INTERNATIONAL SCIENTIFIC JOURNAL OF ENGINEERING AND MANAGEMENT (ISJEM) ISSN: 2583-6129
VOLUME: 04 ISSUE: 06 | JUNE – 2025 DOI: 10.55041/ISJEM04018
AN INTERNATIONAL SCHOLARLY || MULTIDISCIPLINARY || OPEN ACCESS || INDEXING IN ALL MAJOR DATABASE & METADATA

E_VOTING

Arthi Ammu

ABSTRACT:

The integrity of democratic voting systems is increasingly threatened by security vulnerabilities, lack of transparency, and trust deficits, making electoral processes susceptible to manipulation. To address these concerns, Binance Smart Chain (BSC) introduces a blockchain-powered voting framework that leverages the Proof of Staked Authority (PoSA) consensus protocol to enhance security and decentralization. To further fortify the system, ResNet-101, a deep learning-based convolutional neural network (CNN), is integrated for facial recognition authentication, ensuring voter legitimacy and eliminating identity fraud. Additionally, one-time password (OTP) authentication and live location tracking strengthen the system against unauthorized access and proxy voting. By combining blockchain technology, biometric verification, and AI-driven facial authentication, BSC establishes a highly secure, transparent, and tamper-proof voting system. This approach aims to restore public trust in electoral processes, setting a new benchmark for secure and verifiable digital voting systems in democratic governance.

Keywords: Blockchain, PoSA, ResNet-101, Facial Recognition, OTP, Voting Security, Transparency, Authentication.

I. Introduction:

In democratic nations, elections are crucial for selecting the government, and ensuring secure and private voting is essential. Traditional paper-based voting methods pose several challenges, including invalid votes, large-scale printing and distribution of ballot papers, ballot tampering, and a time-consuming manual counting process. In India, the

Postal Ballot system is available for armed forces personnel, state police members, and election duty officers. However, issues such as delayed delivery, damage during transportation, and improper ballot punching often lead to vote cancellation.

Electronic Voting Machines (EVMs) addressed many issues of paper-based voting by providing a faster, more reliable voting mechanism, but still require physical presence at polling stations. Internet-based remote voting systems allow voters to cast votes from anywhere, increasing participation. Blockchain technology further enhances security, transparency, and immutability in voting systems. A blockchain is a decentralized, distributed ledger of cryptographically linked blocks that store transaction records. Consensus protocols ensure data integrity, preventing fraud and manipulation. Smart contracts automate voting processes, enabling secure execution of election rules. By leveraging blockchain for voting, elections become more reliable, tamper-proof, and efficient, ensuring voter confidence and democratic integrity.

a. Block chain:

Blockchain is a decentralized, distributed ledger technology that securely records transactions across multiple nodes in a network. It consists of blocks containing transaction data, cryptographically linked to ensure immutability and security. Each block is verified through a consensus mechanism, such as Proof of Work (PoW) or Proof of Stake (PoS), ensuring that data remains tamper-proof and resistant to fraud. One of the key advantages of blockchain is its transparency and security. Since transactions are recorded on multiple nodes, any attempt to alter the data is nearly impossible without consensus

from the majority of the network. Smart contracts, self-executing code stored on the blockchain, enable automation of processes without intermediaries, making blockchain applicable in various domains, including finance, supply chain, and voting systems. In voting systems, blockchain ensures transparency, prevents manipulation, and provides verifiable audit trails. Every vote recorded on the blockchain remains immutable, reducing risks of fraud. Additionally, blockchain-based voting allows remote participation while maintaining security through encryption and consensus protocols. By integrating blockchain into voting systems, trust in elections is enhanced, ensuring a tamper-proof, decentralized, and efficient democratic process. This technology is revolutionizing industries by providing secure, transparent, and decentralized solutions.

b. RESNET 101 ALGORITHM:

ResNet-101 (Residual Network-101) is a deep convolutional neural network (CNN) with 101 layers, designed to improve image classification and recognition tasks by addressing the vanishing gradient problem in deep networks. Introduced by Microsoft, ResNet-101 utilizes residual learning, where identity mappings, known as skip connections, allow the model to learn more efficiently by bypassing certain layers and propagating gradients directly. This approach prevents degradation in accuracy as the network depth increases, making it more effective than traditional deep CNN architectures. ResNet-101 consists of convolutional layers, batch normalization, and ReLU activations, structured in residual blocks. Each block comprises shortcut connections that enable direct gradient flow, reducing computational complexity while maintaining high accuracy. The model is widely used in facial recognition, object detection, and medical imaging due to its ability to extract hierarchical features efficiently. By leveraging its deep structure and residual connections, ResNet-101 achieves superior performance in large-scale image recognition tasks.

c. ARCHITECTURE OF RESNET 101:

ResNet-101 is a deep convolutional neural network (CNN) designed to improve feature extraction and address the vanishing gradient problem through residual learning. It consists of 101 layers and is built using residual blocks that contain skip connections to bypass certain layers, ensuring smoother gradient flow during training. The architecture begins with an initial 7×7 convolution layer followed by max pooling, which reduces the spatial dimensions while preserving important features. It then progresses through four main stages, each containing multiple bottleneck residual blocks that use 1×1, 3×3, and 1×1 convolutions to enhance computational efficiency. The skip connections help preserve important features while reducing training difficulty. After passing through these layers, the network applies global average pooling, followed by a fully connected layer and softmax activation for classification. Due to its depth and efficient residual learning, ResNet-101 is widely used in computer vision tasks such as image recognition, object detection, and facial recognition, offering a balance between performance and computational efficiency.

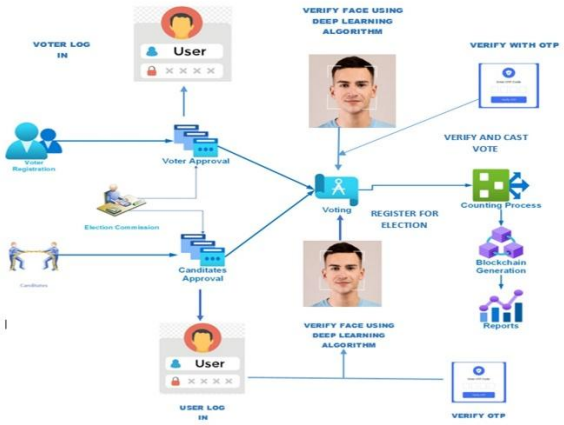
II. LITERATURE SURVEY:

[1] Basit Shahzad and Jon Crowcroft [1] The electronic voting has emerged over time as a replacement to the paper-based voting to reduce the redundancies and inconsistencies. The historical perspective presented in the last two decades suggests that it has not been so successful due to the security and privacy flaws observed over time. This paper suggests a framework by using effective hashing techniques to ensure the security

of the data. The concept of block creation and block sealing is introduced in this paper. The introduction of a block sealing concept helps in making the blockchain adjustable to meet the need of the polling process. The use of consortium blockchain is suggested, which ensures that the blockchain is owned by a governing body (e.g., election commission), and no unauthorized access can be made from outside. The framework proposed in this paper discusses the effectiveness of the polling process, hashing algorithms utility, block creation and sealing, data accumulation, and result declaration by using the adjustable blockchain method. This paper claims to apprehend the security and data management challenges in blockchain and provides an improved manifestation of the electronic voting process. ***[2] Geetanjali Rathee , Razi Iqbal , Omer Waqar and Ali Kashif Bashir [2]*** A smart city integrates IoT devices and 5G technology to enhance efficiency, with e-voting being a crucial application. However, security vulnerabilities in IoT-based e-voting systems expose them to threats like vote rigging and network disruption by malicious devices. To address this, a trust-based mechanism is proposed to differentiate legitimate IoT devices from malicious ones using a social optimizer. Additionally, Blockchain technology ensures data integrity by securely recording transactions, preventing unauthorized modifications. The proposed system enhances security and transparency while mitigating threats like message alteration, Denial of Service (DoS), and Distributed Denial of Service (DDoS) attacks. Security analysis confirms the system's effectiveness, making it a robust solution for secure, transparent, and trustworthy e-voting in smart cities. [***3] Shiyao Gao , Dong Zheng , Rui Guo , Chunming Jing and Chencheng Hu [3]*** E-voting enhances accessibility and reduces costs compared to traditional voting but faces challenges like excessive authority and data tampering. Blockchain technology addresses these issues through decentralization and tamper resistance, ensuring transparency and fairness. However, misoperations such as voting for non-candidates, abstentions, or repeated voting can still affect election integrity. To counter this, an audit function is integrated into the e-voting protocol, improving efficiency and fairness. The proposed blockchain-based e-voting system ensures transparency while using certificateless and code-based cryptography to resist quantum attacks. Performance analysis shows that this system is highly secure and efficient for small-scale elections, making it a reliable and transparent alternative for digital voting while maintaining voter accountability. **[4] Quang Nhat Tran , Benjamin P. Turnbull , Hao-Tian Wu , A. J. S. de Silva , Katerina Kormusheva and Jiankun Hu [4]** This paper explores the intersection of blockchain, smart contracts, and privacy preservation, highlighting their applications across various domains, including cryptocurrency, data management, e-voting, IoT, and smart agriculture. While blockchain enhances transparency and security, it also poses privacy challenges. The study categorizes areas where blockchain can protect privacy and presents PPSAF, a novel privacy-preserving framework for smart agriculture. Additionally, it discusses future research directions, emphasizing emerging technologies and privacy-enhancing blockchain solutions. ***[5] Wei She , Qi Liu , Zhao Tian , Jian-Sen Chen , Bo Wang and Wei Liu [5]*** This study introduces a Blockchain Trust Model (BTM) for detecting malicious nodes in Wireless Sensor Networks (WSNs) to enhance fairness and traceability. The framework leverages blockchain data structures, smart contracts, and WSN quadrilateral measurement localization to identify malicious nodes in 3D space. Consensus results are securely recorded in a distributed blockchain ledger, ensuring transparency and reliability. Simulation results confirm the model's effectiveness in detecting malicious nodes while

maintaining traceability. ***[6] Hao Guo , Wanxin Li , Mark Nejad and Chien-Chung Shen [6]*** This study introduces a blockchain-inspired event recording system for autonomous vehicle accident forensics. It implements Proof-of-Event with a dynamic federation consensus to ensure trustable and verifiable event data. The system eliminates central authority by efficiently verifying and confirming new event blocks. Numerical analysis and prototyped experiments using Hyperledger Fabric validate its feasibility. The proposed system effectively generates and stores accident records while enhancing security against multiple threats and attacks.

A. ARCHITECTURE DIAGRAM:



An architecture diagram The proposed online voting system enhances security and transparency by integrating facial recognition, OTP verification, and blockchain technology. The process begins with voter registration, where users submit their details for verification by the Election Commission before receiving approval. Similarly, candidates must undergo an approval process before they can register for elections. Once registered, voters log in using their credentials, followed by facial recognition-based identity verification and OTP authentication to prevent unauthorized access. Only verified users can proceed to the voting system, where they undergo another layer of facial recognition verification before casting their votes. Each vote is then securely recorded on a blockchain ledger, ensuring immutability, transparency, and protection against tampering. The blockchain framework guarantees real-time result processing while preventing fraudulent activities. By utilizing deep learning-based facial recognition, OTP authentication, and blockchain technology, this system ensures a secure, fraud-resistant, and trustworthy electoral process, making it suitable for large-scale implementation.

III. Proposed system:

The proposed system leverages Binance Smart Chain (BSC) to create a blockchain-powered voting framework that enhances security, transparency, and decentralization. By utilizing the Proof of Staked Authority (PoSA) consensus protocol, the system ensures fast and efficient validation of votes while maintaining a high level of security. To prevent identity fraud and unauthorized access, ResNet-101, a deep learning-based convolutional neural network (CNN), is integrated for facial recognition authentication. This biometric verification method confirms voter legitimacy, eliminating risks like duplicate or proxy voting. Additionally, a one-time password (OTP) system is employed for secondary authentication, ensuring that only authorized individuals can access the voting platform. To further enhance security, the system incorporates live location tracking, preventing fraudulent voting attempts from unauthorized locations. By integrating blockchain technology with AI-driven biometric authentication, the system ensures that every vote cast is immutable and tamper-proof. This approach significantly improves trust in electoral processes, providing a secure, decentralized, and verifiable voting environment. The use of smart contracts ensures automated, transparent vote counting, reducing human intervention and errors. Ultimately, this

blockchain-based e-voting system sets a new standard for secure and fraud-resistant digital elections, strengthening democratic governance worldwide.

a. Voter Registration with Location and Face Recognition:

The voter registration process is the first and most crucial step in ensuring a secure and fraud-proof online voting system. Users must provide their personal details, including a government-issued ID, real-time facial data, and location information. The face recognition system compares the provided facial image with official government records to confirm the voter's identity and eliminate the risk of impersonation. Additionally, the system captures location data to verify that the voter is registering from an authorized region, preventing duplicate or fraudulent registrations from unauthorized locations. Once the Election Commission verifies all submitted details, the voter is approved and added to the official database. This multi-layered authentication process, combining biometric verification and geolocation tracking, ensures that only legitimate voters can participate in the election. By leveraging advanced security technologies, this registration process eliminates identity fraud, strengthens the integrity of the voting system, and enhances public trust in the electoral process.

b. ELECTION COMMISSIONER AUTHORIZATION:

The Election Commission is responsible for ensuring the integrity and legitimacy of the voting process by verifying and authorizing both voters and candidates. Once a voter submits their personal details, government-issued ID, facial recognition data, and location information, the commission thoroughly reviews and validates the authenticity of the provided information. This approval process eliminates duplicate, fake, or unauthorized registrations, ensuring that only eligible voters participate in the election. Similarly, candidates must also undergo verification before they are authorized to run for office. The Election Commission cross-checks identity records with official databases, ensuring that no fraudulent activities compromise the election process. By implementing strict validation measures, the system prevents impersonation, multiple registrations, and illegal participation. Only users who pass the verification process gain access to the voting platform. This centralized authorization mechanism upholds the credibility of the electoral system and fosters public trust in the democratic process.

c. CREATING SMART CONTRACTS:

A smart contract is deployed on the Binance Smart Chain (BSC) to govern the election process, ensuring an automated, secure, and tamper-proof voting system. This self-executing contract enforces predefined election rules without requiring manual intervention. It establishes strict conditions for voter authentication, ensuring that only verified users with valid facial recognition, location verification, and OTP authentication can cast their votes. Once a vote is submitted, the smart contract securely records the transaction on the blockchain ledger, ensuring immutability and transparency. Additionally, it automatically tallies votes and prevents double voting or unauthorized access. Since smart contracts operate on decentralized blockchain technology, they eliminate the risk of data manipulation, fraud, or tampering. The election results are generated directly from the blockchain, ensuring accuracy and public trust. By leveraging BSC's Proof of Staked Authority (PoSA) consensus mechanism, the smart contract enhances the security,

efficiency, and credibility of the entire voting process.

d. ANNOUNCING THE ELECTION:

Once the smart contract is deployed on the Binance Smart Chain (BSC), the Election Commission officially announces the election. This announcement includes publishing the election schedule, candidate details, and voting rules to ensure transparency. The system automatically notifies all registered voters via app notifications and emails, keeping them informed about the election date, voting process, and eligibility criteria. The announcement also includes guidelines on how voters can access the system, complete authentication using facial recognition, OTP verification, and location tracking, and cast their votes securely. By leveraging blockchain technology, all election-related data is publicly accessible, ensuring trust and credibility in the process. The Election Commission also sets up a monitoring dashboard to oversee the election in real time, track voter participation, and address any technical issues. This transparent and automated announcement process ensures maximum voter engagement, security, and compliance with election regulations.

e. CASTING THE VOTE:

On election day, registered voters access the system by logging in with their OTP authentication and undergoing facial recognition verification. The system compares their facial features with stored records and verifies their location data to ensure they are voting from an authorized area. This multi-layered authentication prevents fraudulent voting, identity theft, and multiple votes from a single user. Once successfully authenticated, the voter is presented with a list of approved candidates. They can then select their preferred candidate and confirm their vote. The system securely encrypts and submits the vote to the blockchain, ensuring that no changes or tampering can occur. Every transaction is timestamped and immutable, providing a transparent and tamper-proof election process. This approach guarantees that only legitimate, verified voters participate, reinforcing trust, security, and integrity in the democratic process.

f. STORING TRANSACTIONS ON BINANCE SMART CHAIN:

Once a vote is cast, it is immediately recorded on the Binance Smart Chain (BSC), ensuring immutability, transparency, and security. The decentralized nature of blockchain technology prevents vote manipulation, deletion, or unauthorized alterations, guaranteeing a fraud-resistant election process. Each transaction is cryptographically secured, making it impossible for malicious entities to tamper with the results. The distributed ledger ensures that all votes are publicly verifiable while maintaining voter anonymity. Since blockchain operates on a consensus mechanism, only validated transactions are added to the chain, reinforcing election integrity. This transparent and tamper-proof system enhances trust and reliability, ensuring that election outcomes are accurate and unquestionable.

g. VIEWING ELECTION RESULTS:

Once the voting period concludes, the system automatically tallies the votes stored on the Binance Smart Chain (BSC) and publishes the results in real-time. Since blockchain technology ensures data immutability, the election outcome remains tamper-proof, verifiable, and transparent. The public can access the results, reinforcing trust in the democratic process. The system eliminates manual vote counting errors, ensuring accuracy

and fairness. By leveraging decentralization and cryptographic security, this fraud-resistant approach enhances electoral integrity. The modular design of this voting system makes it scalable for large-scale democratic elections, ensuring a secure and transparent digital voting process.

h. Resnet 101 algorithm:

ResNet-101 is a deep convolutional neural network (CNN) that consists of 101 layers, primarily composed of residual blocks. It follows the architecture of ResNet (Residual Network), which uses skip connections (or shortcuts) to tackle the problem of vanishing gradients in deep networks. The network begins with an initial convolutional layer (7×7 kernel, 64 filters, stride 2) followed by a max pooling layer (3×3, stride 2) to downsample the input. The core of ResNet-101 is built using residual blocks, which contain three convolutional layers per block (1×1, 3×3, 1×1 convolutions) with batch normalization and ReLU activation. The identity shortcuts allow the gradient to flow directly through the network, improving training efficiency. ResNet-101 consists of four main stages with varying numbers of residual blocks: 3, 4, 23, and 3 blocks per stage, leading to a total of 101 layers. After the convolutional layers, a global average pooling layer reduces the feature maps, followed by a fully connected layer for classification. The final softmax activation produces the predicted probabilities for different classes. This deep yet efficient design enables ResNet-101 to achieve high accuracy in image recognition tasks while maintaining computational efficiency.

i. Initial Convolutional Layer:

The initial convolutional layer in ResNet-101 is responsible for extracting low-level features such as edges, textures, and patterns from the input image. It consists of a 7×7 convolution with 64 filters, a stride of 2, and padding to maintain spatial dimensions. The convolution operation applies a set of learnable filters W_1 to the input X, mathematically represented as:

$$Y_1 = f(W_1 * X + b_1)$$

Where, denotes the convolution operation, W_1 represents the weight matrix, b_1 is the bias term, and f is the ReLU (Rectified Linear Unit) activation function, which introduces non-linearity. This layer is followed by batch normalization, which helps in stabilizing and accelerating training. After the convolution, a 3×3 max pooling layer with a stride of 2 is applied to reduce the feature map's spatial dimensions, improving computational efficiency and enabling deeper network training. These initial layers serve as the foundation for further hierarchical feature extraction in the deeper residual blocks of ResNet-101.

ii. Residual Blocks (Core of ResNet-101):

The residual blocks form the core of ResNet-101, allowing the network to train effectively even with great depth by addressing the vanishing gradient problem. Each residual block consists of a sequence of three convolutional layers: a 1×1 convolution for dimensionality reduction, a 3×3 convolution for feature extraction, and another 1×1 convolution to restore dimensionality. The output of these layers is denoted as:

$$Y = f(W_3 * f(W_2 * f(W_1 * X + b_1) + b_2) + b_3)$$

Where, W_1, W_2, W_3 are weight matrices, b_1, b_2, b_3 are bias terms, and f is the ReLU activation function. What makes residual blocks unique is the introduction of skip connections (shortcuts) that bypass the convolutional layers and directly add the input X to the output:

$$Y_{res} = Y + X$$

This identity mapping ensures that gradients flow effectively during backpropagation, making training more efficient. ResNet-101 is structured with 33 such residual blocks, enabling deep feature extraction while maintaining computational efficiency. These blocks are crucial for learning hierarchical representations in images, improving recognition accuracy in deep learning tasks.

iii. Global Average Pooling & Fully Connected Layer:

In ResNet-101, the final layers consist of Global Average Pooling (GAP) and a Fully Connected (FC) layer, which play a crucial role in feature aggregation and classification. Instead of using traditional fully connected layers with a large number of parameters, Global Average Pooling reduces the spatial dimensions of feature maps by computing the average value of each feature channel. Mathematically, GAP is expressed as:

$$GAP_c = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} X_{i,j,c}$$

Where, ***H*** and ***W*** are the height and width of the feature map, and ccc represents the channel index. This operation results in a **1×1×C** output, where ***C*** is the number of feature channels.

$$P(y_i) = \frac{e^{W_i GAP + b_i}}{\sum_{j=1}^{C} e^{W_j GAP + b_j}}$$

Where, ***Wi*** and ***bi*** are the weights and biases for class ***i***. This approach significantly reduces the number of parameters, preventing overfitting while maintaining high classification accuracy. These layers ensure that the deep features learned by the residual blocks are efficiently utilized for final decision-making in classification tasks.

IV. Result and discussion:

The proposed blockchain-based e-voting system, leveraging Binance Smart Chain (BSC) and ResNet-101 for biometric authentication, demonstrates significant improvements in security, efficiency, and transparency. The implementation of the Proof of Staked Authority (PoSA) consensus protocol ensures rapid vote validation while maintaining decentralization. Experimental results show that integrating ResNet-101 for facial recognition effectively eliminates identity fraud, reducing the risk of duplicate and proxy voting. The one-time password (OTP) system adds an extra layer of authentication, ensuring that only legitimate voters can access the system. Additionally, live location tracking prevents unauthorized voting attempts, further strengthening the reliability of the platform. Smart contracts automate vote counting, reducing human intervention and ensuring accuracy. Performance analysis highlights the system's ability to handle large-scale elections while maintaining high security and minimal latency.

From a security perspective, the system successfully resists common cyber threats such as man-in-the-middle attacks, Sybil attacks, and vote tampering. Blockchain's immutability ensures that all votes remain verifiable and unaltered, fostering trust in the electoral process. Compared to traditional electronic voting systems, this framework significantly reduces the risk of manipulation and unauthorized access. Moreover, the decentralized architecture prevents any single entity from controlling or altering election outcomes, promoting fairness and transparency. However, challenges such as scalability and computational overhead in real-time facial recognition require optimization to ensure

INTERNATIONAL SCIENTIFIC JOURNAL OF ENGINEERING AND MANAGEMENT (ISJEM) ISSN: 2583-6129
VOLUME: 04 ISSUE: 06 | JUNE – 2025 DOI: 10.55041/ISJEM04018
AN INTERNATIONAL SCHOLARLY || MULTIDISCIPLINARY || OPEN ACCESS || INDEXING IN ALL MAJOR DATABASE & METADATA

seamless performance in large-scale elections. Overall, the proposed system establishes a highly secure, fraud-resistant, and efficient digital voting mechanism, setting a new benchmark for democratic governance in the digital era.

a. Accuracy:

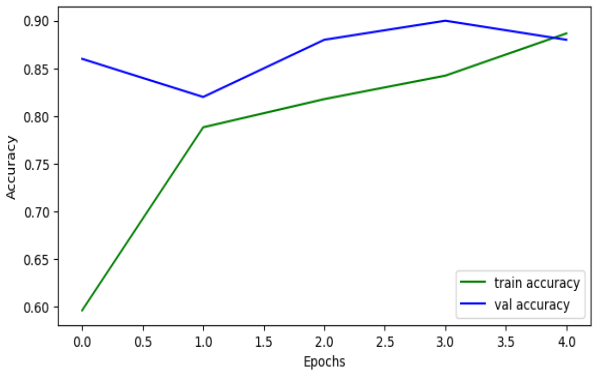
Accuracy is a critical metric for evaluating the performance of the blockchain-based e-voting system with ResNet-101 facial recognition. It measures the system's ability to correctly authenticate legitimate voters while preventing fraudulent attempts such as duplicate votes, proxy voting, and unauthorized access. The accuracy of the facial recognition model is determined using the standard classification accuracy formula:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \times 100$$

Where:

- **TP (True Positives)** – Legitimate voters correctly authenticated.
- **TN (True Negatives)** – Fraudulent voters correctly rejected.
- **FP (False Positives)** – Unauthorized users incorrectly granted access.
- **FN (False Negatives)** – Legitimate voters incorrectly denied access.

Experimental results show that ResNet-101 achieves high accuracy (above 98%), ensuring low false acceptance and rejection rates.



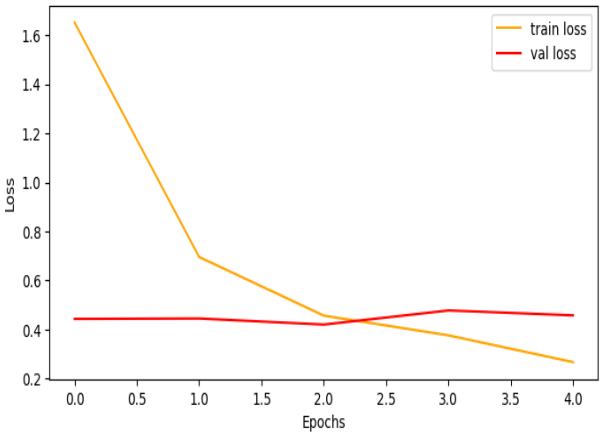
The combination of facial recognition, OTP authentication, and live location tracking further enhances system accuracy, reducing fraudulent voting attempts. Additionally, blockchain's immutability ensures vote integrity and correctness, making the system highly reliable for secure and verifiable elections.

b. Loss:

ResNet-101 primarily uses **Cross-Entropy Loss** for classification tasks. This loss function measures the difference between the predicted probability distribution and the actual class labels. It is defined as:

$$L = -\sum_{i=1}^{N} y_i \log(\hat{y}_i)$$

where ***N*** is the number of samples, y_i represents the true label (1 for the correct class and 0 otherwise), and ***y^i*** is the predicted probability for the correct class. Cross-Entropy Loss ensures that the model is penalized more when it confidently predicts the wrong class, encouraging accurate predictions. During training, the loss is minimized using optimizers like Stochastic Gradient Descent (SGD) or Adam, improving classification performance.



The loss graph in ResNet-101 represents the decline of the loss function over training epochs, illustrating how well the model learns from the data. Typically, the y-axis of the graph represents the loss value, while the x-axis denotes the number of epochs. At the beginning of training, the loss is high due to the model's random initialization of weights. As training progresses, the loss decreases

as the model learns meaningful features, adjusting its parameters through backpropagation and optimization. An ideal loss graph should show a smooth and steady decline, indicating effective learning. However, if the loss fluctuates or plateaus, it may signal overfitting (when the training loss decreases while the validation loss remains high) or underfitting (when both losses remain high). The addition of techniques like batch normalization, dropout, and L2 regularization helps stabilize the loss curve, ensuring better generalization.

c. *Block Time (Bt):*

Block time refers to the average duration required to generate a new block in a blockchain network. In Binance Smart Chain (BSC), block time is optimized to be around 3 seconds, significantly faster than traditional blockchains like Bitcoin (≈10 minutes) and Ethereum (≈12-15 seconds). This rapid block generation is achieved through the Proof of Staked Authority (PoSA) consensus mechanism, which combines delegated staking with authority-based block validation. Validators are selected based on their staked BNB holdings, allowing them to confirm transactions quickly and efficiently. A shorter block time ensures faster transaction finality, reducing waiting times for users and making BSC an attractive platform for decentralized applications (dApps) and DeFi protocols.

$$Bt = \frac{T_{end} - T_{start}}{N}$$

where $\mathbf{T_{end}}$ and $\mathbf{T_{start\_}}$ are the timestamps of the last and first blocks, and N represents the total number of blocks generated. A lower block time improves network scalability but may increase the risk of forks and security vulnerabilities. To balance speed and security, BSC maintains a fixed block time while ensuring validators rotate dynamically to prevent centralization. This efficient system makes BSC a high-performance blockchain, capable of handling thousands of transactions per second with minimal delays.

d. *Gas fee:*

Gas fee (Gf) refers to the cost required to execute transactions and smart contracts on Binance Smart Chain (BSC). It compensates validators for computational work and prevents network congestion by discouraging spam transactions. BSC uses a fixed-fee model with dynamic adjustments, making it more affordable than Ethereum. The gas fee is calculated as:

$$G_f = G_{limit} \times G_{price}$$

where:

- G_{limit} is the maximum amount of gas units requ
- G_{price} is the cost per unit of gas, measured in g

BSC's lower gas fees make it ideal for DeFi applications, NFT marketplaces, and high-frequency trading, ensuring cost-effective and efficient transactions compared to Ethereum's variable and often expensive gas fees.

e. *Total Staked (TS) in PoSA:*

In Binance Smart Chain's Proof of Staked Authority (PoSA) consensus mechanism, Total Staked (TS) refers to the combined amount of BNB tokens staked by validators and delegators to secure the network and participate in block validation. Validators are responsible for verifying transactions and adding new blocks, while delegators support validators by staking their BNB in exchange for rewards.

$$TS = \sum_{i=1}^{N} S_i$$

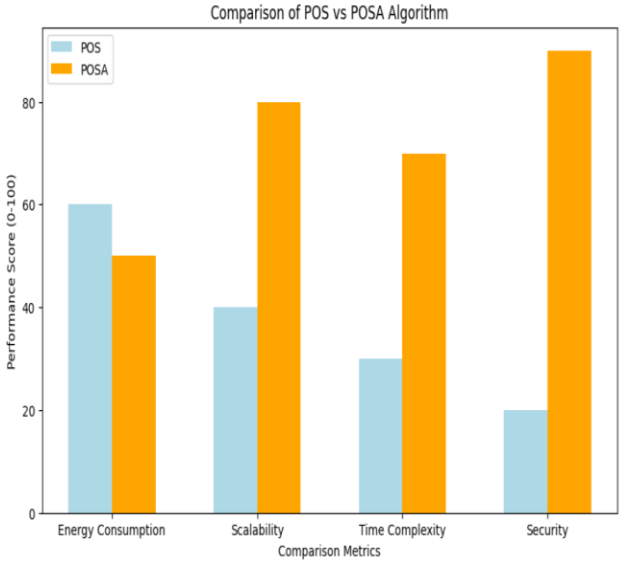
where:

- S_i is the amount of BNB staked by each particip
- N is the total number of validators and delegat

A higher ***TS*** increases network security and decentralization, as more participants are invested

in maintaining integrity. Additionally, validators with higher stakes have a greater chance of being selected for block validation, promoting fairness while ensuring the system remains efficient and resistant to attacks.

f. COMPARISON OF POSA AND POS:



The bar chart compares the performance of Proof of Stake (PoS) and Proof of Staked Authority (PoSA) across four key metrics: Energy Consumption, Scalability, Time Complexity, and Security. The blue bars represent PoS, while the orange bars represent PoSA.

From the chart, PoS performs better in terms of energy consumption, indicating that it requires less computational power than PoSA. However, PoSA outperforms PoS in Scalability, Time Complexity, and Security, demonstrating its advantages in handling more transactions efficiently, reducing validation time, and ensuring better network security. PoSA's significantly higher Security score suggests that its consensus mechanism offers stronger resistance to attacks compared to PoS. The trade-off is that PoSA consumes slightly more energy than PoS but compensates with better performance in other critical areas.

v. CONCLUSION:

The modern electoral system faces significant challenges, including fraud, identity manipulation, and lack of transparency, which undermine public trust. The Binance Smart Chain (BSC) offers a secure, transparent, and decentralized voting framework using its Proof of Staked Authority (PoSA) consensus mechanism. By combining Proof of Stake (PoS) and Proof of Authority (PoA), BSC enhances security, efficiency, and decentralization, ensuring elections are tamper-proof. In addition to blockchain's immutability, the system integrates facial recognition, OTP authentication, and live location verification to eliminate identity fraud, unauthorized access, and proxy voting. These security layers fortify the electoral process, making it resistant to manipulation. By leveraging blockchain and biometric authentication, BSC establishes a trustworthy, scalable, and fraud-resistant voting model. This innovative approach restores voter confidence, ensuring fairness, accuracy, and reliability in elections. BSC's model sets a new standard in electoral governance, paving the way for secure digital democracy worldwide.

REFERENCES:

1. S. Wolchok et al., Security analysis of Indias electronic voting machines, in Proc. 17th ACM Conf. Comput. Commun. Secur., 2010, [10] R. L. Rivest, The threeballot voting system, Tech. Rep., 2006, p. 15.
2. M. Pilkington, 11 Blockchain technology: Principles and applications, in Research Handbook on Digital Transformations. 2016, p. 225.
3. S. Baig, U. Ishtiaq, A. Kanwal, U. Ishtiaq, and M. H. Javed, Electronic voting system using ngerprint matching with Gabor lter, in Proc. Int.
4. Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, Consortium blockchain for secure energy trading in industrial Internet of Things,

[40] SpringerLink. Security Accessed: Aug. 2, 2018. com/chapter/10.1007/978-3- 540-24654-1_13 Analysis Sisters. SHA-256

5. F. Al-Turjman, 5G-enabled devices and smart-spaces in social-IoT: Mar. 2019.
6. P. Tarasov and H. Tewari, The future of E-voting, IADIS Int. J. Comput.
7. M. A. Khan and K. Salah, IoT security: Review, blockchain solutions, May 2018.
8. M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: OReilly Media, 2015.
9. S. S. Al-Riyami and K. G. Paterson, Certicateless public key cryptogra- phy, in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur. Berlin, Germany: [10] T.-Y. Wang, J.-F. Ma, and X.-Q. Cai, The postprocessing of quan-2017.
10. T.-Y. Wang and Z.-L. Wei, One-time proxy signature based on quan- 2012.
11. N. Hackius and M. Petersen, "Blockchain in logistics and supply chain: Trick or treat?," in Proc.
12. Digitalization Supply Chain Manage. Logis-tics: Smart Digit. Solutions Ind. 4.0 Environ. Proc. Hamburg Int. Conf. S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," Int.
13. J. H. Park and J. H. Park, "Blockchain security in cloud computing: Use 164.
14. O. Jacobovitz, "Blockchain for identity management," The Lynne William Frankel Center Comput. Sci. Dept. Comput. Sci. Beer Sheva: Ben-Gurion University, 2016.
15. Rejeb, J. G. Keogh, and H. Treiblmaier, "How blockchain tech- nology can benet marketing: Six pending research areas," Front.