iJournals: International Journal of Software & Hardware Research in Engineering (IJSHRE)
ISSN-2347-4890
Volume 11 Issue 12 December 2023

Cyber Security Architecture for General Election in India

Author: Arun M. Ranvir

Affiliation: Scientist-F and Senior Director (IT)

NIC, MEITY, Amravati IN

E-mail: am.ranvir@nic.in

DOI: 10.26821/IJSHRE.11.12.2023.111209

ABSTRACT

Indian Constitution gives rights to the citizens for representation in house of people by means of Elections. Now a day's Digital Technologies are playing major role in conducting Elections in India. Securing Data, Information and ICT infrastructure have become one of the biggest challenges. This paper presents various Cyber Security challenges encountered in Conducting Elections and Design of Cyber Security Architecture to overcome Cyber security issues for conducting free and fair Elections. Cyber Security Architecture is based on OSI architecture model to overcome the cyber security challenges in Elections. Cyber Security Architecture help to reduce the Risk of vulnerability and Cyber Security issues in General Election and improve the Security measures and offer new possibilities of transparency in General Elections of India.

Keywords: ECI, ICT, Cyber Security, Election, Data, Information, Digital, Systems, Architecture, NIST, CSF

1. INTRODUCTION

As per the Indian Constitution voting is the fundamental right of all citizens over the age of eighteen years. Indian Constitution consists of Articles 324 that provides the power of superintendence, direction and control of Elections to Parliament, State legislatures, the office of President of India and the office of Vice-President of India shall be vested in the Election Commission. The Election Commission prepares, maintains and periodically updates the Electoral Rolls, Organize the polling booths where voting takes place, counting of votes and the declaration of results [1]. Election Commission of India focuses more on use of Digital Technology in Election Process. These Technologies are now playing a major role in Conducting General Election in India. Digital Technology is being used in conducting

Elections for Electronic voting machines, Voters online Registration, Declaration and Disseminations of Results the explosion of these new Technologies and increasing access to citizens and election machinery creates some issues of Cyber Security.

Internet is the fastest growing infrastructure in the world today and we are unable to safeguard our information so Cyber crimes are increasing day by day. The act of protecting ICT systems and their contents has come to be known as Cyber Security. Cyber security is an important tool in protecting privacy and preventing unauthorized surveillance and information sharing [2]. The growing use of technology in the election process has made cyber security a crucial issue. Instances of the spread of fake news, manipulation of voter behaviour and hacking shows how digital technology can be misused. These issues need to be addressed in the long term. The Election Commission tasked with maintaining the sanctity of India's electoral process, has taken several steps to ensure the inviolability of the technical infrastructure, which includes the Electronic Voting Machines (EVMs), voter database, voting software and IT systems [3].

A Cyber security threat includes hacking, compromising private information of voter registration rolls and election results. Distributed denial of service attack which floods a website or service in order to render it unusable for legitimate users, has become a threat to Elections. Commentators and academics alike have warned about the potential for security breaches, threatening the privacy of an individual's vote, erasing or amending election results [4]. The internet opened no. of possibilities in democratic politics in both good and as is increasingly to be bad. Security vulnerabilities can be exploited to electronically disrupt voting or affect counting of vote counts.

Cyber security frameworks are sets of documents describing guidelines, standards, best practices designed for cyber security risk management. Cyber Security framework provides foundation, structure, support to an organizations security methodologies and efforts [5]. NIST Cyber Security Framework is a voluntary framework that consists of standards, guidelines and best practices to manage Cyber Security related risk. Benefits of NIST CSF compliance are helps you better understand, manage and reduce Cyber Security risks, data loss and the subsequent costs of restoration, Enables to determine your most important activities to deliver critical operations and service delivery [6]. The NIST cyber security framework (CSF) helps organizations to increase their cyber security measures and provides an integrated organizing structure for different approaches in cyber security through collecting best practices, standards, and recommendations [7]. ISO/IEC 27001 is an Information security standard describes the information security management system and it places security within the context of the overall management and processes in a company [8].

Security architecture is a design which identifies the potential risks involved in a certain scenario that the threat actors are likely to exploit. It describes how the security controls are positioned and how they relate to the overall systems architecture. It also specifies when and where to apply security controls [9]. Security architecture applies to systems, people and network infrastructure. It enables building security into systems: design, implementation, management, risk management [10]. India is setting up its own Cyber Security Architecture that will comprise the National Cyber Coordination Centre (NCCC) for threat assessment and information sharing among stakeholders, the Cyber Operation Centre that will be jointly run by the NTRO and the armed forces for threat management and mitigation for identified critical sectors and defense and the National Critical Information Infrastructure Protection Centre (NCIIPC) under the NTRO for providing cover to Critical Information Infrastructure [11]. Security architecture contains various set of models, methods and security principles that align with organizations objectives to keep organization safe from cyber threats. Through security architecture is an organization requirement which is translated to executable security requirements. A Security architect must understand the Network, firewalls, defences, detection systems, etc. The OSI Security architecture is an internationally accepted standard and a structured approach to Cyber Security. It outlines certain security services that need to be in place to secure data as it moves across a network [12].

The Recent trends in Digital technologies, there is a need to solve Cyber Security challenges associated with protecting Election Infrastructure. The Election Commission of India using IT Systems to increase elections activities to reduce the elections expenses and to achieve goal of Transparency and faith of citizens in Election system. IT team of Election Commission has taken IT initiatives and developed no. of Election related application and Mobile app for conducting free and fair Elections in India. Election IT infrastructure being faced by Cyber Security challenges need to be addressed and Cyber security solutions and Cyber Security Architecture need to be designed and deployed to conduct the Elections in India.

The remaining part of paper is organized as Section-2 Related Work, Section-3 Cyber Security Architecture Design Considerations, Section-4 Cyber Security Architecture Design aand Section-5 Conclusion.

2. RELATED WORK

Privacy and security of the data, information and IT infrastructure are the top Security measures that any organizations to takes care of. Elections are being conducted in all Countries using recent Digital Technologies for Election Process from Elector enrolment to Result declarations, etc. Performed study of concept, methodology, techniques for some of the recent ICT based Election systems, Cyber Security Frameworks and Cyber Security Architectures for issues encountered and measures deployed to achieve a goal of Cyber Crime free and fair Elections.

Uzma Jafar, Mohd Juzaiddin Ab Aziz, Zarina Shukur, Hafiz Adnan Hussain proposed system provides a safe, transparent, dependable platform for EA and voters. The suggested framework has a favourable outcome in light of the performance assessment of BC technology in VMS. The proposed system uses Ethereum for its distribution and it operates as an OC that is synchronised with the database used at the district level [13]. Khan Farhan Rafat proposed secure framework for i-Voting using the Internet shall warrant transparent, fully autonomous elections with improved efficacy and efficiency and devoid of any litigation. Revision of the existing i-Voting system shall persuade

Governments and citizens in particular, to accept the verdict of digital electoral and consequently stands as a novel contribution to date in this regard [14].

Bruce Potter used five core functions of NIST for US Election namely Identify, Protect, Detect, Respond and Recover. NIST Cyber Security Framework (CSF) is a useful tool for helping orgs increase their overall resilience and response to cyber threats. Given the utility of the CSF, that it's not only useful for corporations but it's helpful for guiding security activities around processes like national elections [15]. R. Ravikumar proposed Cyber Security Framework in Banks circular from RBI sets the guidelines for Banks in India for developing and implementing next-generation cyber defense capabilities. The RBI cyber security framework addresses three core areas Establish Cyber Security Baseline and Resilience, Operate Cyber Security Operations Centre (C-SOC) and Cyber Security Incident Reporting (CSIR). The IT Architecture should be designed in such a manner that it takes care of facilitating the security measures to be in place at all times [16].

A. Lee, designed security architecture methodology builds on output from existing guidelines and processes that are elements of a cyber security risk management strategy. The objective is to build on these existing guidelines and processes that have been used by utilities rather than developing a new approach. Security architecture is one tool that utilities may use to define the current and target architectures including the attack surface and response strategies [17]. U.S Department of Energy Enterprise establishing the DOE IT Security Architecture to provide a holistic framework for the management of IT Security. The architecture is driven by the Department's strategies and links IT security management business activities to those strategies [18]. Arun Mohan Sukumar, Col. R.K. Sharma proposed a security architecture that can improve interagency coordination; help respond to cyber attacks and prevent them in many circumstances. It offers a structure along which the country's cyber security apparatus may be aligned. The convergence of key departments or wings of the armed forces should create an architecture that is more than the sum of its parts [19].

From the above discussions it is observed that Block Chain Technology enable to provide Secure, Cost-efficient and Scalable Framework for electronics voting system, Mobile Phone with Multi-Factor Authentication enable to provide Framework for Secure Cyber Savvy Internet Vote Casting System. NIST Cyber Security Framework (CSF) is a useful tool for helping orgs increase their overall resilience and response to cyber threats. Five core functions of NIST namely Identify, Protect, Detect, Respond and Recover are used for US Election. IT Security Architecture is to provide a holistic framework for the management of IT Security across DOE. Security architecture that can improve interagency coordination, help respond to cyber attacks and prevent them in many circumstances. ICT playing crucial role in conducting Elections in efficient manner but deployment of new Digital Technologies in Elections comes with new Cyber Security issues. In next section we will discuss Cyber security issues and Challenges encountered in Elections and Cyber security Design Considerations in more detail.

3. CYBER SECURITY ARCHIECTURE DESIGN CONSIDERATIONS

In last few years Election Commission of India focus on use of Digital Technology in Election Process. The use of Digital Technologies in Elections has emerged as a key issue in recent years with concerns about Database hacking, Information manipulation and foreign technological interference leading to public concerns. In this section going to present the General Election process in India and Cyber Security design Considerations in detail.

3.1 General Election Process in India

Election Commission of India Conducts General Election in India for Parliamentary and Assembly Constituencies as per the schedule. General Election process divided into three sections depending on the Election activities that need to be carried out as Pre-Election, During- Election and Post- Election as shown in Fig. 1.

In Pre-Election Phase is the initial phase of Election process, Election related activities need to be carried out are Voters Registration by ARO, Preparation and maintenance of Electoral Roll, finalization of Parliamentary Constituencies, Assembly Constituencies, Finalization and Preparation of Polling Booths, Preparation EVM First Level Checking, EVM Demonstrations to Citizens, Training to Election Officers, Man Power Management for Polling, Implementation SWEEP programmee for increasing voting percentage, Filling of Nominations by Candidates, Election Campaign by Candidates, etc

In During–Election Phase, Election related activities need to be carried out are EVM Deployment for Polling Stations, Man Power Deployment for Polling Stations, Voting of the Electors, Online Poll Day

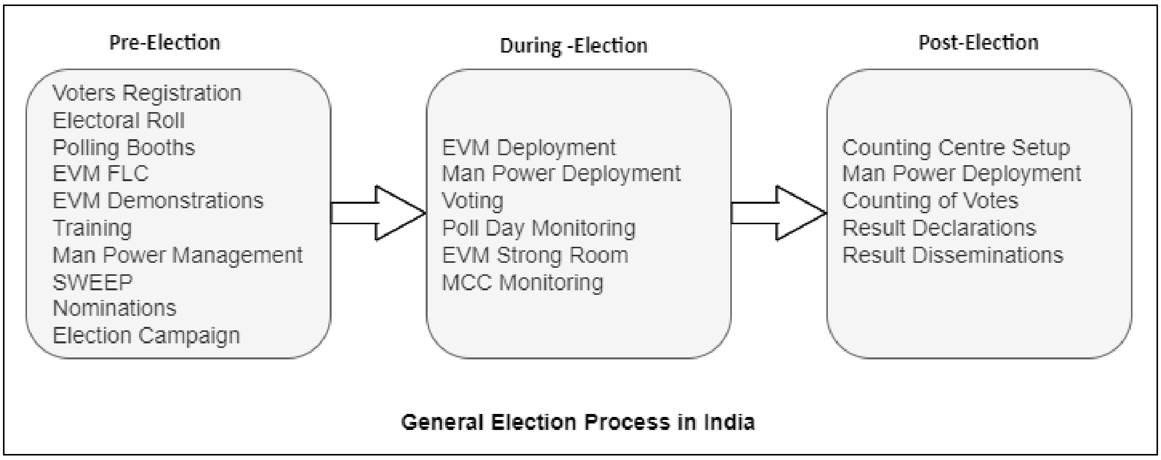

Fig. 1 General Election Process with Activities in India

Monitoring of Voting, Online Violations MCC Monitoring, Setup of EVM Strong Room, etc.

Post–Election Phase is last stage of Election Process, election related activities need to be carried out are Counting Centre Setup for counting of Votes, Man Power Deployment for counting of votes, Result Declarations and Result Disseminations to Election Commission of India.

Citizen, Electors access IT applications for Election related service such as Election enrollment, Deletion, Updating in Election roll, EPIC Card, Violations of Election Module of Conduct etc, upon receipt of request Concerned Election Officer take necessary action and inform accordingly the status of application through SMS. Candidates also request for Permissions for Election meeting, Rally, etc online, Election Officer approve or Reject application accordingly. Election Officers also use these Election related applications during entire Election purpose as per Instructions of ECI and RO handbook. These activities use ICT tool that causes Cyber Attacks for the Election Infrastructure that resulted disruptions in Election process.

Cyber Security Attack trends during Elections

In Election Process some of the Cyber Security issues are Secured identification and authentication, Distributed Denial of Service (DDoS), Web site Hacking, EVM and tamper the results, Illegal Voting, Hacking and Compromising private information are encountered. Some appropriate solutions need to be deployed to overcome the issues. We are going to discuss Cyber attacks in Election Process in detail.

The main targets of hacking attacks against Election-related technology include voter registration technologies, voting, vote counting technologies, result transmission and aggregation technologies, websites for result publication and other online election-related services, institutional and private email accounts and communication systems and broader national infrastructure. Generic attacks often require little sophistication and limited resources and include Denial of Service (DoS) attacks, website breaches and malware and ransomware attacks. Website breaches involve defacing the appearance of websites or manipulating their content. Malware and ransomware attacks can have adverse impacts on elections by making essential systems and data inaccessible. Insider attacks include intentional data and system breaches by users with access to election-related information systems [20]. Election Security issues can impact the equipment and systems voters use to register. Election databases contain the personal data of the voting population within a state, making them extremely appealing to cyber criminals. Failing to prevent election cyber security issues can enable hackers to shut down IT systems and demand ransom fees, steal data and make it available on the dark web and wreak havoc on local and state IT systems. To understand election cyber security threats, it's helpful to understand that all parts of the election process, including voter registrations, ballot creation, voting machines and vote counts, all must be protected. Security vulnerabilities can be exploited to electronically to disrupt voting or Counting of votes in Election Process.

Some of the Cyber Security Attack trends during Elections are Phishing attacks, Digital Dictatorships and Information Warfare, Cybercrimes through Mobile phones, Denial-of-Service Attacks, Malware, Stealing Voter information; Website breaches Attacks, Email Compromise, Networks Attacks, Password Attack, SQL injection, etc. Malicious actors may obtain sensitive information such as User ID and Passwords by pretending to be a trustworthy entity in communications system. Data Servers and Application may be breached to obtain administrator level credentials.

Election Commission of India (ECI) Guidelines: The Election Commission of India guide lines contains precautionary measures for Password Security, Email Security, Mobile Security, Data Storage Protection, Outsourced Staff, Desktops, Data Backup, Wi-Fi Security, Website Security are Password Complexity, Use of Gov, NIC Email, Avoid Whats App for sensitive Official Documents/Communications, Security of sensitive files, Sharing of information/data on need to know basis, Use of supported OS, Devise a data backup policy, Use WPA2 security and Use https for sensitive data interchange respectively [21]. Cyber Security Tips for ECI Officials are Realize that you are an attractive target to hackers, Strong Password, Never leave your devices unattended, be careful when clicking on attachments or links in email and Sensitive browsing [22].

Cbyre Security issues which need to be monitored and controlled by Election Commission of India for the entire Election Process. Election Commission of India therefore needs to initiate additional Cyber Security measures for the long term to conduct free and fair Elections in India.

3.2 Cyber Security Architecture Design Considerations

Cyber Security for the safeguards to avoid any disruption from an attack on Data, Computers, Networks and other Communication devices. Cyber Security covers Confidentiality, Privacy, Availability and integrity of Data and Information for safety and quality. The CIA triad is the backbone of every Cyber Security Architecture. It stands for Confidentiality, Integrity, and Availability, which are three key principles for any security system. Confidentiality ensures that only authorized users have access to sensitive data. Integrity ensures that data is not modified without authorization. Availability is about making sure that systems are available when needed. Data and Information must be protected from unauthorized access, usage, modification, disclosure and destruction. In an organization, to accomplish an effective Cyber Security approach the peoples, processes, computers, networks and technology of an organization should be equally responsible. If all components will complement each other then, it is very much possible to stand against the tough cyber threat and attacks [23].

Initiatives taken by Government of India on Cyber Security: Initiatives are undertaken by Government of India to address Cyber security issues and improve their implementation at the National level. The Indian government has established several cyber security agencies and organizations, such as the National Critical Information Infrastructure Protection Centre (NCIIPC), the Indian Computer Emergency Response Team (CERT-In), and the Cyber Swachhta Kendra, to address cyber threats and protect critical information infrastructure. The National Cyber Security Policy 2013 aims to create a secure cyber ecosystem in India and strengthen the country’s ability to prevent and respond to cyber threats. The policy emphasizes the need for a comprehensive security architecture and framework to ensure the security of India’s cyberspace [24]. However, despite these efforts, cyber security remains a significant challenge in India, with the country facing a growing number of cyber attacks, including data breaches, phishing scams, ransom ware attacks, and malware infections.

Application of NIST Cyber Security Framework: The National Institute of Standards and Technology Cyber Security Framework (NIST CSF) is a set of voluntary standards, guidelines, best practices, recommendations for managing cyber security risk at an organizational level. It is composed of three parts: Framework Core, Framework Implementation Tiers, and Framework Profiles. Election offices should build out a current Framework Profile. The NIST CSF also provides within the document a seven-step process that can be used to create or improve a cyber security program [25]. International legal frameworks and the norms and standards that govern elections must be adapted to cyber elections. Electoral integrity must include the cyber-sphere specifically how it impacts opportunities for deliberation, the quality of participation and the professionalism and transparency of electoral management [26].

Cyber Security Architecture Design Principles: Architect s Guide shows enterprise security architects how they can design and deploy successful, highly automated security solutions based on open architecture and standards to solve cyber security Challenges. TCG's standards and frameworks have been designed to ease the implementation of the six steps as implementation plan as establish consistent architecture, control access, strengthen authentication, encrypt data, layer defenses and automate security [27]. Cyber Security architecture is typically designed using a cyber security architectural framework that specifies the structure, standards, policies and functional behavior of a computer network, including both security measures and network features. To better understand cyber security architecture and its role, by looking at pre-existing standards and the frameworks that support them. Standards set out what must be achieved by various organizations in different industries. NIST framework covers five broad domains (Identify, Protect, Detect, Respond and Recover) and includes categories and subcategories for each. NIST CSF also provides an overview of the separate but interconnected areas that must be addressed when assessing the appropriateness and effectiveness of cyber security architecture [28].

Cyber Security remains a significant challenge as growing number of cyber attacks, including data breaches, phishing, ransomware attacks and malware infections. Cyber security in Election process is a critical issue for election officials and voters. Election officials must develop and follow procedures to ensure the security of all components of the Election process from voter registration through the result declarations. Need to Design a Cyber Security Architecture based on ECI guidelines, NIST framework and OSI architecture structure to overcome the cyber security challenges.

4. CYBER SECURITY ARCHITECTURE DESIGN

ICT tools are being increasingly used in the Election Process to deliver public services and Conduct Election in effective manner but that result into cyber attacks during election process. Cyber Security goals are Authenticate use, Employee access, Keep Data Confidential, Ensure tool reliability and Data Integration [29].

Goals of Cyber Security Architecture are as follows:
1. Protect Organizations ICT Infrastructure
2. Reduce the risk of security breaches
3. Provide Cyber Security Services Confidentiality, Integrity, Availability, Access control and non-Repudiation
4. Prevent, Detect and Respond to the Cyber attacks
5. Design controls for effectively manage risks

Security Architecture contains various set of models, methods and principles that align with organizations objectives to keep organization safe from cyber threats. The OSI Security architecture is an internationally accepted standard and a structured approach to Cyber Security. It outlines certain security services that need to be in place to secure data as it moves across a network. Proposed Cyber Security Architecture for General Election in India is based on OSI Security Architecture which is categorized into three broad categories Security Attacks, Security Mechanisms and Security Services. Security attacks are an attempt to gain unauthorized access to disrupt or compromise the security of an Organization. Security Mechanism that is built to identify security attacks to ICT infrastructure of an organization. Security Services are for maintaining the security and safety of an organization such as confidentiality, integrity, Authentication, Access control and Non-Repudiation [30].

.

Cyber Security Architecture for General Election in India is designed based on OSI Security Architecture which is divided into five components namely Cyber Security Attacks, Cyber Security Mechanisms, Cyber Security Services, Election IT infrastructure and Election Stakeholders as shown in Fig. 2. All components of Cyber Security Architecture interact together to protect the Election IT infrastructure and reduce the cyber security risks during the General Election process to conduct free and fair Elections in the Country. Details of the Cyber Security Architecture Components for General Election in India are as follows:

4.1 Cyber Security Attacks: Cyber Security attacks are the acts of individual or organization to Disrupt or Compromise the security of an Election IT infrastructure such as Systems, Data Base Servers, Application Servers, Application Software, Network, Communication Devices, etc. Cyber Security Attacks are divided into two categories Active attacks and Passive attacks. Active attacks are types of attacks that involve the attacker actively disrupting or altering system, network or device activity. Passive attacks in which an intruder tries to access the data being shared by the sender and receiver by keeping a close watch on the transmission. Some of the Cyber Security Attack during Elections process is Phishing attacks, Digital Dictatorships and Information Warfare, Cybercrimes through Mobile phones, Denial-of-Service Attacks, Malware, Stealing Voter information; Website breaches Attacks, Email Compromise, Networks Attacks, Password Attack, SQL injection, etc.

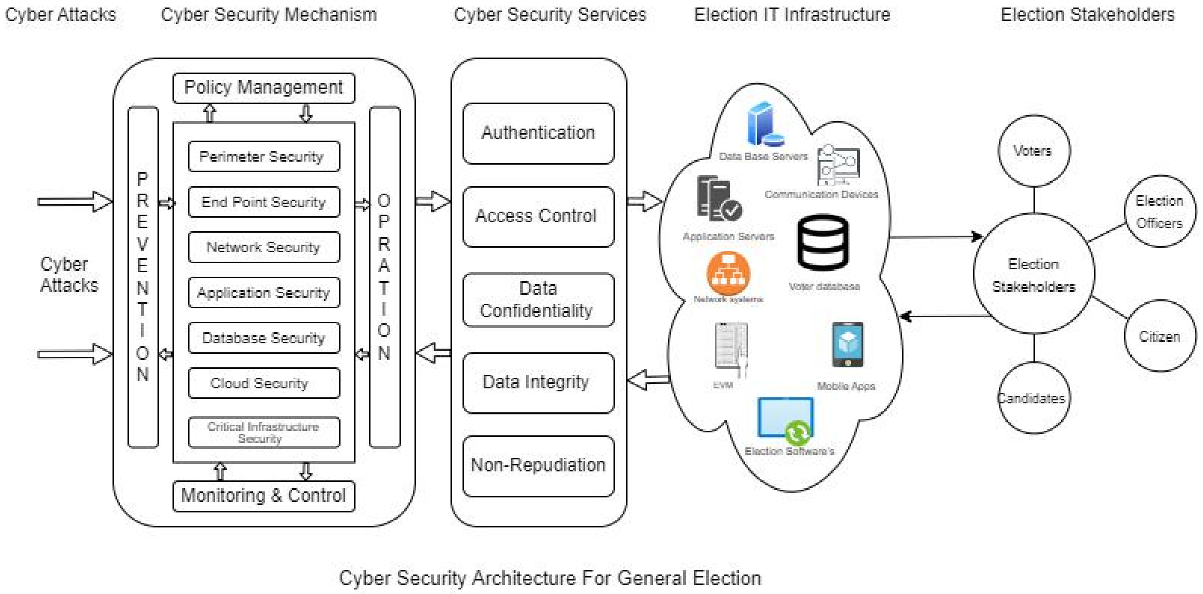

Fig. 2 Cyber Security Architecture for General Election

4.2 Cyber Security Mechanism: The mechanism is one of the major Components of Cyber Security Architecture which is built to identify Cyber Security attacks to Election ICT infrastructure. Cyber Security Mechanism component contains seven security layers namely, Perimeter Security layer, End-Point Security layer, Network Security layer, Application Security layer, Data Security layer, Cloud Security layer and Critical Infrastructure Security layer. It also Contains Prevention, Operation, Policy management, Monitoring and Control Sub-components. These all Sub-Components interact together for Identification and Prevention of Cyber thefts during Election process. Details of seven security layers and controls are as follows:

Perimeter Security layer: Perimeter is the primary interface to the outside world for a System. It contains set of physical and technical security and policies that provide levels of protection against remote malicious activity. It is also used to and protects the back-end Election systems from unauthorized access. Perimeter Firewall, Intrusion Detection System, Intrusion Prevention System, Data Loss Prevention, Data Leak Prevention, etc methods are deployed to ensure Perimeter Security.

Network Security Layer: Network Security deals with ensuring security of Network infrastructure. It contains set of processes that deal with recovery from Security attack. Various mechanisms are designed to recover from attacks at various protocol layers. Enclave Firewall, Virtual Network Security, Voice over Internet Protocol, Network Access Control, Web Proxy Content Filtering, Data Loss Prevention and

Data Leak Prevention methods are deployed to Protect Networks from the Cyber attacks in Election Network Systems.

End Point Security Layer: Endpoint Security Layer is security protection mechanisms and controls that are present on an endpoint device such as computers, laptops, mobile devices, tablets, etc. connected directly with any other network or system. Desktop Firewall, Host Ids and IPs, Content Security, Endpoint Security Enforcement, Patch Management techniques are deployed to achieved End Point Security in an Election

Application Security Layer: Security protection mechanisms and controls that are embedded within the applications while design, development and deployment kept on application servers, computers and Mobile devices. Static Application Testing, Code Reviews, Dynamic Application Testing, Web Application Firewall, Database Secure Gateway, Database Monitoring and Scanning, etc are performed on applications to have a security. Some of the

Election applications are cVIGIL, SUVIDHA, SUGAM, EMS, ERO Net, NVS, PDMS, CDMS, National Grievances Services Portal, ETPBS, etc.

Data Security Layer: Data Security Layer protects data in the organization whether Data is in transmission, at rest or in use. PKI, Data Classification, Data Integrity Monitoring, File integrity monitoring, Data/Drive Encryption, Data Wiping, Data Cleansing, Data Loss Prevention, Data Leak Prevention, etc techniques are used to protect Election Data.

Cloud Security Layer: Cloud Security refers to measures deployed to protect digital assets and data stored online through cloud services providers. Measures to protect Election data include Two-factor authorization (2FA), Use of VPNs, Security tokens, Data encryption and firewall services. Methods of providing cloud security include firewalls, penetration testing, tokenization, virtual private networks (VPN), etc.

Critical Infrastructure Security Layer: Critical infrastructure security is the protection of systems, networks and assets whose continuous operation is deemed necessary to ensure the security. Critical infrastructure of Election includes EVM, VVPAT, Communication systems, etc need to be protected. Access Control, Application Security, and Firewalls techniques are used to protect Critical Infrastructure of Elections.

The Policy Management includes governance processes that take preventive measures ensuring that security implementation and operations are in compliance to the regulations, laws and organizations Security requirements.

The Operations contains tasks for cyber monitoring and response, providing continuous monitoring and management of enterprise cyber security operations in accordance to the security policies.

Prevention is achieved by Policies, procedures, training, threat modeling, risk assessment, penetration testing to posture a secure position.

Monitoring and Control deals with the Monitoring and Control of Cyber Security Mechanism which provides continuous monitoring and management of organizations cyber security operations in accordance to the security policies.

Cyber Security Mechanism Component plays a major role in identification and Prevention of Cyber thefts during Election process.

4.3 Cyber Security Services: Cyber Security Mechanism provides Cyber Security services for maintaining the security and safety of an Election such as Authentication, Access control, Confidentiality, Integrity and Non-Repudiation.

Authentication: Authentication is the process of verifying the identity of a user or device in order to grant or deny access to a system or device. It is achieved by means of Login/Password, Digital Signature Certificate, OTP, Biometric verification, etc

Access control: Access control involves the use of policies and procedures to determine who is allowed to access specific resources within a system. Types of access control are Role-Based-Access Control, Attribute-Based-Access Control, etc.

Confidentiality: Confidentiality ensures that only authorized users have access to sensitive data. Confidentiality achieved by means of two-factor authentication, Data encryption, data classification, biometric verification, security tokens, etc in election process.

Integrity: Integrity ensures that data and information will not get altered, deleted or updated by means of an un-authorized access to the Data Base Systems. Proper measures to ensure integrity in Election process are Group and File permissions.

Non-Repudiation: It involves the use of techniques to create a verifiable record of the origin and transmission of a message, which can be used to prevent the sender from denying that they sent the message.

4.4 Election IT Infrastructure: Election IT infrastructure includes Hardware, Software and Communications systems used to manage Elections process for Voter registration, Votes counting and displaying of election results, Pre and Post-election reporting to ECI. Election IT Infrastructure includes the Electronic Voting Machines (EVMs), VVPATS, Voter database, Data Centers, Data Base Servers, Application Servers, Communication Devices, Network systems, Election Software's and Mobile Apps and other related IT systems, etc. Elections IT Applications which are implemented during Pre-Poll, During the Poll and Post Poll Election Process for successful conduct the General Elections. IT applications being used are cVIGIL, SUVIDHA, SUGAM, EMS, ERO Net, NVS, PDMS, CDMS, National Grievances Services Portal, ETPBS, etc.

4.5. Election Stakeholders: Election stakeholders are individuals who are the part of Election process and responsible for conducting Elections. Major stakeholders are Citizen, Elector, Voters, Candidates and Election Officers. Election Officers includes ECI officials, Chief Electoral Officer, District Election Officers, Returning Officers and Assistant Returning Officers.

Cyber Security architecture helps to demonstrate their integrity and confidentiality to the stakeholders. Strong security architecture must fulfill the three pillars of the CIA Triad Confidentiality, Integrity and Accessibility. Cyber Security architecture provides Security Solutions such as Protect sensitive data across entire Election Network, Secure Election Officers and Voters access to applications and systems, Enhance security operations, Address areas of greatest risk. Ensure that cyber security assessments and services are meeting critical needs and Gain a sound analytic foundation for managing election security risk.

5. CONCLUSION

The increasing adoption and use of ICT has increased the attack surface and threat perception to Election IT infrastructure. Digital Technologies need to solve Security issues associated with protecting Election Infrastructure. Cyber Security architecture for General Election in India based on Election Commission of India (ECI) Guidelines, NIST framework and OSI architecture model to overcome the cyber security challenges. Cyber Security Architecture consists of five components namely Cyber Security Attacks, Cyber Security Mechanisms, Cyber Security Services, Election IT infrastructure and Election Stakeholders. Architecture provides Cyber Security services such as Authentication, Access control, Confidentiality, Integrity and Non-Repudiation. Cyber Security architecture help to reduce the Risk of vulnerability and Cyber Security issues in General Election by deployment of Digital Technologies. It also benefited from Accountability, Transparency, Accuracy, efficiency, etc. Cyber Security architecture for General Election will be implemented effectively during the entire Election Process to ensure that Elections can take place in an orderly and fair manner. Cyber Security Architecture helps to improve the Security measures and offer new possibilities of transparency in General Elections of India.

6. ACKNOWLEDGMENTS

Author was working as a Nodal Officer for Computerization of Election process for General Elections to Parliament and Assembly for Amravati District. I would like to thanks Mr. Saurabh Katiyar District Election Officer for his guidance and motivation during the Elections. I would like to thanks Mrs. Sapna Kapoor SIO Maharashtra for her guidance and motivation. I would like to thanks Mr. Manish Fulzele ADIO and Mr. Yogesh Umak for their support in General Elections and Mr. Abhijeet Ajmire for his IT support for preparation of this Paper.

7. REFERENCES

1. Official Portal of Election Commission of India, https://eci.gov.in
2. Y. Poornima, Y.Naveena and Mr.V.Harsha Vardhan, "Cyber Security Issues and Challenges in India", International Journal of Scientific & Engineering Research, Volume 8, Issue 5, May-2017
3. Sameer Patil, " The Cyber Security Imperative for India's Elections", Gateway House, 18 April 2019
4. Holly Ann Garnett, Toby S. James, "Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity", Election Law Journal, Volume 19, Number 2, 2020
5. Simplilearn, "What is a Cyber Security Framework: Types, Benefits, & Best Practices", https://www.simplilearn.com/what-is-a-cyber-security-framework-article
6. NIST Cyber security Framework, NIST Cyber security Framework | India , www.bsigroup.com
7. Hamed Taherdoost, "Understanding Cyber security Frameworks and Information Security Standards-A Review and Comprehensive Overview"
8. Prameet P. Roy, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard, National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), 2020
9. Security Architecture, AAROH, https://www.aaroh.com.qa
10. Barbara Krasovec and Daniel Kouril, " Security Architecture How to provide secure infrastructure", EGI CSIRT Prague, September 2022
11. Lieutenant General Davinder Kumar, " India's Cyber Security: Architecture and Imperatives", India Foundation / Posts Page / Articles and Commentaries, September 12, 2017
12. Architecture: What it is, Benefits and Frameworks, http://www.dodccrp.org, Threat Intelligence, Jan 25, 2023

13. Uzma Jafar;Mohd Juzaiddin Ab Aziz;Zarina Shukur, Hafiz Adnan Hussain, "A Cost-efficient and Scalable Framework for E-Voting System based on Ethereum Block chain", 2022 International Conference on Cyber Resilience (ICCR), Year: 2022 | Conference Paper | Publisher IEEE
14. Khan Farhan Rafat, "A Framework for Secure Cyber Savvy Internet Vote Casting System: Rebuilding Trust in Digital Electoral", 2022 19th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Year: 2022 | Conference Paper | Publisher IEEE
15. Bruce Potter, " Applying the NIST CSF to U.S. Election Security" , Security Operations, Washington, DC: The National Academies Press, Sep 24, 2019
16. R. Ravi Kumar, " RBI Security Framework", www.rbi.org.in
17. A. Lee , "Cyber Security Architecture Methodology for the Electric Sector", Electric Power Research Institute, Technical Update, December 2015
18. IT Security Architecture, U.S Department of Energy Enterprise Architecture, February 2007
19. Arun Mohan Sukumar, Col. R.K. Sharma, "The Cyber Command: Upgrading India's National Security Architecture", ORF SPECIAL REPORT # 9 , March 2016
20. Sam van der Staak, Peter Wolf, "Cyber Security in Elections" , Models of Interagency Collaboration, IDEA, 2019 International Institute for Democracy and Electoral Assistance
21. Chief Information Security Officer, "Cyber Security General Guidelines for General Election 2019" Election Commission of India
22. Chief Information Security Officer, "ECI Cyber Bulletin, Election Commission of India, October 2019"
23. Cyber Security, https://www.pngegg.com/en/png-wjpvk
24. Cyber Security Compliance in India , https://zcybersecurity.com/cyber-security-compliance-regulations-in-india
25. Election Security Spotlight – NIST Cyber security Framework, https://www.cisecurity.org
26. Holly Ann Garnett and Toby S. James, "Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity" https://doi.org/10.1089/elj.2020.0633, 15 Jun 2020
27. Architect's Guide: Cyber security, Trusted Computing Group, October 2013
28. What is Cyber security Architecture and Why is it Important? , Risk Optics, April 22, 2022
29. Ed Moyale, Diana Kaelley, " Practical Cyber Security Architecture", Packet Publishing, 2020
30. Dr. Dennis, H. McCallam, "An Analysis of Cyber Reference Architectures" NATO S&T Organization, 2691 Technology Drive Annapolis Junction, Maryland