Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 5, 2025

A COMPARATIVE STUDY OF BLOCKCHAIN-BASED E-VOTING SYSTEMS: CHALLENGES, TECHNIQUES, AND IMPLEMENTATION

Syed Shabeeb Raza[1], Mustafa Ahmed Khan[*2], Muhammad Rayan Shaikh[3], Dr. Sana Alam[4], Muhammad Talha[5], Eman Razzaq[6]

[1,6]*Sir Syed University of Engineering & Technology, Karachi, Pakistan*
[*2,4]*Institute of Business Management, Karachi, Pakistan*
[3,5]*Karachi Institute of Economics and Technology, Karachi, Pakistan*

[1]shabeebraza786110@gmail.com ,[*2]mustafa.ahmed@iobm.edu.pk, [3]mr.shaikh@kiet.edu.pk, [4]sana.alam@iobm.edu.pk, [5]m.talha@kiet.edu.pk, [6]eman.razzaq@ssuet.edu.pk

DOI: https://doi.org/10.5281/zenodo.15411734

Keywords
Blockchain, Solana Blockchain, e-Voting, Zero Knowledge Proof, Advanced Encryption Standard (AES)

Article History
Received on 05 April 2025
Accepted on 05 May 2025
Published on 14 May 2025

Corresponding Author: *
Mustafa Ahmed Khan

Abstract

Traditional voting methods require the physical appearance of voters. With the progress of digital technology and the advent of electronic voting systems, voters can now vote from remote locations. However, even such systems have to face many challenges in terms of safety and privacy. Here, we propose our e-voting system based on blockchain technologies to ensure voter information's anonymity, security, and consistency through Merkle trees and hash digests. The data alteration is easily detected, leading to a compromised block's rejection. This research introduces a novel e-voting solution using the innovative approach of blockchain technology, applying the Advanced Encryption Standard (AES) and Zero Knowledge proof algorithms. Our decentralized architecture ensures a highly secure and transparent voting process and provides a robust framework for verifiable and auditable elections. Applying advanced cryptographic techniques guarantees the confidentiality and integrity of each vote. Designed to be user-friendly, accessible, and adaptable for organizations with internal polls. This landmark initiative lights the way to a new voting process, making it different and impossible to counter until now, as it focuses on security, transparency, and accessibility- all of these being a giant leap forward in the evolution of electronic voting technology.

INTRODUCTION

The demand for secure and efficient online voting systems has become increasingly pronounced in today's rapidly evolving technological landscape. While historically effective, traditional voting methods now face significant challenges related to security, transparency, accessibility, and the overall trust of the electorate. As the world progresses towards digitization in various domains, online voting has garnered substantial interest as a potential solution to these challenges. However, implementing such systems requires addressing concerns related to security, voter anonymity, and the integrity of the voting process.

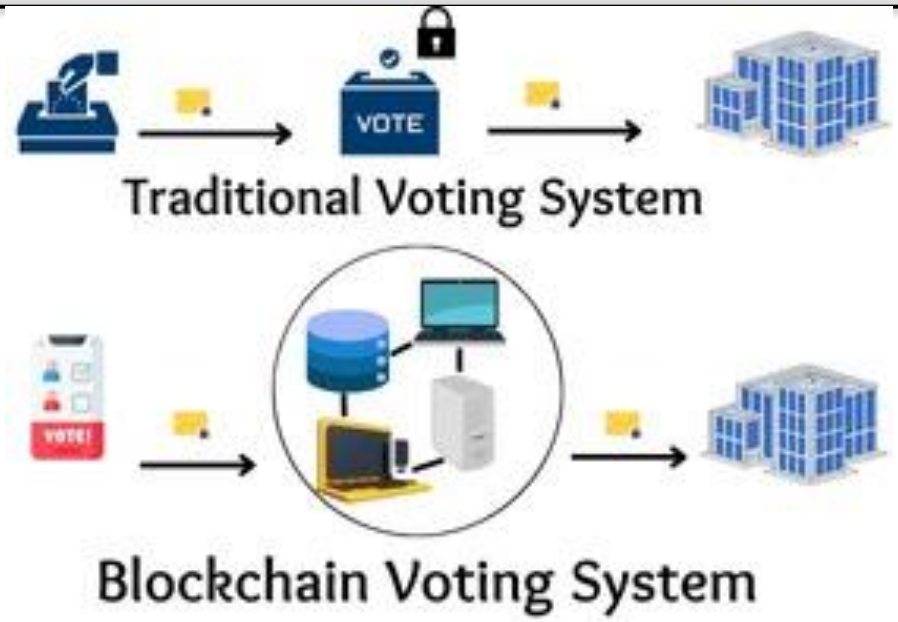

Figure 1: Comparison between Traditional and Blockchain Voting Systems

Blockchain is perhaps the most promising technology for addressing such concerns. Initially conceived as the underlying technology behind cryptocurrency such as Bitcoin, Blockchain has emerged as an adaptable tool used in applications extending far beyond digital currency. The potential use of Blockchain in Internet-based voting has attracted considerable interest among researchers, governments, and technologists all over the globe. Being decentralized, Blockchain enables its users to maintain immutable and transparent records, thus providing an opportunity for the timely and fundamental restructuring of the election process [1][2].

While there is enormous promise for integrating Blockchain technology in e-voting systems, it must be stressed that there are aplenty of hurdles. Some of the challenges would include guarding voter security and anonymity while at the same time ensuring transparency and auditability of the electoral process. Arguably, the other rather pressing challenge would be finding scalable Blockchain solutions for elections in a country or worldwide. Further complicating things is that the legal regulatory framework governing elections varies from place to place. These would lead to difficulties achieving a standardized Blockchain voting system [3].

This paper takes up an extended study in analyzing the application of Blockchain to online voting systems to assess the opportunities and challenges. The primary focus is on evaluating the feasibility of implementing Blockchain-based systems that guarantee secure, transparent, and accessible online voting. While discussing the existing body of research, the paper thus intends to highlight the possible advantages of the Blockchain perspective concerning enhancing the integrity and reliability of online voting systems. At the same time, it will address the limitations and pitfalls of such implementations and place them in real-world examples [4][5].

This analysis was based on previous investigations, including research, technical reports, and specific case studies undertaken in such countries as Estonia and Australia, which have examined or implemented Blockchain voting solutions. The observations from case studies can help better understand some practical challenges and benefits witnessed during real Blockchain implementations in elections. In this investigation, we will act to delineate the possibilities and limitations of applying Blockchain technologies in online voting systems, thereby bringing a more nuanced perspective on its applicability and its potential role in helping to redefine the future of elections [6][7].

1.1. PRELIMINARIES

1.1.1. Architecture and Functionality of Solana Blockchain:

An e-voting system based on Solana will leverage the ability of this solution to facilitate high throughput and low latency to securely and timely handle vast volumes of votes. With architectures designed for thousands of transactions per second, the Solana-based e-voting system will efficiently manage the voting event without delays. Solana has developed a new consensus mechanism called Proof of History (PoH) to timestamp transactions meant to be processed by the Proof of Stake (PoS) consensus algorithm. The hybrid functionality of PoH and PoS is a revolutionary proposal for enhancing speed in transaction processing while ensuring the ledger is immutable and secure. In addition, the PoH instantaneously provides a permanent record substantiating that the event occurred at a particular time, adding another dimension of assurance and transparency critical to a fair election. The voting event is recorded by a decentralized and distributed ledger through Solana, and everything will be recorded immutably and transparently: each transaction (vote). Casting a vote sends the information to the blockchain, where it remains unaltered, permanently cryptographically signed and recorded for that purpose, so it cannot be changed or withdrawn once it's cast. This warrant must be maintained for the trustworthiness of a voter in the e-voting system regarding the security and reliability of the voting system. It means the voting system works with smart contracts within Solana, being a conclusive key to the complete automation of voter registration, vote casting, and the vote counting process. Such a mechanism enables lesser human intervention and enhances the security and reliability of the system by carrying out the process impartially.

1.1.2. Communication Model:

Our e-voting system's communication model allows secure and fast communication among various system components, such as the voters, the blockchain nodes, and the administrative entities.

1. Voter Interaction: Voters interact with the e-voting system through an easy-to-use web-based or mobile portal. This enables voters to register, authenticate, and securely cast their votes. Multi-factor authentication mechanisms incorporating biometric verification and one-time password (OTP) mechanisms can ensure that only eligible voters can participate. Once in, a voter can cast the vote, which will be encrypted immediately and broadcast on the blockchain network.

2. Blockchain Nodes: The voting applications are backed by a network of Solana blockchain nodes. These nodes are responsible for validating transactions (votes), maintaining the ledger, and protecting the entire voting process in terms of security and integrity. Each vote would be sent to multiple nodes, providing redundancy and fault tolerance. PoH and PoS consensus mechanisms will ensure that every node agrees on the ledger's state, negating any chances of double voting and other fraudulent activities.

3. Administrative Entities: Administrative entities such as election commissions or bodies of the organization conducting the elections interact with the system to manage and oversee the voting process. These entities have secure administrative interfaces for monitoring voter registration, supervising voting, and tallying results. Smart contracts can be employed to implement voting rules and ensure that these rules comply with election regulations.

This communication model ensures all interactions are secured, transparent, and auditable. The system uses end-to-end encryption to protect data while being transmitted. At the same time, a service-based mechanism has been developed to create and verify cryptographic signatures on each transaction initiated through the e-voting system.

1.1.3. Blockchain as a Service (BaaS) Model on Solana:

Solana does not directly provide a Blockchain as a Service (BaaS) model like IBM, Microsoft Azure, Amazon, or Oracle. However, the principles and functionalities associated with BaaS can be integrated into or utilized alongside Solana's blockchain. Here's how this translates:

1. **Security Restrictions and Backend Services:** Solana does not offer an out-of-the-box BaaS model. Security and backend services like those described in IBM's BaaS model (authentication, authorization, remote updates, cloud storage, etc.) must be implemented separately using additional tools or services. For example, you might integrate Solana with cloud services (e.g., AWS, Azure) or specialized BaaS providers to manage security and backend operations.

2. **Cloud and Hosting Services:** Solana is primarily a blockchain platform. While it handles transaction processing and brilliant contract execution, hosting, push notifications, and database management are typically managed by third-party services or additional infrastructure layers.

1.1.4. Threat Model concerning Solana:

In the context of Solana, addressing threat models involves understanding the blockchain's security features and how they align with or differ from the models described:

1. **Dolav-Yao (DY) Threat Model:** The DY model focuses on security assumptions for secure channels and authentication. Solana's security primarily relies on its consensus mechanism (Proof of History combined with Proof of Stake) and cryptographic techniques. While Solana provides robust protection against attacks, it does not specifically integrate the DY model. Instead, it utilizes its threat mitigation strategies inherent in its consensus and transaction validation processes.

2. **Canetti and Krawczyk's Adversary Model (CK Adversary Model):** This model deals with session-specific attacks and the compromise of random session credentials. As a public blockchain, Solana does not directly incorporate CK adversary models but employs its own security measures to prevent common attacks like double-spending and replay attacks. Session management and random credential protection would typically be handled at the application level rather than the blockchain protocol level.

2. RELATED WORK

This chapter describes different types of e-voting systems, such as those that rely on blockchain and those that do not, along with their corresponding strengths and weaknesses in terms of security. It goes on to discuss design implementations of these systems and their strengths in protecting the integrity of the voting process against any form of interference. 2005 Estonia became the first country to allow citizens to vote online using a special eID (electronic ID) card. The electronic ID card has an embedded microprocessor chip and an extremely secure code. The ID card also works on a secure platform with a 2048-bit PIN, which ensures maximum safety [8]. Voters download an application, externally prove who they are with an ID card, vote for their candidate of choice, and send their vote online. Security and confidentiality of votes are maintained. Estonians can vote online for 7 days before the official election day. During this time, they can fix any mistakes or change their vote. The system also has a way to keep votes secret and prevent cheating. Voters can even vote multiple times, but only the last vote they send is counted, a rule in place to stop anyone from trying to buy votes. When people vote online, they use a special method called the "double envelope." It's like putting your vote in two virtual envelopes. First, they sign the outer envelope with their eID card. Then, before counting the votes, the system takes off this digital outer envelope to keep everything private and anonymous. As soon as the vote is cast, it will be sent to a vote storage server controlled by the Estonian government [9].

In the **2011 country council elections, Norway** adopted an electronic remote voting system, created by the evoting company **Scytl**. This system closely resembled Estonia's electronic voting system. Around 70,000 Norwegians took the chance to cast an e-vote. This represented about 38% of all the 250,000 people across 12 towns and cities eligible to vote online. Unfortunately, in 2014, Norway decided to halt its I-Voting project due to security concerns [10]. A significant criticism of the Norwegian I-Voting system was the concern that votes might become public during a cyber-attack.

Launched in **2011, New South Wales' iVote system** aimed to boost voter participation, especially for

those with disabilities or living abroad. However, the security snafus, like major glitches in 2015, led to its suspension in 2023. Facing independent reviews and calls for reform, the system's future hangs in the balance as the government weighs security concerns and potential alternatives. [11]:

1) The voter must register with the authorities, receive an 8-digit voter ID, and choose a six-digit PIN.

2) The voter logged in using the iVote ID and PIN to access the voting server or the telephone voting system.

3) They cast their vote and received a 12-digit receipt number.

The vote was encrypted on the client's end, sent to the voting server, and forwarded to a separate verification service. Optionally, the voter could use an interactive voice response (IVR) system for verification by entering the iVote ID, PIN, and receipt number. This service was available until the polls closed. Alternatively, the voter could check the inclusion of her vote in the final count using an online receipt service. No login was required for this service, and it remained active after the polls closed.

Switzerland has also adopted e-voting to boost voter engagement and accessibility. Since 2004, ten cantons have allowed citizens to cast their votes from home electronically. [12] Although praised for its efficiency and increasing participation, especially among younger demographics and people with disabilities, e-voting has encountered scrutiny regarding its security and transparency.

In **2021, a scheme named "MATDAAN"** was introduced. It leverages the Ethereum blockchain to establish a secure e-voting system. Ethereum was chosen for its reliability, open-source nature, and ability to ensure voter anonymity. The scheme involves creating a unique QR code based on user credentials and a one-time password [13].

Table 1: Previous Work & Limitations

FACTORS	[14] [201	[15] [201	[16]	[17] [201	[18] [201	[19] [201 8]	[20] [201 8]	[21] [201 9]	[22] [201 8]	[23] [201 8]	[24] [201 8]
Security	√	√	√	√	√	√	√	√	√	√	√
Eligibility	√	√	√	√	√	√	√	√	√	√	√
Anonymity	√	X	X	√	√	√	√	√	√	√	√
Individual verifiability	√	√	√	X	√	√	√	√	√	√	√
Vote-Privacy	√	X	√	√	√	√	√	√	√	√	√
Robustness	X	X	√	X	X	X	X	X	X	X	X
Coercion resistance	X	√	X	X	X	X	X	X	X	X	X
Receipt-freeness	X	X	√	X	X	√	√	√	X	X	X
Universal verifiability	√	√	√	√	X	√	√	√	√	√	√
Auditability	X	X	√	√	√	√	X	X	√	√	√

Table 2: Comparison Between Different Types Of Zero-Knowledge Proof

Cryptographic Technique	zk-SNARKs [25]	zk-STARKs [25]	Bulletproofs [26]	Transparent Zero-Knowledge Proof [26]	Post-Quantum Cryptography [25]
Proof Type	Succinct Non-Interactive	Succinct Interactive	Succinct non-interactive	Interactive/non-interactive	Various schemes
Trust Assumptions	Trusted Setup	No Trusted Setup	No Trusted Setup	Depends on the underlying protocol	Depends on scheme
Verification Time	Constant	Logarithmic	Logarithmic	Variable	Variable
Proof Size	Small	Large	Medium	Variable	Variable

Computational Complexity	Low	High	Medium	Variable	Variable
Quantum Resistance	No	Yes	Yes	No	Yes
Privacy Guarantee	Strong	Strong	Weak	Strong	Strong

Table 3: Comparison Between Different Blockchain-Based Platforms

Cryptocurrency	Confidentiality	Purpose	Gas Fee	Consensus Algorithms	Transaction Speed (TPS)	Scalability
Solana [25]	Public	Decentralized applications, smart contracts	Low	Proof-of-history, Tower Byzantine Fault Tolerance	65,000 TPS	High
Bitcoin [27]	Public	Peer-to-peer electronic cash system	High	Proof-of-work (PoW)	7 TPS	Low
Ethereum [28]	Public	Decentralized applications, smart contracts	High	Proof-of-work (PoW), Proof-of-stake (PoS)	15 TPS	Medium
Hyperledger Fabric [29]	Permissioned	Enterprise blockchain platform	Varies	A Practical Byzantine Fault Tolerance (PBFT)	1,000 TPS	Medium
Cardano [30]	Public	Decentralized applications, smart contracts	Low	Proof-of-stake (PoS)	257 TPS	Medium

Table 4: Comparison Between Different Techniques Used For Achieving Confidentiality

Factor	Zero Knowledge Proof [31]	Homomorphic Encryption [32]	Secure Multi-Party Computation [33]	Trusted Execution Environments [34]
Confidentiality	Strongest	Weaker	Weaker	Strong
Verifiability	Strong	Strong	Strong	Strong
Flexibility	Low	High	High	Low
Performance	Low	Medium	Low	High
Cost	High	Medium	High	Medium
Trust assumptions	None	Some	Some	Some
Applications	Proof of knowledge, blockchain, voting, digital signatures	Computation on encrypted data, machine learning, and medical records	Data sharing, contract signing, and auctions	Sensitive computations

2.1. Motivation and contribution of the Research:

E-voting systems were designed to bring an element of accessibility to the voting process while enhancing efficiency and securing the process. Problems with conventional voting, like logistical nightmares and accessibility, are tackled, giving way to casting votes by simply pushing a few buttons through the e-voting system. Different technologies like encryption and blockchain are incorporated to ensure that the whole voting process is made safe and secure in terms of privacy. The different e-voting systems available for analysis, or the making light of their implementation, security features, and challenges, include Estonia's pioneer system, Norway's experiment, New South Wales's iVote, and the

adoption in Switzerland. Integrating blockchain into e-voting in initiatives like the MATDAAN scheme is viewed as a leap in securing the integrity and transparency of e-voting.

1. **Increased Accessibility**: E-voting systems enhance voter participation by granting easier access, especially for people with disabilities or citizens living abroad.

2. **Enhanced Security and Privacy:** Advanced procedures for encryption and authentication protect against vote tampering and ensure the secrecy of the voters.

3. **Efficiency and Convenience:** Internet voting is easy, lightens the administrative workload, and allows voting from home.

4. **Innovative Technology Integration:** Using modern technologies like blockchain enhances security and transparency in e-voting systems.

5. **Comparative Analysis:** The general overview compares various e-voting systems, stressing the merits and demerits of the experiences learned from their implementations.

6. **Implementation Challenges:** Insights concerning the difficulties encountered by different systems, such as security threats and system suspensions, serve as a basis for further improvements.

7. **Technological Advancements:** The introduction of blockchain technology to the e-voting process, as witnessed with the MATDAAN scheme, is another leap forward in securing the voting process.

8. **Future Directions:** The study of existing systems would serve as a basis for further studies and research that ought to guide enhancement in e-voting in terms of efficiency and security.

E-voting systems are the next stage of development beyond the traditional methods and early trials of electronic voting systems. In comparing these modern systems to their immediate forebears, one can see how far they have come regarding accessibility, efficiency, and security. Others, like Estonia's e-voting and the blockchain initiatives of MATDAAN, are comparisons with bygone practices as they strive, to a new level, to ameliorate key issues of privacy for the voter and integrity of the vote. On the other hand, the challenges faced by systems like Norway and New South Wales certainly point to the need for further refinement and innovation. By learning from these historical lessons and amalgamating new high-end technologies, e-voting systems have been fast-tracking their evolution to improve democratic participation and ensure secure, transparent electoral processes.

3. PROPOSED SCHEME:

Our proposed e-voting system aims to transform elections by integrating advanced technologies for environmental preservation, financial savings, and enhanced democracy. Utilizing blockchain technology through the Solana network ensures a secure, transparent, and scalable voting process. The decentralized ledger of Solana reduces the environmental impact associated with paper ballots and lowers operational costs. For robust data protection, we employ AES encryption, safeguarding voter information from cyber threats and ensuring the confidentiality and integrity of the voting process. Additionally, Zero-Knowledge Proofs (ZKP) are used to maintain voter anonymity, allowing individuals to verify their eligibility and cast their votes without disclosing personal details or voting choices. This combination of technologies promotes environmental sustainability and cost efficiency and fosters trust and participation in the democratic process.

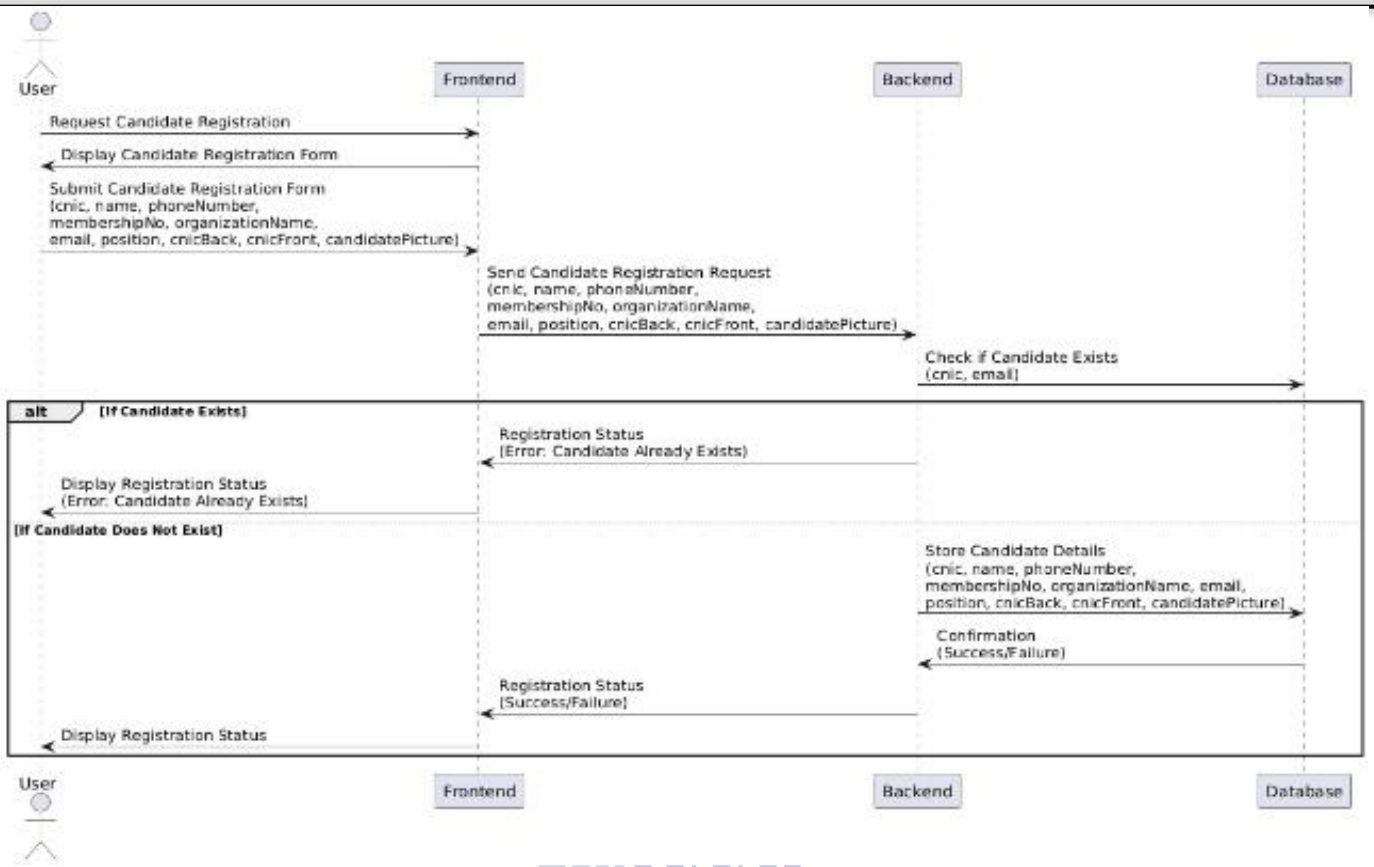

Figure 1: Candidate Registration Phase

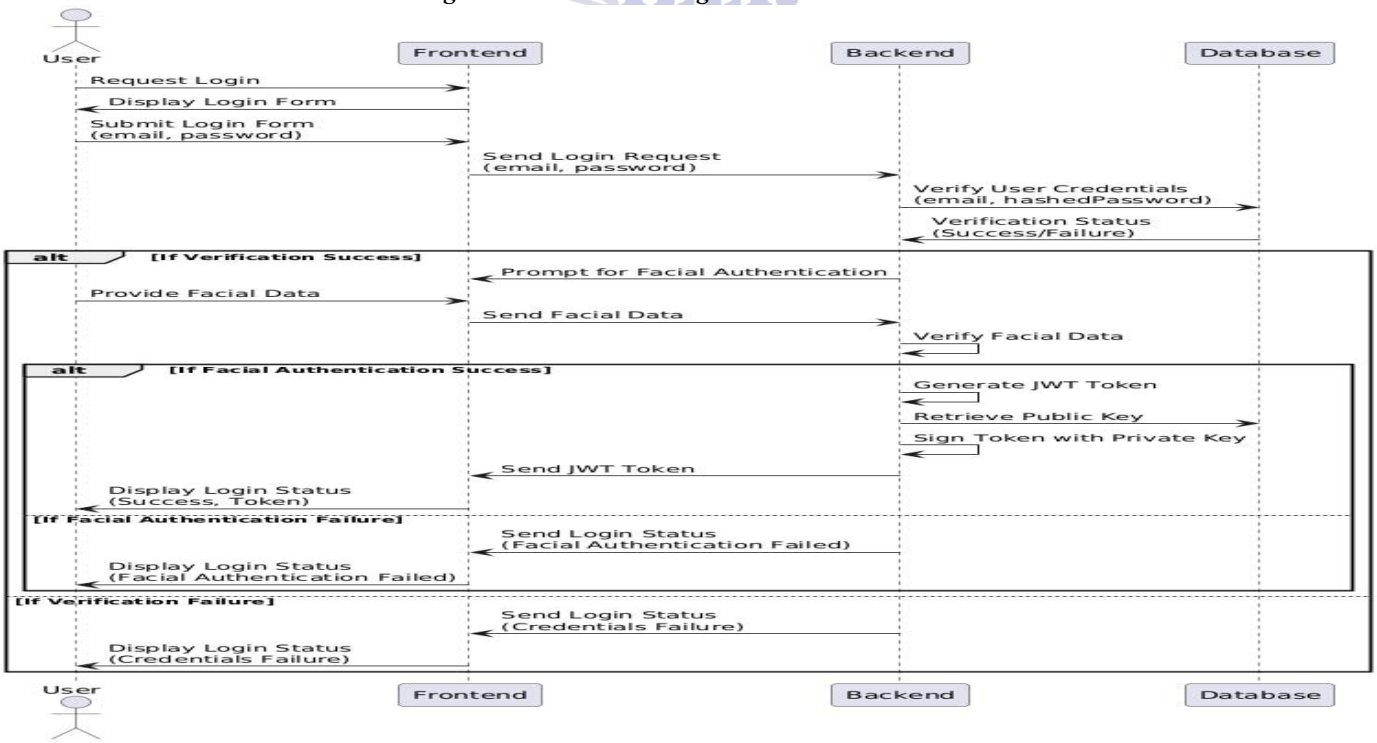

Figure 2: Voter Login and Authentication

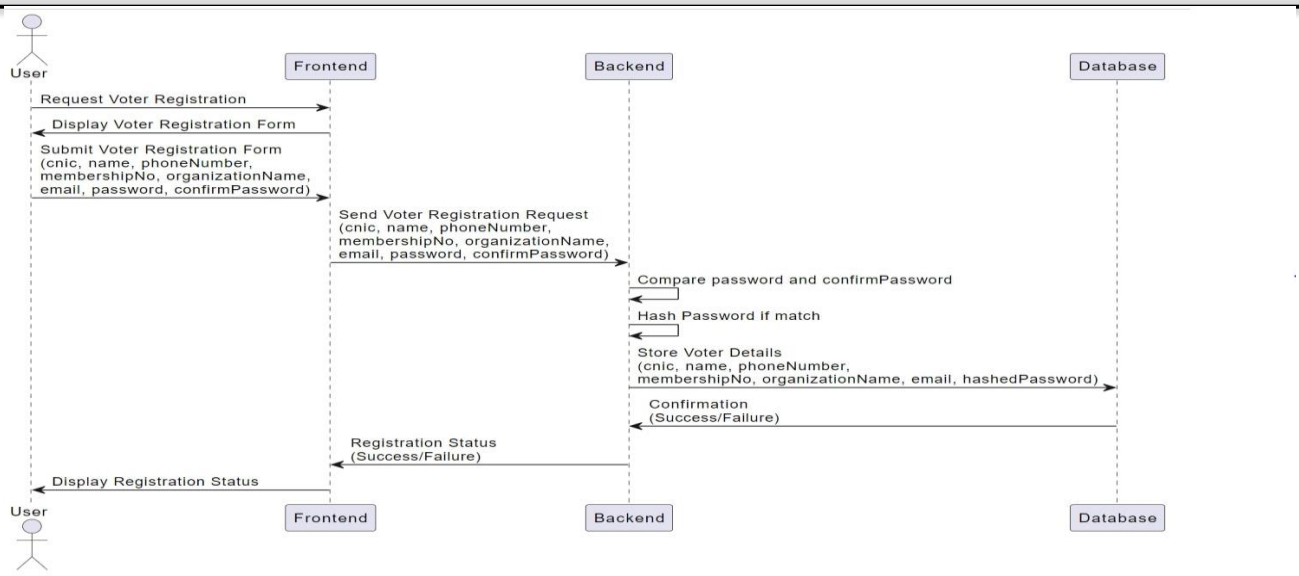

Figure 3: Voter Registration

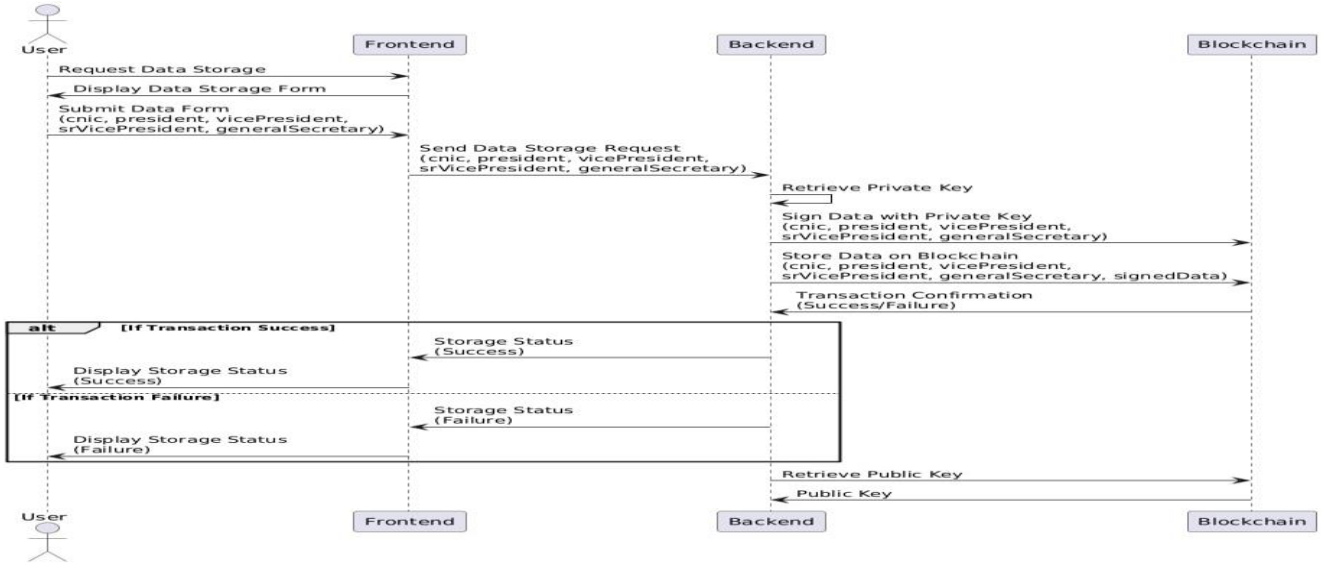

Figure 4: Blockchain Creation and Data Storage

3.1. Result Generation Steps:

Step 1: Retrieve Vote Data

Action: Query the blockchain to retrieve blocks containing vote transactions.

3.2. Pseudo-Equation:

VoteData=RetrieveData(Blockchain)

1. RetrieveData(Blockchain): This function fetches and parses blockchain data.

Step 2: Aggregate Votes

Action: Extract and aggregate votes for each position.

VoteCounts(P)=∑i=1nVotesi(P)

1. VoteCounts(P): Total number of votes for position PPP.
2. Votes_i(P): Number of votes for position PPP in block III.
3. n: Number of blocks or transactions containing votes for the position PPP.

Step 3: Determine Winners

Action: Identify the candidate with the highest votes for each position.

Pseudo-Equation:

Winner(P)=argmaxC(VoteCountsC(P))

1. Winner(P): Candidate with the highest votes for the position PPP.
2. VoteCounts_C(P): Number of votes for candidate CCC in position PPP.
3. argmax_C: Function to determine the candidate CCC with the maximum votes.

Step 4: Generate Results
Action: Compile the aggregated data and results for display.
Results={Position1:Winner(P1),Position2:Winner(P2),...}
1. Results: Aggregated results showing winners for each position.
2. Position_i: Position in the election (e.g., President, Vice President).

3.3. In summary:

Retrieve Vote Data:
VoteData=RetrieveData(Blockchain)

Aggregate Votes:
VoteCounts(P)=∑i=1nVotesi(P)
Determine Winners:
Winner(P)=argmaxC(VoteCountsC(P))
Generate Results:
Results={Position1:Winner(P1),Position2:Winner(P2),...}
These steps ensure that the vote data is accurately aggregated and analyzed to determine the winners for each position in the election:

3.4. Vote Storage In Blockchain Node

Step 1: Voter Sends Encrypted Vote Transaction
Action: The voter (V) sends an encrypted vote transaction to the validator (or a specific program on the Solana network).

Transaction Format:
EKVA(TSi(BlkChni⊕Blki Time))
1. EKV_A: Encrypted vote transaction using the validator's public key.
2. TSi: Vote casting transaction.
3. BlkChni: Current blockchain state.

4. **Block Time:** Timestamp of the vote transaction.

Explanation: The voter creates a vote transaction that includes the current state of the blockchain and the timestamp. This transaction is then encrypted with the validator's public key to ensure it is securely transmitted to the validator.

Step 2: Validator Generates the New Block BLKi
Action: The validator generates a new block BLKi based on the received vote transaction.

Block Generation:
BLKi=(Pi⊕VPi⊕SVPi⊕GSi⊕HPV⊕Fp)
1. Pi_{i}i: Vote for the position of President.
2. VPi_{i}i: Vote for the position of Vice President.
3. SVPi_{i}i: Vote for the position of Senior Vice President.
4. GSi_{i}i: Vote for the position of General Secretary.
5. HPV: Hashed anonymous voter ID.
6. FP: Additional fingerprint or unique identifier (optional).
7. ⊕: Concatenation of information.

Explanation: The validator creates a new block by combining the voter's votes for each position and their hashed ID. This ensures that the ballot is uniquely tied to the voter while keeping their identity anonymous.

Step 3: Validator Appends BLKi to the Blockchain
Action: The validator appends the new block BLKi to the existing blockchain BlkChni.

Blockchain Update:
BlkChni=BlkChni-1⊕BLKi
1. BlkChni-1: Previous state of the blockchain.
2. BLKi: Newly generated block.

Explanation: The validator updates the blockchain by adding the new block to the existing chain. This involves combining the previous blockchain state with the new block, ensuring the blockchain is extended with the latest voting information.

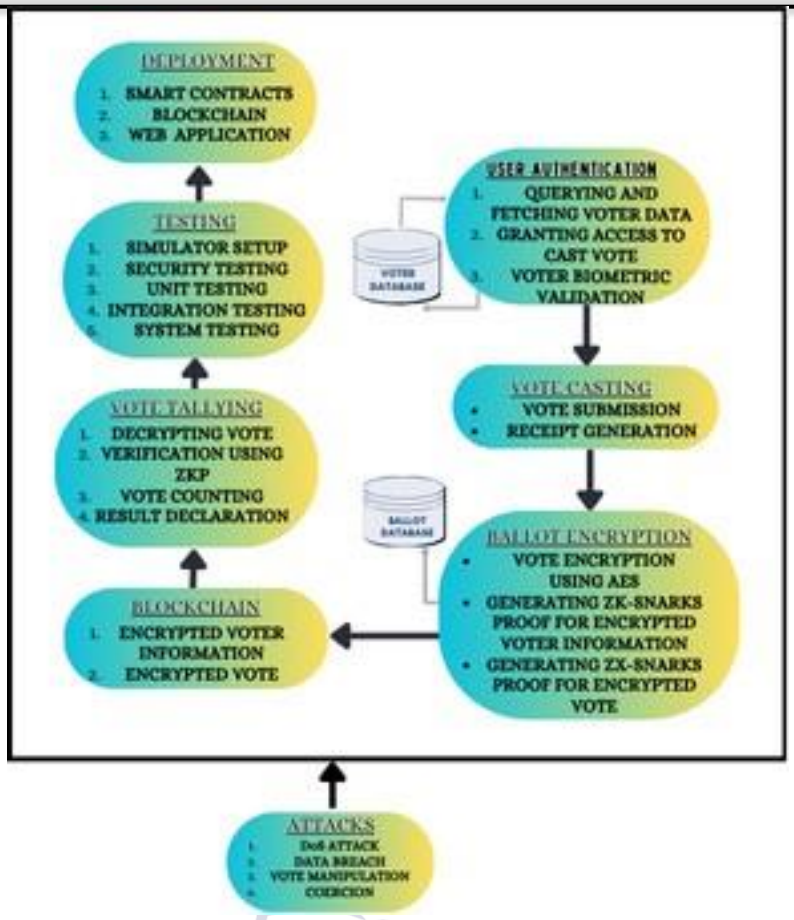

Figure 5: System Architecture

3.5. Security Analysis

3.5.1. DDoS:

A DDoS attack can create a big nuisance in an e-voting system. The servers should be bombarded with massive data streams from multiple sources, rendering the system unreachable for voters. This will have the crucial effect of denying votes to people who otherwise want to register and cast their votes; it may also create doubts about the validity of the elections as they would otherwise be conducted. Remedies against these include load balancers, DDoS protection services, redundancy, and scalability with advanced monitoring and alert systems. Firewalls and HTTPS intrusion detection systems would also act as filters to maximize and pinpoint voting activity without compromise.

3.5.2. Dos:

A barrage of incoming requests from a single source may severely tamper with the voting system and slow down access or make it completely inaccessible to legitimate users who are there to register and vote. It is the result of the attack that would cause enormous numbers of people to be disenfranchised from voting; they would fail to realize the importance of integrity in the electoral process, and might even damage the whole system's reputation. The security of your e-voting system against Denial-of-Service attacks can be achieved by firewalls, making use of Intrusion Detection Systems (IDS), and applying rate-limiting mechanisms for measuring and filtering incoming traffic for fast, smooth, and easy access by genuine users in using the system.

3.5.3. Liveness Attack:

A liveness attack presents considerable threats to the face recognition system that voters use to log in. In such an attack, an assailant tries to outsmart the biometric authentication by using static images, videos, or masks of a legitimate voter's face. With

this capability, the attackers can impersonate voters, cast illicit votes, or obtain vital information concerning voters. Thus, it is imperative for the application to integrate state-of-the-art live detection techniques that can differentiate between a living person and a reproduction, either by observing dynamic movements or through 3D camera techniques. Moreover, multiple-factor authentication may be put in place to provide additional layers of security. Besides, routinely upgrading the face recognition software and raising awareness among users to protect their biometric data are other vital components to secure the system's integrity and instill trust among voters.

3.5.4. Phishing Attack:

Phishing attacks are severe threats that attack users through deception, stealing sensitive information such as CNICs and passwords. These attackers may send fake emails or create fraudulent websites that resemble your official platform. These fraudsters manage to mislead voters into sharing their credentials, enabling unauthorized voting or compromising sensitive voter-specific information. Measures against these phishing attacks should include training users on identifying and avoiding suspicious communications, implementing strong email and website security measures, and using multi-factor authentication as an extra layer to further fortify against attacks. Immediately and regularly monitoring for unusual activities and securing all communication channels may further help safeguard the system and instill voter confidence in the whole election process.

3.5.5. SQL injection:

The critical security loophole through which a person exploits SQL statements with injection, malicious input accessed from forms or URLs. It exposes the database to unauthorized access to sensitive information like voter details or lead records. An example would be malicious SQL input from a login form that can pass through authentication or give unauthorized data. Protecting yourself from SQL injection through parameterized queries and prepared statements ensures purified user inputs. Constantly updated, patched systems, combined with security reviews, further strengthen input and error validation to secure data integrity and confidentiality in your e-voting system.

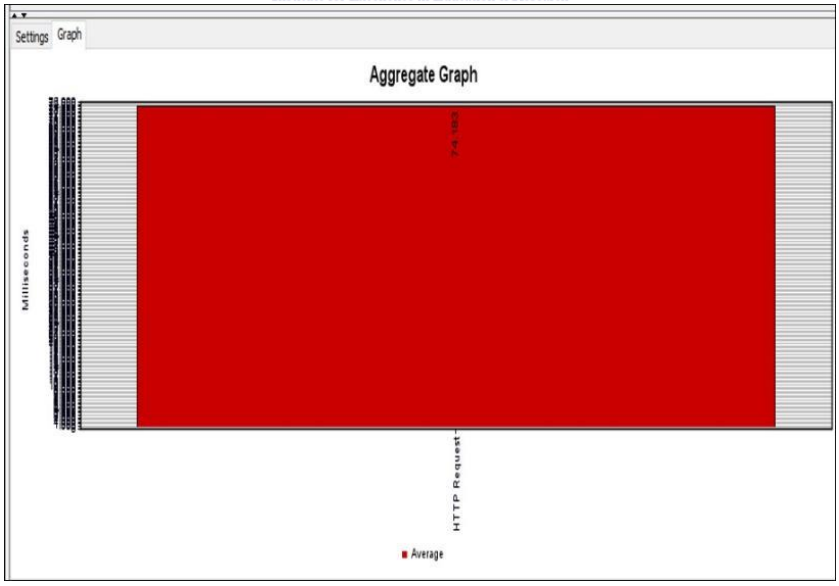

Figure 6: Aggregate Analysis

The overall consideration of HTTP request-response times indicates an average response time of 74,183 milliseconds (approximately 74.18 seconds). This average is established as a measure that allows us to objectively assess the system's performance under some constrained test situation. This data will help

begin the thought process of where response efficiency could be improved. With the establishment of this benchmark, measurable objectives for reducing latency and enhancing user experience can be formulated.

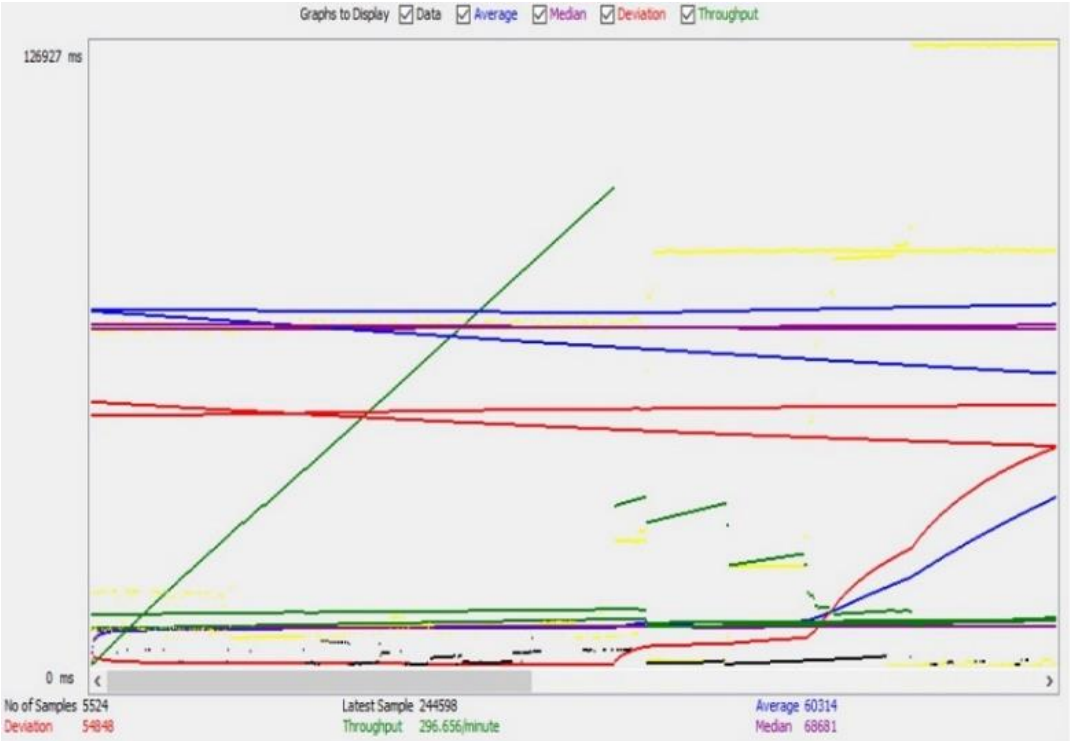

Figure 7: Performance Metrics

The graph depicts the dynamic performance measures over time. It is observed that the data is periodic across low and high activity levels. The average throughput remains high, reaching a maximum of 80,314 samples/min, well in range of the median of 66,831 samples/min, which indicates a positive trend. Notwithstanding the narrow variation (standard deviation = 5,464 samples/min), overall system stability is presumed. Further, the latest sample stood at 244,938 samples/min, signifying the system's capacity to deal with different loads. Therefore, the graph indicates strong performance. Hence, the system is sound and needs more optimization.

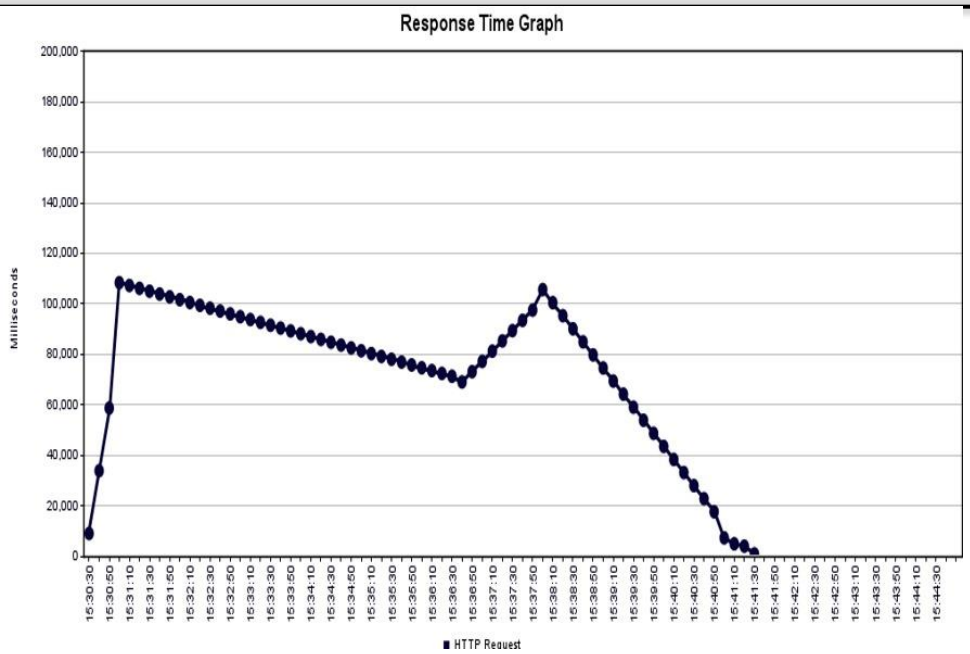

Figure 8: Response Time Graph

The chart shows the performance metrics dynamically over time, with a weight on response time. The points reveal movement of a high and low frequency, thus indicating times when it was more active than others. An important finding is that the response time spikes sharply initially. It significantly peaks at 100,000 milliseconds, only to quickly stabilize, marking the system's adaptive qualities to changing workloads.

Then, the response time increases within a narrower range, from about 20,000 milliseconds to 80,000 milliseconds. This means that the system can ensure relatively uniform performance under variability in workload.

Sample #	Start Time	Thread Name	Label	Sample Time(ms)	Status	Bytes	Sent Bytes	Latency	Connect Time(ms)
5223	15:45:06.233	Users 1-572	HTTP Request	43033		3691	268	176	86
5224	15:45:06.067	Users 1-496	HTTP Request	43201		3691	268	212	129
5225	15:45:06.353	Users 1-546	HTTP Request	42918		3691	268	166	82
5226	15:45:05.969	Users 1-582	HTTP Request	43315		3691	268	219	79
5227	15:45:05.969	Users 1-580	HTTP Request	43324		3691	268	218	79
5228	15:45:06.343	Users 1-391	HTTP Request	42967		3691	268	171	82
5229	15:45:06.352	Users 1-505	HTTP Request	42963		3691	268	164	80
5230	15:45:06.032	Users 1-614	HTTP Request	43346		3691	268	227	144
5231	15:45:06.351	Users 1-533	HTTP Request	43045		3691	268	165	80
5232	15:45:03.012	Users 1-72	HTTP Request	46386		3691	268	162	81
5233	15:45:06.336	Users 1-555	HTTP Request	43120		3691	268	176	88
5234	15:45:05.331	Users 1-447	HTTP Request	44125		3691	268	171	81
5235	15:45:03.026	Users 1-117	HTTP Request	46489		3691	268	159	80
5236	15:45:05.205	Users 1-368	HTTP Request	44313		3691	268	178	80
5237	15:45:03.034	Users 1-135	HTTP Request	46489		3691	268	167	81
5238	15:45:05.112	Users 1-337	HTTP Request	44429		3691	268	165	79
5239	15:45:06.342	Users 1-265	HTTP Request	43216		3691	268	171	83
5240	15:45:03.081	Users 1-215	HTTP Request	46507		3691	268	201	80
5241	15:45:05.136	Users 1-413	HTTP Request	44455		3691	268	160	80
5242	15:45:05.293	Users 1-439	HTTP Request	44308		3691	268	194	92
5243	15:45:06.346	Users 1-248	HTTP Request	43271		3691	268	167	80
5244	15:45:06.333	Users 1-487	HTTP Request	43315		3691	268	179	82
5245	15:45:03.056	Users 1-184	HTTP Request	46702		3691	268	206	81
5246	15:45:03.086	Users 1-204	HTTP Request	46697		3691	268	206	82
5247	15:45:05.331	Users 1-537	HTTP Request	44506		3691	268	170	80
5248	15:45:03.073	Users 1-207	HTTP Request	46770		3691	268	206	80
5249	15:45:05.114	Users 1-396	HTTP Request	44782		3691	268	165	80

Scroll automatically? Child samples? No of Samples 5249 Latest Sample 44782 Average 56415 Deviation 53233

Figure 9: Stress Testing

The graph shows evolving performance metrics over time, especially the response time. Data points reveal a more erratic behavior of being high and low on activity. The average response time is sustained at a high value, achieving a maximum of 47982 milliseconds. This is much higher than the median of 43033 milliseconds, denoting a soft positive drift.

However, some jitter exists over the data, with a standard deviation of 5233 milliseconds, which proves the system's overall steady state. The most recent sample, at 44782 milliseconds, provides further evidence that the system can manage workloads of varying heights.

The overall conclusion from the graph seems to indicate a system that generally stays healthy and can support large thoughts. The recent samples' persistent high average and sporadic spikes denote that the system is robust and can be further optimized.

4. Conclusion:

The scenario is such that fast-paced changes in the digital domain have forced a real need for secure and user-friendly voting systems. The project at hand advances an E-Voting system based on Blockchain technology and strong security. It is a radical change in our voting mechanism. The system can be used for elections held by the government and in societies like KATI, ABAD, FPCCI, and KCCI.

The new E-Voting system addresses problems that existing systems have faced. It is pretty flexible because it can be adapted to change accordingly. The latest technologies, like Blockchain and robust encryption, make online voting much more secure and transparent. This is not only about the technology; this is about changing the way we think about democracy in this fast-paced digital age. So, the argument proves that this new system is not about elections but the sustenance of democratic ideals. It focuses on making voting secure, transparent, and easy for all. This E-Voting system is a prototype of technology enabling us to conduct elections trustworthy and flexibly. It is a further step in making sure democracy is not left behind by the currents of our ever-changing world, hence allowing a fair and inclusive society by making sure everyone gets their due share.

REFERENCES:

1) Taş, Ruhi, and Ömer Özgür Tanrıöver. "A systematic review of challenges and opportunities of blockchain for online voting." Symmetry 12, no. 8 (2020): 1328.
2) Denis González, Camilo, Daniel Frias Mena, Alexi Massó Muñoz, Omar Rojas, and Guillermo Sosa-Gómez. "Electronic voting system using an enterprise blockchain." Applied Sciences 12, no. 2 (2022): 531.
3) Kho, Yun-Xing, Swee-Huay Heng, and Ji-Jian Chin. "A Review of Cryptographic Electronic Voting." Symmetry 14, no. 5 (2022): 858.
4) Panja, Somnath, and Bimal Kumar Roy. "A secure end-to-end verifiable online voting system using zero-knowledge-based blockchain." Cryptology ePrint Archive (2018).
5) Specter, M.A.; Koppel, J.; Weitzner, D. The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in {US}. Federal Elections. In Proceedings of the 29th USENIX Security Symposium (USENIX Security 20), Baltimore, MD, USA, 12–14 August 2020; pp. 1535–1553.
6) Jafar, Uzma, Mohd Juzaiddin Ab Aziz, and Zarina Shukur. "Blockchain for electronic voting system—review and open research challenges." Sensors 21, no. 17 (2021): 5874.
7) Hardwick, Freya Sheer, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis. "E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy." In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1561-1567. IEEE, 2018.

8) Trueb Baltic, "Estonian Electronic ID – Card Application Specification Prerequisites to the Smart Card Differentiation to the previous Version of EstEID Card Application." http://www.id.ee/public/TB-SPEC-EstEID-Chip-App-v3_5-_20140327.pdf
9) Górny, M. (2021). I-voting–opportunities and threats. Conditions for the effective implementation of Internet voting on the example of Switzerland and Estonia. Przegląd Politologiczny, (1), 133-146.
10) BBC News. (2014, June 10). E-voting experiments end in Norway amid security fears. https://www.bbc.com/news/technology-28055678: https://www.bbc.com/news/technology-28055678
11) Halderman, J. A., & Teague, V. (2015). The New South Wales iVote system: Security failures and verification flaws in a live online election. In E-Voting and Identity: 5th International Conference, VoteID 2015, Bern, Switzerland, September 2-4, 2015, Proceedings 5 (pp. 35-53). Springer International Publishing.
12) Swiss Federal Chancellery. (2023). E-voting in Switzerland. Retrieved from https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting.html
13) Jain, N., Upadhyay, P., Arora, P., & Chaurasia, P. (2021). MATDAAN: a secure voting system using blockchain. Int. Res. J. Modern. Eng. Technol. Sci, 3.
14) Kshetri, N., & Voas, J. D. (2003). Voting technology: From punch cards to e-voting. In Encyclopedia of computers and society (pp. 1567-1579). SAGE Publications Ltd.
15) Alomair, W., & Kouakou, A. B. (2020). Blockchain-based voting system: Performance analysis and lessons learned. Sustainability, 12(24), 10057.
16) Singh, Ashish, and Kakali Chatterjee. "Secevs: Secure electronic voting system using blockchain technology." In 2018 International Conference on Computing, Power, and Communication Technologies (GUCON), pp. 863-867. IEEE, 2018.
17) Chaieb, Marwa, Souheib Yousfi, Pascal Lafourcade, and Riadh Robbana. "Verify-your-vote: A verifiable blockchain-based online voting protocol." In Information Systems: 15th European, Mediterranean, and Middle Eastern Conference, EMCIS 2018, Limassol, Cyprus, October 4-5, 2018, Proceedings 15, pp. 16-30. Springer International Publishing, 2019.
18) Liu, Yi, and Qi Wang. "An e-voting protocol based on blockchain." Cryptology ePrint Archive (2017).
19) Zhang, Wenbin, Yuan Yuan, Yanyan Hu, Shaohua Huang, Shengjiao Cao, Anuj Chopra, and Sheng Huang. "A privacy-preserving voting protocol on blockchain." In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 401-408. IEEE, 2018.
20) Wang, Baocheng, Jiawei Sun, Yunhua He, Dandan Pang, and Ningxiao Lu. "Large-scale election based on blockchain." Procedia Computer Science 129 (2018): 234-237.
21) Yi, Haibo. "Securing e-voting based on blockchain in P2P network." EURASIP Journal on Wireless Communications and Networking 2019, no. 1 (2019): 1-9.
22) Khan, Kashif Mehboob, Junaid Arshad, and Muhammad Mubashir Khan. "Secure digital voting system based on blockchain technology." International Journal of Electronic Government Research (IJEGR) 14, no. 1 (2018): 53-62.
23) Hsiao, Jen-Ho, Raylin Tso, Chien-Ming Chen, and Mu-En Wu. "Decentralized E-voting systems based on the blockchain technology." In Advances in Computer Science and Ubiquitous Computing: CSA-CUTE 17, pp. 305-309. Springer Singapore, 2018.
24) Yavuz, Emre, Ali Kaan Koç, Umut Can Çabuk, and Gökhan Dalkılıç. "Towards secure e-voting using Ethereum blockchain." In 2018 6th International Symposium on Digital Forensic and Security (ISDFS), pp. 1-7. IEEE, 2018.

25) https://ethereum.org/en/zero-knowledge-proofs/, “Ethereum.”
26) https://spl.solana.com/confidential-token/deep-dive/zkps , “Solana”
27) https://docs.solana.com/transaction_fees, "Solana".
28) https://btcinformation.org/en/developer-guide#block-chain , “Bitcoin”
29) https://hyperledger-fabric.readthedocs.io/en/release-2.5/whatis.html , “Hyperledger Fabric”
30) Kaufman, Jonathan, and Michael Lapke. "The Effect of Homomorphic Encryption on Voters' Perceptions of Security in Election Systems." (2022).
31) Pereira, Bruno Miguel Batista, José Manuel Torres, Pedro Miguel Sobral, Rui Silva Moreira, Christophe Pinto de Almeida Soares, and Ivo Pereira. "Blockchain-Based Electronic Voting: A Secure and Transparent Solution." Cryptography 7, no. 2 (2023): 27.
32) Kaufman, Jonathan, and Michael Lapke. "The Effect of Homomorphic Encryption on Voters' Perceptions of Security in Election Systems." (2022).
33) Pedin IV, Allan B., and Nazli Siasi. "Secure and Decentralized Anonymous E-Voting Scheme." In Proceedings of the 2023 ACM Southeast Conference, pp. 172-176. 2023.
34) Lee, Dayeol, David Kohlbrenner, Shweta Shinde, Krste Asanović, and Dawn Song. "Keystone: An open framework for architecting trusted execution environments." In Proceedings of the Fifteenth European Conference on Computer Systems, pp. 1-16. 2020.