International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Secure E-voting System based on Elliptic Curve Digital Signature Algorithm with Hybrid Consensus Mechanism

Padmavathi Vurubindi[1*], Sujatha Canavoy Narahari[2], V. Raja Rajeswari[3], Abhishek Gudipalli[4], Jayanth Kumar Mutha[5], Saikiran Reddy Medhimale[6]

Submitted: 05/03/2024 **Revised:** 23/04/2024 **Accepted:** 03/05/2024

Abstract*:* Background: The evolution of technology has brought about significant changes in many existing processes, making them simpler and safer. Electronic voting (E-voting) is a notable example that has replaced traditional voting systems to achieve accurate and reliable results with minimal human interference. However, E-voting faces significant challenges such as vote rigging, vote theft, and various other security threats. Methods Used: To address these security concerns, the elliptic curve digital signature algorithm with hybrid consensus algorithm (ECDSA-HCA) was employed. A secure web-based E-voting approach has been developed to facilitate end-to-end communication between users, ensuring the prevention of vote theft during the polling announcement in the nation. The ECDSA-HCA involves three main stages: the registration process, polling, and the announcement of results. In the proposed model, the election commission utilizes blockchain technology to verify and validate vote data. Subsequently, the ECDSA-HCA method is employed to securely store voter data in the blockchain, utilizing encryption and an e-voting cloud system (ECS) tailored to the data structure of user-specific modelling processes. Results achieved: Upon analyzing the results, it becomes evident that the proposed ECDSA-HCA approach outperforms in terms of communication time (1871 μs), encryption time (1650 μs), latency (24 ms), and throughput (63 Tps). Concluding remarks: In this study, the number of users is extended to 1000 by conducting a simulation network five times, each with 200 users as the size of each set of nodes. To assess the effectiveness of the ECDSA-HCA, it is compared to existing studies such as ECS and ECDSA.

Keywords: *Blockchain, Election Commission, Encrypted model, E-voting, E-voting Cloud System, Elliptic Curve Digital Signature Algorithm, Hybrid Consensus Algorithm*

1. Introduction

The use of computing devices and equipment for voting and obtaining accurate results that reflect the opinions of the voting participants, has been a research emphasis for many years [1]. Different strategies are being put into practice to support the electoral process. Due to its advantages based on end-to-end verifiability, distributed ledger technologies are employed to create electronic voting (E-voting) systems [2]. The process of building democracy in a nation involves elections [3]. Allowing everyone to vote freely and securely is a basic right in any democratic nation. All democracies have a voting procedure that is fundamental to society [4]. Many experts believe that using paper ballots is the only suitable option to protect and ensure that every voter's right to vote is respected [5]. This strategy, meanwhile, is susceptible to errors and abuse [6]. Elections in various underdeveloped countries have historically been marred by errors, difficulties, and institutional fraud, which decreases their effectiveness [7]. In order to guarantee fair and accurate elections, E-voting was suggested as a solution to a number of problems encountered in paper-based voting [8]. E-voting is a voting method that enables voters to cast a secret ballot and have it electronically tallied [9]. The use of E-voting equipment directly accelerates ballot counting, lowers the price of paying people to manually tally ballots, and provides accessibility for voters with disabilities [10]. Nowadays, E-voting is known as one of the legitimate uses for blockchain technology (BCT) [11].

BC's decentralized structure, anonymity, and transparency allow it to effectively overcome numerous problems with existing E-voting methods [12]. BC-based E-voting architecture has the potential to address the majority of issues faced in traditional voting systems and conventional E-voting [13]. Concerns about voter identity, vote casting, vote tabulation, voter privacy protection, vote security, and the veracity of election results are among them [14]. Blockchain offers every feature required for an E-voting system, which is probably the most important component of a democratic culture [15]. The implementation of blockchain to enable E-voting systems with the assurance of voter confidentiality, vote credibility, and end-to-end verification is explored in this study [16]. Additionally, E-voting can benefit from key blockchain properties including the distributed ledger's public accessibility and cryptographic transaction validation framework [17]. Due to this, BCT is particularly effective at addressing the risk of using a voting token more than once as

[1]*Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology, Hyderabad, India.*
Corresponding Author E-mail: padmareddyvch@ieee.org
[2]*Department of Electronics and Communication Engineering, Sreenidhi Institute of Science and Technology, Hyderabad, India.*
[3]*Department of Electronics and Communication Engineering, School of Engineering and Technology, Sri Padmavati Mahila Visvavidyalayam, Tirupati, India.*
[4]*School of Electrical Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu.*
[5]*Department of Computer Science and Engineering, Anurag University, Hyderabad, India.*
[6]*Department of Computer Science and Engineering, Anurag University, Hyderabad, India.*

well as attempts to sway the transparency of the outcome [18]. A blockchain prevents both the modification of historical events and the hacking of live events. Additionally, the system does not accept modifications [19]. The identical results are displayed by any machine or node that is given access, and every vote is tracked back to its source without disclosing the voter's identity [20]. This research focuses on looking at important topics including end-to-end verification, vote confidentiality, and voter anonymity. These factors serve as the cornerstones of a voting system that are effective for maintaining the fairness of the electoral process. This article outlines the attempts to investigate the application of BCT to mitigate the aforesaid problems.

The major contribution of this research is mentioned as follows,

- The primary aim of this system model is to validate the consumer data. In the suggested approach, a secure large-scale E-voting system based on the elliptic curve digital signature algorithm with hybrid consensus algorithm (ECDSA-HCA) is introduced.
- Using a candidate key, users cast their votes and candidates confirm the ECDSA-HCA result announcements. The trusted server should first validate the candidate details and produce a candidate key.
- Using the key and the saved vote data, ECDSA-HCA generates the outcome. This model is used to secure the user information from beginning to end.

The structure of this research is mentioned as follows; section 2 explains the literature review for the existing works. Section 3 provides the description about the proposed method. Section 4 demonstrates the result analysis and its comparisons. Section 5 provides the discussion. Finally, the conclusion and future scope is stated in section 6.

2. Literature Review

A privacy-preserving ledger-based e-voting (PPLE) system used BCT which was developed by Alshehri et al. [21]. In order to guarantee election fairness, the suggested approach assessed whether the score provided by voters falls within the prescribed range before the vote is put to the BC. The effectiveness of this method is assessed in comparison to a number of extensive experiments created to identify the constraints. The outcomes of these simulations and its repercussions show that the suggested system is secure and capable of handling up to 10,000 transactions at once. However, the yes/no voting method necessitates that an eligible voter provides a yes/no for a candidate, whereas the score voting method necessitates that the voter provide a score for every candidate within a predetermined range.

A secure online E-voting cloud system (ECS) for end-to-end users was presented by Shankar et al. [22] in order to prevent vote fraud during the public announcement of the results in the country. The cubic structure of voting data storage was made available in ECS. The user received the encoded information from the cloud so they could search and validate it. The political process is more transparent due to BCT, which also foils attempts to tamper with voting data in order to boost voter turnout. The candidate then uses their key to decrypt the data, enabling the general public to verify the results that the ECS has proclaimed. To decrease the time issue for online E-voting systems, it was significant to improve the relevant procedures for privacy and security.

Rathee et al. [23] implemented a transparent and secure E-voting system utilizing internet of things (IoT) devices. The hazards brought on by an intruder at several levels were identified and resolved using the transparent and secure E-voting process. Then, both national and electoral bodies employed a two-tier structure, and each organization used a blockchain mechanism to guarantee security if IoT devices are compromised. However, there were still some issues that needed to be addressed at different levels, such as a voter's repeated fraudulent registrations at different locations and vote-tampering before the count.

Panja and Roy [24] introduced a direct-recording electronic (DRE) voting system that protects voter privacy and ballot integrity without the use of a tallying system or secure hardware storage. It was further updated as DRE-ip system to ensure that no adversary could generate and upload a legal ballot on the public bulletin board without being noticed. This avoids ballot-stuffing attacks. It is hard to distinguish between the key and the biometric information used to encrypt the biometric data connected with certain voters. But the DRE was unable to lower the Fuzzy Vault Algorithm's False Rejection Rate for fingerprints.

A hybrid consensus model name called proof of stake and credibility-blockchain system (PSCBCS) that combines proof of credibility (PoC) and proof of stake (PoS) was created by Abuidris et al. [25]. The security concerns in the E-voting system were resolved by the PSCBCS. Smart contracts were used to construct a secure computing environment and a dependable public bulletin board in order to ensure the accuracy of the vote results. The PSCBCS hybrid technique was then included to enhance the functioning of the blockchain-based E-voting system. On the other hand, PoC took a significant amount of computation and time.

By implementing corporate BCT to E-voting, González et al. [26] created a solution that assures high dependability while protecting the secret ballot. Listing the collaborating organizations is the first step in creating a network structure for an application. Ballots are non-fungible tokens (NFTs) that can only be produced by accredited institutions. The suggested network structure setup was more adaptable, and substantially shortened the time for counting votes. But in this E-voting system, the proposed procedure could not prevent harmful activities.

For the avoidance of fraudulent voting, Ahn [27] recommended the establishment and early deployment of an Ethereum-based E-voting system. A blockchain-based E-voting technology called Follow My Vote was used online to demonstrate to voters and observers that ballots cannot be tampered with and leaked from the polling booth. For the development of an E-voting system to maintain reliability of vote counting, a Solidity-based smart contract was constructed and distributed among voters. Improving the security and dependability of the E-voting system, was the solution used to address the problem of fraudulent voting. Yet, by comparing the differences among Ethereum's smart contract programming syntax and other languages, the proposed technique needed improvement in terms of availability and sustainability required in smart contract development.

Blockchain-based distributed ledger technology was developed by Ch et al. [28] for a trustworthy E-voting system with statistical evaluation. Every contestant's initial block was created

specifically for them based on their Etherium balance. Each citizen receives a unique BCT-based identification (BCTID) via the Ganache platform. This technique of constructing a blockchain-based E-voting system made use of an Ethereum. However, the method used calls for the implementation of an E-voting system based on a secure blockchain with a facility for digital signatures.

By combining two distinct blockchain, Neziri et al. [29] created a new method for E-voting that achieves privacy and anonymity. The administration of keys took place on the first blockchain, whereas anonymous voting was stored on the second. The distributed key blockchain and the encrypted votes blockchain are two distinct blockchains that take voter confidentiality and anonymity into consideration. Public keys are generated by the distributed key blockchain and used to encrypt ballots by registered voters. By keeping votes and voter information in an independent blockchain and utilising cryptographic techniques and protocols, voter confidentiality and vote secrecy are achieved. The created system did not take into account the voter's isolation from the vote element.

The blockchain-based decentralised mechanism was created by Alvi et al. [30] to guarantee the security of the digital voting mechanism. By storing the voter data as a hash in the blockchain, this technique offers voter anonymity. By maintaining the cast vote encrypted until the election's conclusion, it also ensures impartiality. Smart contracts are written in Solidity, a programming language, using the blockchain exchange Ethereum 2.0. This procedure enables voters to cast their ballots for their preferred candidate using smart devices from anywhere in the world. The one time password (OTP) choice, still was not included in the developed approach for the registration procedure.

A hybrid secure algorithms-based ideal blockchain has been suggested by Rakshitha et al. [31] to improve the performance of the blockchain in terms of security and cloud storage costs. Initially the advanced encryption standard (AES) was used to secure the voting data. The extended elliptic curve cryptography (EECC) is subsequently employed to encrypt the AES secret key. Furthermore, the most suitable blockchain blocks were used to store the encrypted data. The extensible firefly algorithm (EFFA) has been explained for the best block mutation. While they were stored on the cloud server, these blocks were hashed with SHA-256. With minimal storage space needed, the suggested E-voting method accomplished a high level of security. The suggested encryption time, nevertheless, was cut to 32% and 50%, correspondingly.

The safe voting system for the fifth generation wireless (5G) network was presented by Chaudhary et al. [32] on the basis of BCT. To enable an affordable voting process for voters and candidates, the interplanetary file system (IPFS) protocol was integrated with the blockchain. In order to securely and effectively choose the best applicant, the proposed voting process comprised communication between voters, candidates, as well as the election commission through a 5G network. A smart contract for the voting system was deployed, that included a number of capabilities to allow voters to choose a candidate in a safe and open voting environment. Nevertheless, in order to construct smart contracts that would allow users to alter their votes with a high level of security and authentication over a specific period of time, the solution that was given was necessary.

A blockchain-based E-voting system was proposed by Pereira et al. [33] for safety and transparency. The suggested solution used cryptographic techniques to preserve voters' anonymity and privacy while maintaining the validity and verifiability of election outcomes. The poll and its results were shown using a web interface, and an external application programming interface (API) was utilized to collect the constraints and voting variables. The blockchain that managed all of the logic for the voting process was represented by the voting blockchain component. In organizations that required a high level of security and voter registration, the strategy was advantageous. But in order to boost the effectiveness of the voting system, it was necessary to look into other options in addition to the provided approach.

Elliptic curve cryptography (ECC) was used to propose an effective and secure E-voting technique by Chatterjee et al. [34]. The core of the suggested E-voting system was a client-server architecture, in which a voter's smart device mounted an application and the administrator's server loaded a different application tool. It was proved that the suggested approach was secure from all pertinent security attacks utilizing qualitative security analysis and simulation. The comparison of security aspects demonstrated unequivocally that the proposed method was a very appropriate one in context of E-voting. Future work on the suggested approach may examine leveraging identity-based encryption methods to further reduce computation and communication overhead.

The framework to use the blockchain to render the voting process transparent was created by Farooq et al. [35]. Without using any actual polling places, the technology that was suggested offered a framework that could be used for carrying out voting activity digitally through blockchain. The presented design used adaptable consensus algorithms to support a scalable blockchain. The voting transaction was safer due to the chain security algorithm used in the voting system. When a transaction was being carried out in the chain, smart contracts offered a safe connection among the user and the network. By employing the more efficient strategy of constructing a flexible consensus algorithm to cut down on the significant processing resources in the blockchain, the accessibility of this system worked well.

It is important to note that hybrid methods are more useful and effective than other alternatives, as observed in the literature analysis. The term "hybrid scheme" refers to a design that combines two or more methodologies. A hybrid system overcomes the flaws of individual cryptographic tools while inheriting the benefits and security characteristics of combined cryptographic tools. But the applications to which these E-voting techniques are applied determine how they are used. Different E-voting methods may therefore be appropriate for various purposes. Here, a secure large-scale E-voting system based on the ECDSA-HCA is described.

3. Methods

3.1 Blockchain E-voting System Properties

A decentralized public ledger called blockchain, features a rigidly encrypted system for member interoperability. In its most basic form, a blockchain is just a data structure made up of an individually linked list of the nodes in a network, each of which contains numerous blocks that carry the cryptographic data from the block before it.

- Authentication.
- Availability.
- Publicly verifiable.

- Integrity.

3.2 Nodes

This node contains a variety of electronic tools and sites that users can use to interact with the blockchain-based E-voting system. They communicate with one another using smart contracts, also known as chain code on the Hyperledger Fabric, which are the peer servers of the E-voting blockchain [36]. The various peer node categories and the associated duties are as follows:

a. Nodes for E-voting: Main functions of these nodes are to facilitate voter verification and voting, as well as to make sure that all blockchain transactions are properly noted.

b. Administrator nodes: It is used to create blockchain network channels, to specify the degree of access control for specific nodes, to delegate tasks to blockchain nodes, and grant access.

c. Public nodes: These nodes allow for read-only public entry to the E-voting blockchain's transactions. Vote validation is the responsibility of these nodes. They are also employed to verify the legitimacy of the transactions contained in a block.

d. Committing nodes: It is responsible for validating and adding fresh blocks to the blockchain.

3.3 Smart Contract

Each task performed by various blocks in a network is controlled by a prebuilt, precisely defined document known as a "smart contract." All blocks are required to have a smart contract, which specifies their roles and the procedures they must follow. According to [16], Smart contracts are similar to encoded commercial contracts. The agreement is instantly enforceable if and when the pre-established rules are followed. The smart contract functions specify the contractual terms that allow for the tracking of operations in the upper layer of the blockchain network. For example, every node in the blockchain network independently executes the public blockchain to achieve a consensus, leading to the development of a configurable cryptosystem for E-voting systems.

3.4 Security Requirements

Anonymity: To safeguard the privacy of the voter, the voting procedure should be anonymous. Additionally, nobody besides ECDSA-HCA can connect a voter's encrypted ballot to them [37]. The specific and private address numbers help to protect voter identities during the blockchain transaction process. Anonymity has proven useful in systems like E-voting.

Public ledger: All votes cast are recorded in the public ledger, which is indelible and unalterable. Once cast, a vote cannot be withdrawn [38]. It is nearly impossible to alter the ledger because of the consensus mechanism since in order to add a new block, one must first hack all of the prior blocks. Depending on the consensus used, a hacker must get access to at least one-third of the network, and occasionally even half, in order to access the entire system.

3.5 Process of ECDSA-HCA

The proposed system model uses a user-differentiated system model for secure voting and result verification. Users, trusted ECDSA-HCA Servers, trusted vote verification servers (TVVS), online voting servers (OVS), and cloud voting storage servers (CVVS) are the five entities that make up this concept. Voters ($User1, \ldots User\ N$), candidates ($Candidate1, \ldots, Candidate\ N$), and Election Commission Officer personnel are the three categories of users.

Users: The three users in the proposed model are: voters, candidates, and election commission officers. According to this model, voters cast vote and choose a candidate according to their preferences. Candidates make up the model's second user [39]. Candidates enter their information into the ECDSA-HCA Server, and the ward information determines which candidate information will be presented on the online ballot. Finally, the Election Commission Officer or final user in this model announces the outcome according to the output from the trustworthy server for vote verification. As a result, all of the user's information is described above, along with how they use the system.

Trusted server: Since the final user maintains this server, it is utilized to store user information other than their own. This server keeps track of voter and candidate information. User registers their information offline, receiving some private login information in the process. Candidates then enter their information in offline mode, at which point they receive some crucial information. Candidates check the ECDSA-HCA announced result using the key value. Figure 1 shows the block diagram of the proposed method.

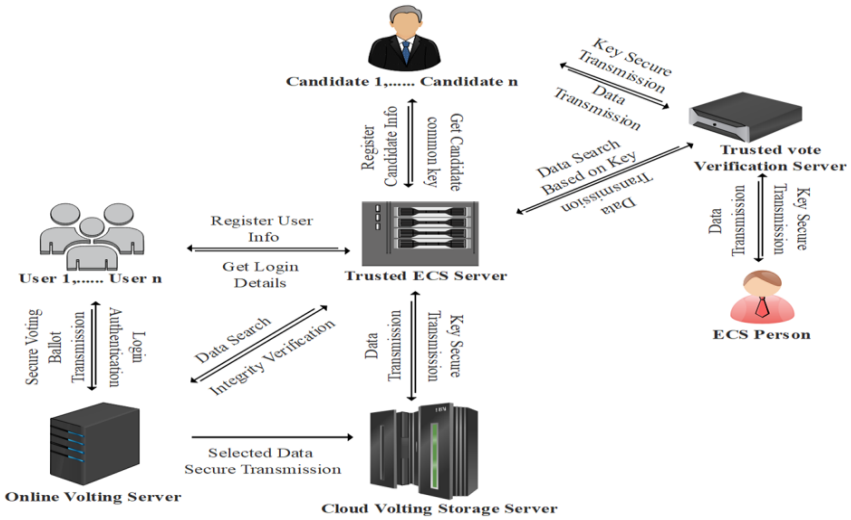

Fig. 1. Block diagram of the proposed method

OVS: Data users access the online voting with the aid of their computers, cell phones, or other devices, and initialize it using their login credentials. At the same moment, the login credentials are validated by the authorized ECS server. Users are only permitted to log in again and participate in polls when the authorized ECS server's verification is accomplished; otherwise, the login request is declined. A user chooses their candidate using the online voting ballot after successfully logging in. The algorithm encrypts and stocks the vote in the cloud storage server based on the information about the selected candidate.

TVVS: The server for trusted vote verification is used to confirm the vote's specifics. Since the ECDSA-HCA delivers unique candidate keys to encrypt and decrypt the result at this stage, there is no option to modify the vote results. The vote is also encrypted and decrypted in the same manner by the candidates. Therefore, user integrity and dual authentication are carried out.

CVVS: According to the key required by both ECS and candidates, the encrypted vote is kept, and the result is decoded and transmitted to the requested individuals.

3.5.1 Registration Phase

The candidate/user enters their information offline in this phase by going straight to the local election office. The user or candidate receives their security information according to the registration. User login and the election voting page opens based on the user registration information. Secure authentication increases voting opportunities and decreases voting fraud [40]. The registered candidate only uses the candidate's security information to confirm the voting information.

3.5.2 Setup Phase

The Setup algorithm, which is what makes up this phase, uses the security parameters as input to generate the following steps:

- **Step S1:** To establish a bilinear pairing $k: PG_1 \times PG_2 \rightarrow PG_t$ such that $k(i^a, j^b) = k(i,j)^{ab}, for\ a, b \epsilon Z_p = \{0, 1, 2 \dots, p-2\}$, the controller chooses a bilinear pairing group $PG = \{PG_1, PG_2, PG_T, p\}$ with the generators $i \epsilon PG_1$ and $j \epsilon PG_2$
- **Step S2:** Four "collision resistant one-way cryptographic hash functions" are chosen by the controller. $H_1, H_4: \{0,1\}^* \rightarrow \{0,1\}_m^l$. Here, l_σ and l_m refers to the length of a vote V and the length of the security parameter respectively.
- **Step S3:** Each attribute authority c chooses $b_c \epsilon Z_p$ at random and distributes $Q_c = k(i,j)^{b_c}$ to every other authority. The system public key is then calculated by each authority as $\alpha = H_1\left(\Pi_{c=1}^{N} Q_c\right)$, which is $H_1(k(i_1, i_2)^{\Sigma b_c})$.

3.6 Voting Process

After registration, election commission authorities determine whether a voter is entitled to vote or not by checking the information obtained from the database. Depending on the Election Commission's rules, users must cast their votes online via the web. The voter must scan his or her finger on a computer or cell phone device before casting a ballot. The vote is then given and saved in the block utilizing the private key in encrypted format. The voter encrypts his/her vote using the election commission's public key, and the commission members decode it using their private keys to verify the votes. Cryptographic processes such as encryption and decryption use asymmetric encryption. This framework includes a method for carrying out operations on encoded data using hash work and a private key. Election officials decode information using square chain hash work calculations by using public keys [41]. All voter information and the vote total will be updated for the election commission on the other end, but for that electoral commission, the data will be encrypted and set up in a cryptosystem.

3.7 ECDSA

ECDSA is one of the more challenging public key encryption techniques. Keys generated by ECC are typically smaller than those generated by digital signature methods. ECC is a form of public key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC is mostly used to generate digital signatures and pseudo-random numbers, among other things. A public key pair and a digital certificate are used as a signature in a digital signature, which is an authentication technique to confirm the sender's or recipient's identity. Two ECC key-pairs are generated by voters throughout the registration procedure. The voter identifies herself/himself to a verifier, who confirms the first key pair, which is the identity key pair, as being hers/his. The voter then secretly registers the second key pair, which is the voting key pair, as being owned by one of the identity keys. Hence, the manner in which this procedure is executed, no one can tell which identity key owns his or her voting key. The voter then uses their voting private key to sign transactions that reflect their votes in the election's contests.

Setup: In the case when $s = 2^m$, pick an elliptic curve N over P_s. Thus, obtain a set of domain parameters for the ECDSA algorithm $DP = (N, P_s, G, n)$ where GC is the curve's generator and n is a large integer that divides s. The choice and verification of ECDSA domain parameters must precisely adhere to the standard for security reasons.

KeyGen: Create a public key depending on the setup phase's domain specifications.

1. Choose a secret key of the form $a \epsilon [1, n-1]$ randomly.
2. Determine the public key using $Z = W_i$.
3. **SigGen:** Use the key generated above to sign a vote V.
4. Choose the random number k between $k \epsilon [1, n-1]$
5. Calculate $kG = (r_1, y_1)$
6. Calculate $a = r \bmod n$
7. Calculate the hash function $h = H(m)$, where H is a one-way function.
8. Calculate $s = k^{-1}(h + ra) \bmod n$
9. r and s make up the tuple of the signature (a, s)

3.8 Verification

The users accept the payload $(a, u) \| v$ and perform the following signature verification:

Verify that the integers a and $u \epsilon [1, n-1]$

Determine $j = H(m)$

Calculate $R = hs^{-1}GC + au^{-1}(mod\ n)$ to confirm the signature.

If $a_1 = a(mod\ n)$, where a_1 is the coordinate of T, then the signature is valid.

3.9 Hashing of blocks in Blockchain

The blockchain is a private record that is partially accessible to all its chain participants. This blockchain has a unique characteristic that makes data recorded inside of it difficult to modify. There are three segments in each square:

1. Data.
2. A hash of the square.
3. The past square hash.

Data: It contains information on popularity trends based on data.
Hash: Known for its reputed performance, it enables stabilization of the hash with a finger impression. When a square is created, its hash code is already determined. If any alterations are found inside the square, the hash code changes. When one needs to identify changes to a square, the hash is helpful. A square is never again a comparison square if the unique finger impression changes. Figure 2 shows the overview diagram of hash functions.

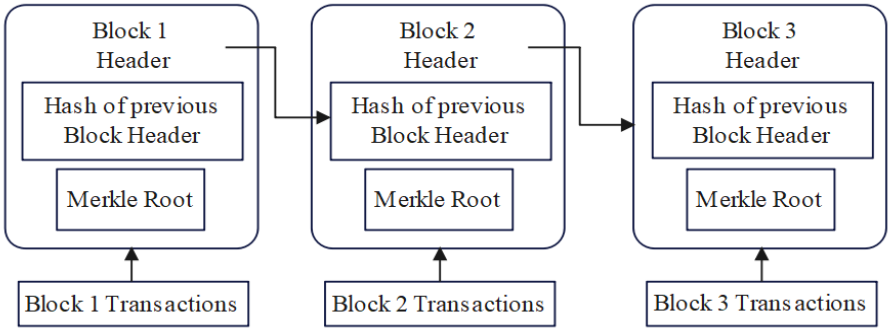

Fig. 2. Hash function

In Figure 2, a new block is initially established after each vote is cast, and a hash is produced utilizing pairs of keys & digital signature. Subsequently, new blocks are continuously created using the prior block's hash by using a hashing algorithm [42]. Using both the private and public keys, a hash is produced. The integrity of the blocks that contain votes and voter data is ensured by this hash.

3.10 Proto Encrypt phase

Executing the proto Encrypt technique is a semi-trusted helping cloud that is familiar with K_2. Proto Encrypt creates the computationally expensive parts of the ciphertext $C_{proto} = \{EP, K_1, K_2,\}$ using an access policy $P \subseteq U, \sigma_k,$ as input. The actions listed below are crucial at this stage:

- Step 1: The semi-trusted supporting cloud determines the access policy $P = p_1, p_2, \ldots\ldots, p_n$ and determines the degree of the polynomial $f(x, P)$ with a maximum of n which is stated at Equation (1):

$$f(x, \mathbb{P}) = \prod_{i=1}^{n} (x + H_4(i))^{1-p_i} \quad (1)$$

where the x^{i}'s coefficient is represented by f_i

- Step 2: The following is then determined by the partially trusted assisting blockchain:

, and $K_{2'} = \prod_{i=o}^{n} (v_i^{f_i}) = h^{K_2 f(\alpha, \mathbb{P})}$ outputs the proto-ciphertext as Equation (2),

$$C_{proto} = \{EP, K_{1'}, K_{2'}\} \quad (2)$$

3.11 Encrypt phase

The encrypt function, which inputs a vote V and outputs the corresponding vote C, performs this phase. There are several steps involved:

- **Step E1:** To acquire $C_{proto} = \{EP, \sigma_k, K_{1'}, K_{2'},\}$ encryption selects at random σ_m, $\sigma_k \in \{0,1\}^{l_6}$ and specifies the access policy (P, σ_k) on a semi-trusted helping blockchain.
- **Step E2:** The encryptor then performs the following calculations.

$r_m = H_1(P, \sigma_m)$, and $R_m = (g^{\alpha})^{r_m} = g^{\alpha r_m}$,

$$K_{1m} = (K_{1'})^{r_m} = h^{K_1 f(\alpha, P) r_m},$$

$$K_{2m} = (K_{2'})^{r_m}) = h^{K_2 f(\alpha, P) r_m},$$

In addition, $C_{\sigma_m} = H_2(e(g,h)^{r_m}) \oplus \sigma_m$ and $C_m = H_3(\sigma_m) \oplus M$.

The ciphertext generated by the encryptor has the following format as expressed in Equation (3):

$$C = \{EP, \sigma_k, R_m, K_{1_m}, K_{2_m}, C_{\sigma_m}, C_m\} \quad (3)$$

3.12 Key Generation

There are many different kinds of cryptographic techniques available. Depending on what kind of algorithms are used, the private and public keys are used to preserve integrity [43]. The document (Vote) is digitally signed in this ECDSA-HCA system using a private key. The public key is utilized by the election commissions to validate the voter's signature on the ballot. When the voter's submitted fingerprint and the fingerprint stored in the database match, a key pair is generated. The digital signature is then created using the fingerprint.

- **KeyGen_k phase**

This step uses the $KeyGen\_k$ method, which is carried out by an attribute authority AA_k, to determine the component keys needed by the KeyGen function. The function is connected to the following actions:

- **Step 1:** As input, a random number r_u yields a partial key s_{u_k} and the contact policy $\{A_{u,k}\}$ for a voter u.
- **Step 2:** The attribute authority AA_k establishes a contact policy $A_{u,k}$ for the voter u.

To calculate, $k \in [1, n]$, the component keys needed by the KeyGen function are determined using Equation (4),
Additionally,
Finally, the output is $\{s_{u_k}, A_{u,k}\}$.

- **KeyGen Phase**

This step uses the $KeyGen\_k$ method, which is carried out by an attribute authority $AA_k k \in [1, N]$ to determine the component keys needed by the $KeyGen$ function.

KeyGen takes the input and returns K_u which is the user u's secret key. There are several steps involved:

- **Step 1:** The controller is selected at random between $r_u \in Z_p$.
- **Step 2:** The controller initiates the below computation via a secure channel for every user attribute authority $AA_k, k \in [1, N]$: $(s_{u_k}. A_{u,k}) = KeyGen_k(\{MSK, MPK\}, r_u)$.
- **Step 3:** In this step, the controller computes $s_u =$ and g^{s_u}. It's important to keep in mind that $s_u = \frac{1}{K_1}\left(\frac{1}{f(\alpha,A)} - K_2.r_u\right)$. The controller additionally determines and generates $K_u = \{A_u, g^{r_u}, g^{s_u}\}$ for the user's secret key.

3.13 Hybrid Consensus Algorithm

A key idea in BCT is consensus and a distributed technology which means that if BCT is used, anyone can join the network. The same data and understanding must be maintained by each node and process. All nodes in a permissioned BCT are familiar with one another, whereas nodes in a permission-less BCT aren't [44]. Due to some malicious nodes failing to adhere to the consensus, voting information may be exposed. With the proposed consensus algorithm, malicious nodes will be predicted and eliminated from the blockchain. It is crucial to eliminate several errors from the E-voting system, such as byzantine, security, crash, software, and temporal errors. If a node in the blockchain exhibits malicious behaviour (attacking), the proof of vote (PoV) algorithm will automatically detect this and remove the offending node from the chain. A consensus is an agreement among nodes that determines whether or not to approve new blocks for the blockchain [45]. The consensus algorithms are divided into two major groups. The first group consists of consensus algorithms based on proofs, and the second category includes methods based on votes. To add a new block to their chain, each node must solve a proof-of-work (PoW) challenge. PoS is an energy-efficient algorithm since it requires less computing power than PoW.

4. Results

This paper provides an illustration of a safe E-voting system based on blockchain. The approach exemplifies how blockchain circumvents the problems with the current voting mechanism. This section discusses the effectiveness of the suggested design paradigm ECDSA-HCA, with various user counts. Until now, users and candidates registered their information with the ECS Server. The ECS then makes some hidden values available for polling through an internet voting server. The user then logs in using an online voting system.

4.1 Performance analysis of Communication and Encryption Time

This section tests the proposed system using a different user from the model. The candidate's common key is produced by the keygen function in accordance with the registration. Within the summing execution of the function, one divisional operation and one modulating operation are performed. Using the candidate common key, ECDSA-HCA verifies and states the vote result. Based on the shared key between the candidates, the ECS [22] will tally the votes. Therefore, the candidate-shared keys are crucial to the functioning of this proposed system model.

Microseconds are used to measure communication time. The results for the proposed ECDSA-HCA are 390µs, 832µs, 1252µs, and 1871µs for 500µs, 1000µs, 1500µs and 2000µs users respectively. Table 1 explains the performance analysis for the communication time of users. Table 2 evaluates the performance analysis of the encryption time.

Table 1. Performance Analysis For Communication Time.

No. of users	Communication time (μs)		
	ECS [22]	ECDSA	Proposed ECDSA-HCA
500	410	392	390
1000	850	833	832
1500	1350	1254	1252
2000	1950	1875	1871

Table 2. Performance Analysis for Encryption Time.

No. of users	Encryption time (μs)		
	ECS [22]	ECDSA	Proposed ECDSA-HCA
500	425	397	395
1000	900	874	872
1500	1200	1113	1111
2000	1800	1652	1650

4.2 Performance analysis of Throughput and Latency

To test the performance, the experimental setup for the suggested ECDSA-HCA model was developed using Python. Finally, the amazon elastic compute cloud (Amazon EC2) was used to run the test simulations. A single entity with two virtual CPUs and four gigabytes of RAM had a simulated network size that ranged from 200 to 1000. By contrasting the throughput and latency of the developed framework with those of the existing ECS [22] and

ECDSA, the test was done to assess the adaptability and efficiency of the suggested ECDSA-HCA.

The proposed ECDSA-HCA model had a latency of about 19 to 24 ms for different users. Table 3 evaluates the comparison of proposed method's latency with those of existing ones. The effectiveness of ECDSA-HCA is much superior when analyzed in par with the conventional models.

Table 3. Comparison of Latency between Proposed and Conventional Methods

No. of users	Latency (ms)		
	PSCBCS [25]	ECDSA	Proposed ECDSA-HCA
200	27	26	19
400	26	25	21
600	28	27	23
800	27.5	27.3	25
1000	27.3	27.1	24

Table 4 demonstrates that the rate at which transactions were handled by ECS and ECDSA did not increase as the number of nodes increased. Nevertheless, the proposed ECDSA-HCA model was able to handle more entries as the number of nodes increased. In comparison to PSCBCS [25] and ECDSA-HCA, whose throughputs were approximately 60 Tps and 61.6 Tps for 1000 users, respectively, when the nodes increased in number upto 1000, the proposed ECDSA- HCA's throughput was 63 Tps for 1000 users. The outcome therefore supports the claim that the ECDSA-HCA technique is extremely scalable.

Table 4. Comparison of throughput between Proposed and Conventional Methods

No. of users	Throughput (Tps)		
	PSCBCS [25]	ECDSA	Proposed ECDSA-HCA
200	10	10.8	12
400	25	25.7	27
600	36	37.2	38.5
800	50	52	53.7
1000	60	61.6	63

4.3 Comparative Analysis

Table 5 shows the comparative analysis of existing PPLE [21] with proposed ECDSA-HCA in terms of throughput and latency. Upto 10,000 transactions, the throughput does not significantly vary at a pace of 200 transactions per second. Above that, throughput typically decreases and latency for read transactions climbs rapidly, while transactions experience a more linear increase in latency.

Table 5. Comparison of Throughput and Latency

No. of Transaction	Throughput (Tps)			Latency (ms)		
	PPLE [21]	Proposed ECDSA-HCA		PPLE [21]	Proposed ECDSA-HCA	
1000	31.4	37.1		11	8	
5000	32.9	37.8		14	10	
10000	34.3	38.6		13	9	

From the Table 5, it clearly shows that proposed ECDSA-HCA achieved better results in all the transactions than the existing PPLE [21]. In the Table 5, the existing PPLE [21] has obtained a throughput of 31.4 Tps, 32.9 Tps and 34.3 Tps for 1000, 5000 and 10000 transactions respectively, and for latency, 11 ms, 14 ms and 13 ms for 1000, 5000 and 10000 transactions respectively. Those results are less effective when compared with proposed ECDSA-HCA method.

5. Discussion

In order to prevent vote fraud during the public disclosure of the polling locations across the country, a secure web E-voting method is established for end-to-end transmission for the users. Three phases make up the ECDSA-HCA: registration, polling, and results disclosure. In the suggested model, the Election Commission searches and verifies vote data on blockchain. Then, using the data structure from the user-differentiated modelling process, the ECDSA-HCA approach enables preserving voter data in the blockchain with encryption and an ECS.

The suggested ECDSA-HCA methods are analyzed in terms of communication, encryption, latency, and throughput.

Additionally, for security purposes, certain protocols limit the quantity of messages that can be signed with a single key. As a result, ongoing key generation is necessary, which uses a lot of processing resources and slows down some blockchain processes. To balance the effectiveness of BCT with key generation and key size difficulties, more research is necessary.

Therefore, to assess its effectiveness, the proposed ECDSA-HCA is contrasted with existing methods such as PPLE [21], ECS [22], PSCBCS [25] and ECDSA. The effectiveness of PPLE [21], ECS [22], PSCBCS [25] and ECDSA are analyzed in terms of communication time, encryption time, latency and throughput.

From the results, the existing PPLE [21] has 34.3 Tps throughput with 11 ms latency for 1000 transactions. While the existing ECS [22], has obtained the output with the communication time and encryption time as 1950 μs and 1800 μs respectively for 2000 users count. At the same time, the existing PSCBCS [25] and ECDSA has attained a throughput of 60 Tps and 61.6 Tps respectively. The proposed ECDSA-HCA strategy outperformed all the existing methods in terms of communication time (1871 s), encryption time (1650 s), latency (24 ms), and throughput (63 Tps).

5.1 Limitations

The risk of errors is increased in BCT, because not all users are proficient with technology, which is a major disadvantage. Data immutability is one of BCT's key drawbacks. There are still obstacles to be addressed before such systems are widely deployed, particularly in terms of increasing their robustness to any flaws. On the other side, privacy protection and transaction speed are the difficulties with blockchain applications that are most frequently raised. Scalability of a blockchain-based E-voting system depends on the security of remote participation being practical and taking transaction speed into account.
Furthermore, it would be intriguing to investigate blockchain-based E-voting with cryptographic techniques that can withstand quantum attacks. The key size needed for cryptosystems, that is typically between 128 and 4096 bits, is bigger than the key size needed for public-key cryptosystems. But the work is not yet complete. In fact, depending on the nature and qualities of the voting, it can always be enhanced. Some enhancements are outlined in the section on future work that comes under next.

6. Conclusion and future work

A secure and reliable voter registration and identification system was proposed. The proposed ECDSA-HCA was implemented in the online E-voting system to ensure secure voting and prevent fraudulent activities. Data was transmitted to users via the cloud without encryption, allowing them to access and verify it. Upon analyzing the results, the proposed ECDSA-HCA was compared to traditional approaches such as ECS and ECDSA to assess its effectiveness. The ECDSA-HCA technique clearly outperformed other methods in terms of communication time (1871 μs), encryption time (1650 μs), latency (24 ms), and throughput (63 Tps). In the future, our aim is to develop an even more secure online voting system, encouraging users to participate in elections while also striving to reduce the time complexity of the online E-voting strategy.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The paper conceptualization, methodology, software, validation, data curation, writing—original draft preparation, writing—review and editing, visualization, have been done by 3rd and 4th author. The supervision and project administration, formal analysis, investigation, resources, have been done by 1st and 2nd author.

References

[1] Wang H, Ma W, Deng F, Zheng H, Wu, Q. Dynamic threshold ECDSA signature and application to asset custody in blockchain. Journal of Information Security and Applications. 2021; 61:102805.

[2] Sun G, Dai M, Sun J, Yu H. Voting-based decentralized consensus design for improving the efficiency and security of consortium blockchain. IEEE Internet of Things Journal. 2021; 8(8):6257-72.

[3] Kara M, Laouid A, Hammoudeh M, AlShaikh M, Bounceur A. Proof of chance: A lightweight consensus algorithm for the internet of things. IEEE Transactions on Industrial Informatics. 2022 Apr 19;18(11):8336-45.

[4] Banerjee S, Roy S, Odelu V, Das AK, Chattopadhyay S, Rodrigues JJPC, Park Y. Multi-authority CP-ABE-based user access control scheme with constant-size key and ciphertext for IoT deployment. Journal of Information Security and Applications. 2020; 53:102503.

[5] Salman SA, Al-Janabi S, Sagheer AM. A Review on E-Voting Based on Blockchain Models. Iraqi Journal of Science. 2022 Mar 30:1362-75.

[6] Zhang S, Wang L, Xiong H. Chaintegrity: blockchain-enabled large-scale E-voting system with robustness and universal verifiability. International Journal of Information Security. 2020; 19(3):323-41.

[7] Yang X, Yi X, Nepal S, Kelarev A, Han F. Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities. Future Generation Computer Systems. 2020; 112:859-74.

[8] Baudier P, Kondrateva G, Ammi C, Seulliet E. Peace engineering: The contribution of blockchain systems to the E-voting process. Technological Forecasting and Social Change. 2021; 162:120397.

[9] Szyjewski G. Keeping the secrecy aspect in mass e-voting. Procedia Computer Science. 2022; 207:4359-68.

[10] Khan KM, Arshad J, Khan MM. Empirical analysis of transaction malleability within blockchain-based E-voting. Computers & Security. 2021; 100:102081.

[11] Sadia K, Masuduzzaman M, Paul RK, Islam A. Blockchain-based secure E-voting with the assistance of smart contract. In IC-BCT 2019: Proceedings of the International Conference on Blockchain Technology 2020 (pp. 161-176). Springer Singapore.

[12] Khan SM, Arshad A, Mushtaq G, Khalique A, Husein T. Implementation of decentralized blockchain E-voting. EAI Endorsed Transactions on Smart Cities. 2020; 4(10):e4.

[13] Mustafa MK, Waheed S. An E-voting framework with enterprise blockchain. In Advances in Distributed Computing and Machine Learning: Proceedings of ICADCML 2020 2021 (pp. 135-145). Springer Singapore.

[14] Díaz-Santiso J, Fraga-Lamas P. E-voting System Using Hyperledger Fabric Blockchain and Smart Contracts. In The 4th Xove TIC Conference 2021; 7(1):11.

[15] Salman SA, Al-Janabi S, Sagheer AM. Valid Blockchain-Based E-Voting Using Elliptic Curve and Homomorphic Encryption. International Journal of Interactive Mobile Technologies. 2022 Oct 15;16(20).

[16] Jumaa MH, Shakir AC. Iraqi E-Voting System Based on Smart Contract Using Private Blockchain Technology. Informatica. 2022; 46(6):87-94.

[17] Chentouf FZ, Bouchkaren S. Security and privacy in smart city: a secure e-voting system based on blockchain. International Journal of Electrical and Computer Engineering. 2023; 13(2):1848-57

[18] Hassan HS, Hassan R, Gbashi EK. E-voting System Based on Ethereum Blockchain Technology Using Ganache and Remix Environments. Engineering and Technology Journal. 2023; 41(4):562-77.

[19] Ali B, Iqbal F, Hussain I, Younas M. An Efficient E-Voting Algorithm and Dapp Using Blockchain Technology. Multidisciplinary International Journal of Research and Development (MIJRD). 2022; 1(03):60-9.
[20] Gupta S, Gupta A, Pandya IY, Bhatt A, Mehta K. End to end secure e-voting using blockchain & quantum key distribution. Materials Today: Proceedings. 2023; 80:3363-70.
[21] Alshehri A, Baza M, Srivastava G, Rajeh W, Alrowaily M, Almusali M. Privacy-Preserving E-voting System Supporting Score Voting Using Blockchain. Applied Sciences. 2023; 13(2):1096.
[22] Shankar A, Pandiaraja P, Sumathi K, Stephan T, Sharma P. Privacy preserving E-voting cloud system based on ID based encryption. Peer-to-Peer Networking and Applications. 2021; 14(4):2399-409.
[23] Rathee G, Iqbal R, Waqar O, Bashir AK. On the design and implementation of a blockchain enabled E-voting application within iot-oriented smart cities. IEEE Access. 2021; 9:34165-76.
[24] Panja S, Roy B. A secure end-to-end verifiable E-voting system using blockchain and cloud server. Journal of Information Security and Applications. 2021; 59:102815.
[25] Abuidris Y, Kumar R, Yang T, Onginjo J. Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. ETRI Journal. 2021; 43(2):357-70.
[26] González CD, Mena DF, Muñoz AM, Rojas O, Sosa-Gómez G. Electronic voting system using an enterprise blockchain. Applied Sciences. 2022; 12(2):531.
[27] Ahn B. Implementation and early adoption of an ethereum-based electronic voting system for the prevention of fraudulent voting. Sustainability. 2022; 14(5):2917.
[28] Ch R, Kumari D J, Gadekallu TR, Iwendi C. Distributed-ledger-based blockchain technology for reliable electronic voting system with statistical analysis. Electronics. 2022; 11(20):3308.
[29] Neziri V, Shabani I, Dervishi R, Rexha B. Assuring Anonymity and Privacy in Electronic Voting with Distributed Technologies Based on Blockchain. Applied Sciences. 2022; 12(11):5477.
[30] Alvi ST, Uddin MN, Islam L, Ahamed S. 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. 2022; 34(9):6855-71.
[31] Rakshitha CM, Hiremani N, Nataraj KR. Hybrid Secure Algorithms and Optimal Blockchain to Ensure E-Voting Data Immutability at Cloud. International Journal of Intelligent Systems and Applications in Engineering. 2023 Jul 16;11(3):721-30.
[32] Chaudhary S, Shah S, Kakkar R, Gupta R, Alabdulatif A, Tanwar S, Sharma G, Bokoro PN. Blockchain-based Secure Voting Mechanism Underlying 5G Network: A Smart Contract Approach. IEEE Access. 2023; 11:76537-50.
[33] Pereira BMB, Torres JM, Sobral PM, Moreira RS, Soares CPA, Pereira I. Blockchain-Based Electronic Voting: A Secure and Transparent Solution. Cryptography. 2023; 7(2):27.
[34] Chatterjee U, Ray S, Adhikari S, Khan MK, Dasgupta M. Efficient and secure e-voting scheme using elliptic curve cryptography. Security and Privacy. 2023; 6(3):e283
[35] Farooq MS, Iftikhar U, Khelifi A. A framework to make voting system transparent using blockchain technology. IEEE Access. 2022; 10:59959-69.
[36] Toma C, Popa M, Boja C, Ciurea C, Doinea M. Secure and Anonymous Voting D-App with IoT Embedded Device Using Blockchain Technology. Electronics. 2022; 11(12):1895.
[37] Danwar SH, Mahar JA, Kiran A. A Framework for e-Voting System Based on Blockchain and Distributed Ledger Technologies. Computers, Materials & Continua. 2022; 72(1):414-440.
[38] Rao KV, Panda SK. Secure electronic voting (E-voting) system based on blockchain on various platforms. In Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021, Volume 2 2022 Oct 5 (pp. 143-151). Singapore: Springer Nature Singapore.
[39] Tanwar S, Gupta N, Kumar P, Hu YC. Implementation of blockchain-based e-voting system. Multimedia Tools and Applications. 2023.
[40] Sallal M, de Fréin R, Malik A. PVPBC: Privacy and Verifiability Preserving E-Voting Based on Permissioned Blockchain. Future Internet. 2023; 15(4):121.
[41] Anitha V, Caro OJM, Sudharsan R, Yoganandan S, Vimal M. Transparent voting system using blockchain. Measurement: Sensors. 2023; 25:100620.
[42] Tang W, Yang W, Tian X, Yuan S. Distributed Anonymous e-Voting Method Based on Smart Contract Authentication. Electronics. 2023; 12(9):1968.
[43] Chaabane F, Ktari J, Frikha T, Hamam H. Low power blockchained e-vote platform for university environment. Future Internet. 2022; 14(9):269.
[44] Kho YX, Heng SH, Chin JJ. A review of cryptographic electronic voting. Symmetry. 2022; 14(5):858.
[45] Diaconita V, Belciu A, Stoica MG. Trustful Blockchain-Based Framework for Privacy Enabling Voting in a University. Journal of Theoretical and Applied Electronic Commerce Research. 2023; 18(1):150-69.

V. Padmavathi holds a Bachelor of Engineering degree in Computer Science and Engineering (CSE) discipline. She completed her M. Tech. and Ph. D in CSE discipline. She works as an Associte Professor in Chaitanya Bharathi Institute of Technology, Hyderabad. Her research areas include Quantum Computing and Cryptography, Classical Cryptography and Information Security, Algorithms, Software Engineering, Data Mining, Machine Learning, Quantum Machine Learning. Dr. Padmavathi has three patents and several International publications to her credit. She has conducted various FDPs, workshops, bridge courses. She is a Program Committee member and reviewer for several International Conferences.
Email: padmareddyvch@ieee.org

C. N. Sujatha, accomplished B.Tech (Electronics & Communication Engineering, 2001), M.Tech (Electronic Instrumentation and Communication Systems, 2005) and Ph.D. (Image Processing, 2018) from S.V. University, Tirupati, A.P, India. She started her career in 2001 as a lecturer in Annamacharya Institute of Science and Technology at kadapa. Presently associated with Sreenidhi Institute of Science and Technology, Hyderabad, Telangana as a Professor, Dept. of ECE. She has presented 18 papers in International and National conferences and published 37 papers in international journals. Her current research interests include Image & Video Processing, Speech & Signal Processing, Machine learning, Deep Learning, Quantum Computing and Antenna Design. She has guided several UG and PG projects, encouraged many of her students to publish papers in reputed journals. She has written 3 books and published 3 patents.

Email: cnsujatha@gmail.com

Mutha Jayanth Kumar is an undergraduate student in the department of Computer Science and Engineering, Anurag University, Venkatapur, Hyderabad, Telangana, India. The author has published a paper on Hybrid Cryptography. His area of interest are Blockchain, Web Development, Android Development.
Email: mutha.jayanth@gmail.com

Saikiran Reddy Medhimale is pursuing undergraduate specialising in Computer Science and Engineering from Anurag University, Venkatapur, Hyderabad, Telangana, India. His areas of interest are Cloud Computing, Blockchain and Web Development.
Email: saikiran.medhimale@gmail.com