a result, there should be a link between UIDAI and ECI servers.

The major issue is caused by UIDAI and ECI Servers. When they are breached, every voter's personal information is accessible. Voting may be cancelled as a result of this. There has been a significant loss of assets, money, and time.[2][5]

Voting entails selecting a candidate who is capable of listening to issues and quickly developing a solution. An isolated atmosphere should be established so that the voter cannot be swayed by outside sources. The country should choose the best candidate.

Trust and openness are essential components of Remote Voting. Even if the government possesses all of the necessary software and hardware. Voters should be



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY