Research Article

Neural-Based Secured Decentralized E-Voting Framework using Blur Image Broadcasting

Samayamanthula Venkata Chinnaiah Gupta[1,*] and Kodati Satya Prasad[2]

[1]University College of Engineering, JNTUK, Kakinada, AP, India
svcgupta@yahoo.com
[2]Technology and Research University, Guntur, AP, India
prasad_kodati@yahoo.co.in
*Correspondence: svcgupta@yahoo.com

Received: 10th March 2024; Accepted: 28th September 2024; Published: 1st October 2024

Abstract: One of the fundamental rights in the modern democracy is voting. Much research has been done to strengthen the voting process and security. The new and safe Neural-Based Secured Decentralised E-Voting Framework employing Blur Image Broadcasting tackles the major issues with standard electronic voting techniques. Neural networks with blurred image broadcasting protected voter confidentiality, ballot integrity, & system security. Therefore, a novel Zebra-based GoogleNet Elliptic Curve (ZbGEC) is provided to upgrade the decentralized e-voting via blur image broadcasting in this study. It authenticates and broadcasts the voter's information safely to the blockchain technology. It additionally demonstrates time consumption, memory usage, and design cost. Only authorized users can view and alter encrypted and decrypted votes via neural networks. This encryption protects voter anonymity and ballot manipulation. Furthermore, blur image streaming obscures voter ballot selections, improving voter privacy. The decentralized design spreads voting over numerous nodes; removing the centralized Spread structure strengthens the system against manipulation and cyber-attacks. Notably, decentralized e-voting time consumption and response time were minimized to an efficient 2 seconds and 5 seconds. The proposed system's design cost was economical at $30, while memory usage was optimized to 300 MB, representing a significant improvement over traditional methods. Neural-based security, decentralized structures, and blurred image streaming produce a reliable e-voting system. This architecture improves security, privacy, openness, and scalability over electronic voting systems. The Neural-Based Secured Decentralised E-Voting Framework utilizing Blur Image Broadcasting might make voting safer, more transparent, and inclusive.

Keywords: ***Blockchain Security; Blur Image Broadcasting; Decentralized E-Voting Framework; Neural-Based***

1. Introduction

Voting is an intrinsic right afforded to all members of a democratic society, granting them the ability to select the prospective leaders of their nation [1]. The prevalence of online voting is increasing in contemporary society [2]. Its goal is to establish a decentralized electronic voting system [3]. Voter registration is possible from any location with internet access [4]. By verifying the voter's identity, an electronic voting system can thwart fraudulent activities [5]. Engineers have developed novel voting systems [6]. Electronic voting is the most widely recognized method because it represents the election [7]. Several anti-corruption safeguards are provided. Blockchain technology makes electronic or decentralized online voting possible [8]. Electronic voting utilizes tools to assist with or replace recording and tallying votes [9]. Implementing online voting may involve using computerized voting instruments or Internet-connected computers, contingent upon the specific method employed [10]. This analysis aims to examine the current state of technology-based voting on blockchain. It projects potential future developments and

Samayamanthula Venkata Chinnaiah Gupta and Kodati Satya Prasad, "Neural-Based Secured Decentralized E-Voting Framework using Blur Image Broadcasting", *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 77-98, Vol. 8, No. 4, 1st October 2024, Published by International Association for Educators and Researchers (IAER), DOI: 10.33166/AETiC.2024.04.004, Available: http://aetic.theiaer.org/archive/v8/v8n4/p4.html.

online voting patterns [11]. Participants read the output data after its validation through the utilization of a Bulletin Board (BB) [12]. Utilizing the paper and ballet box methodology during and after elections is rife with inconsistencies and manipulations [13]. By reducing an image's precision, its detail is also diminished [14]. Camera shake is one of the most prevalent causes of blurry photographs [15]. Visualizing objects in motion is an additional consequence of impaired eyesight [16]. In digital environment, some images were blurry due to a sluggish Internet connection [17]. Internet connectivity is, therefore, essential for electronic polling [18].

Prolonged queues and extensive paperwork constituted significant challenges associated with prior voting protocols in electoral settings [19]. It is possible to vote whenever and wherever one chooses; however, electronic voting technologies have been developed to accommodate those who work in locations where physical polling is impractical for all [20]. Blockchain is ideal for providing organizations with information due to its speed, security, and precision [21]. The exchange of data is vital in voting applications [22]. Blockchain-based electronic voting can only function when a single entity entirely administers the online voting system. The core concept entails integrating encryption and a secret sharing system with blockchain technology to establish a decentralized electronic voting system [23] that is not dependent on a trusted third party. Smart contracts and the blockchain system both incorporate decentralization [24]. By employing dual blockchain methodologies, a decentralized electronic voting system was established [25]. Homomorphic encryption and systems for secret sharing are both available [26]. It is more advantageous to implement an electronic voting system that integrates fingerprint hash algorithms with market network algorithms [27]. The implementation of blockchain technology holds the capacity to significantly streamline the electoral process. At this time, it is deemed unsuitable for individuals to vacate their residences to cast their ballots [28]. In the context of an electronic voting system built on blockchain technology, several smart contracts are essential to ensure the voting process's integrity, security, and transparency. The token contract is responsible for generating and handling tokens that explain the voting rights. The eligible voters get specific tokens to cast their votes. The contract monitors that only one voter uses the token and cannot be given to other voters. It ensures that each voter has the right to vote and their vote counts. One of the key contracts in the e-voting system is the election contract. It allocates the start and end times to cast the votes. This election contract combines with the token contract to check the eligibility of the voters and record the voting results. The vote contract is mainly created to handle the voting process. It manages the privacy of the voter’s information by encrypting it using cryptographic algorithms and decrypting it during the vote-counting session. It ensures the voter's privacy and vote’s integrity. In Proof of Authority (PoA), the consensus mechanism is based on the validator’s reputation. The contract manages the validator’s privacy, and their rights are validated. Also, it makes sure that the authorized validators have participated in the validation process.

Efforts are underway to develop online voting systems that can securely conduct elections and votes, intending to safeguard the voting system against assaults resulting from voters filling ballots improperly [29]. They prevent the necessity of being physically present to cast each ballot as they operate on a digital platform. By simplifying the voting process for citizens, Aadhaar, India's unique identification system, has enabled a significant number of residents to participate in the Digital India initiative, including electronic voting systems [30]. The elimination of paper ballots is one of the advantages of online voting tools [31]. This eliminates expenses, conserves time, and decreases the likelihood of vote-counting errors. Electronic voting systems have been implemented in India for an extended period, facilitating the voting process by simplifying vote counting and reducing manual intervention. Electronic voting has mitigated certain limitations linked to conventional franchises, including inadequate anonymity and inefficiency. Voting is the process by which the opinions of the public are incorporated to improve the organization's administration.

The key contribution of the proposed work is summarized as follows,

- Initially, the blur image broadcasting paradigm is designed for the secret sharing system.
- Consequently, a novel Zebra-based GoogleNet Elliptic Curve (ZbGEC) Blockchain is built and executed to offer privacy parameters.
- Next, preprocessing is done, where the unwanted noises are removed, and then image broadcasting is performed.

- In addition, the voting system is worked based on an acknowledgment strategy, and if the user has received the voter identity, then the voting framework is logged in. Otherwise, the process is blocked.
- This proof is a secure way to validate the authenticity of the voting process.
- Lastly, performance analysis is done regarding time consumption, response time, design cost, and memory usage.

The second half of the research paper summarizes the available literature on the topic by introducing and discussing relevant studies. In the third half of the study, traditional techniques' limitations are examined. Section Four elaborates on the proposed solution to the concerns as mentioned above. The fifth section then covers the validation technique used to determine the effectiveness of the one-of-a-kind solution. The sixth and last sections of the study paper offer a summary of the main findings and insights.

2. Related Works

Some of the most recent works that are relevant to decentralised electronic voting are as follows:

Inadequate voting procedures constitute a significant factor contributing to incidents of electoral violence. To tackle this concern, Chaubey and associates [27] introduced a blockchain-based decentralized voting system that represents the future of electronic voting. Blockchain-based voting systems are proposed as a superior alternative to current electronic voting systems by this method, as they effectively tackle the fundamental challenges associated with the former. Electronic voting has been suggested as a remedy for several of the paper and ballot system's most significant flaws, including the need for many individuals to count votes. Nevertheless, beyond these apprehensions, electronic voting systems present substantial security vulnerabilities that may give rise to additional complications like interference with votes or exposure of voter identities. Electronic voting solutions currently in use encounter challenges about impartiality and regulatory oversight. Lu *et al.* [28] devised a self-evaluation electronic voting system that incorporated public traceability via blockchain technology to tackle this concern. This approach optimizes the administration of justice while maintaining an equilibrium between confidentiality and responsibility. Although a self-assessment electronic voting system satisfies our growing needs, it is afflicted with adaptability and redundancy concerns and cannot guarantee impartiality. Here, both articles highlighted the mechanism of the blockchain model to enhance the privacy, reliability, and transparency of the electronic voting system. It explores the structural aspects of blockchain in voting systems, focusing on tiered frameworks and decentralized authentication mechanisms, respectively. However, research is needed to enhance the adaptability and scalability of blockchain-based voting systems to ensure they can handle varying election sizes and conditions.

Vladuku *et al.* [29] are cited. Globally, the prevalence of electronic voting technologies in elections for public office is increasing. This progression can be attributed to these systems' advantages, including the ability to vote remotely and expeditiously. Moreover, this research investigates the challenges blockchain electronic voting systems face and pinpoints areas that warrant skepticism in future studies. Oprea and his associates [30], by utilizing blockchain tables and novel interactions between participants and two software components, aims to develop a conceptual framework with two tiers—voting and verification, layers, and role separation. As a proof of concept, the initial steps required to implement the proposed solution are also visualized. An unintended consequence of this system is the reliance on human enumeration, which may result in fraudulent activities or by-products. These models marked the advantages of decentralization in e-voting systems, such as improved remote voting capabilities and transparency through distributed networks, but they lack adaptability and scalability concerns.

Talla-Zumbitas *et al.* [31] are the authors. The blur image transmission technology achieves an average inaccuracy of less than half and increases transmission power by more than 10%. By employing blurring techniques, one can examine the transfer of minuscule data into additional images. The 94 percent accuracy reported in this article demonstrates the immense potential of this novel technique. This approach possesses a drawback. Securing image clarity becomes a more arduous task. Exploring hybrid models that combine blur image transmission with other security measures could address the clarity issues and improve overall security.

Syada *et al*. [38] created blockchain technology to ensure the voting system's anonymity, integrity, mobility, security, and fairness. The hashing of voter information in the blockchain improved the anonymity, and also, at the final stage, the voters can verify their votes to improve their verifiability. In addition, the introduction of smart contracts protects information from third parties. The model improved the security measures. However, the model didn't store the data due to the cost expenses, so it cannot be used at the election final counting.

Ramayadevi and Priya [39] modeled a three-tiered OTP mechanism for voting system security. The model gives an alert OTP to notify the threats and an authentic OTP to cast a vote. The model safeguards the voting system against authorization and coercion. However, it has a limited viability in terms of time. Also, voters in areas with poor connectivity might face difficulties.

Hossain *et al*. [40] proposed an internet-based blockchain voting paradigm to avoid manipulating the voting results. The model utilized biometric authentication, such as face and fingerprint recognition, to ensure security. The results show that out of 100, 87% of the participants registered their voting section with their biometrics identity. It is a decentralized and distributed data network that maintains transparency. The model lacks encrypted storage protocols.

Beula *et al*. [41] suggested the cloud-based online voting model to address the flaws seen in the conventional voting system. The model diffused three phases: registration, vote casting, and vote counting. A timestamp-based authentication process is adopted to validate the voters during the registration and vote-casting phase. The smart contract allocation avoids the third-party disturbance. The latency, response time, and vote alterations are reduced.

In the reviewed literature, various blockchain technologies-based voting systems found innovative solutions to address the security issues in the electronic voting system. However, they show shortcomings, such as data preservation cost, adaptability, reliability, prediction error, delay and third-party access. The presented research created a new model to address these issues by combining advanced machine learning, cryptographic techniques, and blockchain technology. The model utilizes ECC to provide strong cryptographic security while maintaining efficiency. ECC ensures that votes are encrypted and decrypted securely. GoogleNet, a convolutional neural network (CNN), improves the adaptability of the voting system by effectively handling large datasets and complex patterns using the zebra fitness process. This enables the system to scale efficiently with increasing numbers of voters and voting transactions. The blockchain structure in the researched model distributes the voting process across multiple nodes. This reduces the load on any single point and increases the efficiency and speed of vote processing. Processing in separate layers for voting and verification, supported by GoogleNet’s robust feature extraction capabilities, enhances the system's reliability.

3. System Model and Problem Statement

Implementing blockchain technology to secure large datasets is a slightly more intricate process. Hence, obscured data can efficiently alleviate potential security weaknesses when transmitting data among users.

The present research paper introduces the blur image secret method, considering these benefits. Furthermore, the main objective of this undertaking is to create a robust electronic voting system. A clandestine image exchange system was built to enhance the electronic voting technique's confidentiality. Furthermore, a cutting-edge blockchain method is utilized to protect the vote data.

Figure 1 illustrates the difficulties encountered by the conventional voting system. The decentralized system faces challenges, particularly in handling large databases, leading to issues. Furthermore, security processes are complex. To overcome these challenges, a proposed method is presented, the Zebra-based GoogleNet Elliptic Curve (ZbGEC) technique.

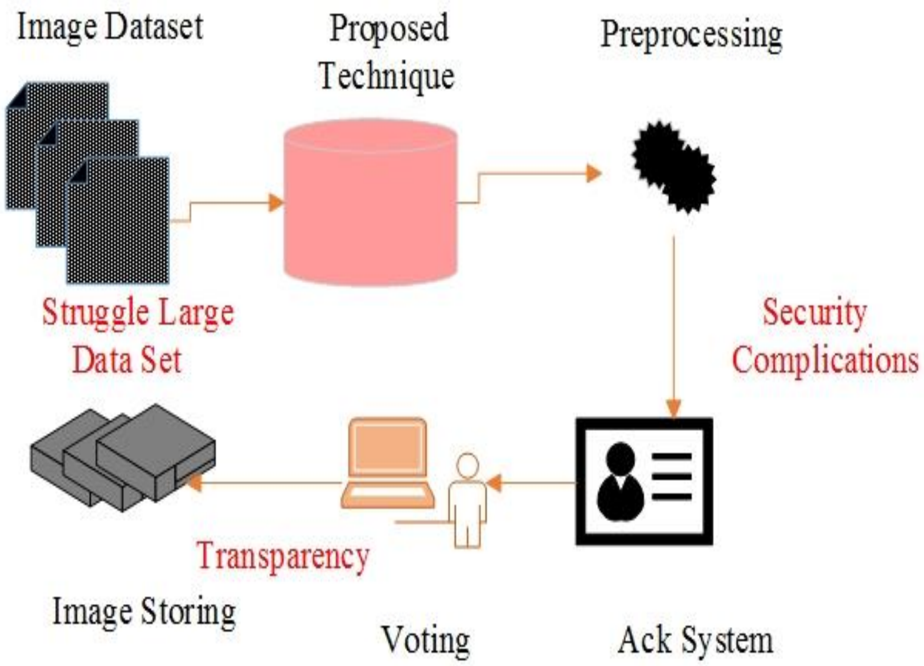


Figure 1. Difficulties of the Standard Voting System

4. Proposed Methodology

An initial evaluation of obscured image data is conducted to determine the robustness. Consequently, a novel multi-secret sharing framework was constructed using a zebra-based GoogleNet Elliptic Curve (ZbGEC). The distorted images were subsequently employed to train the noise elimination function, which was carried out in the preprocessing frame. After the acknowledge process has been completed and the voting system has been duly acknowledged, the voting details are once more concealed using the Elliptical curve cryptography before being transferred to the blockchain memory. The final performance assessment evaluates memory utilization, design cost, response time, and time consumption.

Figure 2 presents a diagrammatic representation of the structure of the proposed methodology. This study aims to develop a decentralized voting system by leveraging a dataset of images. The performance improvement observed when conducting image analyses across multiple databases is substantiated by comparative studies.

The suggested model integrated the concepts of googlenet, zebra optimization, and Elliptic curve cryptographic algorithm to provide security to the voting system. Here, the input voter image is processed using the GoogleNet function of the presented ZbGEC model. Googlenet is the deep learning architecture that gives higher training results and mitigates load issues such as overfitting, gradient explosion, and disappearance. The model improves the training results by extracting efficient features for the prediction process. The layers in the GoogleNet architecture include the convolutional layer, inception module, pooling, and fully connected layer. The layers are created with multiple filter sizes, such as 1x1, 3x3, and 5x5, for preprocessing, feature extraction, and prediction. However, hyperparameter tuning is the foremost step in utilizing the full advantage of GoogleNet. Manual tuning is time-consuming and not assured to get the higher results. Therefore, the network introduced the zebra optimization process in it. It developed the finely tuned model to get enhanced training and prediction accuracy. Here, the model is trained to predict the blurred image of the input voter images for authentication and the voting process. After the blur image prediction, the model initializes the authentication process to verify the voter based on the input image, ID, and password. If the user is authenticated, the voting option will be available for the voters to vote for the respective candidate. Subsequently, the voters and their voting information are encrypted and broadcast to the blockchain for future access. The information is encrypted using the Elliptical curve cryptography algorithm. It generates public and private keys to encrypt the data and sign it for future authentication. It ensures confidentiality and integrity; only authorized users can decrypt and verify votes.

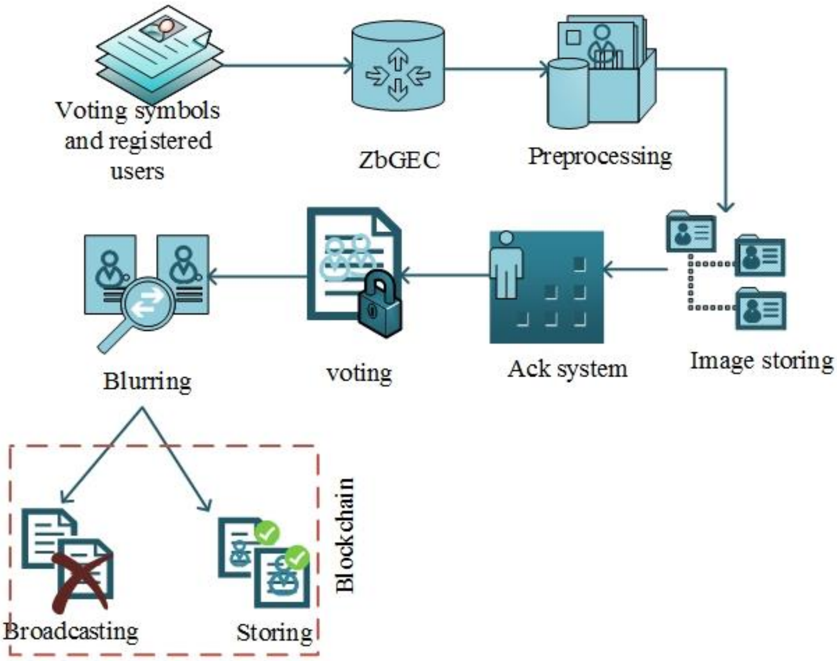


Figure 2. Proposed Methodology

4.1. Process of the proposed methodology

The proposed approach comprises the input, convolutional, max pooling, fully connected, and output layers. Another option is to use the GoogleNet Elliptic Curve based on zebras to carry out the operation. A neural network includes it. The ZbGEC convolutional layer filters in this case.

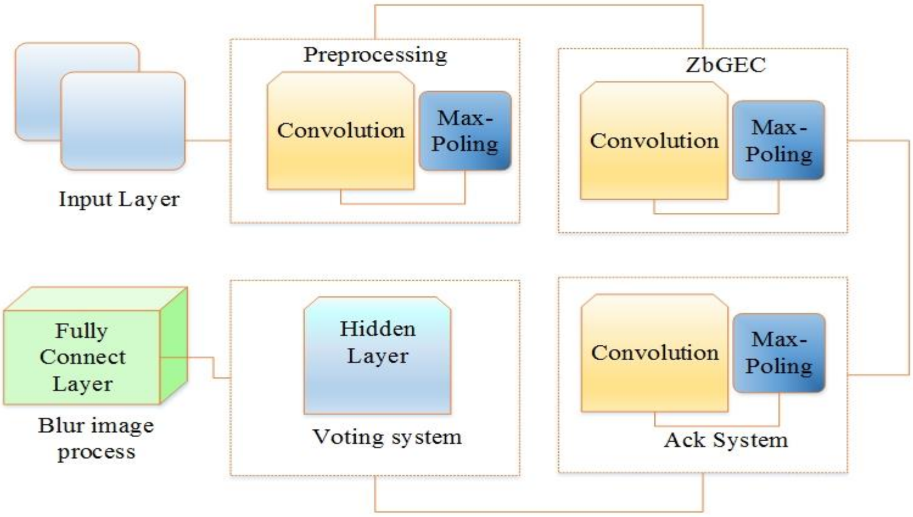


Figure 3. The processing layer of the proposed model

Figure 3 shows the Zebra-based GoogleNet Elliptic Curve voting mechanism. Voting systems aim to improve accuracy. The voting process requires every network node to vote on the input image's predicted class. The ultimate predicted class is the node with the most ballots. The ZbGEC algorithm derives characteristics from the input image, consistent across all voting system nodes.

4.1.1. Commence data initialization and preprocessing

In the beginning stage, the image data was gathered and imported. The Eqn. (1) can describe the data training function.

$$S = s_1 + s_2 + .. s_n \quad (1)$$

Where S is denote the image dataset and $s_1 + s_2 + .. s_n$ are the initialize of the entire data's. Preprocess the collected data by cleaning, normalizing, and transforming it into suitable input formats for training the convolution neural network. This may involve feature extraction, data augmentation, or encoding techniques specific to ZbGEC. During the preprocessing stage of the blur picture broadcasting paradigm, any undesirable noise in the blurred image is eliminated. Because of this, the rebuilt image is guaranteed to be clean and devoid of noise.

$$P(x,y) = \frac{1}{N}\sum_{i,j}^{n} B'\,(x,y) \tag{2}$$

Where N denotes the Normalization factor. $B'(x,y)$ is the blurred image and $P(x,y)$ is an image that has been preprocessed. i and j are the ith and jth iteration of the data. The normalization factor is utilized to guarantee that the preprocessed picture has the same intensity range as the original image.

4.1.2. Proof of Authenticity

The voting system could use a password verification method to verify that the user owns the matching identity. Along with that registered user in the database, all the details like voter, id, and password were saved. During the testing process if the given password in the GUI is matched with the registered account then the voting symbols were displayed.

$$Login = V(I, id, Password) \tag{3}$$

Where V represent the verification. I described the identification of the uploaded image. The information included in the user's identification, and the voting system receives answer. To compare the image with our preprocessed images. It obtains the image corresponding to the voter identification and is connected to it.

$$R_S = \begin{cases} if\ Authenticate & Granted \\ \quad else & Blocked \end{cases} \tag{4}$$

Access to the voting process is allowed to the user if the verification is successful (Verification=Authenticate). This occurs when the voting system recognizes the user's identity. It is possible that the user's identity cannot be validated if the verification is unsuccessful (Verification=Unauthenticated). In this case, access is denied.

Upon casting the vote, the system created the cryptographic token. In the presented architecture, the elliptical curve function generates the token, which provides the encrypted information of the vote and the voter's details. The created token is sent to the voters to acknowledge casting the vote. The record of this is stored in the ledgers for traceability and immutability. Further, the tokens are validated to confirm they match the vote details. The consensus mechanism included the token generation to ensure only valid tokens is acknowledged. When it comes to voting systems, the acknowledgment procedure frequently entails using cryptographic methods to guarantee the safety and genuineness of the user's identification. Voter identification is a crucial aspect of any voting system, ensuring the integrity and security of the electoral process. It serves as a mechanism to verify the identity of voters and prevent unauthorized voting attempts. A voter identification, which may be a password or a one-of-a-kind identifier, is presented by a user whenever they seek to cast a vote.

$$V_S = ACK(Option_{(1-n)}) \tag{5}$$

Where V_S represent the voting system. $(1-n)$ described the voter information.

4.1.3. Storing the vote results in blur format

One further layer of secrecy may be added to each secret share by employing a method known as blur image broadcasting. One way to do this is to utilize an algorithm for picture blurring or other image processing techniques. The blur effect might be represented mathematically shown as Eqn. (6),

$$B'(x,y) = \sum_{i=1}^{n}\sum_{j=1}^{n} w(i,j) \times B(x+i, y+j) \tag{6}$$

Where $B'(x,y)$ is the blurred image, $B(x,y)$ is the original image, and $w(i,j)$ represents the weights of the filter kernel at position. The blurred voting information is stored in the image storing block present in the blockchain technology. This block likely stores the voted information in cipher format, encrypted using the designed ZbGEC model. The blockchain involves multiple users for different transactions without a third party. The third party's access is denied through verification and validation of the transactions done by the special blocks called miners. The presented model utilized the hyper ledger fabric blockchain technology. The permissioned blockchain model provides strong support for data storing and is known for scalability, flexibility, and confidentiality, which are essential for the secure e-voting system. The hyper ledger handles the voting information. Each transaction in the blockchain is processed depending on the previous transactions.

Algorithm 1. ZbGEC

```
Start
{
                                    $\boldsymbol{int\ F_x = \{1, 2, 3, \ldots\ldots n\}}$
//Initialize the image dataset
Preprocessing
{
$int\ N, P(x, y), B'(i, j);$
//initialize the preprocessing variables
                                    $P(x, y) = \frac{1}{N}\sum_{i,j}^{n} B'(x, y)$
//Eliminating the noise features and storing the data
}
Proof for Authenticity
{
$int\ V, I, Password;$
//initialize the Authenticity variables
        $Login = V(I, id, Password)$
        // Retrieves the corresponding public key
        {
                                    $if\ (Authenticate)$
            {
            Access Granted
            }
            $else(Unauthenticate);$
            {
            Access Denied
          //Verify the identity
            }
        }
        Voting System
        {
            $int\ V_S, (n-1);$
            //initialize the voting variables
            $V_S = ACK(Option_{(1-n)})$
          //Select the voting
        }
        Storing Voted outcome in blur format
        {
        $int\ w, x, y, i, j;$
        //initialize the blurring constraints
        $B'(x, y) = \sum_{i=1}^{n}\sum_{j=1}^{n} w(i, j) \times B(x + i, y + j)$
      //image Broadcasting using weights of the filter kernel and then storing the blur image
        }
}
Stop
```

The chain of the blocks is created by the previous block's hash created using the SHA-256 algorithm. The attacker wants to modify all the chain hash codes to modify the stored data, which is difficult to carry out. Thus, the blockchain became a tampered proof. Miners try to mine the blocks on their own with the transaction list. The data are broadcasted for verification after the miner mines the block. The block with the highest consensus among the numerous blocks in the network will be approved for inclusion. The network later discards the other blocks since they are deemed orphan blocks. Orphan blocks may contain transactions that have not yet been considered, but they also contain some transactions that have already been added to the valid block. A fork is any chain that is not the legitimate one. An unmined block may occasionally be linked to the orphan chain, preventing it from joining the longest chain. These linked blocks create a fork. In any blockchain system, the Genesis Block is also called Block 0. All subsequent blocks in the chain will follow this ancestor. Provenance refers to the ability to track the history and origin of a vote. ZbGEC might leverage blockchain's inherent immutability to ensure a verifiable voting history. By chaining together encrypted votes, tampering with a vote without detection becomes impossible.

A collection of pictures is partitioned. Algorithm 1 demonstrated the sequential procedure of the methodology. Execute the Python code and verify the data following the instructions. Algebraic function parameters were used as method parameters. Members receive shares through a clandestine pooling mechanism. It is common practice to require a certain minimum number of shares to restore the original secret.

Figure 4 illustrates the recommended procedure. Following the procedures depicted in the illustration, the suggested Zero-Based Genetic Engineering Control (ZbGEC) was rigorously validated utilizing a battery of criteria. By meticulously following the steps outlined in Figure 4, a thorough assessment of the ZbGEC approach may be carried out. Due to the wide variety of characteristics included in the evaluation technique, a comprehensive picture of the performance and effectiveness of the proposed strategy was produced.

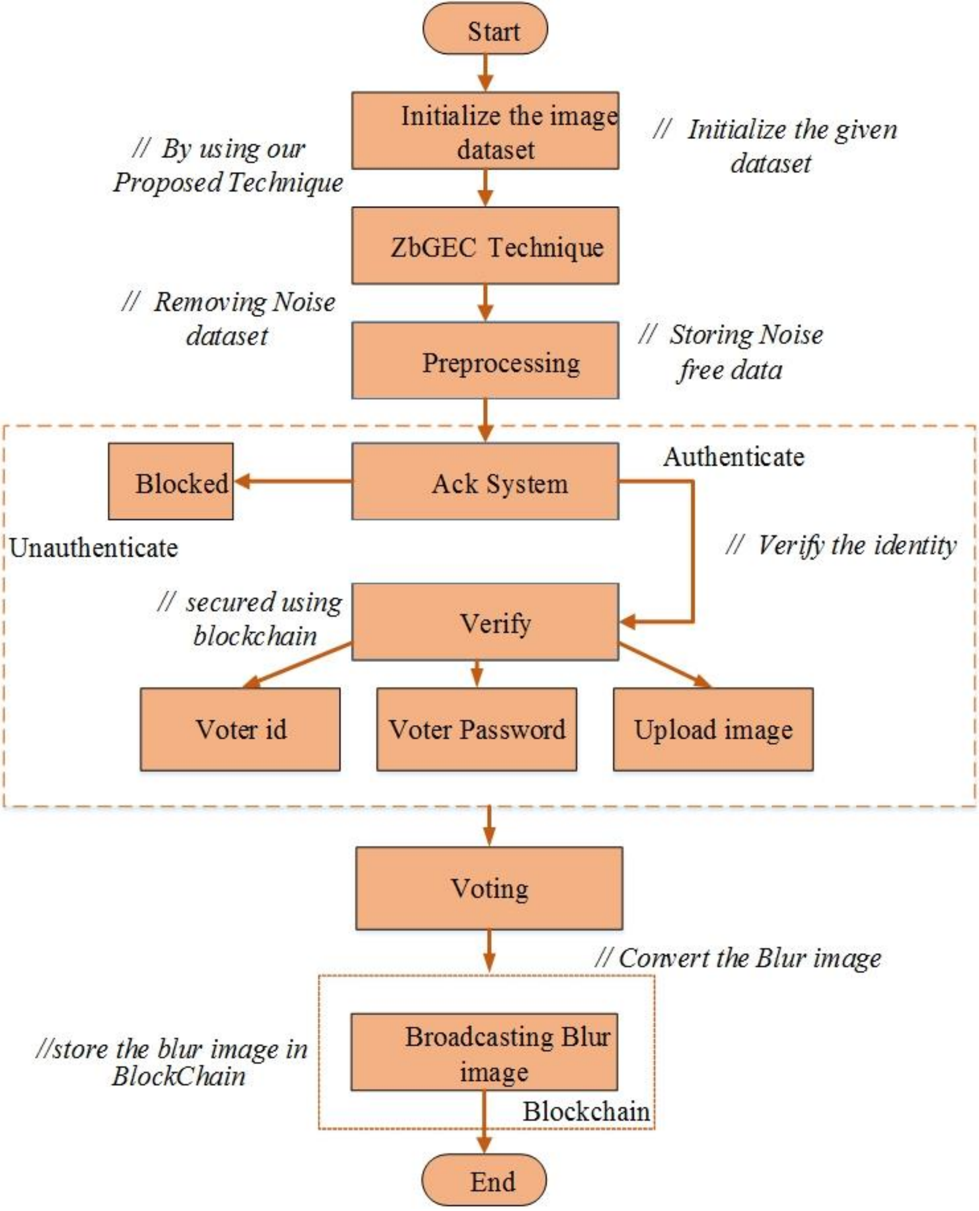

Start
Initialize the image dataset
// Initialize the given dataset
// By using our Proposed Technique
ZbGEC Technique
// Removing Noise dataset
Preprocessing
// Storing Noise free data
Blocked
Ack System
Authenticate
Unauthenticate
// Verify the identity
// secured using blockchain
Verify
Voter id
Voter Password
Upload image
Voting
// Convert the Blur image
//store the blur image in BlockChain
Broadcasting Blur image
Blockchain
End

Figure 4. Flow diagram of the proposed methodology

5. Result and Discussion

This section, like the laboratory setting, discusses the efficiency of the supplied technique. A variety of metrics are utilized to assess the system's efficacy. These measures are reaction time, memory, cost, and time consumption. These metrics are utilized with the aid of neural networks and cryptography.

5.1. Experimental setup

The new idea, The ZbGEC, is built on a mathematical platform limited to Python. It has an Intel(R) Core(TM) i5-3570 processor that runs at 3.40GHz and 8GB of random access memory. Table 1 will illustrate the specifications of the parameters. To validate the ZbGEC for decentralized e-voting via blurred image broadcasting on hyper-ledger fabric, factors such as voting schemes, counting methods, and other relevant details must be defined. The factors include schemes like Anti-quantum, Open Vote Network (OVN), Date, Ballot Encryption Scheme (BES), Blind Voter Authentication (BVA), and the counting method. The anti-quantum cryptographic process prevents attacks from quantum machines. Integrating lattice-based cryptography and an Elliptical curve preserved voter data and ballots against intrusions. The OVN is a decentralized e-voting protocol that ensures transparency and verifiability. The date has to be set for the time-based voting scheme, where votes can be cast only within a specified timeframe. The time-based access control is implemented in Hyper ledger Fabric, allowing votes only within the designated voting period. BES ensures voter privacy and integrity by encrypting the ballots. The elliptical curve process encrypts the votes before being broadcasted as blur images, ensuring that only authorized nodes can decrypt and count them. BVA allows voters to cast their votes without revealing their identities. Blind signatures and zero-knowledge proofs are introduced within hyper ledger Fabric to authenticate voters without disclosing their identities. The cast votes are counted using the third-party tallying method to announce the results.

Table 1. Execution parameters specification

Description of parameters	
Programming Environment	Python
Operating system	Windows 10
RAM	8GB
Processor	Intel(R) Core(TM) i5-3570
Tool	Hyper ledger Avalon
Optimization	Zebra based optimization

5.2. Implementation of ZbGEC

In the present research, the proposed scheme is trained with the voter's normal face images and blurs images collected from the face blurring image dataset available on the GitHub websites (https://github.com/baselhusam/Face-Blurring). The collected dataset contains 324 voter images with voter ID and password features, split into 80:20 ratios for training and testing. The dataset features are described in Table 2. Here the voter details are collected from Indian General Election data downloaded from Kaggle source. The utilized GoogleNet component in the designed ZbGEC predicted the blurred image of the voters for verification before voting. After uploading the input face images and entering login details, the vote casting was opened in the following step.

Table 2. Dataset features

Features	**Description**	**Data Type**
voter_id	Unique identifier for each voter	String
name	Voter's full name	String
age	Voter's age	Integer
gender	Voter's gender	String
address	Voter's residential address	String
registration_date	Date when the voter registered	Date
voting_status	Indicates if the voter has voted	Boolean
ballot_choice	Voter's selected choice in the election	String
timestamp	Timestamp of when the vote was cast	Timestamp
block_hash	Hash of the block containing the vote	String
transaction_id	Unique identifier for the voting transaction	String
node_id	Identifier for the blockchain node processing the vote	String

For the suggested method to work, a detailed, step-by-step implementation plan must be created that starts with a full study of current systems. After this, the suggested changes are put into action in a way that makes sure they fit in smoothly and cause as little trouble as possible. Continuous review and monitoring are important parts that allow changes and improvements to be made in real-time.

The login form will be shown in Figure 5. People who want to vote can safely access their accounts through the login page. Verification is done by the required fields of person ID and Password, which ensure the person is who they say they are. An uploaded picture is also used to further verify and authenticate the voter.

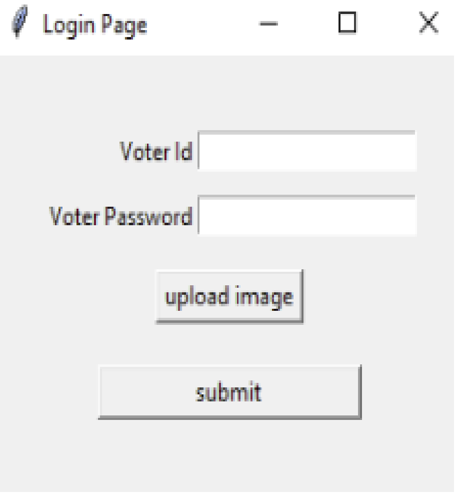
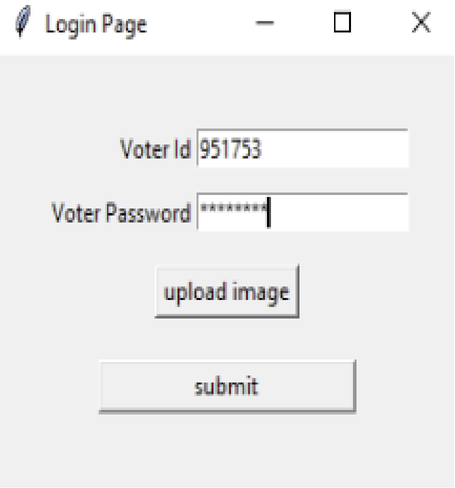


Figure 5. Login

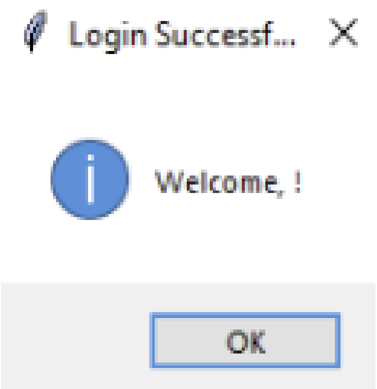


Voter Id 951753

Voter Password ********

Figure 6. Verification

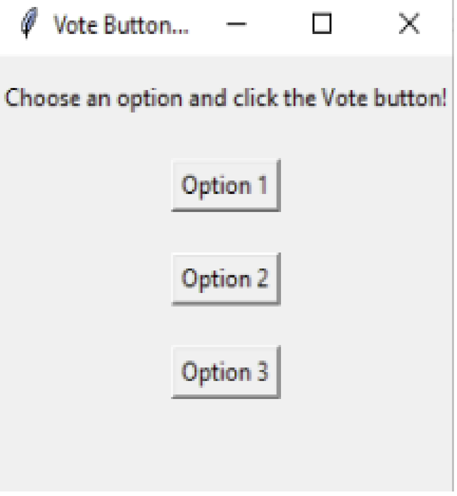
Figure 6 shows how the testing process works. Users must confirm their name on the verification page before moving on to the next step of the voting process. If the name given doesn't match what the system knows about the user, they won't be able to move on to the next voting steps, and the client will still not be authenticated.



Welcome, !

Figure 7. Successful notification

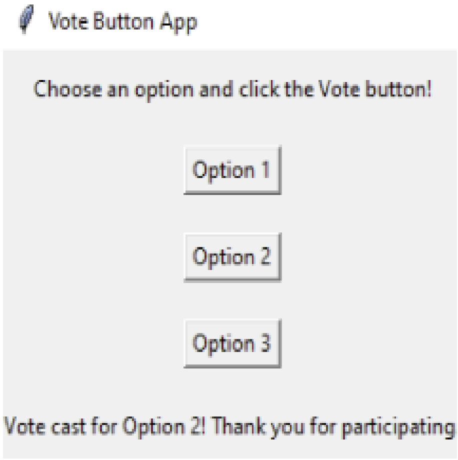
Figure 7 makes use of the notice that is being verified. A popup message should display when the client details have been verified. This message should indicate that the verification procedure has been completed.



Choose an option and click the Vote button!

Figure 8. Voting Process

The procedure for voting is depicted in Figure 8. A voting process will occur in the subsequent phase, during which participants will select their preferred alternative from a list of available voting possibilities. These choices include information about the voter.



Choose an option and click the Vote button!

Vote cast for Option 2! Thank you for participating

Figure 9. Complete the process

Once you have clicked on the option that you have selected, a notification will immediately display to confirm that you have successfully selected it. Your selection has been successfully recorded or processed, and this notification acknowledges that fact, as shown in Figure 9.

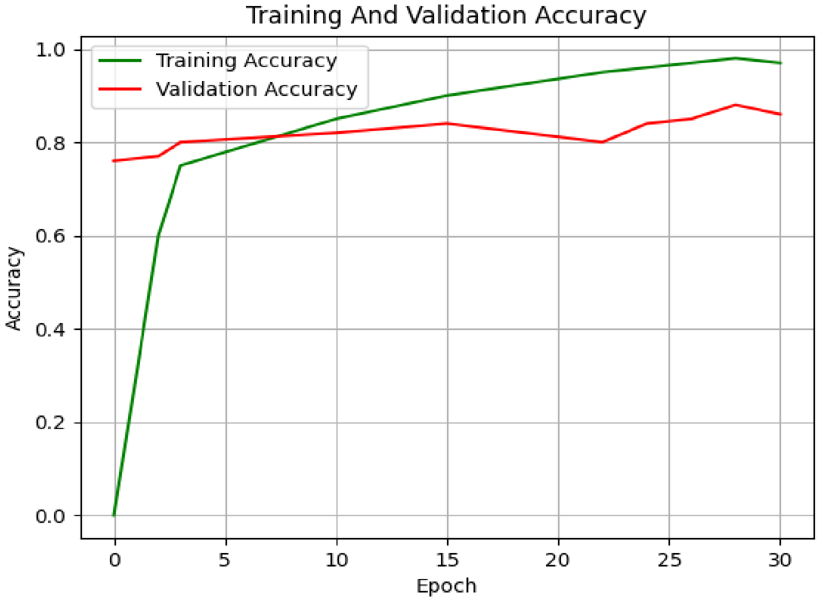


Figure 10. Training and validation Accuracy

Figure 10 depicts the accuracy of both the training and validation processes. E-voting systems use many different security measures to ensure they are very accurate. When these steps are taken, they help make sure that the verification process only looks at votes that have been approved and are real. This lowers the chance of fake or illegal voting.

5.3. Performance Metrics

This part goes into great detail about both the trial setting and the usefulness of the suggested method. Some factors, such as time used, reaction time, design cost, and memory use, are considered to improve to make the computer voting better.

5.3.1. Time consumption

The time that an electronic voting system needs to complete the voting process, from starting the voting session to recording the vote and storing or validating it afterward, is called the system's time consumption.

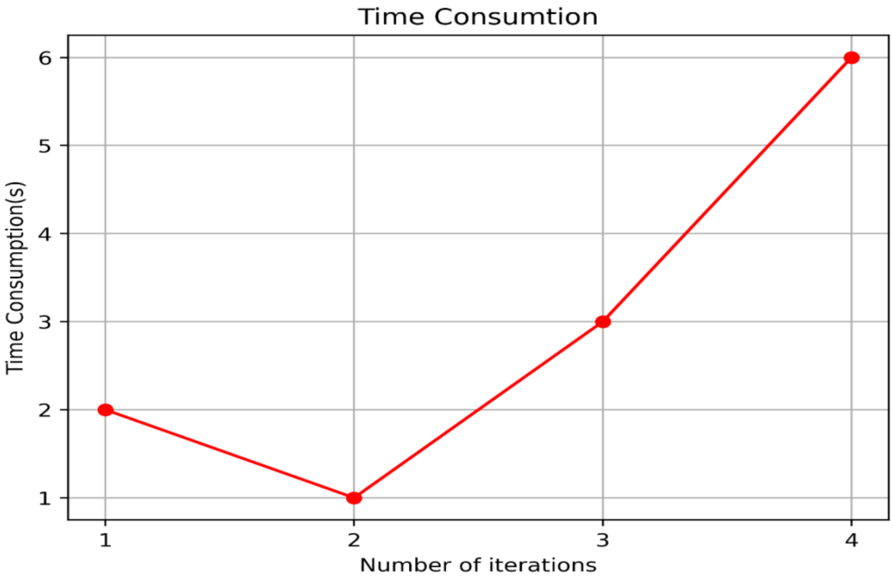


Figure 11. Time consumption of the proposed method

Our proposed method takes 2 seconds for the voting process to start the voting session. The time needed for the suggested method is shown in Figure 11. The number of iterations used to measure the trade-off between time/resources.

5.3.2. Response time

A neural-based security system can change the reaction time of an electronic voting system based on several factors. These factors include how well the cryptographic methods work, the hardware infrastructure, the total number of voters, and how hard the voting process is. Figure 12 illustrates the response time. The scenario in the line graph shows the response time of a system for five different iterations. The response time is the time it takes for the system to respond to a request. The expression for response time calculation is shown in Eqn. (7).

$$T_R = T_A + T_C + T_B + T_K \tag{7}$$

Here T_R denotes the response time computing variable, T_A indicates the authentication time, T_C represents the vote casting time, T_B denotes the blockchain transaction time, and T_K expresses the acknowledgement time.

Since both technology and cryptographic methods develop, it is usually expected that the response time for these systems will normally decrease. This will make them more efficient and viable for large-scale electronic voting applications. To ensure that the system can handle the required demand and provide voters with appropriate response times, extensive testing and optimization are required.

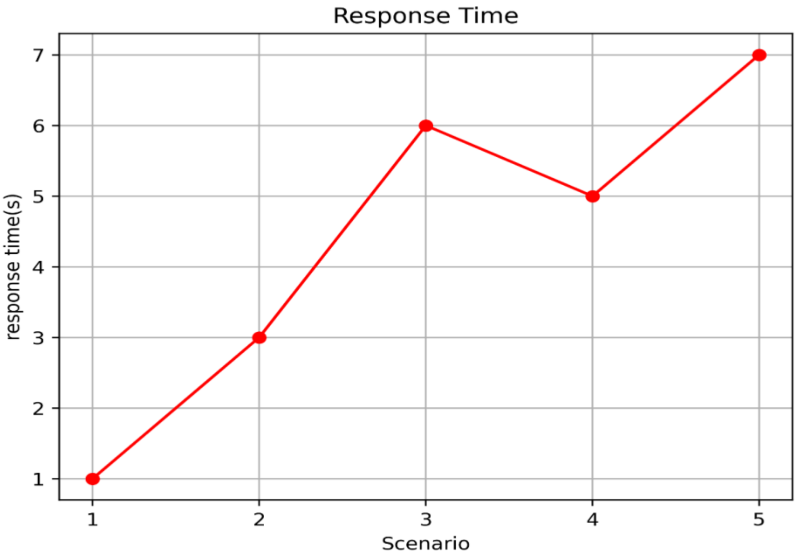


Figure 12. Response Time of Proposed Method

5.3.3. Designing cost

The cost of developing an electronic voting system with neural-based security may vary significantly depending on various factors. Knowledge in various disciplines is required to construct a safe and reliable electronic voting system. This is the cost of creating the proposed method, as shown in Figure 13. The formula for calculating the design cost is defined in Eqn. (8).

$$C_d = C_I + C_D + C_M \tag{8}$$

Here C_d denotes the total design cost, C_I indicates the infrastructure cost, C_D represents the development cost and C_M defines the maintenance cost.

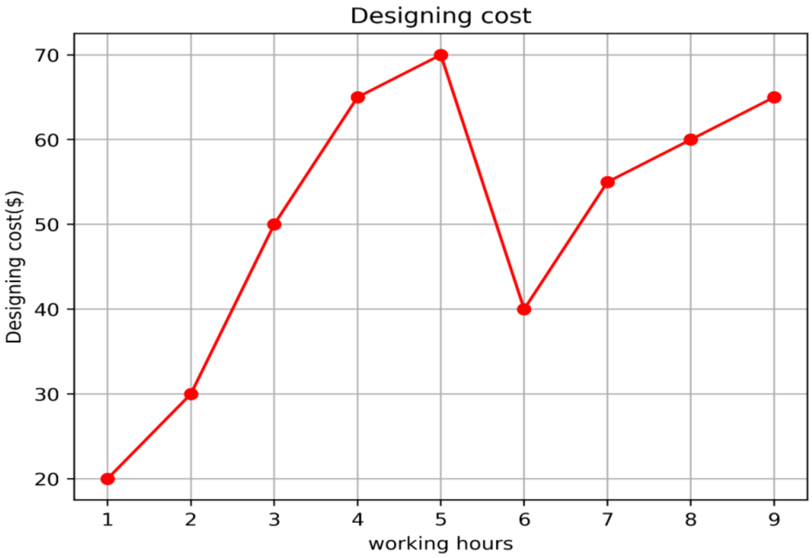


Figure 13. Designing of the proposed method

To provide a dependable and trustworthy electronic voting solution, it is critical to strike a careful balance between the system's numerous characteristics, including usability, security, and dependability. The image shows a line graph of design costs over working hours.

5.3.4. Memory usage

A number of factors can influence the amount of memory used by an electronic voting system, such as neural-based security. These considerations include the size and quantity of images, the number of voters, the complexity of operations, and the data structures employed by the system. Figure 14 depicts the proposed technique for memory usage. The formula for the calculation of memory usage is shown in Eqn. (9).

$$M = N_b \times (H + N_T + T + M) \quad (9)$$

Here M represents the memory usage, N_b indicates the number of blocks, H denotes the header size, $N_T + T$ expresses the number of transactions and their sizes, and M indicates the metadata overhead size.

A more comprehensive understanding of memory utilization across different scenarios can be achieved by employing performance assessments and load evaluations involving an approximate sample size of voters.

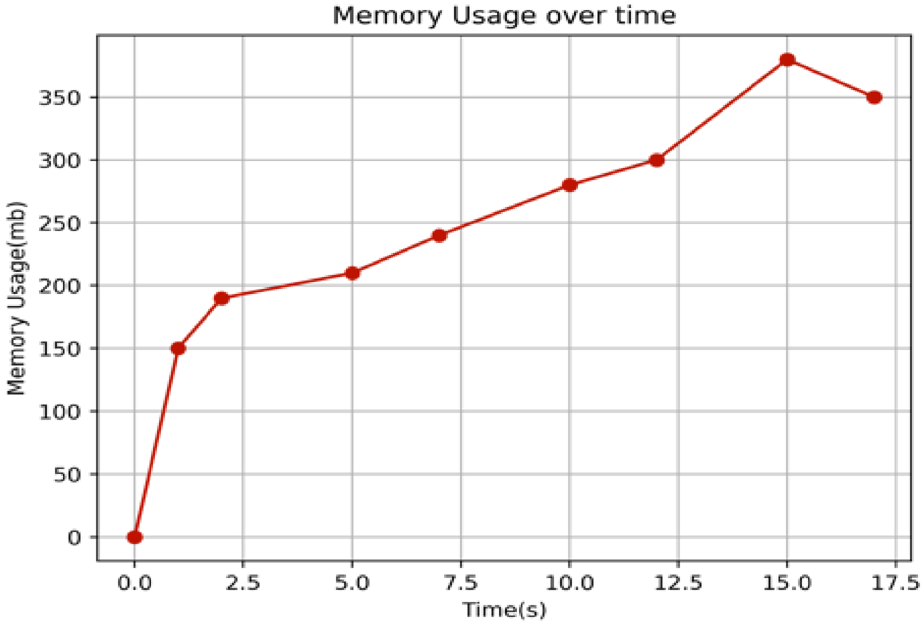


Figure 14. Memory usage of the proposed method

To validate the efficiency of the proposed ZbGEC in the electronic voting system, it was tested under different attack scenarios such as message alteration, DoS, DDoS, and authentication delay. Message alteration is modifying small and large information to perform malicious acts in the voting network. Authentication delay is the time required to validate the participating and communication nodes. The authentication delay represents the variation between the time utilized for authentication and the time allocated by the requested node. DoS, brute force, and DDoS are the attack types where the voters try to obtain possible pay for the message communication and are in charge of malicious pattern prediction without any cryptographic key or hash. The validated results under the different attack scenarios are recorded in Table 3.

Table 3. Performance validation under different attacks

Metrics	**Different vulnerable conditions**				
	Message alteration	**Authentication delay**	**Brute force attacks**	**DoS**	**DDoS**
Accuracy	92%	94%	95.3%	94.3%	94.6%
confidentiality	95%	95.4%	90%	96.4%	96%
Time consumption	10s	12.5s	14s	13s	11.6s
Response time	9s	11s	12s	14s	12.8s

Furthermore, the results are validated for the different voting conditions in different areas. The robustness validation of developed ZbGEC is recorded in Table 4.

Table 4. Performance validation under different voting conditions

Metrics	**Different vulnerable conditions**		
	Small-scale election (100 votes)	**Medium-scale election (1000 votes)**	**Large-scale election (more than 10,000 voters)**
Accuracy	91.9%	95.6%	94.6%
confidentiality	95%	95.4%	90%
Time consumption	12s	14.5s	11s
Response time	8.67s	9.5s	11.7s

The designed ZbGEC model implements various key mechanisms within its framework, ensuring all stakeholders' transparency and accountability in the voting process. The Hyper ledger blockchain confirms the recording of all the votes and verifies its integrity to create trust. Broadcasting blurred images and encrypted voting data verifies that votes are cast without revealing voter identities. Mechanisms such as token contracts, election contracts, vote contracts, and PoA contracts manage the accountability of the present voting mechanisms. Authorities involved in the PoA consensus mechanism are vetted and periodically audited to ensure they perform their duties honestly and transparently.

5.4. Analysis of comparisons

To ascertain whether the suggested design fulfills the specifications of the specific application, this comparative analysis was conducted utilizing pre-existing contemporary models that had been implemented on the Python platform. Hence, the following contemporary methodologies were considered in this proposed research endeavor: Proof of Stake Blockchain (PSC-B chain) [34], Elliptic Curve Digital Signature Algorithm (ECDSA) [32], Elliptic Curve Cryptography (ECC) [33], Secure e-Voting System [35], Decentralised Anonymous and Transparent E-Voting System (DATE) [36], and homomorphic Protocol [37].

5.4.1. Time Consumption

In this section, a comparison is made between the time utilization of our suggested model and that of alternative alternatives, such as ECDSA, ECC, and PSC-Chain. There is a time consumption value of nine, seven, and seven and a half minutes.

Alternatively, the proposed model achieved a time consumption of around two seconds, an insignificant amount of time. The diagrammatic representation of the amount of time spent on the comparison may be found in Figure 15. Because of this, the model we proposed achieved a minimal time value for deployment compared to the tactics that are now being utilized.

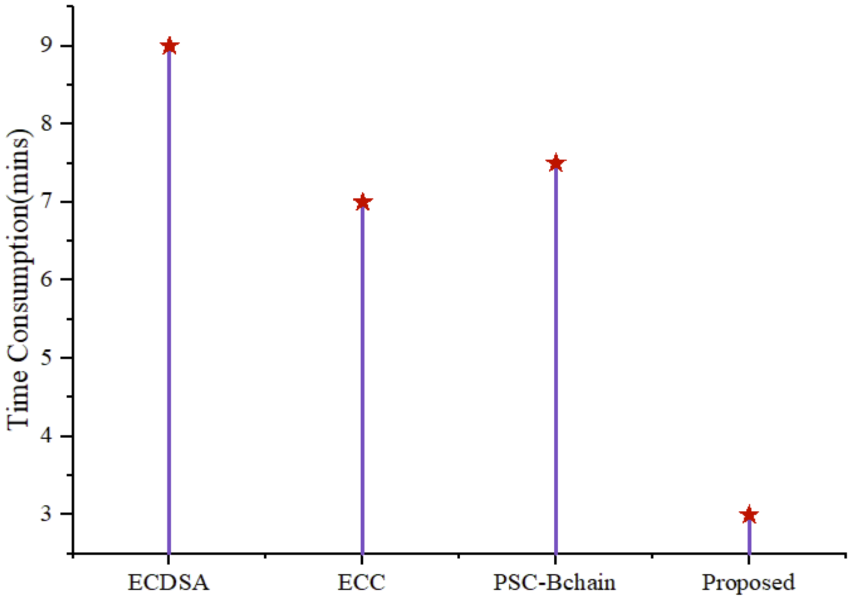


Figure 15. Comparison of Time Consumption

5.4.2. Response time

Within the scope of this discussion, the reaction time value of our suggested model is evaluated in comparison to the values obtained from various approaches, including ECDSA, ECC, and PSC-Bchain. On the other hand, the reaction time values for these three approaches are fifteen minutes, eight minutes, and eleven minutes, respectively.

In contrast, the model we proposed achieved a low reaction time value of roughly 5 seconds. This was a significant achievement. A diagrammatic representation of the comparison of reaction time consumption can be seen in Figure 16.

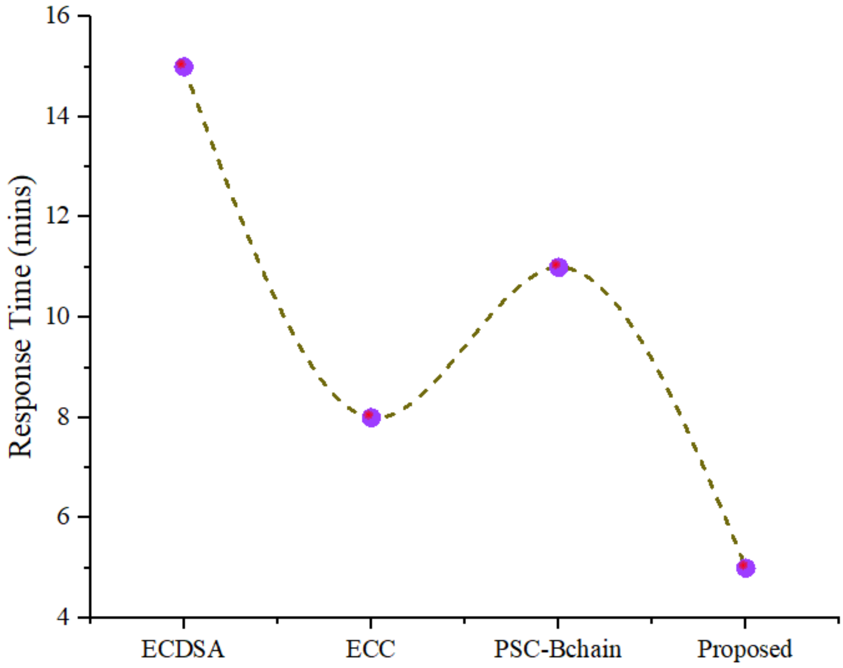


Figure 16. Comparison of Response time

5.4.3. Designing cost

Within this conversation, the calculation rate value of our proposed model is evaluated in comparison to the values of existing techniques, such as ECC, DATE, and SVS. This evaluation is carried out inside the scope of this debate. The computation cost is related to a value of $70, $100, and $50, respectively, according to the value.

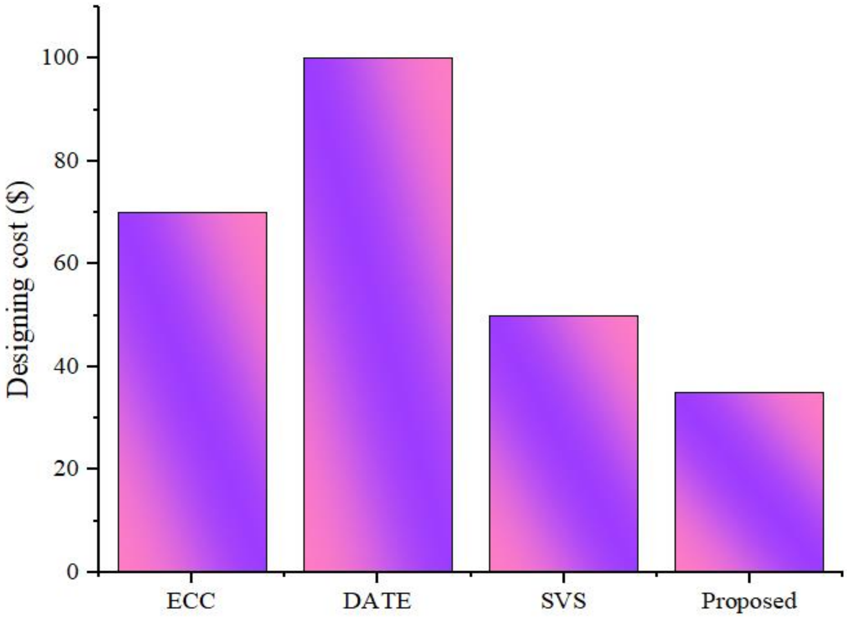


Figure 17. Comparison of design cost

On the other hand, the approach that we have provided results in a low calculation value of approximately 30$. An illustration of the comparison of the costs of computation may be seen in Figure 17, which is a diagrammatic representation. Our proposed model obtained a low compute cost value in contrast to other tactics, resulting from efforts.

5.4.4. Memory Usage

This part compares the memory use value of our proposed model and the values obtained from other methodologies, such as Homomorphic and SVS estimations. In terms of memory use, 1000 MB, 700 MB, and 400 MB have been allocated, respectively.

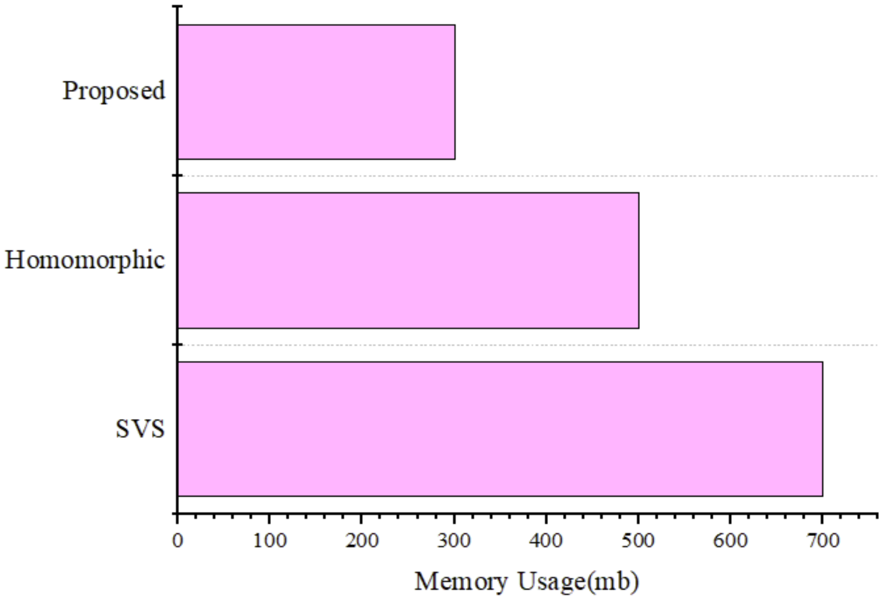


Figure 18. Comparison of memory usage

The model we showed, on the other hand, reached a low memory use estimate of approximately 300 megabytes. A diagrammatic illustration of the comparison of the required quantity can be found in Figure 18. As a consequence of this, the model that we proposed utilized a relatively low amount of MB compared to other tactics that are currently being implemented.

5.4.5. Scalability analysis

The scalability of the created blockchain for the e-voting system is analyzed by certain factors such as generation time, Hash rate, Transactions per second, mining difficulty, and power consumption. The block is generated at the interval of every 15 seconds. It is an average time taken for the block generation. When transactions are built and committed from several remote concurrent clients, with network latency also playing a role, the influence on the block production rate may increase. Here, the transaction speed of the system is 13.80 transactions per second, which appears to be the e-voting system in a very stable state and results in robustness concerning scalability. The mining difficulty level ranges from 1 to 6. However, for the presented approach, the mining difficulty level is kept constant for all the iterations so that it does not affect the input data and builds a direct relationship with the transaction counts and access time to check the scalability. The hash rate is 31.750 hashes per second. The computational power in terms of hashes per second of the machine could be found against every mined transaction. The total power consumed by the system is 141.4 W.

5.5. Discussion

Within this section's scope, the suggested model's performance rate was considered. The proposed model also achieves a higher parameter rate, an additional benefit.

Table 5. Proposed ZbGEC Performance

Overall performance of ZbGEC	
Time consumption (s)	2 seconds
Response time (s)	5 seconds
Designing cost ($)	30 $
Memory usage (MB)	300 MB

Table 5, which may be accessible through this link, contains the definition of the whole performance evaluation that you might find useful. The outcomes that the recommended model produces are superior to those that are produced by the models that are currently in use when the rate of performance of the new model is compared to the models that are already in use.

6. Conclusion

In conclusion, our research introduces a novel approach to e-voting utilizing Zebra-based GoogleNet Elliptic Curve for data preprocessing, ensuring enhanced security and efficiency. The study successfully implemented a multi-step process, including image authentication, option selection, and Image blurring for additional security in the voting process. Storing the voting information in a blockchain further fortifies the system's integrity. Initially, the proposed architecture preprocesses the input data for noise removal. Subsequently, the authentication process is carried out to verify the voters for vote casting. The voting option is only enabled for authenticated users. After casting their votes, the voter information is encrypted, and their images are blurred for data broadcasting and storage in blockchain.

The performance evaluation of our proposed methodology yielded impressive results. Notably, decentralized e-voting time consumption and response time were minimized to an efficient 2 seconds and 5 seconds. The proposed system's design cost was economical at $30, while memory usage was optimized to 300 MB, representing a significant improvement over traditional methods. The validation of our methodology affirms its high performance and potential applicability in real-world scenarios. The proposed model utilized the smart contract to guarantee the voter's privacy. Using the Hyperledger Fabric blockchain, the system can send several transactions per second. The proposed work demonstrated superior security, transparency, and scalability performance than the traditional voting mechanism. Future work should focus on delving deeper into cryptographic techniques to continually enhance the security measures safeguarding user information in decentralized e-voting processes. This avenue of research will be instrumental in advancing the field and ensuring the sustained reliability and robustness of decentralized e-voting systems. Future efforts will optimize the system for scalability, transparency, and security, operating it from start to finish, and simulating it with a more realistic system. The suggested approach assumes that the election's conclusion depends on the system time, another area of future work. To strengthen the time dimension's security, the system might be enhanced.

References

[1] Sunny Harris Rome, "Why voting matters", in Promote the Vote: Positioning Social Workers for Action, Singapore: Springer Nature, 4th December 2022, Ch. 2, pp. 31-49, Online ISBN: 978-3-030-84481-3, Print ISBN: 978-3-030-84482-0, DOI: 10.1007/978-3-030-84482-0_2, Available: https://link.springer.com/chapter/10.1007/978-3-030-84482-0_2.

[2] Michał Pawlak and Aneta Poniszewska-Marańda, "Trends in blockchain-based electronic voting systems", *Information Processing & Management*, Online ISSN: 1873-5371, Print ISSN: 0306-4573, Vol. 58, No. 4, pp. 102595, 4th July 2021, Published by Elsevier Ltd, DOI: 10.1016/j.ipm.2021.102595, Available: https://www.sciencedirect.com/science/article/abs/pii/S0306457321000947.

[3] Sarvesh Tanwar, Neelam Gupta, Prashant Kumar and Yu-Chen Hu, "Implementation of blockchain-based e-voting system", *Multimedia Tools and Applications*, ISSN: 1573-7721, Vol. 83, No. 1, pp. 1449-1480, 6th May 2024, Published by Springer Netherlands, DOI: 10.1007/s11042-023-15401-1, Available: https://link.springer.com/article/10.1007/s11042-023-15401-1.

[4] Aaron Hamlin and Whitney Hua, "The case for approval voting", *Constitutional Political Economy*, Print ISSN: 1043-4062, Vol. 34, No. 3, pp. 335-345, 19th December 2023, Published by Springer New York, DOI: 10.1007/s10602-022-09381-x, Available: https://link.springer.com/article/10.1007/s10602-022-09381-x.

[5] Siddhant Prateek Mahanayak, Barat Nikhita and Saurabh Bilgaiyan, "Enhancing E-Voting Security with Quantum-Resistant Encryption: A Blockchain-Based Approach Utilizing Elliptic Curve Diffie–Hellman and Decentralized Storage", *SN Computer Science*, ISSN: 2661-8907, Vol. 4, No. 5, pp. 642, 2023, Published by Springer, DOI: 10.1007/s42979-023-02041-3, Available: https://link.springer.com/article/10.1007/s42979-023-02041-3.

[6] Patricia Baudier, Galina Kondrateva, Chantal Ammi and Eric Seulliet, "Peace engineering: The contribution of blockchain systems to the e-voting process", *Technological Forecasting and Social Change*, Online ISSN: 1873-5509, Print ISSN: 0040-1625, Vol. 162, pp. 120397, January 2021, Published by Elsevier Inc., DOI: 10.1016/j.techfore.2020.120397, Available: https://www.sciencedirect.com/science/article/pii/S0040162520312233.

[7] Qi Zou, Zijun Mao, Rongxiao Yan, Shuai Liu and Zheng Duan, "Vision and reality of e-government for governance improvement: Evidence from global cross-country panel data", *Technological Forecasting and Social Change*, Online ISSN: 1873-5509, Print ISSN: 0040-1625, Vol. 194, pp. 122667, September 2023, Published by Elsevier Inc., DOI: 10.1016/j.techfore.2023.122667, Available: https://www.sciencedirect.com/science/article/pii/S0040162523003529.

[8] Gabriel Guerrero-Contreras, Sara Balderas-Díaz, José Luis Garrido, María José Rodríguez-Fórtiz and Gregory MP O'Hare, "Proposal and comparative analysis of a voting-based election algorithm for managing service replication in MANETs", *Applied Intelligence*, Electronic ISSN: 1573-7497, Print ISSN: 0924-669X, Vol. 53, No. 16, pp. 19563-19590, 9th March 2023, Published by Springer Netherlands, DOI: 10.1007/s10489-023-04506-7, Available: https://link.springer.com/article/10.1007/s10489-023-04506-7.

[9] Shuli Yan, Qi Su, Zaiwu Gong, Xiangyan Zeng and Enrique Herrera-Viedma, "Online public opinion prediction based on rolling fractional grey model with new information priority", *Information Fusion*, Online ISSN: 1872-6305, Print ISSN: 1566-2535, Vol. 91, pp. 277-298, March 2023, DOI: 10.1016/j.inffus.2022.10.012, Published by Elsevier B.V., Available: https://www.sciencedirect.com/science/article/abs/pii/S1566253522001816.

[10] Xuechao Yang, Xun Yi, Andrei Kelarev, Fengling Han and Junwei Luo, "A distributed networked system for secure publicly verifiable self-tallying online voting", *Information Sciences*, Print ISSN: 0020-0255, Online ISSN: 1872-6291, Vol. 543, pp. 125-142, 8th January 2021, DOI: 10.1016/j.ins.2020.07.023, Published by Elsevier Inc., Available: https://www.sciencedirect.com/science/article/abs/pii/S0020025520306861.

[11] Diego Escobari and Gary A. Hoover, "Late-Arriving Votes and Electoral Fraud: A Natural Experiment and Regression Discontinuity Evidence from Bolivia", *World Development*, Print ISSN: 0305-750X, Online ISSN: 1873-5991, Vol. 173, pp. 106407, January 2024, Published by Elsevier B.V., DOI: 10.1016/j.worlddev.2023.106407, Available: https://www.sciencedirect.com/science/article/abs/pii/S0305750X23002255.

[12] Bin Han, Yicheng Lin, Yan Dong, Hao Wang, Tao Zhang and Chengyuan Liang, "Camera Attributes Control for Visual Odometry With Motion Blur Awareness", *IEEE/ASME Transactions on Mechatronics*, Print ISSN: 1083-4435, Electronic ISSN: 1941-014X, Vol. 28, No. 4, pp. 2225-2235, 8th February 2023, Published by IEEE, DOI: 10.1109/TMECH.2023.3234316, Available: https://ieeexplore.ieee.org/abstract/document/10040760.

[13] Haobo Zuo, Changhong Fu, Sihang Li, Kunhan Lu, Yiming Li and Chen Feng, "Adversarial blur-deblur network for robust UAV tracking", *IEEE Robotics and Automation Letters*, Electronic ISSN: 2377-3766, Vol. 8, No. 2, pp. 1101-1108, 12th January 2023, DOI: 10.1109/LRA.2023.3236584, Published by IEEE, Available: https://ieeexplore.ieee.org/abstract/document/10015799.

[14] Qiucheng Wu, Yifan Jiang, Junru Wu, Victor Kulikov, Vidit Goel, Nikita Orlov *et al.*, "Broad Spectrum Image Deblurring via an Adaptive Super-Network", *IEEE Transactions on Image Processing*, Print ISSN: 1057-7149, Electronic ISSN: 1941-0042, Vol. 32, pp. 5270–5282, 18th September 2023, Published by IEEE, DOI: 10.1109/TIP.2023.3312912, Available: https://ieeexplore.ieee.org/abstract/document/10254493.

[15] Bosheng Ding, Ruiheng Zhang, Lixin Xu, Guanyu Liu, Shuo Yang *et al.*, "U 2 D 2 Net: Unsupervised unified image dehazing and denoising network for single hazy image enhancement", *IEEE Transactions on Multimedia*, Print ISSN: 1520-9210, Electronic ISSN: 1941-0077, Vol. 26, pp. 202 – 217, 29 March 2023, Published by IEEE, DOI: 10.1109/TMM.2023.3263078, Available: https://ieeexplore.ieee.org/abstract/document/10086612.

[16] Maria-Victoria Vladucu, Ziqian Dong, Jorge Medina and Roberto Rojas-Cessa, "E-voting meets blockchain: A survey", *IEEE Access*, Electronic ISSN: 2169-3536, Vol. 11, pp. 23293-23308, 6th March 2023, Published by IEEE, DOI: 10.1109/ACCESS.2023.3253682, Available: https://ieeexplore.ieee.org/abstract/document/10061373.

[17] Piret Ehin, Mihkel Solvak, Jan Willemson and Priit Vinkel, "Internet voting in Estonia 2005–2019: Evidence from eleven elections", *Government Information Quarterly*, Print ISSN: 0740-624X, Online ISSN: 1872-9517, Vol. 39, No. 4, pp. 101718, October 2022, Published by Elsevier Ltd, DOI: 10.1016/j.giq.2022.101718,Available: https://www.sciencedirect.com/science/article/pii/S0740624X2200051X.

[18] Fotios Zantalis, Grigorios Koulouras and Sotiris Karabetsos, "Blockchain Technology: A Framework for Endless Applications", *IEEE Consumer Electronics Magazine*, Print ISSN: 2162-2248, Electronic ISSN: 2162-2256, Vol. 13, No. 2, pp. 61-71, 24 February 2023, Published by IEEE, DOI: 10.1109/MCE.2023.3248872, Available: https://ieeexplore.ieee.org/abstract/document/10052716.

[19] Itzhak Aviv, Artem Barger, Alexander Kofman and Roye Weisfeld, "Reference Architecture for Blockchain-Native Distributed Information System", *IEEE Access*, Electronic ISSN: 2169-3536, Vol. 11, pp. 4838-4851, 11th January 2023, Published by IEEE, DOI: 10.1109/ACCESS.2023.3235838, Available: https://ieeexplore.ieee.org/abstract/document/10014995.

[20] Deepika Varshney and Dinesh Kumar Vishwakarma, "An automated multi-web platform voting framework to predict misleading information proliferated during COVID-19 outbreak using ensemble method", *Data & Knowledge Engineering*, Online ISSN: 1872-6933, Print ISSN: 0169-023X, Vol. 143, pp. 102103, January 2023, Published by Elsevier B.V., DOI: 10.1016/j.datak.2022.102103, Available: https://www.sciencedirect.com/science/article/pii/S0169023X22000945.

[21] Srijanee Mookherji, Odelu Vanga and Rajendra Prasath, "Blockchain-based e-voting protocols", in Blockchain Technology for Emerging Applications, Amsterdam, The Netherlands: Elsevier B.V., 27th May 2022, Ch. 5, pp. 239-266, ISBN: 978-0-323-90193-2, Published by Elsevier, DOI: 10.1016/B978-0-323-90193-2.00006-5, Available: https://www.sciencedirect.com/science/article/abs/pii/B9780323901932000065.

[22] Zhaosen Shi, Zeyu Yang, Alzubair Hassan, Fagen Li and Xuyang Ding, "A privacy preserving federated learning scheme using homomorphic encryption and secret sharing", *Telecommunication Systems*, Electronic ISSN: 1572-

9451, Print ISSN: 1018-4864, Vol. 82, No. 3, pp. 419-433, 8th December 2023, Published by Springer Netherlands, DOI: 10.1007/s11235-022-00982-3, Available: https://link.springer.com/article/10.1007/s11235-022-00982-3.

[23] Muhammad Shoaib Farooq, Usman Iftikhar and Adel Khelifi, "A framework to make voting system transparent using blockchain technology", *IEEE Access*, Electronic ISSN: 2169-3536, Vol. 10, pp. 59959-59969, 3rd June 2022, Published by IEEE, DOI: 10.1109/ACCESS.2022.3180168, Available: https://ieeexplore.ieee.org/abstract/document/9787540.

[24] Sachi Chaudhary, Shail Shah, Riya Kakkar, Rajesh Gupta, Abdulatif Alabdulatif, Sudeep Tanwar, Gulshan Sharma and Pitshou N. Bokoro, "Blockchain-based secure voting mechanism underlying 5G network: A smart contract approach", *IEEE Access*, Electronic ISSN: 2169-3536, Vol. 11, pp. 76537-76550, 20th July 2023, Published by IEEE, DOI: 10.1109/ACCESS.2023.3297492, Available: https://ieeexplore.ieee.org/abstract/document/10188663.

[25] Anitha, Orlando Juan Marquez Caro, R. Sudharsan, S. Yoganandan and M. Vimal, "Transparent voting system using blockchain", *Measurement: Sensors*, Online ISSN: 2665-9174, Vol. 25, pp. 100620, February 2023, DOI: 10.1016/j.measen.2022.100620, Available: https://www.sciencedirect.com/science/article/pii/S2665917422002549.

[26] Vu Tuan Truong, Long Bao Le and Dusit Niyato, "Blockchain meets metaverse and digital asset management: A comprehensive survey", *IEEE Access*, Electronic ISSN: 2169-3536, Vol. 11, pp. 26258 – 26288, 14th March 2023, DOI: 10.1109/ACCESS.2023.3257029, Available: https://ieeexplore.ieee.org/abstract/document/10068493.

[27] Anushka Chaubey, Anubhav Kumar, Vikalp Pandey, Bharat Bhushan and Priyambada Purohit, "Leveraging Secured E-Voting Using Decentralized Blockchain Technology", in Data Analytics for Internet of Things Infrastructure, Cham, Switzerland: Springer Nature, 20th September 2023, Ch. 15, pp. 265-290, Print ISBN: 978-3-031-33807-6, Online ISBN: 978-3-031-33808-3, DOI: 10.1007/978-3-031-33808-3_15,Available: https://link.springer.com/chapter/10.1007/978-3-031-33808-3_15.

[28] Yichao Lu, Huilin Li, Le Gao, Jiaxin Yu, Yong Yu and Hexing Su, "Self-tallying e-voting with public traceability based on blockchain", *Computer Standards & Interfaces*, Print ISSN: 0920-5489, Online ISSN: 1872-7018, Vol. 88, pp. 103795, March 2024, Published by Elsevier B.V., DOI: 10.1016/j.csi.2023.103795, Available: https://www.sciencedirect.com/science/article/abs/pii/S0920548923000764.

[29] Maria-Victoria Vladucu, Ziqian Dong, Jorge Medina and Roberto Rojas-Cessa, "E-voting meets blockchain: A survey", *IEEE Access*, Electronic ISSN: 2169-3536, Vol. 11, pp. 23293-23308, 6th March 2023, Published by IEEE, DOI: 10.1109/ACCESS.2023.3253682, Available: https://ieeexplore.ieee.org/abstract/document/10061373.

[30] Simona-Vasilica Oprea, Adela Bâra, Anca-Ioana Andreescu and Marian Pompiliu Cristescu, "Conceptual architecture of a blockchain solution for E-voting in elections at the university level", *IEEE Access*, Electronic ISSN: 2169-3536, Vol. 11, pp. 18461-18474, 22nd February 2023, Published by IEEE, DOI: 10.1109/ACCESS.2023.3247964, Available: https://ieeexplore.ieee.org/abstract/document/10049991.

[31] Reewos Talla-Chumpitaz, Manuel Castillo-Cara, Luis Orozco-Barbosa and Raúl García-Castro, "A novel deep learning approach using blurring image techniques for Bluetooth-based indoor localisation", *Information Fusion*, Online ISSN: 1872-6305, Print ISSN: 1566-2535, Vol. 91, pp. 173-186, March 2023, DOI: 10.1016/j.inffus.2022.10.011, Available: https://www.sciencedirect.com/science/article/pii/S1566253522001804.

[32] Uzma Jafar, Mohd Juzaiddin Ab Aziz and Zarina Shukur, "Blockchain for electronic voting system—review and open research challenges", *Sensors*, ISSN: 1424-8220, Vol. 21, No. 17, pp. 5874, 6th July 2021, Published by Multidisciplinary Digital Publishing Institute (MDPI), DOI: 10.3390/s21175874, Available: https://www.mdpi.com/1424-8220/21/17/5874.

[33] De Xu and Qing Yang, "The Systems Approach and Design Path of Electronic Bidding Systems Based on Blockchain Technology", *Electronics*, ISSN: 2079-9292, Vol. 11, No. 21, pp. 3501, 14th September 2022, Published by Multidisciplinary Digital Publishing Institute (MDPI), DOI: 10.3390/electronics11213501, Available: https://www.mdpi.com/2079-9292/11/21/3501.

[34] Yousif Abuidris, Rajesh Kumar, Ting Yang and Joseph Onginjo, "Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding", *Etri Journal*, Online ISSN: 2233-7326, Print ISSN: 1225-6463, Vol. 43, No. 2, pp. 357-370, 30th November 2021, Published by John Wiley & Sons Inc., DOI: 10.4218/etrij.2019-0362, Available: https://onlinelibrary.wiley.com/doi/full/10.4218/etrij.2019-0362.

[35] Kashif Mehboob Khan, Junaid Arshad and Muhammad Mubashir Khan, "Investigating performance constraints for blockchain based secure e-voting system", *Future Generation Computer Systems*, Online ISSN: 1872-7115, Print ISSN: 0167-739X, Vol. 105, pp. 13-26, April 2020, Published by Elsevier B.V., DOI: 10.1016/j.future.2019.11.005, Available: https://www.sciencedirect.com/science/article/abs/pii/S0167739X19310805.

[36] Wei-Jr Lai, Yung-Chen Hsieh, Chih-Wen Hsueh and Ja-Ling Wu, "Date: A decentralized, anonymous, and transparent e-voting system", in *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, 15-17August 2018, Shenzhen, China, Electronic ISBN: 978-1-5386-4870-4, Print ISBN: 978-1-5386-4871-1, pp. 24-29, Published by IEEE, DOI: 10.1109/HOTICN.2018.8605994, Available: https://ieeexplore.ieee.org/abstract/document/8605994.

[37] Anjima, V. S. and N. N. Hari, "Secure cloud e-voting system using fully homomorphic elliptical curve cryptography", in *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, 15-17 May

2019, Madurai, India, Electronic ISBN: 978-1-5386-8113-8, Print ISBN: 978-1-5386-8114-5, pp. 858-864, Published by IEEE, DOI: 10.1109/ICCS45141.2019.9065871, Available: https://ieeexplore.ieee.org/abstract/document/9065871.

[38] Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta_Islam and Sajib Ahamed, "DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system", *Journal of King Saud University-Computer and Information Sciences*, Print ISSN: 1319-1578, Online ISSN: 2213-1248, Vol. 34, No. 9, pp. 6855-71, 9th October 2022, Published by King Saud bin Abdulaziz University, DOI: 10.1016/j.jksuci.2022.06.014, Available: https://www.sciencedirect.com/science/article/pii/S1319157822002221.

[39] R Ramyadevi and V Priya, "Block Chain-Powered E-Voting System: A Secure and Transparent Solution with Three-Tiered OTP Security Mechanism," in *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)*, 9-10th February 2024, Greater Noida, India, Electronic ISBN: 979-8-3503-8354-6, Print ISBN: 979-8-3503-8355-3, pp. 728-731, Published by IEEE, DOI: 10.1109/IC2PCT60090.2024.10486507, Available: https://ieeexplore.ieee.org/abstract/document/10486507.

[40] Md Jobair Hossain Faruk, Fazlul Alam, Mazharul Islam and Akond Rahman, "Transforming online voting: a novel system utilizing blockchain and biometric verification for enhanced security, privacy, and transparency," *Cluster Computing*, Electronic ISSN: 1573-7543, Print ISSN: 1386-7857, Vol. 27, pp. 4015–4034, 19th April 2024, Published by Kluwer Academic Publishers, DOI: 10.1007/s10586-023-04261-x, Available: https://link.springer.com/article/10.1007/s10586-023-04261-x.

[41] Beulah Jayakumari, S Lilly Sheeba, Maya Eapen, Jani Anbarasi, Vinayakumar Ravi, A. Suganya and Malathy Jawahar, "E-voting System using Cloud-based Hybrid Blockchain Technology," *Journal of Safety Science and Resilience*, Online ISSN: 2666-4496, Vol. 5, No. 1, pp. 102-109, March 2024, DOI: 10.1016/j.jnlssr.2024.01.002,Available: https://www.sciencedirect.com/science/article/pii/S2666449624000069.