Geocrypt: Location-Based Secure File Encryption and Access Control

Thenmozhi P [1], Saralesh V D[2], and Sakthi R[2]

[1]Assistant Professor, Dept of Electronics and Communication Engineering, St. Joseph's College of Engineering, Chennai
[2]Final Year Under Graduate Student, Dept of Electronics and Communication Engineering, St. Joseph's College of Engineering, Chennai

Abstract. In the digital age, traditional file-sharing systems are vulnerable to unwanted access, data manipulation, and a lack of transparency, especially in applications that depend on location and have time limits. Secure Timeshare, a dual encryption system that uses geographic and time-based controls, along with blockchain technology, is the solution this project offers to address these issues. Users and administrators can safely upload and exchange encrypted files using RSA. Access is tightly regulated, hinging on both the user's physical location and time-limited sessions. Ethereum smart contracts, deployed using Truffle and Ganache, create unchangeable records of file-sharing transactions. This setup ensures openness, accountability, and the capacity to conduct audits. The system supports both direct user-to-user exchanges and broadcasts managed by administrators, all while providing robust monitoring and rule-based access control. The innovation lies in the integration of several key elements: dual-layer encryption, geolocation for location verification, time-limited access controls, and the unalterable nature of the blockchain. This creates a highly secure, decentralized, and context-sensitive platform for file sharing. It's particularly well-suited for sensitive applications within government, corporate, healthcare, and defence environments.

1. Introduction

In today's digital world, secure and controlled data sharing is essential for governments, corporations, and individuals. As online communication and cloud storage become more common, sensitive information is increasingly vulnerable to unwanted access, data breaches, and privacy violations. Traditional file-sharing systems, which rely on centralized servers, are vulnerable to security issues [1]. These include data modification, unauthorized access, and the risk of a single point of failure. These flaws are very concerning, especially when secrecy, integrity, and responsibility are crucial.

Furthermore, while conventional encryption techniques provide a basic level of security, they fail to address contextual requirements such as location-based and time-constrained viewing, both of which are essential for effectively controlling the dissemination of sensitive data in practical scenarios.

To address these challenges, the project suggests a decentralized and secure file-sharing system. This system integrates cryptographic methods with geolocation and temporal access controls. Furthermore, it leverages blockchain technology to provide transparency and immutability. The system supports both one-to-one and one-to-many communication methods [2]. It also allows for secure file sharing between users and administrators, with strict limits on who may access the data and under what conditions. By including geographical coordinates as metadata in the files and setting time limits, the system restricts access to users who are in the right place and during the approved time.

Through multi-level security, the system prevents unauthorized use, reduces the possibility of data leakage, and keeps sensitive information password-protected and only accessible by the intended recipients. The employment of RSA encryption ensures [3] that files are secret throughout storage and transmission, and the use of blockchain technology offers an immutable record of all file-sharing operations. Smart contracts running on the Ethereum blockchain via Truffle and executed on the Ganache test net register all transactions, such as upload of files, requests for access, approvals, and expirations. Since the decentralized ledger provides for auditability and accountability, the access histories can be confirmed and malicious or unauthorized tries can be identified by the administrators and stakeholders.

[1] Corresponding author: thenmozhip@stjosephs.ac.in

A central authority is no longer needed and the system has therefore built up trust and at the same time decreased the possibility of any compromise, user module that grants access based on geofencing, owner approval, and time-limited conditions, and the use of temporary decryption tokens to ensure that there are no misuse or unauthorized sharing of access.

The system keeps meticulous records of every request, permission, and viewing session, which bolsters both openness and the capacity to track everything. The admin module takes things a step further, allowing the administrator to oversee the entire system. This includes monitoring user actions and making it easy to share files with multiple users simultaneously. Administrators have the ability to upload files, making them accessible to several users within a designated area. They can also approve or reject access requests [5], adjust permissions that are time-sensitive, and revoke access as necessary. Admin actions are recorded on the blockchain, creating a transparent audit trail. This ensures accountability and helps meet regulatory requirements. The combination of centralized control and decentralized transaction authentication provides a balanced approach to both governance and security.

The solution, by using dual encryption, location-based access controls, temporary viewing periods, and blockchain technology to ensure data integrity, overcomes the shortcomings of standard file-sharing programs. It's built for robust security, controlled dissemination, and trustworthy verification in digital communications. This makes it well-suited for sensitive uses, as outlined in [6], including government data transfers, corporate information sharing, healthcare record management, and defense- related applications. Ultimately, the project offers a decentralized, transparent, and secure framework for encrypting sensitive data. It also facilitates verifiable and accountable information transmission within today's digital environments.

This work structured with Section II as a review of the existing literature. Section III describes the methodology, focusing on how it works in practice. Section IV contains the results and discussions. The final section, Section V, presents the main findings and offers recommendations.

.

2. Literature Survey

The exponential growth of digital communication and cloud storage elevated the necessity for secure and regulated mechanisms for sharing files. Centralized server- dependent systems available thus far are prone to hackers, data manipulation, and unauthorized use. Though basic security is offered through traditional encryption solutions, the contextual issues like geospatial use and time-limited usage are usually not catered for. Latest studies propose the incorporation of blockchain, geolocation authentication, and time-limited accessibility for improved security and openness. This literature survey considers the existing work done on secure file-sharing systems with an emphasis on the deficiencies of multi-level security, auditability, and regulated diffusion, which the system under proposal intends to cover effectively.

Audio communication is the cornerstone of both personal and commercial applications, calling for advanced security. Biological sequences carry enormous information encoding possibility, motivating an innovative framework that successively encrypts and compresses audio frames. The technology allows for secure audio communication, using both general and frequency-specific technical information, without needing user interaction [7]. The experimental results indicate strong resilience to security threats, suggesting that bio-inspired encryption could be useful in real-time audio applications. This technology is a step toward creating intelligent, automated, and highly efficient encryption systems. These systems are designed to protect sensitive conversations and manage data effectively, while also maintaining data integrity under different streaming settings.

The rising popularity of cloud storage is attributed to cost-effectiveness and sharing advantages for data, but it decreases server utilization when duplicate storage occurs. It is difficult for encrypted data with the complexity of maintaining privacy to de-duplicate information. A system facilitates the secure identification and elimination of duplicate files and enables authorized users to recover encrypted content securely. Through re-encryption key [8] appends within ciphertext chains, the system allows for any user to decrypt and access shared data. Evaluation and simulation validate the strategy of striking a balance among cloud environment security, efficiency, and usability and resolving both storage optimization and privacy retention without conceding accessibility or imposing substantial user or cloud server computational overhead.

Video transmission is subjected more and more to security threats with the growth of computing powers. Combining quantum encryption with classical transmission techniques provides increased security. A hybrid system employs pseudorandom keys for the purpose of the XOR operations along with secure network protocols for encrypting video streams. Experimental results [9] demonstrate an improvement in the quality of encryption, the suppression of correlation among encrypted frames, and an increased resistance to attacks. The performance evaluation clearly shows substantial gains compared to the old methods, and it also points to a promising future for secure communication. This approach represents an initial stride toward incorporating quantum-safe methodologies into commercial electronics, so ensuring the confidentiality and integrity of video data while simultaneously facilitating its efficient transmission across modern networks.

As the demand for satellite imagery grows, the security of these images becomes a major concern, especially considering the potential vulnerabilities in transmission networks. Encrypting photos during both transmission and storage safeguards sensitive data. In addition, the batch mode allows for the simultaneous encryption of large data sets. Using distributed computing methods [10], encrypted images are both consistent and resistant to modern attacks. The experimental results support strong protection, and the processing overhead is acceptable. The approach, which ensures the secure processing of large amounts of satellite data, improves operating efficiency and also supports privacy. By examining pixel distributions and ensuring encryption strength, the system shows potential in securing geospatial data pipelines from interception or modification. This is critical for defense, environmental monitoring, and commercial satellite applications.

3. Methodology

In today's digital age, the secure and controlled exchange of files is crucial, mainly because of the growing number of cyber risks, data breaches, and privacy issues. Traditional centralized systems sometimes lack transparency, thorough access control, and accountability, especially when dealing with data that depends on location and time. Secure Timeshare is a new project, a decentralized platform designed for file sharing. It leverages RSA encryption, geolocation authentication, time-sensitive access controls, and the power of blockchain technology. Users can communicate information securely, with conditional access in place. Administrators, meanwhile, have the ability to monitor actions and manage one-to-many broadcasts. By weaving together cryptographic safeguards, constraints on location and time, and the unchangeable nature of blockchain records, the system effectively addresses problems of illegal access, data tampering, and the need for reliable audits. This creates a secure framework for sensitive digital communications.

3.1 System Architecture Design

The design of the system prescribes the interactions among the users, administrators, and the components of the system, all of which are directed towards the secure, decentralized, and auditable file sharing. The document describes the steps in the uploading of files, encrypting them, processing access requests, giving approvals, and finally, interpreting the data. The system applies RSA encryption for data protection, geolocation for access based on location, time-limited session management, and blockchain technology for maintaining an immutable record of transactions. The movements of the users whether done directly or via the administration are monitored very carefully thus giving a very clear picture of all the activities happening. The data flows are set in a way to prevent unauthorized access but still, they are user-friendly. This first step on the other hand provides a basis for modular development, secure key management, and the integration of client-side, server-side, and blockchain components to happen smoothly. All these parts together create a solid and flexible framework that can meet the changing security needs and provide the ability to audit in the future system upgrades.

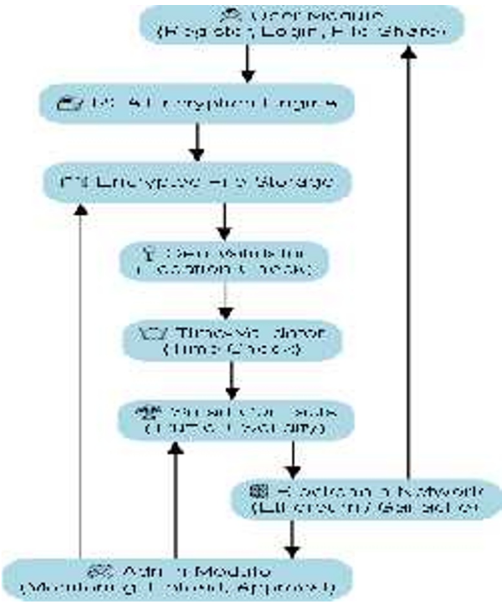

Fig. 1: System Architecture

Ultimately, the architecture has the capability to allow the platform to grow together with the users and the security requirements that will always increase. Thus, the system will always be unbreakable, clear, and flexible throughout its lifespan. Eventually, the platform will be able to adopt new technologies and compliance standards as they come up. Moreover, this strategic foundation is not only for the present but guarantees long-term reliability and trust for all the stakeholders..

3.2 User and Administrator Module Development

The user module handles secure registration and authentication, along with the ability to upload files that include geographical data. It also manages access requests. Access to the files is restricted to users who have received approval, and they can only see them within the specified timeframe. The admin module streamlines management, allowing for oversight of user activities. It also handles the approval of simultaneous access requests and supports file uploads for distribution to multiple users. These two modules work together with the encryption, geolocation, and blockchain features to enforce security regulations. The system ensures that user credentials are always valid, manages sessions correctly, and records access histories on the blockchain. This development promotes accountability, privacy, and smooth interaction among the participants and the system's components.

3.3 Geo-Based Encryption Implementation

Before storage and transmission, the documents are encrypted using RSA. In addition, the metadata includes geolocation coordinates. When a user requests access, the system checks the requester's current location against the boundaries of the set geofence. Access is only given if the approved zone includes the person making the request, and they're actually present within that area. To ensure location verification, mechanisms like sensor and network authentication are used to prevent spoofing. Decryption tickets are only sent out after geofence authentication in conditional key release systems. Access requests, together with their geolocation data, are stored on the blockchain to ensure they can't be changed. This module stops encryption keys from being used on their own to circumvent regional restrictions. It also makes file sharing both context-aware and secure.

3.4 Blockchain Implementation

Smart contracts, written in Solidity, are deployed on the Ethereum blockchain using Truffle and Ganache. Every key activity – from uploading files and requesting access to approvals and session specifics – is logged as an unchangeable transaction. The blockchain only stores important metadata, such as the file hash, owner ID, geofence positions, and access time. The actual encrypted files are kept off the blockchain. Blockchain events create a permanent, tamper-proof record of every activity taken by users and administrators. This feature significantly boosts both accountability and the capacity to conduct thorough audits. By decentralizing how transaction records are stored, the system reduces the risk of single points of failure and manipulation. This approach guarantees that file-sharing activities are open to scrutiny, resistant to manipulation, and capable of being reconstructed, hence adhering to stringent security protocols for handling sensitive information.

3.5 Installing Time-Limited Access Controls

Time-bound access imposes time limits on how long a file can be viewed. Upon approval of a request, the system creates temporary session tokens or decryption keys. These tokens and keys include embedded expiry timestamps. Access to files is limited to a specific timeframe. Once a session expires, it's automatically ended, and any associated tokens become useless. This is done to stop anyone from accessing the system without permission.

Blockchain event logs record start and end times, offering irrefutable evidence of adherence to schedules. The module's design incorporates geolocation validation and encryption, providing security that spans both space and time. Countdown indicators, the opportunity to re-request access, and emergency revocation are all features designed to keep things user-friendly, even as they rigorously enforce access regulations.

3.6 Upload and Access Workflow Files

Files are encrypted by users using RSA before being uploaded, accompanied by information that includes geolocation data and any time constraints. When you upload, a blockchain transaction is triggered. This transaction serves to record the file's ownership, its geofence, and the settings governing who can access it. To begin an accessibility request, the requester must be present at the designated place. These requests are then forwarded by either the file owner or the administrator. Once approved, the temporary decryption keys or session tokens are issued, and they're only good for a certain time. The system keeps tabs on active sessions, terminating them automatically when the time runs out. Every decision, whether an acceptance or a denial, is etched into the blockchain. This ensures both transparency and a reliable audit trail. This process integrates encryption, geolocation tracking, time-sensitive access controls, and blockchain- based record-keeping.

3.7 System Testing and Validation

The system undergoes comprehensive testing to confirm the security of its encryption, the accuracy of its geolocation, the effectiveness of its time-limited access, and the reliability of its transaction records on the blockchain. Test scenarios encompass a range of issues: inaccurate locations, sessions that time out, simultaneous requests, and network disruptions. Functional testing confirms that only allowed conditions allow users to access files, and it also verifies that the blockchain accurately records all interactions. Security testing examines for faults like key abuse, location forgery, and extension of sessions unauthorized. Usability and performance are tested for fast and intuitive workflows. In this phase, all modules run together harmoniously, realizing the project objectives of secure, decentralized, and verifiable file sharing for sensitive applications.

4. Result and Discussion

The integration of Secure Timeshare proved the unification of RSA encryption, geolocation authentication, time-limited access control, and blockchain recordation of transactions within a single, decentralized system for sharing files. Users, during the course of testing, could register, log in, and upload geolocation-tagged and specified-access-duration files containing embedded metadata. The RSA encryption module protected the content of the files such that raw data never became available either en transit or at rest. Encrypted files, upon uploading, created matching blockchain transactions that stored the file hash, owner identity, geofence locations, and authorized access duration, creating immutable evidence of the ownership of the files and the security policies.

In unison, the combination of the cryptography and the blockchain created a system that established data integrity, accountability, and transparency throughout the entire system. User requests for access were stringently tested under different circumstances for the purpose of evaluating the geo-based restrictions for access. Requests were only accepted from and by users who were physically within the specified geofence, and requests for accessing files from beyond the approved region were duly denied through the system. Anti-spoofing functionalities such as server-side authentication and network confirmation of GPS coordinates were tested and proved capable of firmly preventing manipulation of the location. Spatial limitations were effectively enforced through the geolocation module such that the sole possession of the decryption key proved ineffective for retrieving the files.

Users who were within the location parameters could make requests, which were passed on to the owner or the administrator of the files for their nod.

Fig. 2: Login panel and

The workflow for approval proved smooth, and the blockchain transactions were stored for all actions taken, ensuring an indelible and tamper-evident record of who requested and when and under what circumstances. Ephemeral decryption keys, which had specific expiration times, were used to confirm time-bound access control. Access to approved files was limited to a designated period. The system then automatically terminated access when the session concluded. This system prevented illegal ongoing access, which reduced the chance of sensitive data being exposed for a lengthy time. Tests that involved simultaneous access requests, overlapping geofences, and expired sessions validated the system's consistent execution of time-based constraints. The blockchain's records, which documented the start and end timings of each session, provided reliable proof that could be used for auditing. By combining time-based limits with location- based verification, a two-part security system was built, which improved the overall safety of files.

Figure 3 displays the secure administrator login screen. This screen is designed to allow access only to authorized users who have strong credentials and use multifactor authentication. Upon logging in, the admin control panel appears. This central hub provides a single dashboard,allowing for the review of users, requests, and transactions secured by blockchain technology. Figure 4 illustrates the data sharing

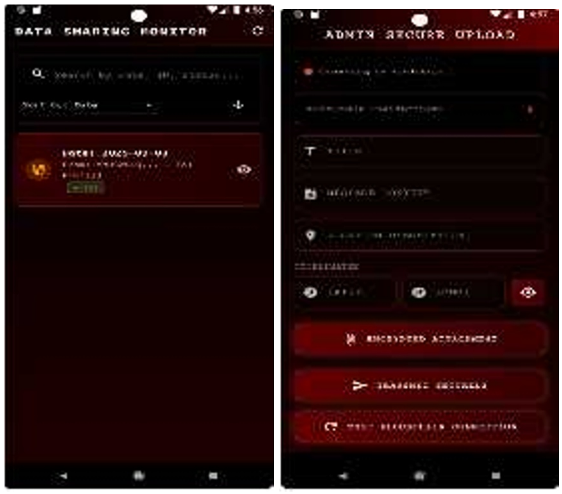

Fig. 3: Admin login and Admin control panel

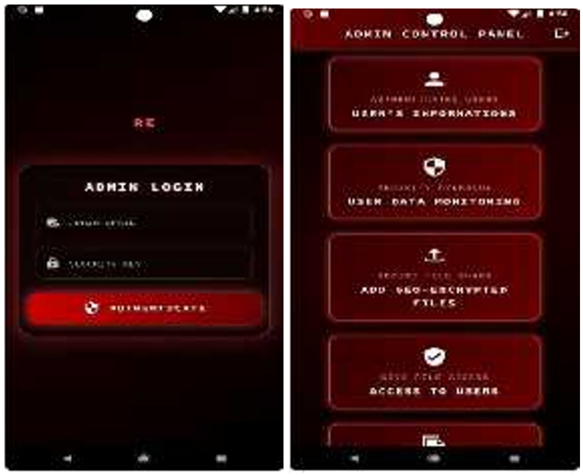

Fig. 4: Data sharing monitor and Admin secure upload

monitor. This tool allows the administrator to track active sessions, pending approvals, and geofence-based verifications as they happen. Finally, the admin secure upload tool allows administrators to encrypt and upload files. This process incorporates pre-set geofences and time constraints. The goal is to facilitate controlled, one-to-many delivery. Furthermore, the tool ensures immutable recording on the blockchain, which is essential for both auditability and accountability.

The administrator module displayed its ability to monitor and control things thoroughly. Administrators had the ability to monitor user actions, keep tabs on requests awaiting approval, and oversee the distribution of files to several users, all within designated geofences. Access permissions for many users were granted and revoked without issue, and every transaction was logged on the blockchain, guaranteeing both transparency and accountability. The system's capacity to audit its activities, find unusual trends, and export records for compliance purposes verified its suitability for sensitive areas, including business, healthcare, and government applications. Moreover, the system's ability to respond efficiently to security incidents was demonstrated by testing emergency key revocation and policy modifications.

Figure 5 shows the user login screen, where registered users confirm their identity by entering their credentials to access the system. For first-time users, the sign-up screen appears. This screen allows them to register using secure authentication methods, ensuring their identities are verified. Upon logging in, the user is greeted with a secure home screen.

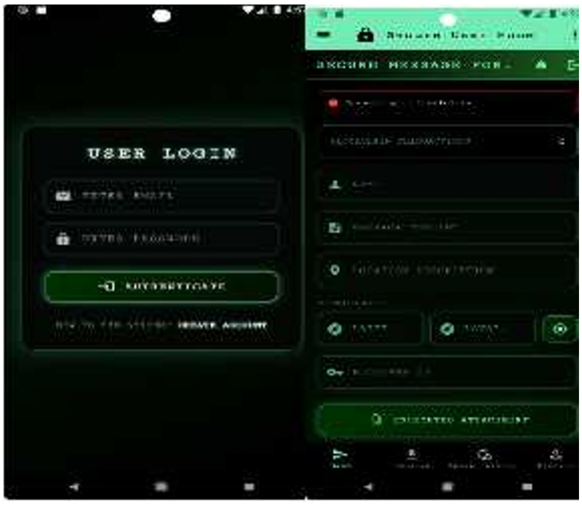

Fig. 5: User login and User sign up

Fig. 6: Secure user home and User message panel

Figure 6 serves as the main interface, allowing users to access functions including file uploads, requests, and activity tracking. The user message panel is designed to facilitate communication between file owners and those requesting access. It ensures that approvals, denials, and notifications are all handled openly. Together, these interfaces offer a straightforward, secure, and manageable environment for sharing files in a decentralized manner.

The system showed almost no delay when uploading data, encrypting them, and processing access requests, even when many users were using it at the same time. Storing encrypted files off-chain, together with maintaining important metadata on-chain, significantly decreased the use of blockchain resources and the costs associated with gas fees. The user interface was straightforward, designed for ease of use by both end-users and administrators. It prioritized intuitive navigation without compromising security protocols. Error management, encompassing issues like incorrect location identification, session timeouts, and network disruptions, functioned effectively. It provided users with unambiguous feedback, thereby preventing unwanted access.

The findings clearly show that Secure Timeshare successfully achieves its primary objectives: secure, decentralized, and user-friendly file sharing. The double- layer encryption system, together with geolocation and time-based restrictions, effectively prevents illegal access while also maintaining usability. Blockchain's integration brings transparency, ensuring that every file-sharing action is recorded in a way that's both permanent and easily traceable. The system's capacity to control access based on space and time, maintain encryption, and create unchangeable logs supports the conclusion that it is a secure platform for sharing sensitive information. This project's novel approach, which combines these solutions, results in a secure, context-sensitive platform. It's designed to address contemporary issues in digital communication, providing both users and administrators with confidence in the confidentiality, integrity, and accountability of the files being shared.

Secure Timeshare's findings indicate a strong technical foundation, together with great potential for practical use in real-world applications. The system's security hinges on a two-pronged approach. RSA encryption works in tandem with geolocation and time-limited access controls. This combination safeguards sensitive data, even when the stakes are high. Immutable blockchain records offer verifiable audit trails. The administrative module, on the other hand, enables thorough monitoring, real-time control, and the ability to revoke keys in an emergency. Secure Timeshare's features make it particularly ideal for important military, defense, and intelligence applications, where secure, controlled, and context-aware information sharing is crucial. Moreover, the platform's versatility extends to corporate, healthcare, and government applications. This adaptability ensures secure cooperation, safeguarding data from any breaches. Combining time and place constraints with encryption ensures that only authorized people can access information at specific times and locations. This provides realistic security, which in turn improves operational reliability and accountability.

5. Conclusion

This study indicates that combining encryption, geolocation-based authentication, time-limited access, and blockchain's unchangeable nature provides a complete solution for securely and effectively sharing data in computer systems. Secure Timeshare, the approach we're proposing, marries cryptographic security with contextual access controls. This means papers are only accessible from allowed locations and at specified times. By using smart contracts to record all transactions on the blockchain, the system offers transparency, accountability, and protection against tampering. This approach addresses the constraints of centralized systems. The architecture, built with two modules, supports both user and administrator roles. This design allows for flexible communication, accommodating both one-to-many and one-to-one interactions. Users can securely and privately share files, with the administrator overseeing and supervising larger-scale releases.

The smooth interplay of the modules highlights the practical advantages of using advanced technology in real- world applications that require confidentiality, trust, and the capacity to be audited. The research provides evidence supporting the potential of a decentralized, context-aware, and cryptographically secure system for private online conversation. This system is adaptable for high-security environments, including government operations, corporate settings, healthcare facilities, and defense sectors. Through the resolution of main concerns regarding unauthorized entry, insufficient clarity, and abuse of information, the system lays the groundwork for future development of secure file-sharing applications.

References

1. Rubin, Security considerations for remote electronic voting over the Internet. AT&T Labs Research (2001). http://avirubin.com/evoting.security.html
2. T.G. Rossler, E-voting: A survey and introduction. (2011). http://wiki.agoraciudadana.org/images/5/56/An%2BIntroduction%2Bto%2BElectronic%2BVoting%2BSchemes.pdf
3. H. Agarwal, G.N. Pandey, Online voting system for India based on AADHAAR ID. in Proc. Int. Conf. ICT Knowl. Eng. (2013). https://doi.org/10.1109/ICTKE.2013.6756265
4. Kiayias, T. Zacharias, B. David, A. Russell, SCV: End-to-end verifiable Internet voting. in Proc. USENIX Security Workshop (2016). https://www.usenix.org/conference
5. P. McCorry, S.F. Shahandashti, F. Hao, A smart contract for boardroom voting with maximum voter privacy. (2017). https://eprint.iacr.org/2017/110.pdf
6. End-to-end verifiable voting systems. National Academies / NIST Workshop Report (2017). https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8112.pdf
7. BSI, A study of mechanisms for end-to-end verifiable online voting. BSI Report (2017). https://www.bsi.bund.de
8. Y. Zhang, Q. Wu, D. Chen, Real-time interaction on the web: How WebSockets change application performance. J. Web Eng. **18**, 1–24 (2020)
9. Marathe, HTTP, WebSocket, and SignalR: A comparison of real-time online technologies. Int. J. Sci. Res. Eng. Trends (IJSRET) **9** (2020)
10. Live audience polling system. PubNub Blog (2020). https://www.pubnub.com/blog/live-audience- polling-system/
11. M.P. Singh, A.R. Shrestha, S. Kumar, H. Kim, WebSocket adoption and the landscape of the real-time web. in Proc. ACM Internet Meas. Conf. (IMC) (2020). https://dl.acm.org/doi/10.1145/3419394.3423641
12. Real time polling system. Int. Res. J. Eng. Technol. (IRJET) **6** (2019). https://www.irjet.net/archives/V6/i5/IRJET-V6I5658.pdf
13. S. Gupta, Communicating and displaying real-time data with WebSocket. IEEE Internet Comput. **23**, 75–81 (2019). https://doi.org/10.1109/MIC.2019.2913447
14. S. Deshmukh, Android based application for e-voting. Int. J. Sci. Eng. Res. **7**, 1–4 (2016) A. Patel, Enhancing real-time web applications with WebSockets. Int. J. Nat. Res. Dev. (IJNRD) **6** (2021). https://www.ijnrd.org/papers/IJNRD2104043.pdf
15. A. Patel, Enhancing real-time web applications with WebSockets. Int. J. Nat. Res. Dev. (IJNRD) **6** (2021). https://www.ijnrd.org/papers/IJNRD2104043.pdf
16. Scaling live experiences: Horizontal vs vertical scaling for WebSockets. Ably Blog (2021). https://ably.com/topic/websockets
17. A. Kumar, V. Sharma, S. Bhattacharya, R. Singh, Blockchain for electronic voting system—review and open issues. Appl. Sci. **12**, 12251 (2022). https://www.mdpi.com/2076- 3417/12/23/12251
18. A. Cetinkaya, H. Tekin, Blockchain-based e- voting systems: A technology review. Electron. **11**, 2146 (2022). https://www.mdpi.com/2079-9292/11/14/2146
19. R. Kshetri, J. Voas, Blockchain-enabled e-voting. IEEE Softw. **35**, 95–99 (2018). https://www.sciencedirect.com/science/article/pii/S2214212617301256