ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb823

Secure Online Voting Protocol with Blind Signatures and Identity Verification

Kenneth Richard Dike[1]; Dr. Ugbari Augustine[2]; Dr. Martha Ozohu Musa[3]

[1]Department of Software Engineering and Technology, Energy Technology Institute, University of Port-Harcourt, Port Harcourt, Nigeria
[2]Department of Computer Science, University of Port Harcourt, Port Harcourt, Nigeria
[3]Department of Computer Science, University of Port Harcourt, Port Harcourt, Nigeria

Publication Date: 2026/02/28

Abstract: Delays and security remain major issues in traditional manual voting, while in the emerging electronic voting, trust and privacy remain issues in its adoption. This research presents the design and development of a secure electronic voting protocol that combines biometric verification of a standard identity with cryptography to preserve election integrity. This research follows the Design Science Research Methodology, producing the protocol as an artefact, beginning with quick work on it and iteratively improving it during development. The proposed architecture uses a combined National Identity verification and Liveness detection procedure for user authentication, ensuring voter uniqueness and preventing impersonation. It also integrates the RSA blind signature protocol to prevent direct linking of votes to their voters. It uses Paillier encryption to safeguard votes both in transit and at rest, and this encryption scheme has a homomorphic property that enables aggregation of encrypted votes and decryption of the final tally. It uses the SHA-256 cryptographic hashing algorithm, the HMAC authentication technique and the AES-GCM encryption to secure the integrity of data. It also uses zero-knowledge proofs to demonstrate the correctness of encrypted votes and decrypted tallies. Testing showed that it prevented a photo spoofing attempt and also blocked authentication using a person's mother's identity data. Also, when the blinded vote is compared with the unblinded, via local logs on the development system, there is no direct link. The whole system shows a secure electronic voting protocol that is easy to use and can be trusted.

Keywords: *Blind Signatures, Identity Verification, National Identity, Biometrics, Liveness Detection, Electronic Voting.*

How to Cite: Kenneth Richard Dike; Dr. Ugbari Augustine; Dr. Martha Ozohu Musa (2026) Secure Online Voting Protocol with Blind Signatures and Identity Verification. *International Journal of Innovative Science and Research Technology*, 11(2), 1884-1893. https://doi.org/10.38124/ijisrt/26feb823

I. INTRODUCTION

Elections have been in use since ancient times, like ancient Greece and ancient Rome, and during the Medieval period to bring rulers to power, such as the Holy Roman Emperor and the Pope. (Election - Wikipedia, n.d.). Elections used to be conducted manually, and the results processed and announced by humans. Electronic voting is now in the picture, and it aligns well with the digitalisation of other aspects of life. Since it is an automated process, it has advantages ranging from speed, relatively lower costs and manpower, accuracy, and security, among others.

Several studies have attempted to address the issues in electronic voting. Existing works fall short in at least these areas. First, many protocols rely on credentials and static facial biometrics, which are vulnerable to impersonation due to the absence of a reliable verification mechanism of the voter's presence. Second, systems that remove the direct link between voters and their votes – using mechanisms like blind signatures – rarely integrate practical identity validation mechanisms, leading to weak authentication or cumbersome enrolment requirements. Consequently, there is a gap in integrating modern identity verification and the removal of the direct link between voters and their votes, while maintaining a simple system, in a single, coherent framework.

This project intends to build a secure online voting protocol that uses blind signatures for removing the direct link between voters and their votes, and uses the National Identity Number with facial liveness checks for identity verification and eligibility. It will be designed with emphasis on unique identity verification, relative ease of use and protection of the voter's choice/vote from the public.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb823

II. REVIEW OF RELATED WORKS

➢ *Works Related to the Study are Presented as Follows:*

Chaum (1983), introduced blind signatures with focus on blindness (i.e. the signer should not have the ability to link the signature given to a later submission that used the signature). This lets a user obtain a valid authorisation on a hidden message, and using that, they can obtain a signature that the issuer cannot trace to a particular signing session when presented via an anonymous session/submission.

Schmid & Grünert (2008), presented a report that is meant to summarise and explain blind signatures, provide an overview of electronic voting, focusing on privacy, and show how blind signatures are used in electronic voting systems. The work was not aimed at presenting new findings, but serves as a summary and introduction to the subject. The authors claimed that many reports on blind signature electronic voting protocols are not so easy to understand, and they want their report to be understandable with a basic knowledge of cryptographic methods, so they did not include scientific proofs of some problems or other properties in the protocols they mentioned. In the paper, they report under the following areas: how blind signatures work, the RSA blind signature scheme, privacy classification of blind signatures, uses of blind signatures, voting security requirements, voting structure reference, privacy within electronic voting protocols, blind signatures within electronic voting protocols, verifiability versus receipt-freeness, and outlook.

Prêt à Voter is a voting system which originated from Ryan (2004) as a variant of Chaum (2004)'s voter-verifiable election scheme. It is an end-to-end verifiable voting system, and its distinguishing idea is the use of ballots with a randomised candidate list, which removes any direct connection between the voter's choice and their receipt. After selection, the ballot is separated into two halves – one is discarded, and the other, which contains the cryptographically encrypted position of the voter's choice is posted to a Web Bulletin Board and retained as a receipt. The encryption mentioned is done with secret keys, which are held by different tellers; therefore, an individual machine in the election should not be able to link a given voter to a particular decrypted vote. Voters can confirm after the election that their receipts appear correctly on the Web Bulletin Board. After this, the tellers now perform mixes for anonymisation and then decrypt the receipts. All the intermediate phases of this process are audited later (Prêt à Voter - Wikipedia, n.d.). The protocol establishes many of the core principles of modern end-to-end voting systems and is therefore considered a foundational protocol. It has also been implemented in pilot trials, notably during a state election in Victoria (Australia) (Culnane et al., 2015).

Jóźwik & Pouwelse (2025), introduced SmartphoneDemocracy, an electronic voting protocol that integrates European Digital Identity (EUDI) Wallets for verification of unique identity, Zero-Knowledge Proofs for preservation of privacy and peer-to-peer blockchain (TrustChain) for tamper-evident record-keeping and homomorphic encryption together with threshold decryption for tallying of votes. It also uses BBS signatures for issuing privacy-preserving voting credentials. The system enables voters to register and to vote anonymously (yet verifiably) using their smartphones.

Kareem & Balkrishna (2025), presented the design and implementation of a secure online voting system that uses a multi-stage rigorous authentication mechanism to ensure the principle of "one person, one vote" stands, and the chances of impersonation/fraud are reduced significantly. The work combines Aadhaar/Voter ID validation and biometrics verification. The voting flow is in this order: authentication, Aadhaar/Voter ID validation, face capture and fingerprint enrolment, real-time/live face verification for identity confirmation before selection of the vote option, and a final fingerprint verification for voter presence authentication before submission of the vote. The system also has a vote-counting visualisation.

M. et al. (2023)'s study emphasised the integration of pragmatic face and fingerprint verification for enhanced authentication of voters. Basically, riding on the advancements at that time and practical considerations, the paper projected the potential of biometrics in transforming the voting procedures while handling identity-verification-related concerns. Its voting procedures are as follows: user face and fingerprint scanning, after which fetching of Aadhaar Card details from the server is done, then if both scanned face and fingerprint data match the data in the Aadhaar details, the user can vote, and the vote is recorded; else, the user is not permitted to vote.

Yan et al. (2022), presented reviews on two approaches of privacy-preserving voting systems – Blind Signature based voting and Homomorphic Encryption based voting. They mention that Blind Signature based Voting is simple, stable, and can scale, but will require an anonymous mechanism during the communication with the blockchain. For Homomorphic Encryption based Voting, on the other hand, they mention that it protects the privacy of voting against traffic analysis attacks, but is vulnerable to extra votes attack, cooperation interruption attack, and has limited scalability. They then applied sampling to mitigate issues like scalability and (with the assumption of an honest majority), cooperation interruption. They also simulate its performance using different voting group sizes and sampling numbers.

Pooshideh et al. (2024), carried out a systematic literature review of biometric Presentation Attack Detection (PAD), which is a verification check on face recognition systems against Presentation Attack (the use of a mask, photograph, or video of a target person as the live face of the person). They mention analysing and comparing different Presentation Attack Detection methodologies, and giving an organised presentation of different feature extraction techniques used in Presentation Attack Detection. They also mention highlighting distinct properties, pros, cons, and use cases of each method while considering factors such as generalisability, computational efficiency, and user involvement, among others.

Moser et al. (2024), presented a systematic study of internet voting systems used in practice, investigating which

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb823

security mechanisms they use to achieve verifiable and secret elections. The work used a framework consisting of six categories – Cast (ballot formation process), Authentication (ballot/voter authentication), Cast verification (assurance of correct ballot formation), User Record (voter device data storage operations), System Record (system data storage operations) and Tally (ballots list cleansing, anonymize and decrypt operations). In their conclusion, they mention an observation of gaps between practice and research. They state that almost all systems use security as a sales argument, but do so independently of the actual implementation (and public documentation) of security measures. They also state that most systems do not claim to implement verifiability, and most of those that do have poor documentation of their solution.

Akintoye & Araoye (2015), proposed a biometric electronic voting system for Nigeria as a response to the drawbacks and declining trust in the conventional paper ballot election system. The mode of authentication in the electronic voting system is the use of biometrics combined with a voter identification number and a voting code, which is generated after registration for each voter. They mention that to achieve a perfect framework of an electronic voting system in Nigeria, there must be a constant electricity power supply and good internet infrastructure, and also mention that the system must not only work, but Nigerians must believe it works.

Meera et al. (2024), proposed a voter verification and authentication electronic system that uses biometrics. The system integrates both face recognition and fingerprint authentication biometric technologies, and it is implemented in MATLAB. They mention a key feature of the system as its real-time transparency (through the use of a dashboard). Also, they contrast fingerprint verification with face verification, mentioning that fingerprint verification requires physical contact with a sensor while face recognition simply involves image capture of the voter's face. They state that face recognition has a key advantage of ease of use and non-intrusiveness.

In Nur'allifa et al. (2025)'s study, they set out to develop an electronic voting protocol where the voter's participation in the security processes of the system is reduced. They implemented a blind signature protocol that uses the RSA algorithm, making all the cryptographic processes (blinding, signing, and unblinding) to be carried out by the system and entities that are authorised. They mention that their findings show that, when voters' technical part in the cryptographic process is reduced and the processes from blinding to unblinding are handled by the system, security is improved and errors are minimised. Also, the protocol is modified to incorporate digital signatures into the access request process in communication between parties, preventing forgery and unauthorised access.

Loss (2022), presented the synthesis of blind signature development in past times, their current state (as of then), and future directions (from then) at NIST's Secure Techniques for Privacy-Preserving Authentication (STPPA) workshop. The talk revisited the contribution of (Chaum, 1983), who introduced blind signatures. It also revisited how blind signature works, and its security properties of blindness and unforgeability. It presented past developments of blind signatures, during which it says that interest in blind signatures faded from 2003-2018. Coming to the current time of the work (i.e. 2019-2022), it mentioned that blockchain led to renewed interest in blind signatures. Finally, looking into the future from that time (2023 and beyond), it mentions open challenges.

Sreenivasa et al. (2023), outlined an online voting system that combines facial recognition with Indian Aadhaar verification and voter card verification as a three-step verification process to guarantee the authenticity and dependability of the entire voting procedure. The first step involves face verification, which is subdivided into three phases: the pre-processing of photos ahead of verification, the detection of face using the Haar Cascade algorithm, which takes eyes as unique element to identify the face of the voter, and the recognition of the identity of the person after face detection, after which the voter is forwarded to the subsequent steps. The second verification step involves Aadhaar verification (where Aadhaar is a means of uniquely identifying Indian residents based on their biometrics and demographic data (Aadhaar - Wikipedia, n.d.)) via the official Aadhaar website. The third step involves Voter ID verification via the official Election Commission's website.

Gaikwad et al. (2025), developed an online voting website using PHP and MySQL. In the system, voters register by submitting their information, and they are verified via Aadhaar / Voter ID / PAN (Permanent Account Number). When logging in, voter do so with registered mobile number, undergoes OTP verification, then can see active elections (based on eligibility). Also, sensitive data like Aadhaar and PAN were encrypted in the database.

Ostapets & Motylenko (2025), analysed different approaches to implementing electronic voting systems and showed their comparative characteristics. They focus on blockchain, homomorphic encryption, blind signatures, and zero-knowledge proofs. Requirements that were considered during the analysis are anonymity, verifiability, fairness, robustness, and receipt-freeness. As a result of their comparative analysis, they mention that systems based on homomorphic encryption and blind signatures require additional cryptographic proof mechanisms, which makes their use without zero-knowledge proofs unfeasible. Also, they mention that the comparison shows that blockchain technology can only be used when combined with other cryptographic methods. They also mention that modern zero-knowledge proofs satisfy almost all the required properties. They mention that the only issue with such systems is that of trust in the server, and that blockchain technology solves that problem. Therefore, they propose a hybrid system of blockchain and modern zero-knowledge proofs.

Ibrahim et al. (2003), implemented a voting system where RSA blind signatures are used for voters' privacy, and RSA digital signatures for voters' authentication. The system uses National Identity Card numbers in voters' eligibility

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb823

verification. Also, the system was said to satisfy universal verifiability.

Despite the contributions of the existing works, not many of them produce a completely remote electronic voting system where voters are uniquely identified, preventing impersonation while using the blind signature protocol to contribute to the anonymity of votes, in an overall, relatively simpler voting process. This project aims to produce that.

III. METHODOLOGY

Fig 1 shows the architecture of the electronic voting system. The Client (Voter) Layer contains user interfaces for system interactions by voters, which include: National identity liveness authentication, elections, voting, and results/bulletins interfaces. It runs on the web, and was developed using the Next.js framework.

The next is the Application Layer. This layer runs the business logic, which includes: administrator election setup request, combined identity and biometric liveness system of authentication, blind signature issuance, vote recording, vote tallying, and bulletin data generation. It runs on the infrastructure of the third-party services used – Firebase Functions with the integration of QoreID and Firebase Authentication – and Firebase Functions was implemented with the Node.js Framework.

The next is the Data Layer which stores data such as voter data, election and vote data, and bulletin/result data. It also stores files such as voter photos. This layer runs on the infrastructures of Firebase Cloud Firestore database and Firebase Cloud Storage.

Finally, the Admin Layer contains user interfaces for system interactions by administrators, which include: email/password login and election setup. It runs on the web, and was developed using the Next.js framework.

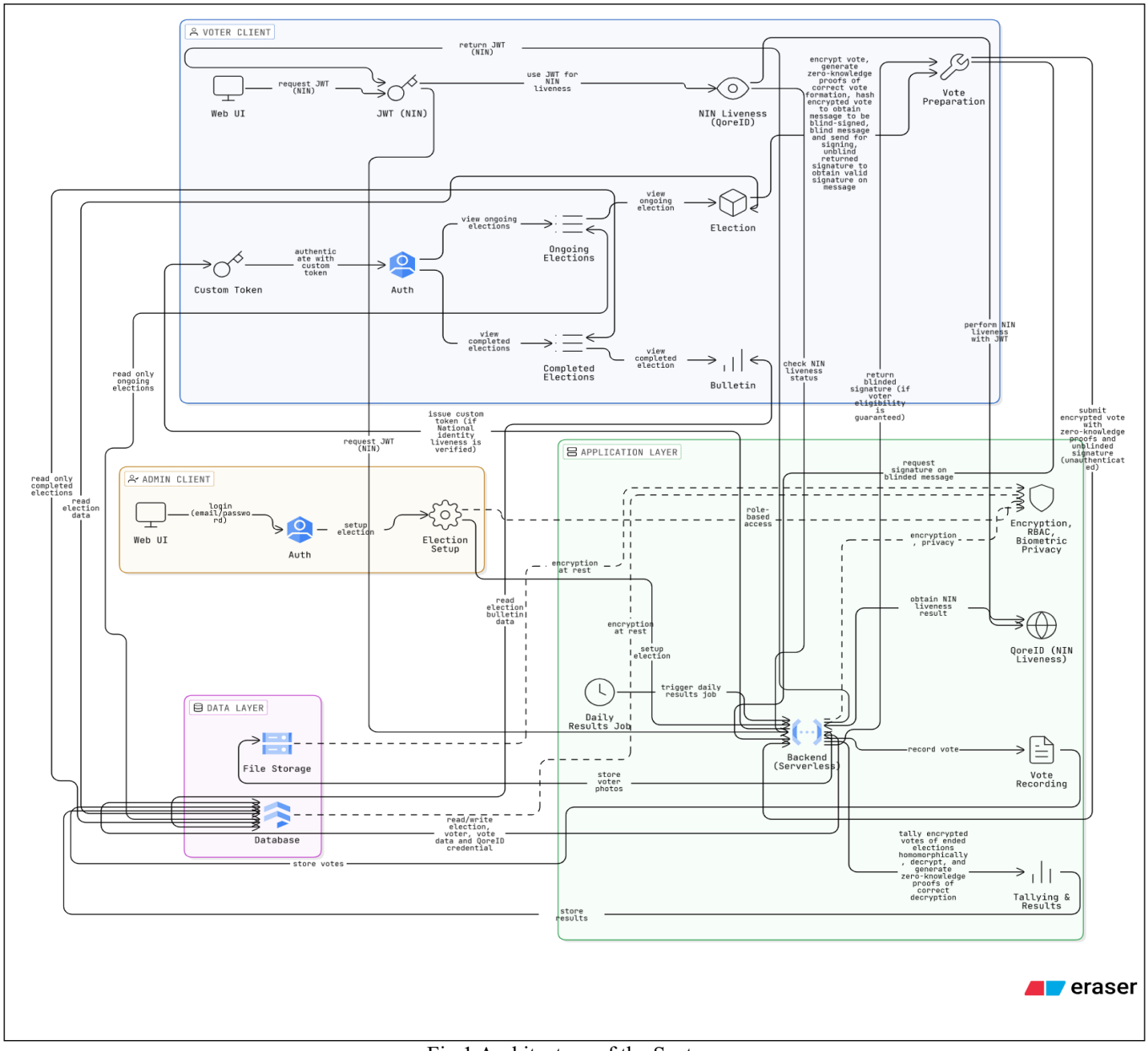

Fig 1 Architecture of the System

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb823

A. Interactions/Workflows

First, for the admin login and election setup, administrator logs in with credentials (email/password) via the admin web application. After login, the administrator sets up an election with its options, schedule, and NINs that are eligible for participation, making a request to the server – a serverless Firebase Function (role-based access is used to ensure that the request is from a valid administrator).

Second, for the voter authentication, voter sends NIN to the server in a request for a JWT, which will be used as a reference for QoreID NIN Liveness verification request. Upon receipt of the JWT, QoreID NIN Liveness verification is initiated with the QoreID's SDK, using the user's inputted NIN, with the JWT (received from the server) serving as a reference. QoreID handles the verification with its SDK (requesting extra user data). After verification is done on the client, the server is queried by the client for verification confirmation and issuance of a token to be used for authentication with Firebase. The received token is used to log in via Firebase Authentication.

Third, for the ongoing elections' view and voting process, an authenticated voter sees ongoing elections and selects one to vote in. Then they choose from options and the vote is encrypted with Paillier encryption. Zero-knowledge proofs of correct formation of the vote are then generated, and encrypted vote is hashed and blinded to obtain a message for blind signing. Voter ensures to have had a recent liveness verification, and then requests a blind signature on the message. Server confirms voter passes certain necessary criteria for the election and issues a blinded signature which voter unblinds to obtain a valid signature on the message. Voter then casts an unblinded vote that is encrypted, but not hashed, together with the zero-knowledge proofs and the signature. Server verifies the validity of the zero-knowledge proofs, the signature (which is tied one-to-one to the unique encrypted vote that was signed, yet not able to directly expose voter identity), and that the vote has not been recorded before. Encrypted vote is hashed and stored in Firestore, together with the zero-knowledge proofs and signature.

Fourth, for tallying & results, using a daily cron job, the ended elections are retrieved together with their votes, for results generation. Retrieved votes are homomorphically aggregated while encrypted, and then decrypted, after which zero-knowledge proofs of correct decryption are generated. Then, results together with proofs are saved in Firestore.

Finally, for completed elections' view and results (bulletins) display, user sees completed elections and selects one to view the outcome. If the outcome of the election is ready, the user sees the election bulletin, which contains the results together with zero-knowledge proofs of correct decryption and all the ballot hashes that contributed to the result.

B. System Techniques/Components

The proposed system provides a secure framework for online voting that combines strong identity verification with cryptographic mechanisms to contribute to the privacy and integrity of votes. Each identity and cryptographic component has an important function in making the system more trustworthy, preventing impersonation, vote duplication, invalid or malformed votes and unauthorised access to data. A number of the techniques/components are presented.

- *National Identity Liveness Verification*

The system integrates the combination of National identity data verification with liveness detection as a very important step in ensuring that voters are unique and impersonation is prevented. Before a voter is issued a blind signature, they must have been authenticated via the combined mechanism recently. If authentication is not recent, they must undergo a liveness detection to strengthen assurance that they are still the same person using the account (as the person who authenticated). The liveness verification involves confirming that the voter is an actual human that is physically present at the time of verification, not a spoof (an inanimate photo, a video, or a mask), while the National identity data verification confirms that the identity number is valid, and the first and last names on the identity record match the names inputted during verification. In the combination of both verifications, a photo frame from the liveness verification procedure is checked against the photo on the identity record for a match. The system uses a trusted third-party – QoreID – to perform these verifications. QoreID has a combination of National Identity Number verification and Liveness detection in one flow/verification called "NIN Liveness verification". The system uses this and extends it, also verifying the first and last names to achieve its own National Identity Liveness verification.

This National Identity Liveness verification ensures strong voter authentication, preventing multiple voting, identity theft and proxy voting, which are common threats in online voting systems. The system's confirmation of both the voter's presence (via liveness detection) and the authenticity of their identity (using the National Identity System) guarantees that a person can only cast one vote, and no more. The system also uses this verification to make it possible for voters to vote without a bulky pre-registration process.

The process of its use works as follows: the voter provides their NIN, and the server uses it to generate a reference for that verification request. The reference is tied to the provided NIN on the backend. Rather than the raw NIN, the HMAC of the NIN is what is saved in the backend, with the issued reference tied to it. When the voter receives the reference, they use it to undergo the verification on the client. After undergoing the verification procedure, the server is queried for confirmation of verification. If liveness is confirmed, identity number is valid, identity first and last names match inputted names, and photo from liveness procedure matches identity photo, verification is said to be successful, then the verification timestamp is updated on the database, and the remaining part of the initiated flow continues.

- *SHA-256 (Secure Hash Algorithm 256-bit)*

The system employs the SHA-256 cryptographic hash function in the course of preventing vote duplication. After a vote has been verified to be valid using the blind signature protocol, the vote is hashed using SHA-256 to produce a

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb823

unique fingerprint, or digital digest, of the vote. This fingerprint is then checked against existing records to ensure the submission is unique, preventing duplicate voting.

SHA-256 ensures that each vote has a fixed-sized, unique identifier. This identifier is stored in the database and enables easy querying to ensure that a vote does not already exist before adding it to the database. If it is not used, then when the system needs to check for the existence of a vote, it has to fetch all votes' data (ciphertexts, among others) and begin comparison of each piece of data to ensure that no vote data exactly matches the one about to be added. SHA-256's inclusion strengthens the overall efficiency, security and integrity of the voting process.

The process of its use works as follows: the vote data is converted into a fixed-length 256-bit hash, which produces a unique digital fingerprint. It works in such a way that the slightest change in the vote data will result in an entirely different hash, making it difficult to find two votes with the same hash. The system then compares this hash against existing hashes to find and prevent duplicate votes, ensuring the integrity of the voting process.

- *HMAC (Hash-based Message Authentication Code)*

The system implements HMAC based on SHA-256 to secure voter identifiers, while enabling their lookup. When identifiers such as NINs are to be stored, the system computes their HMAC using a secret key. This allows the server to ensure the uniqueness of voters while keeping their personally identifying numbers secure.

HMAC enhances voter privacy and ensures that personally identifying numbers cannot be obtained or misused if the database is compromised. It also makes it possible to look up a given existing data without storing it raw, while ensuring the uniqueness of voters. By maintaining confidentiality while supporting unique identity verification, it balances security and data utility in the voting system.

The process of its use works as follows: the voter's NIN is fed into the HMAC function along with a secret key, generating a hash output that is stored. Later, when the system needs to check for the existence of a given NIN, for instance, when it wants to decide if it will create a new user with the given NIN or retrieve the existing user, it hashes the NIN with the same secret key and verifies the existence of the NIN without exposing all other existing NINs.

- *Paillier Encryption*

The system employs Paillier encryption to contribute to the prevention of unauthorised access to votes while in transit and at rest. During the tallying of votes, only the server, having the encryption private key, can then perform decryption. Paillier encryption also allows arithmetic operations on encrypted data, meaning votes can be tallied while encrypted. Then the final encrypted tallies can be decrypted.

By using Paillier encryption, the system contributes to the end-to-end privacy of votes, as anyone who in some way gets access to the sent vote will not be able to see its actual data without the encryption private key.

The process of its use works as follows: each vote is encrypted on the client using the Paillier public key and then sent to the server for storage. During the tallying of votes, the server tallies up the encrypted votes and then decrypts the aggregated tallies with the Pallier private key, revealing the total count for each voting option.

- *Zero-Knowledge Proofs (ZKPs)*

The system integrates Zero-Knowledge Proofs to allow voters to demonstrate that their ballot was correctly encrypted without revealing their choice. During tallying, zero-knowledge proofs are also generated as proofs that votes were correctly aggregated and decrypted, providing evidence of honest computations by the server.

Zero-Knowledge Proofs contribute to the transparency and trust in the system. They prevent the submission of invalid or malformed votes because, with vote encryption and the collective (rather than individual) decryption of votes, such wrong votes could otherwise go undetected and alter the results, negatively impacting the integrity of the voting procedure. They also ensure the server tallying the results proves its honesty.

The process of its use works as follows: Voters create Zero-Knowledge Proofs with their encrypted vote, showing it is correctly encrypted. The server verifies the proofs without having to check the vote. During tallying, after aggregating and decrypting the votes, the server generates ZKPs to prove it performed the aggregation and decryption honestly.

- *AES-GCM (Advanced Encryption Standard in Galois/Counter Mode)*

The system employs AES-GCM (Advanced Encryption Standard in Galois/Counter Mode) with 256-bit keys, together called AES-256-GCM, as the primary encryption scheme for safeguarding both election private components/keys (because these private components/keys are stored in the database) and retrievable copies of the NINs. AES-256-GCM provides authenticated encryption, combining confidentiality with integrity in one cryptographic operation. This ensures that encrypted data remains a secret while ensuring that it has not been tampered with. While Paillier encryption is used specifically for encrypting vote contents, AES-256-GCM secures other sensitive information, including personally identifying numbers.

AES-256-GCM plays an important role in preserving the secrecy of private keys in the system without having to store them all outside the database. It is also used to achieve the storage of retrievable (encrypted) NINs, so that they can be obtained later when only the liveness of users need to be verified on the client (i.e. confirmation of liveness against National identity data entered during authentication). It ensures that while private and personally identifying numbers are stored in the database, if the database is compromised, they cannot be obtained without the secret key used in encrypting them. AES-256-GCM is also fast and optimised

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb823

with hardware acceleration and parallel processing capabilities.

The process of its use works as follows: when an election is created and its blind signature public and private components are generated, the public components are saved directly to the database, while the private component is encrypted using the AES-256-GCM algorithm. Also, the private Paillier encryption components (generated also during election creation) are encrypted using the same algorithm before being saved, unlike the public component. Also, the private key used in signing the bulletin payload (to show authenticity of results) after computing the results is encrypted using the same algorithm before being saved. When any of these components/keys need to be used (e.g. during blind signing), their corresponding encryption secret is used to decrypt them before usage.

IV. RESULTS AND DISCUSSION

A. *functional Testing*

Certain components of the system were tested, and the results contribute to the validation that the system works as expected. The results are shown in Table 1.

Table 1 System Components Test results

S/N	Component	Test Performed	Expected Result	Outcome
1	Admin Login	Log in with valid admin credentials.	Valid credentials log in.	Passed
2	Election Setup	Create election	The election can be viewed as an ongoing election during its scheduled timeframe, and voters can participate in it.	Passed
3	National Identity Liveness authentication	Perform verification in the browser with valid identity data and a matching face	Valid combination authenticates	Passed
		Perform verification in the browser with invalid identity data or an unmatching face	Invalid combination fails to authenticate	Passed
4	Vote Casting	The voter selects an option from the list of options and casts their ballot	Receipt of the ballot is acknowledged	Passed
5	Results/Bulletin	Navigate to view the results/bulletin of a completed election	Completed election with available results/bulletin shows results/bulletin.	Passed
			Completed election with unprocessed results/bulletin yet informs the user that the bulletin is not available yet.	Passed

B. *Discussion 0f Results*

- When verification is attempted with a spoof (a photo image), as shown in Fig 2 and Fig 3, verification fails (Fig 4). This shows liveness detection's resistance to spoofing with a photo.

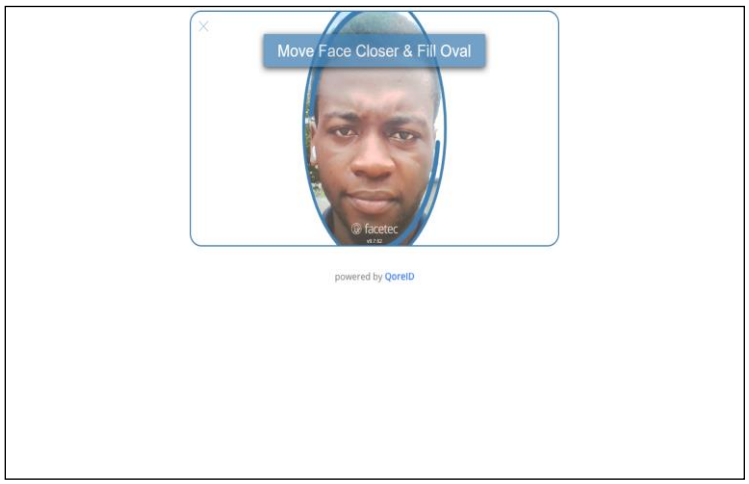

Fig 2 Verification with a Spoof – Photo (1/2)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb823

Here, the spoof (a photo on a smartphone) is made more obvious.

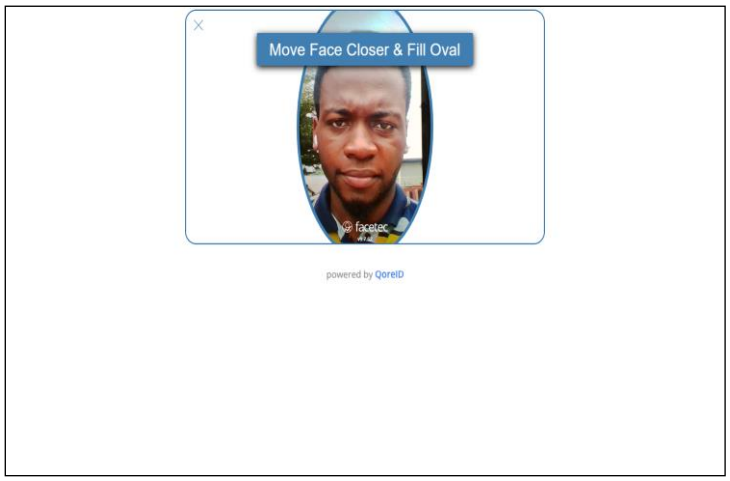

Fig 3 Verification with a Spoof – Photo (2/2)

- When verification is attempted with correct national identity details, but combined with the face of the son of the owner of the identity, the verification also fails (Fig 4). This effectively proves the resistance of the system to impersonation.

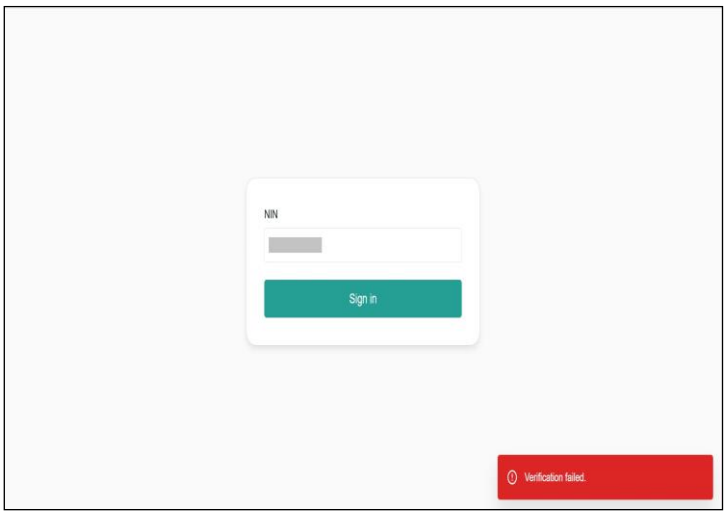

Fig 4 Failed Verification for Verification with Spoofs and also for Verification with Correct Identity Details, yet with the Face of the Son of The Identity Owner

- From local logs of a blinded message and the corresponding unblinded message shown in Fig 5, the blinded message is in no way related to the unblinded message, and no one can directly link any unblinded message to a blinded message without knowing the random number, r, used by the voter client in blinding the message. This prevents the ability to directly link votes to voters.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb823

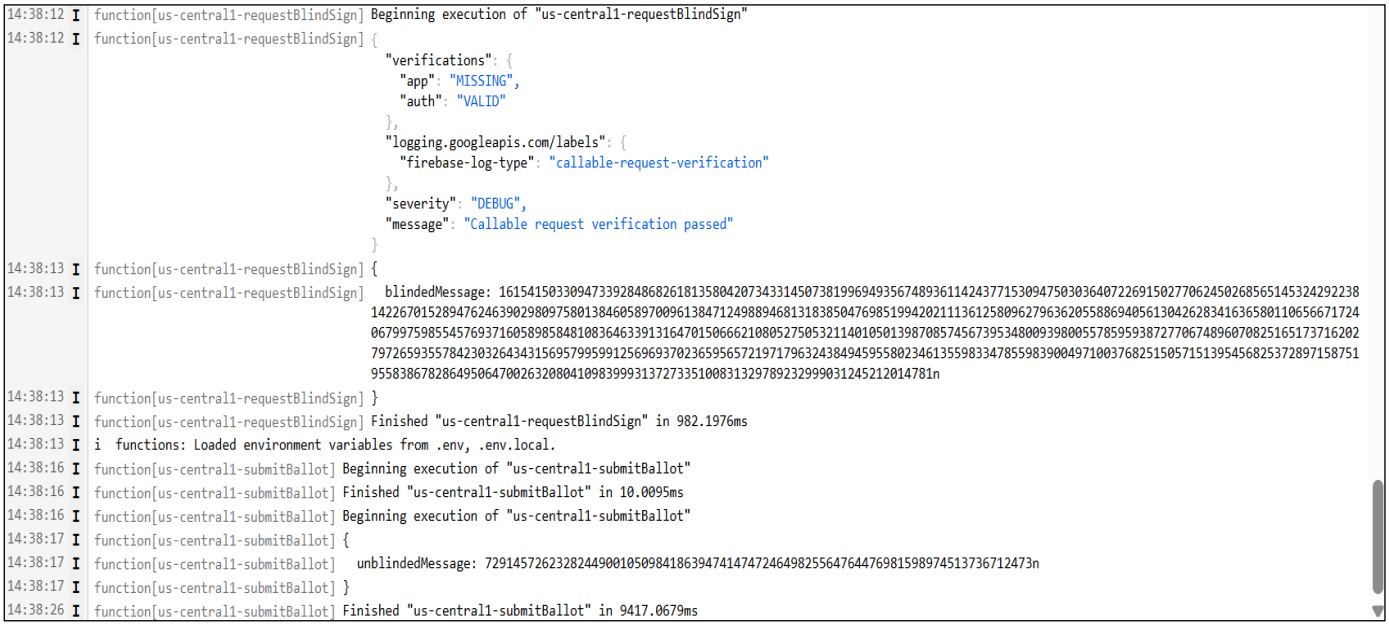

Fig 5 Local Logs of a Blinded Message and the Corresponding Unblinded Message

V. CONCLUSION

This work successfully designed and implemented a secure electronic voting protocol that integrates a National Identity Liveness authentication mechanism for identity verification and blind signature cryptography for contribution to vote privacy. The system solves problems such as voter impersonation, the potential for direct linkage of a vote to the voter and bottlenecks in manual procedures.

The developed system shows the viability of working with standard digital identity systems, using the identity data in combination with biometric liveness verification to strengthen the integrity of elections, while also using blind signatures to conceal the choices of voters from the server that validates them.

It is good to note that while the system prevents direct linking of voters' identities to the ballots using blind signatures, administrators with privileged access can view the logs of the system and potentially connect ballot submission requests (which are done via unauthenticated requests) to ballot signing requests (which are done via authenticated requests) using metadata like timestamps and user agents from the requests. This would be left for researchers who would have an interest in mitigating it.

With further improvements and adoption into standard systems, this protocol has the potential to make elections easier and secure, increasing participation and trust in democratic exercises.

REFERENCES

[1]. Aadhaar - Wikipedia. (n.d.). Retrieved 17 August 2025, from https://en.wikipedia.org/wiki/Aadhaar
[2]. Akintoye, K. A., & Araoye, O. I. (2015). A BIOMETRIC E-VOTING FRAMEWORK FOR NIGERIA. Jurnal Teknologi (Sciences & Engineering), 77(13). https://doi.org/10.11113/jt.v77.6363
[3]. Chaum, D. (1983). Blind Signatures for Untraceable Payments. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 199–203. https://doi.org/10.1007/978-1-4757-0602-4_18
[4]. Chaum, D. (2004). Secret-Ballot Receipts: True Voter-Verifiable Elections. In IEEE Security and Privacy (Vol. 2, Number 1). IEEE. https://doi.org/10.1109/MSECP.2004.1264852
[5]. Culnane, C., Ryan, P. Y. A., Schneider, S., & Teague, V. (2015). V Vote: A verifiable voting system. ACM Transactions on Information and System Security (TISSEC), 18(1), 1–30. https://doi.org/10.1145/2746338
[6]. Election - Wikipedia. (n.d.). Retrieved 15 August 2025, from https://en.wikipedia.org/wiki/Election
[7]. Gaikwad, A. A., Shinde, S. T., Shinde, T. P., & Ghante, S. S. (2025). Online Voting System. International Scientific Journal of Engineering and Management (ISJEM), 4(6). https://doi.org/10.55041/ISJEM04549
[8]. Ibrahim, S., Kamat, M., Salleh, M., & Aziz, S. R. A. (2003). Secure E-voting with blind signature (IEEE, Tran.). 4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings, 193–197. https://doi.org/10.1109/NCTT.2003.1188334
[9]. Jóźwik, M. J., & Pouwelse, J. (2025). SmartphoneDemocracy: Privacy-Preserving E-Voting on Decentralized Infrastructure using Novel European Identity.
[10]. Kareem, S., & Balkrishna, R. S. (2025). Enhancing E-Voting Security: A Multi-Layered Biometric Authentication System with Aadhaar/Voter ID Integration. International Journal of Scientific Research and Engineering Development, 8(3). https://ijsred.com/volume8/issue3/IJSRED-V8I3P468.pdf
[11]. Loss, J. (2022). Blind Signatures: Past, Present, and Future. Special Topics on Privacy and Public Auditability (STPPA) - Event 4. https://csrc.nist.gov/presentations/2022/stppa4-blind-sigs

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb823

[12]. M., U., Patil, A. L., N., K. K., & T., B. H. (2023). BIOMETRIC-ENABLED VOTING SYSTEM DESIGN USING IOT. International Journal For Technological Research in Engineering, 11(4). https://ijtre.com/wp-content/uploads/2024/01/2023110408.pdf

[13]. Meera, S., Rasika, R., Kowsalya, V., & Kanimozhi, P. (2024). A Unified Biometric Voter Verification and Authentication E-Voting System Through CNN. https://doi.org/10.1234/jes.2020.12.3.45

[14]. Moser, F., Kirsten, M., & Dörre, F. (2024). SoK: Mechanisms Used in Practice for Verifiable Internet Voting. In E-Vote-ID 2024 - 9th International Joint Conference on Electronic Voting. https://doi.org/10.18420/e-vote-id2024_10

[15]. Nur'allifa, E. N., Putra, R. R. J., & Nursalman, M. (2025). RSA Blind Signature sebagai dasar pengamanan pada sistem e-voting dengan Prinsip Frictionless User : studi desain dan tinjauan keamanan. Jurnal Komputer Teknologi Informasi Sistem Informasi (JUKTISI), 4(2), 782–793. https://doi.org/10.62712/juktisi.v4i2.527

[16]. Ostapets, D., & Motylenko, V. (2025). Analysis of approaches of electronic voting systems implementation. Системні Технології, 6(155), 50–60. https://doi.org/10.34185/1562-9945-6-155-2024-06

[17]. Pooshideh, M., Beheshti, A., Qi, Y., Farhood, H., Simpson, M., Gatland, N., & Soltany, M. (2024). Presentation Attack Detection: A Systematic Literature Review. ACM Computing Surveys, 57(1), 1–32. https://doi.org/10.1145/3687264

[18]. Prêt à Voter - Wikipedia. (n.d.). Retrieved 7 September 2025, from https://en.wikipedia.org/wiki/Pr%C3%AAt_%C3%A0_Voter

[19]. Ryan, P. Y. A. (2004). A Variant of the Chaum Voter-verifiable Scheme. Technical Report CS-TR-864, School of Computing Science, Newcastle University. https://nuhc.ncl.ac.uk/assets/pdf/TRs/864.pdf

[20]. Schmid, M., & Grünert, A. (2008). Blind Signatures and Blind Signature E-Voting Protocols. University of Applied Science Biel: Bern, Switzerland. https://www.e-voting-cc.ch/images/pdf/blindsignatures.pdf

[21]. Sreenivasa, N., Agarwal, G., & Jain, R. (2023). Online Voting System by Using Three Step Verification. ITM Web of Conferences, 57, 01010. https://doi.org/10.1051/itmconf/20235701010

[22]. Yan, Z., Jiang, Z., & Li, Y. (2022). Towards Better Privacy-preserving Electronic Voting System. ArXiv Preprint ArXiv:2205.12094.