International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Cloud Based Encrypted Online Voting System

Ms. M. Samyuktha
Asst. Professor
Mahatma Gandhi Institute of Technology
Kokapet (V), Gandipet (M), Hyd-75
Affliated to JNTUH
msamyuktha_cse@mgit.ac.in
Computer Science and Engineering

Ms. K. Shirisha
Asst. Professor
Mahatma Gandhi Institute of Technology
Kokapet (V), Gandipet (M), Hyd-75
Affliated to JNTUH
kshirisha_cse@mgit.ac.in
Computer Science and Engineering

Gowdappagari Mokshith Reddy
Student of Computer Science and Engineering
Mahatma Gandhi Institute of Technology
Hyderabad 500075, India
gmokshithreddy_cse2405u6@mgit.ac.in

Kanneboina Sai Charan
Student of Computer Science and Engineering
Mahatma Gandhi Institute of Technology
Hyderabad 500075, India
ksaicharan_cse2405v2@mgit.ac.in

***Abstract*—In today's digital era, secure and accessible online platforms have become essential for conducting efficient and transparent election processes. The Cloud-Based Encrypted Online Voting System is a secure and efficient web-based platform designed to enable users to cast their votes remotely through cloud infrastructure. The system ensures confidentiality and integrity by encrypting votes before storing them in the cloud database, thereby preventing unauthorized access and tampering. It includes modules such as user registration, secure login authentication, candidate management, vote casting, and result generation. By leveraging cloud technology, the platform offers scalability, accessibility, and real-time data management while reducing the limitations of traditional voting methods. This project aims to provide a reliable, transparent, and user-friendly solution for modern digital elections.**

***Index Terms*--AES-256 Encryption, bcryptjs, Cloud Computing, Express.js, JWT Authentication, MongoDB, Node.js, Online Voting System, Role-Based Access Control.**

I. Introduction

The rapid growth of digital technologies has significantly transformed the way organization manage communication, administration, and decision- making processes. Among these transformations, the voting and election process has emerged as one of the most important areas requiring modernization. Traditional voting systems, which rely on paper ballots, manual verification, and physical presence, often face several challenges such as time-consuming procedures, higher operational costs, human errors, delayed result declaration, and limited accessibility. These limitations become more critical when elections involve a large number of participants and require secure, transparent, and tamper-proof result management.

The emergence of cloud computing and secure web technologies has enabled the development of efficient digital voting platforms that overcome the drawbacks of conventional systems. A cloud-based voting platform provides centralized election management, remote access, real-time data processing, and improved scalability. Furthermore, advanced security mechanisms such as JWT-based authentication, role- based access control, password hashing, and AES-256 encryption ensure confidentiality, integrity, and protection against unauthorized access or vote tampering. The CloudBased Encrypted Online Voting System is developed as a secure and efficient web-based application that modernizes the complete election workflow. The system also provides dedicated interfaces for administrators and voters, enabling secure registration, election creation, candidate management, vote casting, encrypted vote storage, automated result generation, and election analytics. By leveraging cloud infrastructure, the proposed system improves reliability, transparency, and user accessibility while reducing manual effort and administrative complexity.

A. Background and Significance

In the present digital era, secure online platforms have become essential for simplifying administrative and organizational processes. Election systems are one of the most critical applications where security, transparency, and reliability are of utmost importance. Traditional voting methods often involve manual verification, paper ballots, and physical counting, which can lead to delays, human errors, duplicate voting, and reduced transparency. With the advancement of cloud technologies and secure web frameworks, online voting systems have emerged as an efficient solution to overcome these limitations. The significance of this study lies in developing a secure cloud-

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

based platform that ensures one-time voting, encrypted vote storage, and transparent result generation while improving accessibility and reducing administrative effort.

B. Definitions and Scope

The Cloud-Based Encrypted Online Voting System is a secure web-based application developed to conduct elections digitally through cloud infrastructure. The system enables both administrators and voters to interact through dedicated interfaces. Its scope includes voter registration, secure authentication, election creation, candidate management, vote casting, encrypted data storage, result processing, and election.

Transparent election management is required. By integrating technologies such as JWT authentication, AES-256 encryption, bcryptjs, Node.js, Express.js, and MongoDB, the system is designed to support scalable and secure real-world deployment.

C. Purpose and Relevance of the Study

The purpose of this study is to design and implement a secure and efficient digital voting platform that modernizes the election process. This study is highly relevant in today's environment, where institutions and organizations increasingly require reliable online systems for conducting transparent elections. The proposed system addresses the limitations of conventional voting methods by providing secure authentication, duplicate vote prevention, encrypted vote storage, automated result generation, and real-time accessibility. This makes the system highly relevant for modern digital governance and institutional election processes.

D. Objectives

The primary objective of the proposed system is to design and develop a secure cloud-based online voting platform that simplifies and modernizes the election workflow. Specific objectives are listed below:

1. Provide reliable user authentication using JWT and bcryptjs with role-based access control for administrators and voters.
2. Ensure vote confidentiality through AES-256 symmetric encryption before database storage.
3. Prevent duplicate voting by enforcing a strict one-vote-per-election policy per eligible voter.
4. Automate vote counting and result generation to minimize manual effort and errors.
5. Improve scalability, transparency, and accessibility through cloud-based architecture and real-time monitoring.

II. LITERATURE SURVEY

A. Existing Studies and Comparative Analysis

The literature survey provides an understanding of the existing approaches, technologies, and methodologies used in online voting systems. Several researchers have proposed digital voting platforms to improve election transparency, accessibility, and operational efficiency. Earlier systems primarily focused on web-based voting applications with basic authentication and manual result processing. While these systems simplified the voting process compared to traditional paper-based methods, they often lacked advanced security mechanisms such as strong encryption, secure session management, and role-based access control.

The literature survey provides an understanding of the existing approaches, technologies, and methodologies used in online voting systems. Several researchers have proposed digital voting platforms to improve election transparency, accessibility, and operational efficiency. Earlier systems focused on web-based applications with basic authentication and manual result processing. While these simplified voting compared to paper-based methods, they lacked advanced security mechanisms such as strong encryption, secure session management, and role-based access control.

Kumar and Singh [1] proposed a blockchain and AES-based hybrid secure online voting system that combines blockchain integrity with AES encryption for tamper-proof vote storage and improved election transparency. However, the approach suffers from blockchain latency and complex deployment requirements, reducing practicality in large-scale implementations.Sharma et al. [2] presented an AI-driven secure cloud e-voting system with AES encryption, where artificial intelligence is used for anomaly detection and fraud prevention. The system offers cloud-based scalability but requires high computational resources and stable internet connectivity.Chen and Patel [3] introduced an end-to-end verifiable e-voting system on cloud infrastructure, focusing on encrypted vote transmission and transparent result verification. While it improves voter trust, the complex verification steps and limited real-world testing remain significant drawbacks.Reddy and Gupta [4] proposed a secure online voting system using AES-256 encryption, designed as a simple web-based portal with secure user authentication. However, the system lacks scalability analysis and multi-factor authentication, affecting its reliability in large-scale environments.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

TABLE I
COMPARATIVE ANALYSIS OF VOTING SYSTEMS

Parameter	Traditional System	Existing System	Proposed System
Accessibility	On-site only	Remote limited	Cloud access
Security	Basic	Moderate	AES-256 secured
Authentication	Manual	Login based	JWT based
Accuracy	Variable	High	Very high
Transparency	Limited	Moderate	High
Results	Manual	Semi-auto	Automated

Recent studies have introduced more sophisticated solutions by integrating cloud computing, encryption algorithms, and authentication frameworks. Some systems use AES-based encryption to ensure secure vote storage, while others employ JWT-based authentication and cloud deployment for scalability and accessibility. Although these approaches provide improvements over conventional methods, challenges such as limited real-time monitoring, complex deployment, and insufficient vote confidentiality still remain.

B. Research Gap and Need for Study

Despite the significant progress in online voting technologies, several limitations continue to exist in existing systems. Many previously developed platforms focus mainly on basic authentication and vote storage, without providing strong encryption, scalable cloud infrastructure, and reliable duplicate vote prevention mechanisms. Some systems offer secure login facilities but do not ensure full vote confidentiality, while others provide encryption but lack accessibility and real-time processing and the analytics. Therefore, there is a clear need for a secure and scalable cloud-based voting platform that combines advanced encryption, role-based authentication, duplicate vote prevention, and automated result generation within a unified system.

III. METHODOLOGY

The methodology adopted for the proposed system focuses on developing a secure, scalable, and reliable platform for conducting digital elections. The study follows a systematic implementation-oriented approach involving requirement analysis, system planning, secure backend development, encrypted vote storage, and automated result generation. The methodology emphasizes security, accessibility, and transparency throughout the election lifecycle.

A. Research Design

The research design of this study is based on a practical development and implementation approach. Initially, the limitations of traditional and existing online voting systems were analyzed through the literature survey. Based on the identified research gap, a secure cloud-based voting framework was designed to address issues such as weak authentication, insufficient vote confidentiality, and limited transparency.The design process includes database schema planning, user role separation, authentication logic, encryption-based vote storage, and result automation. Special emphasis was given to ensuring one-time voting, secure access control, and cloud-based deployment for improved scalability.

B. Frameworks and Tools

The proposed system is developed using modern full-stack web technologies and security frameworks. [1] The frontend interface is built using HTML, CSS, and JavaScript to provide a responsive and user-friendly experience. [2] The backend services are implemented using Node.js and Express.js, enabling scalable server-side processing and RESTful API integration. [3] MongoDB is used as the cloud database for storing user information, candidate details, and encrypted vote records. [4] Security is ensured through JWT-based authentication, bcryptjs password hashing, and AES-256 encryption for secure vote storage. [5] Development and testing tools include Visual Studio Code and GitHub.

C. System Architecture

The system architecture is structured into six principal modules that work together to deliver a secure and seamless election experience:

- **User Interface Module:** Provides interactive web pages for login, registration, dashboard, candidate listing, active elections, vote casting, and result display. It acts as the communication layer between the user and backend server.
- Authentication Module: Performs role-based user verification using JWT and bcryptjs, ensuring only authorized users access admin controls or voter pages.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

- Election Management Module: Allows administrators to create elections, add candidates, manage voter details, set schedules, and monitor election activities in real time.
- Voting Module: Enables secure, one-time vote casting by eligible voters. Votes are encrypted before storage to prevent tampering.
- Database Module: Uses MongoDB to store user credentials, election details, candidate records, encrypted vote logs, and audit information.
- Result Processing Module: Performs automatic vote counting, tally generation, and transparent result display with graphical analytics.

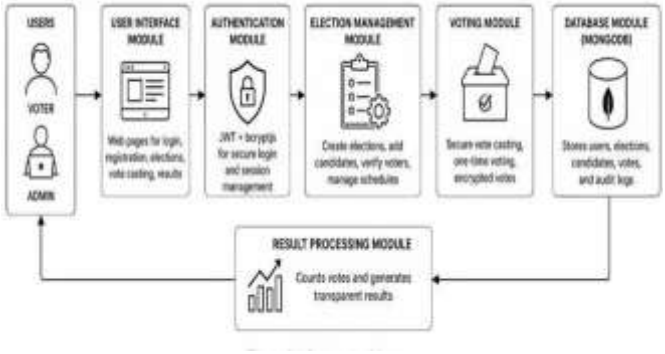

Fig. 1. System Architecture of the Proposed Voting System.

D. Security Mechanisms

Three core security mechanisms are employed in the proposed system:

JSON Web Token (JWT) is used for secure authentication and session management. After a user successfully logs in, the server generates a signed token that validates subsequent requests and controls access to protected routes based on user role. JWT is lightweight, stateless, and ideal for role-based access control in RESTful APIs.

AES-256 Encryption, implemented through the Node.js Crypto module, encrypts all vote data before it is stored in the database. This symmetric encryption standard uses a 256-bit key to convert vote information into ciphertext, ensuring that even if the database is compromised, vote data remains unreadable. Proper key management is essential to maintain the integrity of this mechanism.

Bcryptjs is used for password hashing and secure storage of user credentials. Before storing passwords, bcryptjs applies a strong hashing algorithm with configurable salt rounds. This ensures that original passwords cannot be retrieved even if the database is breached, and it effectively resists brute-force and rainbow table attacks.

IV. IMPLEMENTATION

The implementation phase of the proposed Cloud-Based Encrypted Online Voting System focuses on translating the designed methodology into a fully functional and secure web application. A full-stack development approach was adopted to ensure seamless integration between the frontend user interface, backend services, and cloud-based database. The system was developed in a modular architecture to enhance scalability, maintainability, reusability, and security of the application components.

A. Frontend Implementation

The frontend of the system was developed using HTML, CSS, and JavaScript to create an interactive, responsive, and user-friendly interface. The design follows a role-based structure, providing separate dashboards for administrators and voters, ensuring controlled access to system functionalities.The voter interface includes modules for secure registration, login authentication, election participation, candidate viewing, and vote casting. The administrator interface provides functionalities such as election creation, candidate management, voter verification, and real-time result visualization.Special emphasis was placed on responsive web design principles, ensuring compatibility across desktops, tablets, and mobile devices. Dynamic page updates were implemented using JavaScript to improve user experience by reducing page reloads and enhancing interactivity. Form validations were also integrated at the client side to minimize incorrect data submissions before server processing.

B. Backend Implementation

The backend of the system was developed using Node.js and Express.js, which serve as the core of server-side processing and API management. The backend is responsible for handling authentication requests, processing votes, managing elections, and interacting with the database.A set of RESTful APIs was designed and implemented to enable communication between the frontend and backend layers. These APIs include endpoints for user authentication, voter registration, election creation, vote submission, and result retrieval.To ensure secure access control, role-based authentication mechanisms were implemented, restricting administrative operations to authorized users only. Middleware functions in Express.js were used to validate incoming requests, verify JWT tokens, and enforce security policies before granting access to protected routes.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Additionally, error handling and request validation mechanisms were incorporated to ensure system stability and prevent unexpected failures during runtime.

C. Database and Security Integration

The database layer was implemented using MongoDB, a NoSQL database that provides flexibility in handling structured and semi-structured election data. The database stores critical information such as user credentials, voter profiles, candidate details, election metadata, and encrypted vote records.To enhance security and ensure data integrity, multiple cryptographic techniques were integrated into the system:

- JWT (JSON Web Token) was used for secure user authentication and session management, ensuring that only authenticated users can access protected resources.
- bcryptjs hashing algorithm was applied to securely store user passwords in hashed form, preventing plain- text password exposure.
- AES-256 encryption was implemented for encrypting vote data before storage, ensuring confidentiality and protecting votes from unauthorized access or tampering.

The combination of these security mechanisms ensures end-to- end protection of sensitive election data, maintaining confidentiality, integrity, and authenticity throughout the voting process. The cloud-based database architecture also enables high availability and efficient data retrieval during election operations.

V. Results And Discussion

The proposed system was successfully developed and tested under normal operational conditions. The system was evaluated based on parameters such as security, accessibility, response time, transparency, and result processing efficiency. The results indicate that the proposed system significantly improves the reliability and usability of digital election management when compared with traditional and existing online voting platforms.The implementation of JWT-based authentication and AES-256 encryption ensured secure access control and confidential vote storage. The cloud-based deployment enabled efficient real-time data processing and automated result generation.

A. User Module Results

The Home Page provides navigation options for Home, About, and Elections sections, enabling users to explore the system. The About Page describes system features including transparent elections, role-based access, and secure voting mechanisms. The Elections Center Page displays ongoing, upcoming, and past elections in a tabbed layout. Each election card presents the election type, candidate count, and action buttons for voting, viewing candidates, and viewing results. The Login Page provides role selection (Voter/Admin), and upon successful JWT authentication, users are redirected to their respective dashboards.

B. Voting Module Results

The Vote Casting Page displays a modal with candidates' names and symbols for the selected election. Only ongoing elections allow voting. Upon selection and submission, the encrypted vote is transmitted to the backend, validated by JWT middleware, and stored in MongoDB after AES-256 encryption. The Vote Confirmation screen confirms successful submission and updates the election card to display 'Vote Recorded', disabling further voting for that user in that election. This enforces the one-vote-per-election policy at both the frontend and backend levels.

C. Admin Module Results

The Admin Dashboard provides a unified control panel for managing elections, candidates, voters, and reviewing election performance. The Election Performance section displays summarized metrics including total candidates, registered voters, votes cast, and winner status for each election. The Election Analytics section provides live bar charts showing candidate and voter counts, and pie charts visualizing vote distribution by party. The Create Election and Add Candidate interfaces allow administrators to configure election schedules, types, and candidate details. The Manage Elections and Verify Voters interface enables status updates and voter approval workflows.

D. Performance Analysis

The performance analysis demonstrates fast response times during login authentication, vote submission, and result generation. The automated backend processing reduces manual effort and minimizes errors. JWT-based authentication ensures secure, stateless session handling that scales effectively with increasing users. AES-256 encryption introduces minimal overhead during vote submission and result decryption, which is negligible compared to the security benefit. The MongoDB cloud database supports concurrent user sessions and provides reliable data persistence.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

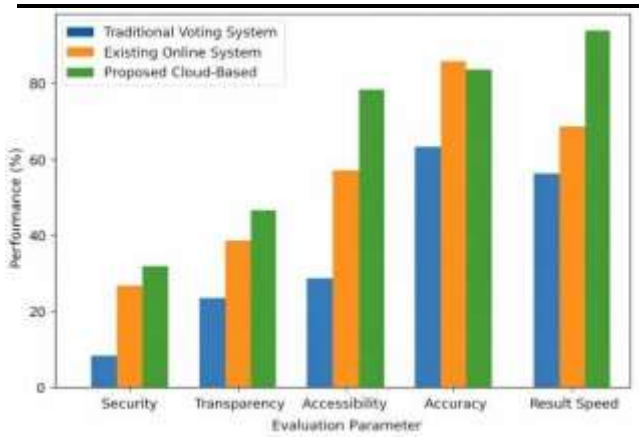

Fig. 2. Comparative Performance Analysis of Voting Systems.

Figure 2 illustrates the comparative performance evaluation of three voting systems: Traditional Voting System, Existing Online Voting System, and Proposed Cloud-Based Voting System across five key evaluation parameters: Security, Transparency, Accessibility, Accuracy, and Result Speed. The proposed cloud-based voting system demonstrates superior performance in most parameters, particularly in Accessibility and Result Speed, indicating enhanced efficiency and user convenience. The existing online voting system shows moderate performance across all parameters, while the traditional voting system records comparatively lower values, especially in Security and Accessibility. Overall, the analysis highlights the effectiveness of the proposed cloud-based voting system in improving the reliability, speed, and accessibility of the voting process.

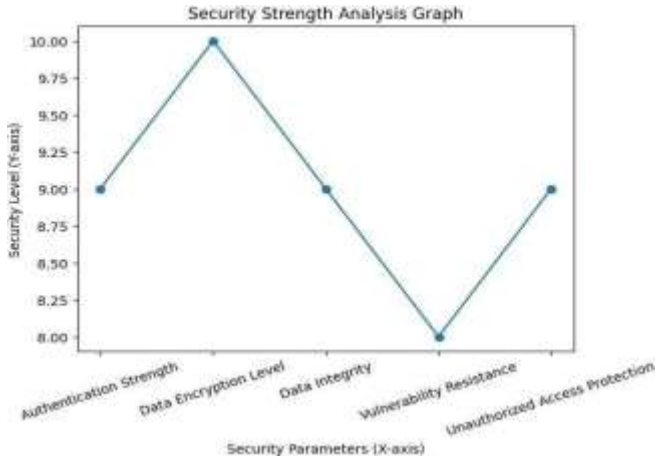

Fig. 3. Security Strength Analysis Graph

The Security Strength Analysis Graph provides a visual assessment of how well the system performs across key security dimensions. It evaluates critical parameters such as authentication strength, encryption level, data integrity, vulnerability resistance, and protection against unauthorized access.From the graph, the system demonstrates consistently high security performance, with particularly strong results in data encryption (AES-256) and authentication mechanisms (JWT-based). While all areas score well, vulnerability resistance is slightly lower, indicating a minor scope for further strengthening.Overall, the graph highlights that the system is robust, reliable, and well-protected against common security threats, making it suitable for secure applications.

VI. Conclusion And Future Scope

A. Conclusion

The Cloud Based Encrypted Online Voting System demonstrates the development of a secure and efficient platform for conducting digital elections. The system enables voters to participate through an easy-to-use interface while maintaining confidentiality, preventing duplicate voting, and ensuring transparent result generation. Features such as JWT-based user authentication, AES-256 encrypted vote storage, role-based access control, automated result visualization, and a comprehensive admin module collectively enhance the security, reliability, and transparency of the election process.Compared to traditional and existing systems, the proposed platform significantly reduces administrative effort, eliminates manual result processing, and enforces strict one-vote-per-election integrity. The cloud-based architecture provides the scalability and accessibility needed for real-world deployment in educational institutions, organizations, and committees. Overall, the system provides a reliable, user-friendly solution that modernizes election administration while upholding the highest standards of data security and process transparency.

B. Future Scope

Future enhancements to the Online Voting System include integrating biometric verification, facial recognition, and One- Time Password (OTP)-based login mechanisms for multi- factor authentication. Incorporating end-to-end cryptographic protocols and blockchain-based immutable audit logs can further strengthen the system's suitability for large-scale governmental elections. Mobile-based applications for iOS and Android will increase accessibility and voter participation. Additional planned features include multilingual support, screen-reader accessibility for visually impaired users, real- time push notifications for election schedules, and advanced data analytics dashboards for deeper insights into voter participation trends. These enhancements

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

will make the system more scalable, secure, and adaptable for modern digital governance.

REFERENCES

[1] R. Kumar and P. K. Singh, "Blockchain and AES-Based Hybrid Secure Online Voting System," *Int. J. Cyber Security and Digital Forensics*, vol. 14, no. 2, pp. 101–110, 2025.

[2] A. Sharma, R. Gupta, and M. Patel, "AI-Driven Secure Cloud E-Voting System with AES Encryption," *J. Cloud Computing: Advances, Systems and Applications*, vol. 14, no. 1, pp. 45–57, 2025.

[3] L. Chen and S. Patel, "End-to-End Verifiable E-Voting on Cloud Infrastructure," *IEEE Trans. Inf. Forensics Security*, vol. 19, no. 4, pp. 2310–2322, 2024.

[4] K. Reddy and P. Gupta, "Secure Online Voting Using AES-256 Encryption," *Int. J. Comput. Appl.*, vol. 185, no. 12, pp. 22–28, 2023.

[5] R. L. Rivest, "Electronic Voting," *Commun. ACM*, vol. 51, no. 11, pp. 46–50, Nov. 2008.

[6] D. Chaum, "Secret-Ballot Receipts: True Voter-Verifiable Elections," *IEEE Security Privacy*, vol. 2, no. 1, pp. 38– 47, Jan.–Feb. 2004.

[7] A. Fujioka, T. Okamoto, and K. Ohta, "A Practical Secret Voting Scheme for Large Scale Elections," in *Advances in Cryptology—AUSCRYPT*, Berlin: Springer, 1992, pp. 244–251.

[8] K. Suresh and P. K. Sharma, "Secure Online Voting System Using Web Technologies," *Int. J. Comput. Appl.*, vol. 179, no. 21, pp. 15–19, 2018.

[9] S. Neha and R. Kumar, "Design and Implementation of an Online Voting System," *Int. J. Eng. Res. Technol.*, vol. 9, no. 6, pp. 112–116, 2020.

[10] M. H. Ibrahim and A. K. Singh, "Web-Based Secure Online Voting System Using Authentication Techniques," *Int. J. Adv. Res. Comput. Sci.*, vol. 10, no. 2, pp. 45–50, 2019.

[11] I. Sommerville, *Software Engineering*, 10th ed. London: Pearson Education, 2016.

[12] Node.js Foundation, "Node.js Documentation," 2024. [Online]. Available: https://nodejs.org/docs

[13] MongoDB Inc., "MongoDB Documentation," 2024. [Online]. Available: https://www.mongodb.com/docs