FMDB *Transactions on Sustainable Intelligent Networks*

Designing an E-Voting System Architecture Using the STAP Protocol

Edwin Shalom Soji[1, *], S. Karthik[2], S. Silvia Priscila[3], D. Kerana Hanirex[4], S. Suman Rajest[5], Alycia Sebastian[6]

[1,3,4]Department of Computer Science, Bharath Institute of Higher Education and Research, Chennai, Tamil Nadu, India.
[2]Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Chennai, Tamil Nadu, India.
[5]Department of Research and Development (R&D) & International Student Affairs (ISA), Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India.
[6]Department of Information Technology, Al Zahra College for Women, Muscat, Sultanate of Oman.
edwinshalomsoji.cbcs.cs@bharathuniv.ac.in[1], karthiks1087@gmail.com[2], silviaprisila.cbcs.cs@bharathuniv.ac.in[3], keranahanirex.cse@bharathuniv.ac.in[4], sumanrajest414@gmail.com[5], alycia@zcw.edu.om[6]

Abstract: E-voting is an innovative strategy that empowers citizens to vote for preferred candidates through secure electronic platforms. Implemented across various countries, e-voting systems are tailored to meet specific national requirements. This paper introduces a distinctive approach to the e-voting process, incorporating rigorous verification from government servers and a reliable authentication mechanism to ensure the integrity and security of both e-voting machines and voters' choices. The system employs a Specialized Security Key Algorithm to provide robust security for voters and the e-voting infrastructure. Python and SPSS were used to analyze data and validate security measures, while MS Excel was used to organize and visualize the data. The likelihood of communication channel breaches between the system's central server and the e-voting machines is minimized, eliminating significant data breach risks. By adhering to a carefully crafted architectural approach, this system enhances efficiency and achieves superior accuracy and throughput levels, outperforming other e-voting systems. The core methodologies employed in the system comply with stringent security standards and protocols, with all analyses and simulations verified through tools like Python, SPSS, and Excel. This architectural approach significantly elevates the security framework of the e-voting system, making the entire process more secure, reliable, and tailored to modern democratic needs.

Keywords: E-Voting System; Communication and Security; Integrity Channel; Security and Authentication; Data Analysis; Specialized Security Key Algorithm; Direct Recording Electronic (DRE).

Received on: 25/01/2024, **Revised on:** 19/03/2024, **Accepted on:** 01/05/2024, **Published on:** 07/06/2024

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSIN

DOI: https://doi.org/10.69888/FTSIN.2024.000212

Cite as: E. S. Soji, S. Karthik, S. S. Priscila, D. K. Hanirex, S. S. Rajest, and A. Sebastian, "Designing an E-Voting System Architecture Using the STAP Protocol," *FMDB Transactions on Sustainable Intelligent Networks*., vol.1, no.2, pp. 96–109, 2024.

1. Introduction

The cornerstones of democracy are free and fair elections. Conversely, elections are when the majority gets to choose their representatives and say what kind of governance they want. Ergo, if the electoral process is not free and fair, it undermines democracy at its core [1]. With technological advancement, digital solutions have taken over almost all conventional sectors,

*Corresponding author.

including e-voting. It has been proven that e-commerce security and trustable online transactions are a part of everyday life, and we have seen an increase in secure electronic voting systems [2].

In Myanmar, for example, the authorities are now considering a shift from conventional paper ballots to electronic voting systems as it would save time and human resources. Deploying safe and efficient e-voting is necessary so citizens can confidently vote [5]. The central purpose of e-voting is to facilitate a no-frills voting process for the citizens so that they can easily vote without having to wake up early and wait in lines. Many methods and technologies have been suggested to secure e-voting systems to protect the electoral process from various threats such as fraud, hacking, or unauthorized access. Secure electronic voting systems update the electoral process and reinforce democratic institutions [8]. The investigation of solutions that may expedite the process and solve many e-voting problems has intensified. Still, it is necessary to focus on developing secure systems to avoid forgetting aspects like fairness and transparency [20].

Projecting a democracy is a major part of our very front social solicitations. According to this, conservative applications are being made and sent on state-of-the-art cells to influence the projecting of a democratic process, which is fundamentally progressively immediate and persuading [21]. These applications have raised our way of life by which individuals can coordinate the entire world at their fingertips‟-projecting a democratic framework that has known about updating two or three highlights of the delegate technique [1]. It is, by and large, seen as a mode for moving vast majority rules structure, establishing trust in electoral institutions, enhancing the credibility of election results, and improving the overall efficiency of the electoral process, which are crucial goals [2]. It is widely acknowledged that, when implemented correctly, an online voting system can reduce fraud, expedite the tabulation of results, and make voting more accessible to the public [22].

However, if not properly designed and implemented, online voting could undermine trust in the electoral process [2];[3]. This research explores the development of a web-based voting system for school-level annual elections. This system will be entirely paperless, eliminating all manual tasks. Students can access the application on their mobile phones anytime, anywhere, and cast their votes for student representatives as long as they have an internet connection [23]. The system will provide real-time results, eliminating the need for students to wait for extended periods. The system successfully achieved its predetermined aims and objectives. It will benefit users who wish to vote as the voting process will be streamlined through the application [24]. However, following testing, we plan to incorporate additional image verification features for enhanced security and privacy, further safeguarding sensitive voting information [25].

Moreover, a commencement clock can be known to set the race's beginning and end seasons. Close, the Clients are told of the beginning time through a message and can begin projecting democracy. Amid this, assessments are given, and when the clock is finished, the projecting of a democratic method is impeded regularly, and the Clients can see the last outcomes [26]. The coming of electronic democratic (e-casting a ballot) frameworks denotes a huge change in the popularity-based process, offering the commitment to improved productivity, openness, and uprightness in decisions [27]. E-casting a ballot includes innovations, from straightforward electronic democratic machines (EVMs) to refined web-based casting ballot stages. This paper investigates the turn of events, advantages, difficulties, and future possibilities of e-casting a ballot framework, featuring their capability to upset constituent cycles worldwide [28].

The theoretical idea of electronic voting (e-voting) has a decades-long history, starting in the 1960s with early versions of electronic counting and punch-card systems. Largely computerized vote-counting systems for voting machines achieved a significantly high level of use in the United States in the late 1960s and early 1970s. The first of these systems sought to remedy the inefficiencies and inaccuracies that came with manual vote counting. In the 1990s, Direct Recording Electronic (DRE) voting machines were brought in, which allowed voters to cast ballots straight into a computer interface. The initial objective of DRE systems was to expedite the voting process, minimize chances for human error, and have the output displayed immediately. But, with concerns about security, transparency, and voter verifiability that emerged soon after, they started forcing various advances in e-voting technology [29].

E-voting systems generally exist in two categories. Electronic Voting Machines (EVM) are deployed at polling stations and remote Internet-based electronic voting. EVMs are standalone polling stations that record and tally votes, usually with a touchscreen or button interface [30]. They are built to be simple for the end user, minimizing mistakes made by otherwise valid ballots and assuring that votes get counted properly. Although these EVMs offer many benefits, they have been criticized on various grounds, such as software tampering and hardware malfunction [31]. On the other hand, remote internet voting systems permit voters to vote online from any location in a convenient way that is unmatched by anything else – useful particularly for expatriates, military, and persons with disabilities. To secure that process, the vote is sent over the Internet and handled through various security measures such as encryption, digital signatures, multi-factor authentication, etc. Still, cyberattacks and malware threats appear to be a more common worry [32]. The advantages of E-voting systems are more efficient & faster, better accessibility and inclusiveness, cost savings, and they are also environmentally friendly. However, several issues associated with e-voting must be addressed before any possible implementation's success would depend on such a system.

The increasing demand for secure, transparent, and efficient electronic voting systems necessitates the development of robust architectures that can withstand evolving cybersecurity threats. The challenge lies in designing an e-voting system architecture that ensures voter anonymity and data integrity and addresses scalability and user accessibility. Implementing the STAP protocol, known for its enhanced security features, offers a potential solution. This study focuses on integrating the STAP protocol into the e-voting system architecture, aiming to optimize security measures while maintaining the system's operational efficiency and user-friendliness.

1.1. Future Possibilities and Advancements

The fate of e-casting a ballot framework holds promising developments toward tending to existing difficulties and upgrading the majority rule process. The main interest of blockchain in the voting system is that it solves several problems related to the transparency of the votes or security. Since this information is immutable and cannot be tampered with, blockchain technology can greatly increase voter verifiability and prevent manipulation. Initial results from several pilot projects and research initiatives show promise in using blockchain for e-voting.

An innovative way that could be a landmark in E-voting systems is the integration of biometric identity verification with it, such as fingerprint or facial recognition, which will then add further security and access to such voting services. This watershed policy initiative is expected to leverage technology and use biometrics in its simplest form of data capture as a means of virtually permanently ticking off the requirement enshrined in sections 63-65 to save from incapacitation for voter verification (reducing instances of impersonation)—thus enabling only legitimate voters. On the same level, artificial intelligence (AI) and machine learning (ML) have been identified as important in enhancing the efficiency and security of e-voting systems.

Through AI, cyber threats can be dynamically detected and dealt with during operation, while ML ensures optimal performance within process control to improve overall user experience. These technologies also help analyze trends in voting and identify any irregularities, which helps to protect the integrity of the election process. E-voting systems are a major development in democratic processes and offer advantages in efficiency, accessibility, cost reduction, and environmental impact. Yet, the mere consideration of these reforms falls short if the challenges related to security concerns, transparency issues, and opacity in the e-voting process, as well as narrowing the digital divide gap, ensure electronic voting reliability.

With learning from across the globe and introducing cutting-edge technologies, including Blockchain, Biometrics, AI & ML, etc., the future of e-voting speaks for itself with more inclusive, secure, and reliable elections. This progress is imperative for the continued health of democracy throughout the world. It needs to be ongoing to keep prices elections fair & square whilst being accessible by every citizen. As technology progresses, so will how nations can continue ensuring their citizenry has fair and open democratic mechanisms, translating into more secure electoral systems worldwide.

1.2. The Modern Extent of E-Casting Ballot Frameworks

E-casting a ballot framework, which influences electronic means to project, record, and count votes, fundamentally affects how races are directed all over the planet. As innovation progresses quickly, the potential for e-casting a ballot framework to change vote-based processes is huge. This article investigates the modern extent of e-casting a ballot framework, inspecting emerging innovations, possible advantages, challenges, and the groundbreaking effect these frameworks could have on the worldwide majority ruling government.

Modern e-voting systems use digital technology to allow voters to cast their ballots electronically, either at polling stations with voting machines or remotely via the Internet. These systems focus on improving convenience, accessibility, and efficiency while ensuring security, accuracy, and voter privacy. Key aspects include:

- **User Interface:** Easy-to-use interfaces that guide voters through the process.
- **Security:** Advanced measures such as encryption, blockchain, biometric authentication, and secure hardware to prevent tampering and ensure vote integrity.
- **Auditability:** Features for auditing and verifying results, often including paper trails or independent verification.
- **Accessibility:** Options that support voters with disabilities, allowing independent and private voting.
- **Scalability:** The ability to handle large numbers of voters efficiently, suitable for national and local elections.

While these systems offer many benefits, they face challenges like cybersecurity risks, maintaining voter trust, and ensuring everyone can access the necessary technology.

1.3. Verifiable Setting and Present Status of E-Casting a Ballot

1.3.1. Verifiable setting

E-voting systems have advanced significantly, focusing on enhancing security, accuracy, and transparency. Modern e-voting includes technologies like Direct Recording Electronic (DRE) machines and remote internet voting. These systems now incorporate measures such as:

- **User Interfaces:** Intuitive and user-friendly designs to guide voters through the process.
- **Security Measures:** Advanced methods like encryption, biometric authentication, and blockchain technology to protect vote integrity.
- **Auditability:** Voter-verified paper audit trails (VVPAT) and end-to-end verifiability features that allow voters to confirm their votes have been accurately recorded and counted.

1.3.2. Present Status

E-voting systems are now widely used in various forms, from polling station machines to remote internet voting platforms. Key aspects of their current state include:

- **Polling Station E-Voting:** Utilizes advanced DRE machines with security features and accessibility options for disabled voters.
- **Remote Internet Voting:** Offers convenience for overseas citizens and those with mobility issues, employing robust security protocols to mitigate cyber threats.
- **Challenges:** Despite advancements, issues like cybersecurity threats, voter trust, the digital divide, and the need for standardized regulations remain critical concerns.

While e-voting systems have significantly improved the electoral process, continuous efforts are needed to address security, accessibility, and trust issues.

2. Review of Literature

Throughout the long stretch, titanic work has been centred around organizing and making secure electronic prevalence-based (e-projecting a surveying structure) frameworks to safeguard the conventionality of votes, guarantee occupant protection, and foster confidence in e-projecting democratic structure structures [5]. The limitations of traditional paper-based voting form systems, which are susceptible to errors and failures, and the ease with which surveying structures can be tampered with have fueled the development of e-voting [6]. Electronic majority rule machines (EVMs), viewed as a strategy for accelerating the popularity-based cycle, reducing bumbles, and further fostering security, were the focus of early research into e-projecting a voting form [7]. Despite this, concerns regarding the ease of use and security of electronic voting machines (EVMs) prompted researchers to investigate more advanced developments, such as blockchain and cryptographic displays, to increase public trust in these machines [8].

Much writing has been written about cryptographic conventions, which guarantee votes' honesty, credibility, and secrecy [9]. By ensuring resident insurance and thwarting terrorizing, early essential work on secure multi-party computation influences e-projecting some polling form systems [10]. E-casting ballot frameworks that arrange beginning to end (E2E) have become potential because of these progressions and headways in cryptographic techniques like homomorphic encryption and zero-data checks [11]. This implies that electors can autonomously confirm that their votes were given a role as expected without uncovering how they cast a ballot [12].

In addition, experts have investigated incorporating blockchain technology into electronic polling form systems [13]. Blockchains' public, decentralized ledgers guarantee transparency by making it impossible to change votes without leaving traces [14]. For instance, two or three scientists have proposed utilizing blockchain advancement to make direct and notoriety-based records that anybody can use to check political decision results [15]. Even though blockchain-based majority rules in the government are more appealing than paper-based vote-based systems, there are still issues with adaptability and viability, particularly regarding the enormous scope of public races [16].

The STAP (Secure Transmission and Authentication Protocol) protocol has recently been proposed for implementing a secure communication channel in e-voting systems [2]. STAP was created to mitigate the weaknesses of existing communication protocols and establish a foundation for securely transmitting votes from voting machines to central servers [11]. A study of the STAP protocol has emphasized its properties in thwarting various forms of cyber threats, such as man-in-the-middle attacks, data tampering, and others that could compromise the security posture across all layers involved during a voting process [14].

Several studies have shown that STAP effectively improves the security of electronic voting systems, particularly where trusted and secure communication is needed [5].

Moreover, biometric authentication has been well-researched to improve the security and usability of e-voting systems [4]. Biometric methodologies like fingerprint recognition, facial recognition, and iris scanning provide reliable ways to verify a voter's identity, thus also helping prevent impersonation [7]. It helps reduce the risk of election rigging and, at the same time, provides a frictionless, user-friendly way to vote from anywhere, with acceptable levels of ease [18]. However, incorporating biometrics in e-voting systems also raises questions about privacy and the misuse of biometric data [9]. To mitigate these concerns, researchers in recent studies have investigated privacy-preserving biometric authentication techniques that enable secure voter verification without revealing private information [10].

Artificial intelligence (AI), particularly machine learning, has been identified as the cornerstone for e-voting systems regarding security robustness [11]. Voting processes can be monitored in real-time using AI-driven algorithms to watch for anomalies that could evolve into threats, maintaining the integrity and transparency of the voting process [12]. These functions have been the focal point of active research on leveraging AI and ML to enhance existing e-voting systems by being able to predict cyberattacks, improving voter accessibility, and safeguarding vote-count accuracy. The use of AI in e-voting also poses ethical issues, especially regarding the transparency of decision-making processes and susceptibility to bias in algorithms.

The literature reviewed also examined the legal and regulatory issues around e-voting systems. Adopting e-voting technologies necessitates a gamut of legal frameworks around electoral processes in general, data protection regulations, and cybersecurity [5]. Several studies have highlighted the need for legal and regulatory norms to be established to keep e-voting systems safe, transparent, and accessible while at the same time guaranteeing that no citizen is deprived of their voting rights [8]. These studies underscore the necessity for global collaboration and regulation standardization to promote universal acceptance of e-voting systems [17].

User experience of e-voting systems and accessibility is another important research area [8]. They can be successful only if they are accessible and user-friendly to all voters, including voters with disabilities [9]. Research has investigated the development of e-voting interfaces that work for all voters, including those with visual and motor disabilities [16]. The design of universally available e-voting systems is a complex challenge, requiring insights from human-computer interaction (HCI), accessibility studies, and voter behaviour research [11].

The scalability and reliability of e-voting systems have also been significant areas of concern in this literature [12]. National-level high-scale elections need a system that can handle millions of votes without sacrificing security or performance [3]. Research on scalability in e-voting has explored different architectures for large-scale voting systems, focusing on maintaining performance and availability during peak voting times [1]. These works highlight the necessity of rigorous testing and redundancy to prevent system failures and guarantee reliable performance from e-voting systems during elections [15]. Lastly, the literature emphasizes the need for public trust in voting technologies [16].

Public mistrust in the security and reliability of e-voting systems is a significant barrier to their successful implementation due to their potential impact on election integrity [17]. Research has shown that maintaining transparency in developing and effectively communicating the protective measures integrated into e-voting systems can help build public trust [18]. Public education campaigns, stakeholder consultations, and independent audits are crucial for building and maintaining trust in e-voting systems [19].

3. Proposed Architecture

This is a very important part of the proposed design because it relates to how effective and secure the system is. The core of this architecture is creating a secure communication channel that addresses practical applications, such as e-voting. This architectural diagram shows a government server and a private server playing their roles in authenticating users. The system must always operate confidentially, following all security protocols to secure the process. These security measures are essential as the e-voting system is intrinsically sensitive. Authentication is intentionally stringent, with users needing to authenticate via two methods: one provided by the public server and another by the private server.

Authentication at national and device levels enhances security and adds integrity to voting. The servers used in this system incorporate a two-layer authentication process, making them even more resistant to possible threats. This two-stage security, one specifically at each of the three levels and another across them, ensures that all aspects of the servers are robust, providing a strong foundation for the entire e-voting structure. This proposed solution, compliant with this secure architecture, aims to solve the main challenges associated with e-voting systems, leading to a more reliable election.

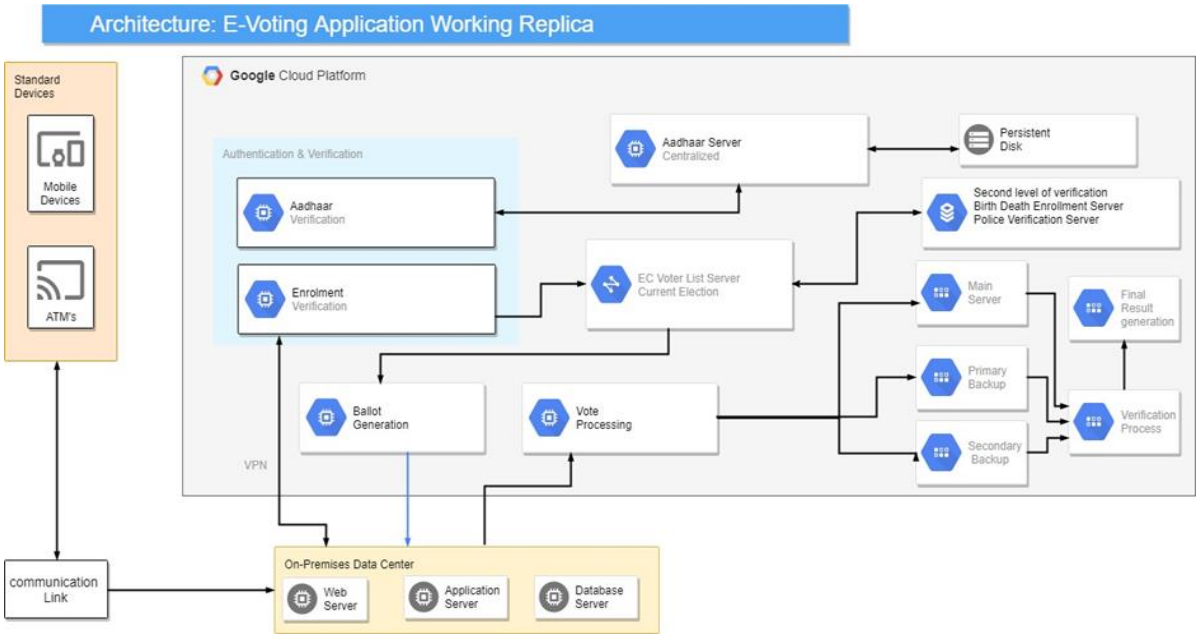

Figure 1: Systematic Architecture for the Proposed e-Voting System

3.1. Client-Side Architecture

The client side of engineering examines the framework's general exhibition and its functioning presentation. The framework will contribute to the client side as the client of the framework assumes a more significant part in the engineering. The E-Citizen needs to show off his abilities as the verified elector, as every one of the certifications the client is giving will be authorized by the public authority server regarding the information available in the public authority store.

Figure 1 explains the E-voting application's working replica using cloud and on-premise hardware. It starts with authentication and verification, where services are provided for voters to authenticate through Aadhaar Voter Authentication and Enrollment Verification, which are interfaced on the Aadhaar Server on Google Cloud. After authentication, the voter's details are checked against the EC Voter List Server for the current election. Upon successful verification, the system generates ballots and processes votes within an on-premise data centre.

The data centre contains essential components like the Web Server, Application Server, and Database Server, all connected through a VPN for secure communication. Votes are processed through the Vote Processing Module, backed up on both Primary and Secondary servers. The Biometric Enrollment Server and Police Verification Server are used as a second verification level to ensure the voter's authenticity. Finally, the votes are routed to the Main Server, where they are processed and backed up, leading to the generation of final results. The architecture employs a hybrid design, using cloud-based services for authentication and on-premise resources for secure vote processing, ensuring data integrity and system reliability.

The Client-side partners with the whole portion of the Client association. The client is the person who takes on the structure for the e-tossing of their specific votes. The Client-side server acts as the client's end for the client to settle on their decision. On the Client end, the device which is taken for the settling on of the decision is thought about Around here. The different approval processes for the productive tossing of the data check affirm the sectored e-projecting of a voting form device. The client-side component involves a temporary database and a reasoning server. The concise dataset, ensuring data consistency, gathers client information from various polling devices and stores it within this temporary database. This temporary database is connected to the visualization dashboard, which, in turn, has a controlled connection to the unified dataset.

The integrated server, dynamically connected to the cloud server, establishes a streamlined method for processing data generated by client-side devices. An effective e-polling system should execute the majority of these functions while adhering to regulatory standards and addressing robust requirements related to security, accuracy, reliability, speed, privacy, auditability, accessibility, cost-effectiveness, scalability, and environmental sustainability. Electronic projecting of a polling form headway can intertwine punched cards, optical yield projecting a voting form frameworks and express projecting a voting form corners

(counting independent direct-recording electronic projecting a voting form structures, or DRE). It can likewise integrate the transmission of tickets and votes by strategies for phones, confidential PC systems, or the web.

3.2. The Side-Server Engineering

The server-side component receives and processes data transmitted from the client side. This data is then integrated into the corresponding server for efficient storage. When the client-side component is activated, and the client initiates the authentication process from the voting machine, a request is sent to the server side for comprehensive validation and data synchronization. The server verifies the information provided by the client against the authoritative data stored in the Aadhar seeding server. This ensures accurate authentication. Authentication is successful if all the client-provided details align with the data-sharing server. Secondary verification involves unique fingerprint authentication facilitated by the Unique Fingerprint Server and its associated dataset. When a fingerprint authentication request is generated from the client side for vote casting, the fingerprint data is transmitted from the voter's device to the fingerprint authentication database for access and successful validation. Upon successful verification, the voter is authorized to cast their vote.

The third verification server is the regional access server. Each voter must be authenticated against the designated regional server, which houses the voter's regional information. The voter's precise location is shared from their voting device. This location data is then compared against the regional data sharing database information. Upon successful matching, the voter is permitted to proceed with their vote. The final verification occurs on the server side and involves various incidental data the client provides. This data is cross-referenced with the data-sharing server for thorough verification. Once all four access servers provide positive authentication, the designated voter can cast their e-vote.

4. Result and Discussion

The proposed framework employs a homomorphic encryption algorithm, which utilizes a single key for data encryption and decryption. The lattice-based cryptographic structure integrated into this framework ensures robust isolation and security. The administrator or user must interact with the security system using the Homomorphic Token key, which is provided upon securing the sensitive data.

During the setup above, the client inputs their credentials, which are verified against the capabilities database. Upon successful authentication, the client gains access to the key verification module. Here, the client-provided key is compared against the key generated by the key distribution centre. If the keys match, the client can access the mining scheme to execute mining operations. If the keys do not match, the client is denied access and cannot perform mining tasks within the system.

The vote generation algorithm is as follows:

$$B = M \times C \qquad (1)$$

Where:

B represents the total number of ballots generated.
M is the number of voting machines connected to the system.
C is the constant factor representing the number of ballots each machine can generate

(for example, per session or time unit).

Algorithm for Encryption of Data

Input: Ballot Vote Data (Total Data)
Output: Vote Encryption
Start
For each input in A, do the following:

If (Ballot Data= Voted Casted Data G
Initialize the Data Encryption;
Ma=AMa+ {(AMa, Signature)}
Else if (input! has attribute in G)
Ma=Ama
Return Ma

End

The above-referenced count is used for the powerful encryption of data being secured in the database, and the key is made reliant on the data being secured in the database. The Key Distribution Center holds all the keys made using the encryption approach.

Key Generation Algorithm

Input: Ballot Credentials
Output: Access Rights Upon Successful Verification of Key for Admin
Start
For each ballot input Key A
If Input A →Ma (KCC)
Check the B=Ma (KCC)
If Yes
Allow the Admin to Access the Data in the Cloud
Else
Revoke the String Access of Admin
Then
Repeat the Key A,
Return Access Rights to Admin

Once the Ballot Machine is completely encrypted, the Client end can make the system more compliant with the user, giving the client the right to cast their vote and directly reach the respective repositories mentioned in the architecture. The decryption algorithm states that more overwork is done for the system to make the vote counting more efficient.

Algorithm for Decryption of Data

Input: Ballot Vote Data (Total Data)
Output: Vote Decryption
Start
For each input in A, do the following:
If (Ballot Data= Voted Casted Data G {(Total, Attribute})
Initialize the Data Decryption;
Ma=AMa+ {(AMa, Signature)}
Ma=AMa+ {AMa+, Signature, Key, KCC Data)
Else if (Decrypt in G)
Ma=AMa+
Return Ma
End

Table 1: Total number of Servers and their Capacitated Ballot Generation with TER, SER and TRR

Input Server	Voting Machine 1	Voting Machine 2	Voting Machine 3	Ballot Generation	Typical Error Rate	Systematic Error Rate	TRR
10	50	50	50	50x3 = 150 150x100 =1500	0.0568s	0.4552s	1.225
20	100	100	100	100x3 =300 300x100 = 3000	0.1026s	0.9004s	2.445s
50	250	250	250	250x3=750 750x100 = 7500	1.254s	1.9524s	3.522s
100	500	500	500	500x3=1500 1500x100 = 15000	2.5225s	3.2122s	4.152s

Table 1 provides a detailed analysis of input servers, their corresponding voting machines, and the ballot generation capacity concerning the Typical Error Rate (TER), Systematic Error Rate (SER), and Total Response Rate (TRR). As input servers increase from 10 to 100, a local controller manages up to three voting machines per server. The capacity is calculated by multiplying three by the number of voting machines and then by 100, allowing for simultaneous voting. The table also indicates that as input servers increase, TER and SER tend to grow accordingly (TER from 0.0568 to 2.5225 seconds, SER from 0.4552 to 3.2122 seconds). The TRR, which stands for Total Round-trip Response Time, grows over time, moving from 1.225 seconds with ten input servers to about 4.152 seconds with 100 input servers. These numbers highlight the scalability of the voting system, where more servers lead to greater ballot processing capacity and increased errors and response times.

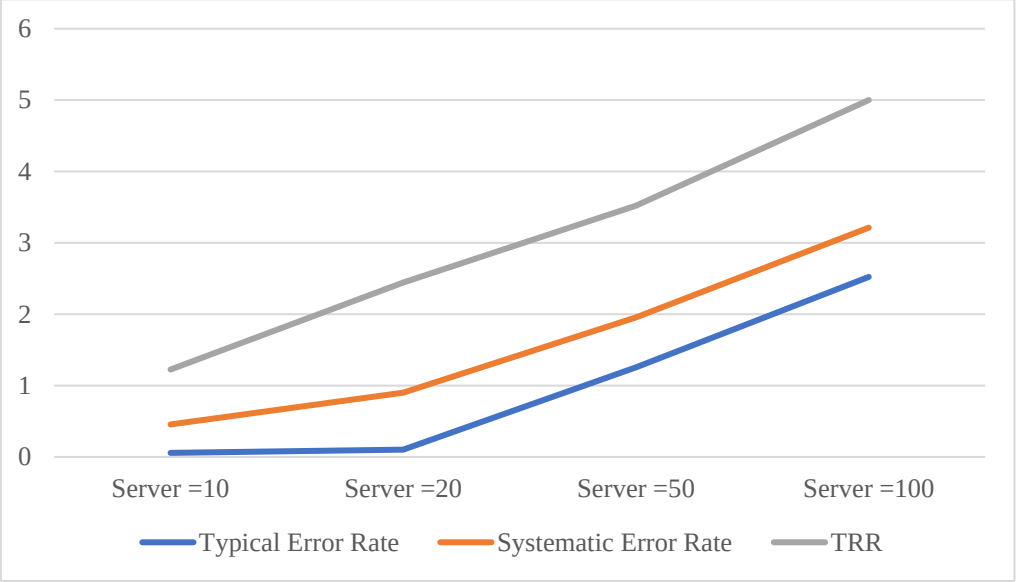

Figure 2: Server Rate to TER, SER and TRR

Figure 2 shows the relationship between the number of servers and three critical performance parameters in an e-voting system: Typical Error Rate (TER), Systematic Error Rate (SER), and Total Response Rate (TRR). As the number of servers increases from 10 to 100, all three metrics exhibit an upward trend. The TER, shown by the blue line, starts low and increases slightly as more servers are integrated, indicating that each additional server introduces more errors. The SER, represented by the orange line, shows a faster increase, compounding the rate at which systematic errors grow with additional servers. The TRR, depicted by the gray line, experiences the most dramatic rise, signalling a significant system-wide increase in response time as the number of servers grows. This substantial rise in TRR suggests that while the system can handle more load, it does so at the cost of longer response times, potentially impacting the efficiency of the scheduling mechanism during high-demand situations. The graph effectively represents the relationship between error rates and response times as the e-voting system infrastructure scales up, highlighting the need to balance system expansion with performance optimization. Error rate calculation is given by:

$$E_{tota1} = E_{typica1} + E_{systematic} \qquad (2)$$

Where:

E_{tota1} is the total error rate in the system.
$E_{typica1}$ represents the typical error rate, which is generally consistent and predictable.
$E_{systematic}$ represents the systematic error rate, which might arise from specific issues in the system or protocol.

E Result is determined with the three restrictive worths, which are the Average Blunder Rate (TER), Orderly Mistake Rate (SER), and Limit Returning Rate (TRR). However, the TER relates the Common Mistake rates with the quantity of the info servers for the polling form age; the SER compares with the Deliberate Blunder which emerges when the Polling form is created and served for the projecting, and The TRR Compares with the Returning span of the polling form regarding the TER and SER; additionally, it involves the absolute edge that is being produced by the E-casting a ballot framework concerning the Encryption and Decoding of the Information that is being furnished from the Voting form Machine as for the worth. Total Response Rate (TRR) is:

$$TRR = \sum_{i=1}^{n}(T_{typica1,i} + T_{systematic,i}) \quad (3)$$

Where:

TRR represents the total response rate of the system.
$T_{typica1,i}$ is the typical response time for the i^{th} server.
$T_{systematic,i}$ is the systematic response time for the i^{th} server.
n is the total number of servers in the system.

4.1. Execution of Equipment Geography and Security Approaches

In the systematic era of equipment geography, ensuring the seamless flow of top-tier information from client to server is paramount. Various security strategies are employed to rigorously assess the entire system's integrity against potential threats.

Authorized Client Access: A comprehensive inventory of authorized clients, the "final list," must be compiled. Only those individuals whose client access credentials appear on this list will be granted access to the system.

Convention IPSec: The IPSec protocol establishes a secure communication channel over the Internet Protocol.

Restricting Port: Port filtering is a configuration mechanism that dictates the specific destinations and methods by which messages can be transmitted or received.

Correspondence HTTPS: HTTPS communication provides end-to-end security between the client and server, safeguarding the communication channel against attacks compromising the integrity of transmitted data.

Log Server Arranged with Interloper Distinguishing Proof Bot: An automated bot is deployed to monitor for potential intrusions and identify any direct or indirect intruders by tracking their socket addresses.

Specialized System: The client-specific application is granted access solely to the front-end server on the designated supporter's server. Direct access to the Vote Server is prohibited for the client.

Equipment Sniffer: Sniffer tools also detect potential attacks and hacking vulnerabilities at the hardware and software levels.

Execution Cloud: All servers directly connect to the cloud for data transmission and storage. A hybrid cloud model offers numerous advantages and is employed for server operations.

Triple Partner Idea and Secret Sharing: Accessing the server, which processes data transmitted from the voting server, requires three generated keys produced during data encryption. A Key Distribution Center is maintained to facilitate secure key sharing among authorized parties. A security key will be generated and securely shared among three stakeholders:

- The Election Commission
- The Ruling Party's Agent
- The Opposition Party's Agent

All created three keys will be Scrambled organization, and information getting to concede consent will be given just when the three partners address their singular key with particular to one another in the Server Confirmation. E-voting systems are poised to reshape the democratic process as technology advances significantly.

From enhanced security measures to increased accessibility and efficiency, the future scope of e-voting holds transformative potential. This essay explores the prospects of e-voting systems, examining emerging technologies, potential benefits, challenges, and their overall impact on global democracy.

4.2. Emerging Technologies in E-Voting

Several emerging technologies are set to revolutionize e-voting systems by addressing current limitations and enhancing functionality.

4.2.1. Blockchain Technology

Blockchain technology offers a decentralized and transparent method for recording votes, ensuring they cannot be altered or deleted once a vote is cast. This technology provides an immutable transaction ledger accessible to all stakeholders, increasing trust in the electoral process. Blockchain can also facilitate secure, remote voting, making it easier for expatriates, military personnel, and voters in remote areas to participate in elections.

Benefits of Blockchain in E-Voting

- **Transparency and Trust:** Every vote cast is recorded on a public ledger, allowing easy verification and auditing.
- **Security:** The decentralized nature of blockchain makes it resistant to hacking and tampering.
- **Efficiency:** Blockchain can streamline the voting process, reducing the time and cost of traditional voting methods.

4.2.2. Biometric Authentication

Biometric authentication can robustly verify voter identity, including fingerprint, facial recognition, and iris scanning. This technology ensures that only eligible voters can cast their votes, reducing the risk of impersonation and fraud.

Benefits of Biometric Authentication

- **Enhanced Security:** Biometrics are unique to each individual, making it difficult for unauthorized persons to vote.
- **Convenience:** Biometric systems are user-friendly and can speed up the voting process.
- **Inclusivity:** Biometric authentication can help ensure that all eligible voters, including those who may not have traditional forms of identification, can participate in elections.

4.2.3. Artificial Intelligence and Machine Learning

AI and machine learning can improve the security, efficiency, and user experience of e-voting systems. AI algorithms can detect and respond to cyber threats in real time, while machine learning can optimize system performance and analyze voting patterns to detect anomalies.

Benefits of AI and Machine Learning

- **Security:** AI can identify and mitigate cyber threats, ensuring a secure voting process.
- **Efficiency:** Machine learning can optimize voting system performance, reducing downtime and improving the user experience.
- **Fraud Detection:** AI can analyze voting patterns to detect and prevent fraudulent activities.

4.2.4. Quantum Computing

Quantum computing, though still in its early stages, has the potential to provide unprecedented levels of security for e-voting systems. Quantum encryption techniques can create virtually unbreakable codes, making it nearly impossible for malicious actors to tamper with voting.

Benefits of Quantum Computing

- **Unprecedented Security:** Quantum encryption can protect against even the most sophisticated cyberattacks.
- **Speed:** Quantum computers can process information much faster than traditional computers, potentially speeding up voting.
- **Scalability:** Quantum computing can handle large volumes of data, making it suitable for national and international elections.

4.3. Potential Benefits of Futuristic E-voting System

Integrating emerging technologies into e-voting systems offers numerous benefits that could transform the democratic process.

4.3.1. Enhanced Security and Integrity

Combining blockchain, biometric authentication, AI, and quantum encryption can create an e-voting system with unparalleled security. These technologies can work together to prevent unauthorized access, detect and mitigate cyber threats, and ensure that votes are accurately recorded and counted. This will maintain the integrity of the electoral process and build public trust.

4.3.2. Increased Accessibility and Participation

Futuristic e-voting systems can significantly enhance accessibility, making it easier for people with disabilities, the elderly, and those living in remote areas to participate in elections. Mobile voting applications and biometric authentication can allow voters to cast their ballots from anywhere, eliminating the need to visit polling stations. This convenience can lead to higher voter turnout and a more inclusive democratic process.

4.3.3. Cost Efficiency and Environmental Benefits

Although the initial investment in advanced e-voting technologies may be high, the long-term cost savings can be substantial. E-voting systems reduce the need for physical ballots, printing, storage, and transportation, leading to significant financial savings. Additionally, reducing paper usage contributes to environmental sustainability, aligning with global efforts to minimize waste and promote eco-friendly practices.

4.3.4. Real-Time Results and Transparency

E-voting systems can provide real-time vote counting and instant results, reducing the time between voting and the announcement of election outcomes. This rapid process minimizes the window for disputes and enhances public confidence in the electoral system. Moreover, the transparency provided by blockchain technology allows voters to verify that their votes have been accurately recorded, further increasing trust in the system.

5. Conclusion

This paper presents a novel approach for encrypting and decrypting data transmitted over an e-voting system, which plays an important role in contemporary voting operations. These days, there are online voting and remote e-voting options in which citizens can use their smartphones to vote for their favourite leader or candidate. However, it is of the utmost importance that these systems are secure and safe — after all, they store voter data, and certifying processes should not be handled lightly. This prevents such issues, as the specific process addresses this by implementing a novel method to connect strong authentication procedures with organizational servers. It secures the usage of the system to only authorized users and provides optimal verification on polling machines.

This process preserves individual choice, enabling voters to vote so that their ballots are cast securely. It uses a Specific Security Algorithm created to provide the maximum level of protection for both the voter and the voting machine. This algorithm will reduce the risks of unauthorized access from intercepting data and manipulating information between a system or server, where it is appropriated, then to e-voting machines. The above system can prevent data breaches up to a great extent, only because attackers would find it impossible to get hold of the voter's private confidential information. In addition, the system's design leads to higher accuracy and throughput than other existing e-voting systems regarding operations. The e-voting is secure, reliable, and assured as security protocols align with well-known standards. This novel approach enhances the security model of e-voting systems and guarantees their performance reliability in election arenas.

5.1. Future Scope

In the future, the E-Voting system architecture deploying the STAP (Secure, Transparent, and Auditable Protocol) protocol will be highly sought after, considering the increasing demand from digital democracies for more secure and transparent electoral processes. Given the growing dependence on digital platforms, STAP can become a crucial component in enhancing the credibility of e-voting systems by incorporating strong authentication, end-to-end encryption, and irrevocable audit trails. This emphasis on transparency and audibility makes the protocol well-suited to counter challenges related to voter fraud, tampering, or privacy concerns three key elements vital for trust in any e-voting system.

Additionally, STAP can be combined with distributed ledger systems to bolster the security and robustness of e-voting against cyber-related and systemic risks as blockchain technology continues to evolve. Furthermore, the application of STAP-based e-voting architectures could be broadened to other sectors that require secure voting mechanisms, such as corporate governance and online community decision-making processes, including referendums. The future could also see enhanced voter

accessibility, with opportunities for secure remote voting and widespread global participation. Continued research in this direction could result in standardized protocols that might achieve global acceptance, sparking the design of e-voting systems that are secure, transparent, and universally accepted.

Acknowledgement: I am deeply grateful to my co-authors for their expertise and dedication, which greatly enriches this work.

Data Availability Statement: The data for this study can be made available upon request to the corresponding author.

Funding Statement: This manuscript and research paper were prepared without any financial support or funding

Conflicts of Interest Statement: The authors have no conflicts of interest to declare.

Ethics and Consent Statement: This research adheres to ethical guidelines, obtaining informed consent from all participants. Confidentiality measures were implemented to safeguard participant privacy.

References

1. C. Castillo, G. Rouskas, and K. Harfoush, "On the Design of Online Scheduling Algorithms for Advance Reservations and QoSin Grids," in Proc. IEEE Int'l Conf. Parallel and Distributed ProcessingSymp. (PDP), California, United States of America, pp. 1–10, 2007.
2. N. Doulamis, A. Doulamis, A. Panagakis, K. Dolkas, T. Varvarigou, and E. Varvarigos, "A Combined Fuzzy -Neural Network Model for NonLinear Prediction of 3D Rendering Workload in GridComputing," IEEE Trans. Systems, Man, and Cybernetics (SMC)-Part-B, vol. 34, no. 2, pp. 1235–1247, 2004.
3. E. Arkin and E. Silverberg, "Scheduling Tasks with Fixed Start and End Times," Discrete Applied Math, vol. 18, no. 1, pp. 1–8, 1987.
4. R. Lucky, "Cloud computing [reflections]," IEEE Spectr., vol. 46, no. 5, pp. 27–27, 2009.
5. K. Singh, E. İpek, S. A. McKee, B. R. de Supinski, M. Schulz, and R. Caruana, "Predicting parallel application performance via machine learning approaches," Concurr. Comput., vol. 19, no. 17, pp. 2219–2235, 2007.
6. M. Maheswaran, K. Krauter, and R. Buyya, "A Taxonomy and Survey of Grid Resource Management Systems for Distributed Computing," Software," Software: Practice and Experience, vol. 32, no. 2, pp. 135–164, 2002.
7. R. J. Al-Ali et al., "Analysis and provision of QoS for distributed grid applications," J. Grid Comput., vol. 2, no. 2, pp. 163–182, 2004.
8. M. S. Fineberg and O. Serlin, "Multiprogramming for hybrid computation," in Proceedings of the November 14-16, 1967, fall joint computer conference on - AFIPS '67 (Fall), California, United States of America, 1967.
9. A. Stankovic, "Implications of Classical Scheduling Results for Real Time Systems," Computer, vol. 28, no. 6, pp. 16–25, 1995.
10. P. Kokkinos and E. A. Varvarigos, "A framework for providing hard delay guarantees and user fairness in Grid computing," Future Gener. Comput. Syst., vol. 25, no. 6, pp. 674–686, 2009.
11. D. Jackson, Q. Snell, and M. Clement, "Core algorithms of the Maui scheduler," in Job Scheduling Strategies for Parallel Processing, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 87–102, 2001.
12. B. Bode, "The Portable Batch Scheduler and the Maui Scheduler on Linux Clusters," in Proc.Usenix Conf, California, United States of America, 2000.
13. Platform"High performance computing (HPC) server and storage solutions," Platform.com, [Online]. Available: http://www.platform.com,. [Accessed: 17-Nov-2023].
14. H. Casanova, A. Legrand, D. Zagorodnov, and F. Berman, "Heuristics for scheduling parameter sweep applications in grid environments," in Proceedings 9th Heterogeneous Computing Workshop (HCW 2000) (Cat. No.PR00556), Mexico, United States of America, 2002.
15. R. Buyya, M. Murshed, D. Abramson, and S. Venugopal, "Scheduling Parameter Sweep Applications on Global Grids: A Deadline and Budget Constrained Cost-Time Optimisation Algorithm," Software," Software: Practice and Experience, vol. 35, no.5, pp. 491–512, 2005.
16. N. Doulamis, E. Varvarigos, and T. Varvarigou, "Fair scheduling algorithms in grids," IEEE Trans. Parallel Distrib. Syst., vol. 18, no. 11, pp. 1630–1648, 2007.
17. K. Rzadca, D. Trystram, and A. Wierzbicki, "Fair Game-Theoretic Resource Management in Dedicated Grids," Proc. IEEE Seventh Int'l Symp. Cluster Computing and the Grid (CCGrid), Rio, Brazil, pp. 343- 350, 2007.
18. V. Martino and M. Mililotti, "Scheduling in a Grid Computing Environment Using Genetic Algorithm," in Proc. 16th Int'l Parallel and Distributed Processing Symp, Milan, Italy, 2002.

19. S. Kim and J. B. Weissman, “A genetic algorithm based approach for scheduling decomposable data grid applications,” in International Conference on Parallel Processing, 2004. ICPP 2004, Quebec, Canada, 2004.
20. A. Thirunagalingam, "Federated Learning for Cross-Industry Data Collaboration: Enhancing Privacy and Innovation," International Journal of Sustainable Development Through AI, ML and IoT, vol. 2, no. 1, pp. 1–13, 2023.
21. A. Thirunagalingam, "Improving Automated Data Annotation with Self-Supervised Learning: A Pathway to Robust AI Models," International Transactions in Artificial Intelligence, vol. 7, no. 7, pp. 1–22, 2023.
22. E. Varvarigos, N. Doulamis, A. Doulamis, and T. Varvarigou, Timed/Advance Reservation Schemes and Scheduling Algorithms for QoS Resource Management in Grids,” Engineering the Grid. Am. Scientific Publishers, California, United States of America, 2006.
23. G. Ye, R. Rao, and M. Li, “A multiobjective resources scheduling approach based on genetic algorithms in grid environment,” in 2006 Fifth International Conference on Grid and Cooperative Computing Workshops, Hunan, China, 2006.
24. I. Foster, C. Kesselman, C. Lee, B. Lindell, K. Nahrstedt, and A. Roy, “A distributed resource management architecture that supports advance reservations and co-allocation,” in 1999 Seventh International Workshop on Quality of Service. IWQoS’99. (Cat. No.98EX354), London, United Kingdom, 2003.
25. M. Kommineni, "Explore Knowledge Representation, Reasoning, and Planning Techniques for Building Robust and Efficient Intelligent Systems," International Journal of Inventions in Engineering & Science Technology, vol. 7, no. 2, pp. 105–114, 2021.
26. M. Kommineni, "Explore Scalable and Cost-Effective AI Deployments, Including Distributed Training, Model Serving, and Real-Time Inference on Human Tasks," International Journal of Advances in Engineering Research, vol. 24, no. 1, pp. 07–27, 2022.
27. P. Pulivarthy, "Enhancing Dynamic Behaviour in Vehicular Ad Hoc Networks through Game Theory and Machine Learning for Reliable Routing," International Journal of Machine Learning and Artificial Intelligence, vol. 4, no. 4, pp. 1–13, 2023.
28. P. Pulivarthy, "Performance Tuning: AI Analyse Historical Performance Data, Identify Patterns, and Predict Future Resource Needs," International Journal of Innovations in Applied Sciences and Engineering, vol. 8, no. 2, pp. 139–155, 2022.
29. S. Temara, “Harnessing the power of artificial intelligence to enhance next-generation cybersecurity,” World Journal of Advanced Research and Reviews, vol. 23, no. 2, pp. 797–811, 2024.
30. S. Temara, “Maximizing Penetration Testing Success with Effective Reconnaissance Techniques Using ChatGPT”, Asian Journal of Research in Computer Science, vol. 17, no. 5, pp. 19–29, 2024.
31. S. Temara, “The Ransomware Epidemic: Recent Cybersecurity Incidents Demystified”, Asian Journal of Advanced Research and Reports, vol. 18, no. 3, pp. 1–16, 2024.
32. W. Smith, I. Foster, and V. Taylor, “Scheduling with advanced reservations,” in Proceedings 14th International Parallel and Distributed Processing Symposium. IPDPS 2000, Cancun, Mexico, 2002.