International Journal of Multidisciplinary Engineering in Current Research - IJMEC

Volume 11, Issue 4s, April-2026, http://ijmec.com/, ISSN: 2456-4265

Full Length Article

Secure And Transparent E-Voting System Using Blockchain, Smart Contracts, Differential Privacy, And Email-Based Voter Authentication

Mohammed Sattar[1], M Fardin[2], Mohammed Junaid[3], Dr .Md Zainlabuddin[4]

[1,2,3]B.E.Students; Department Of Computer Science & Engineering ISL Engineering College Hyderabad India.

[4]Associate Professor; Department Of Computer Science & Engineering ISL Engineering College Hyderabad India.

Mail id; mohammadsattar3690@gmail.com, mrfardin99@gmail.com, junaidddd007@gmail.com

Accepted 24-04-2026

ABSTRACT

Election is the key process typically utilized for maintaining democracy in a given society. Recent technological advancements, such as Blockchain (BC), have been already deployed in previous works to realize non-conventional e-Voting systems. The main goal for such proposals is to provide the necessary level of security and reliability, while maintaining transparency, trust, and remote elections. However, the distributed and publicity nature of BC brought new challenges related to privacy and performance trade-off. This paper aims to address existing privacy and performance issues in e-voting by integrating smart contracts for reliability and transparency, Differential Privacy to enhance vote anonymity, and Self-Sovereign Identities (SSI) for managing decentralized identity and verifiable credentials.

Keywords:

Electronic Voting, Blockchain, E-Voting System, Smart Contracts, Differential Privacy, Self-Sovereign Identity (SSI), Decentralized Identity, Privacy Preservation, Secure Voting, Verifiable Credentials, Distributed Ledger Technology, Transparency, Remote Voting, Cybersecurity, Digital Democracy.

INTRODUCTION

Voting has been a critical tool for maintaining democracy worldwide throughout history. Traditionally, voting proce dures are classically performed using centralized, paper based systems that are inefficient in terms of cost and public liability. To solve for these issues, e-Voting frameworks have been proposed in the literature, activating the use of electronic devices or systems to cast or count votes in an election [1]. Despite being mostly centralized and suffer from single-point(s) of failure limitation, e-Voting still provides many advantages over traditional paper-based voting, such as higher efficiency, lower cost, and greater accessibil ity [2]. Because of these advantages, many proposals and initiatives around the world have been announced [3], [4], motivating the adoption of e-Voting schemes to enhance the prosperity of the democratic process in their countries (e.g. Switzerland [5], Kenya [6], Sri Lanka [7], Australia [8], India [9], Brazil [10], Nigeria [11], Russia [12], among others [13]). More sophisticated and reliable decentralized solutions typically use the Blockchain (BC) technology to achieve the required levels of decentralization, leading to public trust. BCis a revolutionary technology that allows for the creation and maintenance of a distributed ledger of transactions (TXs) that is secure, transparent, and immutable [14]. This technol ogy wasfirst introduced by Satoshi Nakamoto in 2008, as the underlying technology for the bitcoin cryptocurrency [15]. Since then, BC has been applied to various domains, such as Internet of Things (IoT) [16], finance [17], supply chain [18], healthcare [19], and Electronic Voting (e-Voting) [20]. BC technology offers a potential solution to some of the aforementioned challenges, by providing a decentralized and distributed platform for e-Voting that can enhance the trustworthiness and transparency of the voting process [21]. BC-enabled e-Voting systems can store the votes in an immutable and tamper-proof way, and allow anyone to verify the validity and correctness of the votes. They can also protect the privacy and anonymity of the voters, by using cryptography techniques such as encryption, hashing, and zero-knowledge proofs [22]. However, state-of-the-art solutions do not typically adhere to the most recommended privacy-by-design principles, and thus they are hardly adopted in realistic scenarios. BC-based e-Voting also faces many challenges, related to ensuring the security, integrity, privacy, and verifiability of the voting process and results [23].].

https://doi.org/10.63665/IJMEC.1104s.30
ISSN: 2456-4265
IJMEC 2026

For instance, despite the technological advancements, current e-Voting systems often suffer from insufficient privacy measures, which can compromise the integrity of voter data and undermine trust in these systems. Moreover, scalability and performance issues are critical considerations [24], particularly for deploying e-Voting systems across various network tiers, from small communities to large-scale elections. Additionally, BC-based e-Voting systems need to provide user-friendly interfaces and experience for the voters, who may not be familiar with the technical aspects of the system. Front-end DevOps teams are typically aware of the security and privacy threats related to their parts of the solution implementation. Yet, addressing privacy concerns in the back-end is directly related to the understanding of the BC technology as an enabler to e-Voting through several different approaches (e.g. Smart Contracts).

LITERATURE REVIEW

Title: Implementation of blockchain-based e-voting system.
Author: S. Tanwar, N. Gupta, P. Kumar, and Y.-C. Hu,
Year: 2024.
Description:
An electronic voting portal should provide security, integrity, vote transparency, and voter privacy. Electronic voting, or e-voting, has been used in many ways since the 1970s, with essential advantages over paper-based systems, such as higher efficiency and fewer errors. However, attaining widespread acceptance of such systems remains a problem, particularly in enhancing their resistance to potential mistakes. Blockchain is a cutting-edge technology that has the potential to improve the overall security of electronic voting systems. This paper uses smart contracts to develop an e-voting Decentralized Application (DApp) on the Ethereum blockchain and develops a frontend to access the DApp easily on the blockchain

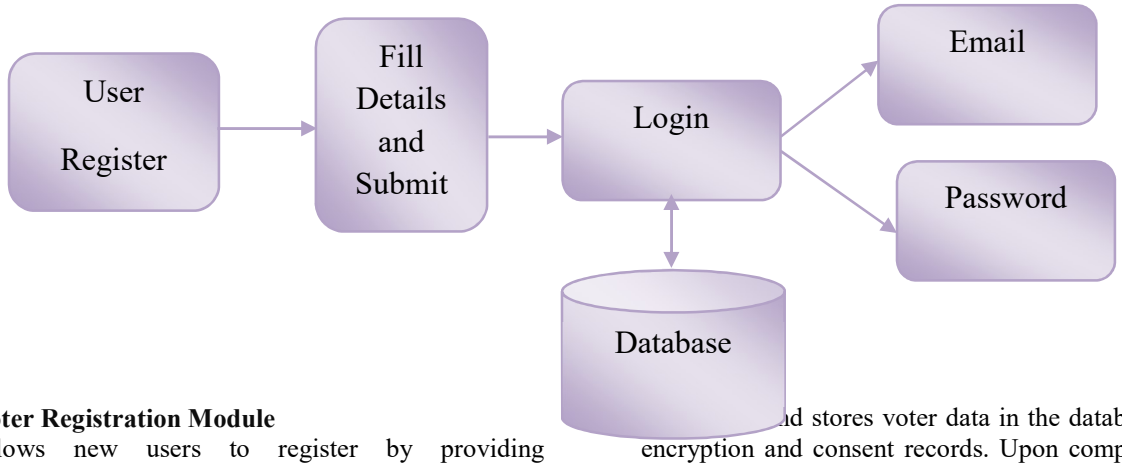
METHODOLOGIES

MODULES NAME: These following modules of this Project:

Module Name	Description
1. User Authentication Module	Manages secure voter and admin login with password hashing.
2. Voter Registration Module	Enables new voters to register with unique credentials.
3. Voter Verification Module	Allows admin to verify and approve registered voters.
4. Candidate Management Module	Lets admin add, view, and manage candidate details.
5. Voting Module	Allows approved voters to securely cast their votes.
6. Vote Validation Module	Enables admin to verify and confirm submitted votes.
7. Result Visualization Module	Displays election results through dynamic charts and tables.
8. Blockchain Vote Ledger Module	Records verified votes in a tamper-proof blockchain ledger.

User Authentication Module
This module manages secure login for both voters and administrators. Passwords are hashed using SHA-256 or bcrypt before storage to prevent credential leaks. Role-based access ensures that voters and admins access only their respective dashboards. The system also tracks login attempts, supports session management, and may include CAPTCHA or OTP verification for enhanced security.

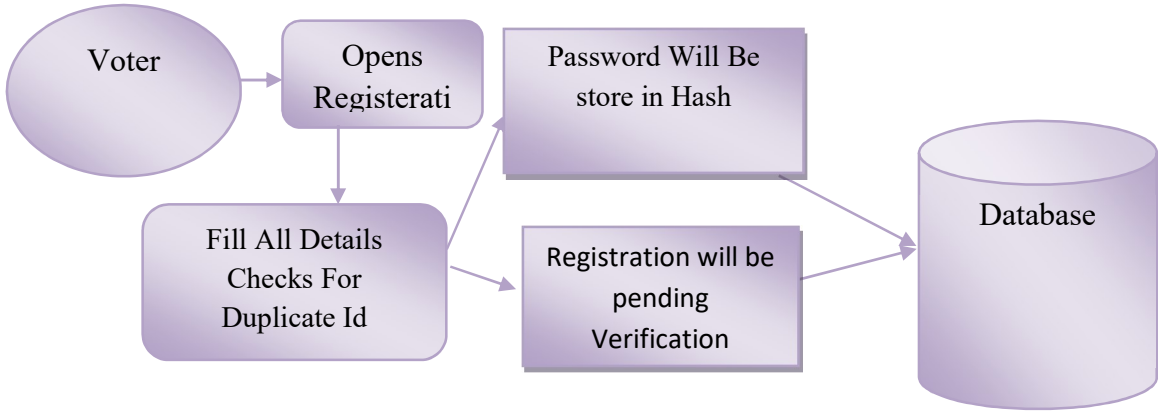
https://doi.org/10.63665/IJMEC.1104s.30
ISSN: 2456-4265
IJMEC 2026



Voter Registration Module

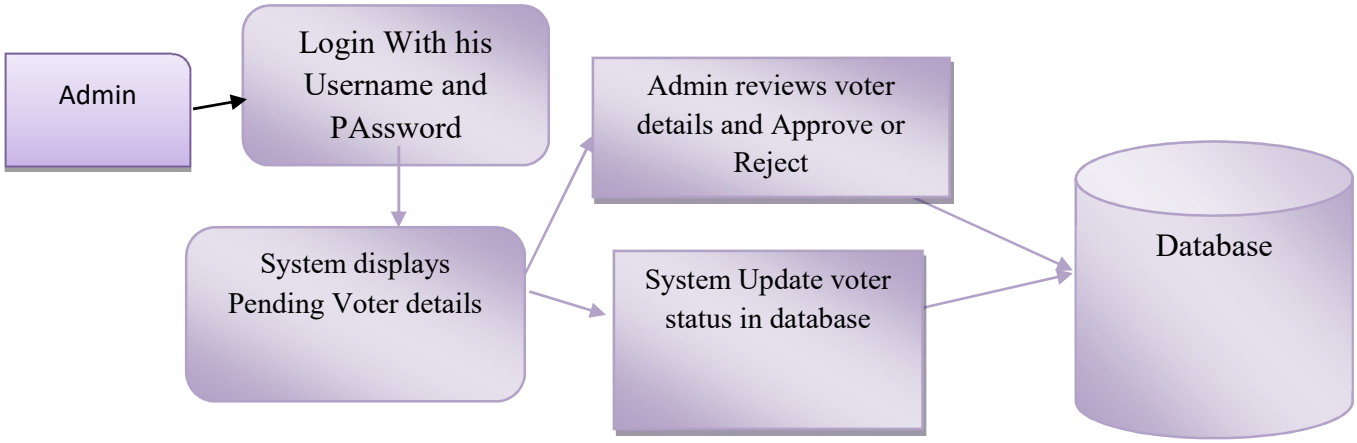
Allows new users to register by providing identification details (name, email, voter ID, etc.). During registration, the system validates uniqueness of

nd stores voter data in the database with encryption and consent records. Upon completion, a verification token is generated and sent for admin approval before activation.



Voter Verification Module

This module enables administrators to verify registered voters. The admin can review voter details, validate identity documents, and either approve or reject registrations. Approved voters receive activation emails and can then log in to cast votes. The verification ensures only legitimate and unique voters participate in the election.



https://doi.org/10.63665/IJMEC.1104s.30
ISSN: 2456-4265
IJMEC 2026

TECHNIQUE USED OR ALGORITHM USED PROPOSED ALGORITHM

BP-Vot (Blockchain-based Private Voting with Differential Privacy and SSI)

In the modern digital era, ensuring the privacy, transparency, and integrity of electronic voting systems has become a critical challenge due to the increasing threats of data tampering, identity fraud, and centralized manipulation. The **BP-Vot algorithm**, or Blockchain-based Private Voting with Differential Privacy and Self-Sovereign Identity (SSI), is an advanced cryptographic voting framework that integrates decentralized blockchain technology with privacy-preserving techniques and identity self-sovereignty principles. The primary goal of BP-Vot is to build a secure and auditable e-voting environment where voter anonymity, data confidentiality, and verifiable integrity are guaranteed without relying on a central authority. Unlike conventional electronic voting systems that depend on centralized databases vulnerable to breaches or manipulation, BP-Vot distributes voting records across a blockchain ledger, thereby ensuring immutability, non-repudiation, and tamper-proof storage. Each transaction in BP-Vot corresponds to a single vote, encrypted and hashed before being appended to the chain. The blockchain structure guarantees that once a vote is recorded, it cannot be modified or deleted, ensuring end-to-end verifiability and transparency of the election process.

A core innovation of BP-Vot lies in the **integration of Self-Sovereign Identity (SSI)**, which empowers voters to control and manage their digital identities independently. SSI is based on decentralized identifiers (DIDs) and verifiable credentials (VCs), allowing each voter to authenticate securely without exposing sensitive personal details to the election authority. During the registration phase, the voter generates a unique cryptographic identity (public-private key pair) stored within their SSI wallet. This wallet acts as a trust anchor, providing cryptographic proofs of authenticity without relying on any centralized identity provider. Through the use of blockchain-based decentralized identity frameworks, BP-Vot ensures that each voter can verify their eligibility and authenticity while remaining pseudonymous on the public ledger. The system eliminates the need for storing or sharing personally identifiable information (PII) directly with the voting servers, thus significantly reducing the risk of identity theft or data leakage. The SSI layer further facilitates zero-knowledge proof (ZKP) protocols, where a voter can prove their eligibility to vote without revealing their real identity or underlying credentials.

Another critical feature of BP-Vot is its **differential privacy (DP)** mechanism, which ensures that no statistical analysis of voting data can reveal information about individual voters' choices. Differential privacy introduces carefully calibrated random noise to aggregated voting data or intermediate computations, ensuring that even if the system or dataset is analyzed, the likelihood of identifying a specific voter's decision remains negligible. This method mathematically guarantees privacy protection while still enabling accurate computation of election outcomes. The differential privacy component in BP-Vot typically operates at the tallying stage, where the system aggregates encrypted votes and adds controlled noise before publishing final statistics. The addition of noise is done in a way that the overall voting results remain statistically valid but prevent any adversary from inferring individual vote preferences. This approach strikes a balance between transparency and privacy, a challenge that traditional blockchain-based voting schemes often struggle with due to the public visibility of ledger data.

In the **tallying phase**, the BP-Vot framework employs a homomorphic decryption mechanism that enables vote counting without decrypting individual votes, preserving end-to-end confidentiality. The system aggregates ciphertexts and applies decryption only to the final sum, ensuring that no individual vote is exposed at any stage. To further enhance privacy, differential privacy algorithms are applied to the decrypted aggregate results to introduce minimal noise before final publication. This prevents adversaries from correlating voting results with potential identity patterns or small constituency groups. The final results are then published on the blockchain, allowing any stakeholder to independently verify the integrity of the outcome using the public ledger. This decentralized verification model builds trust among voters and election authorities by ensuring that every step of the voting process — from voter registration to result declaration — is transparent, verifiable, and tamper-proof.

CONCLUSION

Java offers several features that make it well-suited for interacting with databases. One of its key strengths is the Java Database Connectivity (JDBC) API, which provides a standard interface for connecting to relational databases. JDBC enables Java applications

https://doi.org/10.63665/IJMEC.1104s.30
ISSN: 2456-4265
IJMEC 2026

to execute SQL queries, update data, and manage database connections, allowing developers to work with databases in a consistent and platform-independent way. Java also supports Object-Relational Mapping (ORM) frameworks like Hibernate, which simplify the interaction between Java objects and relational database tables, reducing the need for boilerplate SQL code.

FUTURE ENHANCEMENT

To provide a proof of principle, we designed and implemented our differential privacy method such that a single pivot candidate is selected. As we have shown, this is practically sufficient to achieve anonymity of all votes regardless of their originally elected candidate. Meanwhile, only approximated vote number values are published which does not provide sufficient information to deduce who originally elected whom. In the future, we plan to investigate the applicability and potential of a parallel differential privacy method, where several pivot candidates guide the anonymization mechanism, instead of a single pivot.

REFERENCE

[1] J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, ‘‘A review of E voting: The past, present and future,’’ Ann. Telecommun., vol. 71, nos. 7–8, pp. 279–286, Aug. 2016.

[2] W. Bokslag and M. de Vries, ‘‘Evaluating e-voting: Theory and practice,’’ 2016, arXiv:1602.02509.

[3] M. Hapsara, ‘‘Reinstating e-voting as a socio-technical system: A critical review of the current development in developing countries,’’ in Proc. IEEE Region 10 Symp. (TENSYMP), May 2016, pp. 282–287.

[4] S. Risnanto, Y. B. A. Rahim, and N. Suryana, ‘‘Success implementation of E-voting technology in various countries: A review,’’ in Proc. FoITIC, Jan. 2020, pp. 150–155.

[5] L. E. Pleger and A. Mertes, ‘‘Use and assessment of E-voting systems: Findings from an online-survey among Swiss nationals living abroad,’’ Yearbook Swiss Administ. Sci., vol. 9, no. 1, p. 1, Sep. 2018.

[6] J. JumaandC.O.Oguk,‘‘Election results’ verification in e-voting systems in Kenya: A review,’’ Int. J. Social Sci. Inf. Technol., vol. 2020, pp. 1–14, Dec. 2020.

[7] R. H. A. Rathnayake, ‘‘Electronic voting system based on blockchain for Sri Lanka: Conceptual overview,’’ Int. J. Sci. Res., vol. 12, no. 2, pp. 114–125, Feb. 2023.

[8] T. Haines, ‘‘Review of the overseas e-voting (OSEV) system used in the Australian capital territory,’’ in Proc. 7th Int. Joint Conf. Electron. Voting, 2022, p. 102.

[9] M. Alam, I. R. Khan, and S. Tanweer, ‘‘Blockchain technology: A critical review and its proposed use in E-voting in India,’’ in Proc. Int. Conf. Innov. Comput. Commun. (ICICC), Jan. 2020, pp. 1–8.

[10] O. Okuro, ‘‘Comparative review of e-voting in India and Brazil: Key lessons for Kenya,’’ Lagos Historical Rev., vol. 21, no. 1, pp. 26–56, 2021.

[11] O. Osho, V. L. Yisa, and O. J. Jebutu, ‘‘E-voting in Nigeria: A survey of voters’ perception of security and other trust factors,’’ in Proc. Int. Conf. Cyberspace (CYBER-Abuja), Nov. 2015, pp. 202–211.

[12] A. Polushin, Y. Lanrong, and M. S. Nisar, ‘‘Exploring e-voting in Moscow region, Russia: A survey of voters’ perception of trust in government and other factors,’’ Int. J. Basic Sci. Appl. Comput., vol. 2, no. 5, pp. 1–9, 2018.

[13] M.O’Meara,‘‘Survey&analysisofe-votingsolutions,’’ M.S. thesis, Univ. Dublin, Dublin, Ireland, 2013. [14] H. Baniata, A. Anaqreh, and A. Kertesz, ‘‘Distributed scalability tuning for evolutionary sharding optimization with random-equivalent security in permissionless blockchain,’’ Internet Things, vol. 24, Dec. 2023, Art. no. 100955.

[15] S. Nakamoto, ‘‘Bitcoin: A peer-to-peer electronic cash system,’’ Decen tralized Bus. Rev., Oct. 2008, Art. no. 21260, doi: 10.2139/ssrn.3440802.

[16] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, ‘‘On blockchain and its integration with IoT. Challenges and opportunities,’’ Future Gener. Comput. Syst., vol. 88, pp. 173–190, Nov. 2018.

[17] P. Treleaven, R. Gendal Brown, and D. Yang, ‘‘Blockchain technology in f inance,’’ Computer, vol. 50, no. 9, pp. 14–17, 2017.

[18] P. Dutta, T.-M. Choi, S. Somani, and R. Butala, ‘‘Blockchain technology in supply chain operations: Applications, challenges and research oppor tunities,’’ Transp. Res., E, Logistics Transp. Rev., vol. 142, Oct. 2020, Art. no. 102067.

https://doi.org/10.63665/IJMEC.1104s.30
ISSN: 2456-4265
IJMEC 2026