IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SafePaper: Blockchain-Based Secure Examination Paper Storage with Shamir's Secret Sharing

Ghanesh Ghatti
Dept of Computer Science and Engineering
AMC Engineering College
Bengaluru, India

Prof. G Muralitharan
Dept of Computer Science and Engineering
AMC Engineering College
Bengaluru, India

Prof. Praveen Kumar B
Dept of Computer Science and Engineering
AMC Engineering College
Bengaluru, India

Harish K
Dept of Computer Science and Engineering
AMC Engineering College
Bengaluru, India

Harish R
Dept of Computer Science and Engineering
AMC Engineering College
Bengaluru, India

Kumar M
Dept of Computer Science and Engineering
AMC Engineering College
Bengaluru, India

***Abstract*—The reliability of the inspection process is frequently compromised by unauthorized leaks and survey manipulation. This paper necessitates the safekeeping and organization of secure paper, a reliable and expandable system, employing blockchain technology and encryption key releases. The system enhances data privacy and access control by incorporating Shamir's secret sharing algorithms and distributing decryption keys to multiple trusted parties. Access to encrypted paper is restricted unless the specific thresholds are combined using the designated key. This prevents singular fusion or misuse. The platform provides an administrative web interface that enables users to upload encrypted files and assign access roles. The main way of distributing the information is through secure email services, ensuring that it is delivered quickly and kept confidential. Cloud storage is utilized to handle encrypted documents and ensure scalability and availability. The suggested approach can enhance the security, transparency, and dependability of question paper processing and can be customized by educational institutions to optimize the testing system.**

Keywords—Blockchain, Secure Storage, Shamir Secret Sharing, Examination Paper, Cloud System, Role-Based Access, Education Technology

I. INTRODUCTION

A. Background and Motivation

In recent times, the trustworthiness of educational establishments has been steadily declining as a result of recurring occurrences of examination paper leaks. The conventional methods employed for storing and distributing question papers depend on centralized infrastructure that lacks proper access control and traceability. These systems are susceptible to insider threats, unauthorized duplication, and delayed detection of misuse. In light of these difficulties, there is an urgent requirement for secure, transparent, and tamper-proof systems for managing examination content.

B. Problem Statement

The current methods of storing question papers do not have enough security measures in place to prevent unauthorized access and tampering. These centralized systems lack the ability to provide permanent logging records and do not have mechanisms in place for decentralized verification. Consequently, organizations are unable to track down unauthorized actions or prevent collusion among individuals with privileged access.

C. Main Purpose of Research

The primary objective of this research is to develop and enhance a secure system for storing examination papers, which we have named Safepaper. This system strives to:

- Securing Multi-Factor Authentication.
- Safeguard data through encryption and cloud integration.
- Ensure openness and traceability by utilizing blockchain technology.
- Automate transmission of information to reduce mistakes and latency.

D. Suggested Solution

Safepaper combines blockchain technology with Shamir's secret sharing algorithm to safeguard confidential examination materials. Question papers are protected by encryption and stored in the cloud, with the decryption keys distributed among several trusted individuals (guardians). Only when a specific number of these important shares are combined, the paper be decrypted. The blockchain ledger securely records unchangeable logs of all uploads and access events, bolstering trust and accountability.

E. Contributions of the Paper

This study introduces the following key findings:

- A reliable examination management system that ensures secure access by utilizing cryptographic secret sharing.
- A distributed ledger technology-based record of all document activities.
- Automated Key Distribution System via Secure Email.
- A role-based access control model is incorporated into a dynamic admin dashboard.

A flexible deployment approach utilizing advanced web technologies and cloud services.

II. System Design and Architecture

This section explains the different parts of the Safepaper system and how it works. The design prioritizes secure storage, decentralized key management, tamper-proof logging, and an easy-to-use admin interface for institutional use.

A. System Architecture Overview

The framework is composed of three layers: a web interface, an application layer, and a database layer. The presentation layer is a dynamic web interface constructed using HTML, CSS, and JavaScript (React.js for the admin panel) to offer role-based access to users, such as admins and guardians. The application layer, implemented using Node.js and Express.js, is responsible for managing request processing, cryptographic operations, email automation, and access validation. The storage and security layer: Examination papers are encrypted and stored in protected cloud environment. A private blockchain ledger ensures that all activities are recorded in a secure and unalterable manner. Shamir's secret sharing is employed for managing distributed decryption keys.

B. Shamir's Secret Sharing Mechanism

The Safepaper utilizes Shamir's secret sharing (SSS) algorithm to ensure that only authorized individuals can access the question papers. The decryption key is divided into n segments and assigned to n designated guardians. To reconstruct the original key, a minimum of k key shares (where k is less than or equal to n) is necessary. This threshold mechanism guarantees that no single person can undermine the system.

- The admin uploads a test paper. A random symmetric key is created for encryption.
- Key splitting: The symmetric key is divided into n shares using SSS.
- Key distribution: the key shares are automatically sent to n verified guardians via Nodemailer.

C. Blockchain Incorporation

A private blockchain is employed to keep a record of all events in the system, ensuring that they are in a read-only format

- File transfers.
- Key creation and dissemination.
- Decryption access requests.

Each transaction is hashed and recorded in a block, guaranteeing transparency and the ability to trace its origin. This feature deters collusion and unauthorized manipulation.

D. Dashboard and permission-based access control

The admin dashboard is designed for ease of use and protection. Key features include:

- Implementing secure login authentication.
- File upload interface.
- Parameter selection (choosing n and k values).
- Guardian management (add/edit email and role details).
- Audit logs with blockchain validation.

If there is a key breach or loss, emergency key regeneration is available to ensure access to the premises. Access control is regulated by session-based authentication and token validation. Every action is recorded and connected to a particular administrative identity.

E. Data Protection and Cloud-based Storage

The Examination papers are securely stored on a cloud platform that only allows authorized individuals to access them. Cloud authentication tokens have a predetermined lifespan, providing an extra level of security.

III. Security Features and Threat Model

The Safepaper system is designed to address the critical need for secure examination paper management in educational institutions. This section highlights the multiple layers of security, cryptographic mechanisms, and threat mitigation strategies employed to protect examination content against unauthorized access, leakage, and tampering.

A. Data Confidentiality and Integrity

To ensure the question papers are both confidential and tamper-proof:

- Advanced Encryption Standard (AES-256) is used to encrypt each question paper before being uploaded to cloud storage. This prevents anyone without the decryption key from viewing the content.
- SHA-256 Hashing: Each paper is hashed using SHA-256, and the resulting digest is stored immutably on the blockchain. During retrieval, the hash is recalculated and verified against the blockchain-stored value to ensure the file has not been modified post-upload.

This dual mechanism guarantees end-to-end confidentiality and integrity.

B. Shamir's Secret Sharing (SSS) for Key Management

To mitigate the risk of single-point failure or insider misuse:

- The AES decryption key is split using Shamir's Secret Sharing algorithm (k, n), where k is the threshold number of shares needed to reconstruct the key, and n is the total number of shares distributed.
- Shares are emailed securely to n guardians. Only when k or more of them collaborate can the key be reconstructed.
- This ensures that even if one or two guardians are compromised or unavailable, the system remains secure and functional.

C. Role-based Access Control (RBAC)

Each user in the system is given a specific role, with defined privileges:

- Admin: the ability to upload, delete, and manage papers, as well as assign guardian roles.
- Guardian is entrusted with secret key shares and can work together with other Guardians to reconstruct the AES key.

In emergencies, a super admin can temporarily grant access to the system, but they do not have a key share. This

reduces the impact of any compromised account and promotes the principle of least privilege.

D. Secure Email Communication

All key shares are distributed via nodemailer, which is integrated with TLS encryption for secure SMTP communication. Each email contains:

- The decrypted document.
- Metadata like Exam ID and time stamp.
- An optional security measure, such as a token or confirmation code, can be used to prevent phishing and spoofing attempts.
- The system records all emails sent for audit.

E. Blockchain Anchoring

To guarantee paper integrity and accountability:

- Each submitted paper's unique identifier is securely recorded on a public or private blockchain ledger.
- Blockchain entries are securely timestamped and digitally signed, ensuring that no unauthorized changes or rollbacks can occur.
- This serves as a tamper-evident record, enhancing trust among exam authorities and stakeholders.

F. Threat Model and Risk Mitigation

TABLE I. THREATS AND CORRESPONDING MITIGATION STRATEGIES

Risk	Mitigation Strategy
Insider threat	Key split among guardians using SSS.
Unauthorized access	role-based login + password hashing + rate limiting.
Data manipulation	SHA-256 hashing + blockchain storage.
Server breach, secure	paper storage + remote digital ledger.
Email interception	SSL encryption + token-based share validation.

G. Review and Recording

Each action, such as uploading files, logging in, sending emails, and reconstructing shares, is documented with a timestamp and user ID. These logs are kept in a safe place and can be checked by a verifier or an external authority to make sure they are following the rules.

IV. IMPLEMENTATION AND DEPLOYMENT

This section provides a detailed explanation of the practical steps, tools, and deployment plan utilized to implement the Safepaper system. The architecture integrates advanced encryption methods with an intuitive web interface to simplify and protect the distribution of examination papers.

A. Codebase

The platform was created using the MERN stack (MongoDB, Express.js, React.js, Node.js), selected for its flexibility, ability to handle large amounts of data, and compatibility with contemporary web applications. The backend is responsible for managing secret sharing, authentication, file management, and email notifications, while the frontend provides a user-friendly interface for administrators and guardians.

Additional tools and libraries:

- Shamir's secret sharing(sss): a method used to divide and reconstruct the secret encryption key.
- Nodemailer: integrated for secure email dispatch of key shares.
- Mongoose: used as a tool to interact with the MongoDB database.
- bcryptjs: employed for password hashing and user credential security.

B. Backend Implementation

The backend is built with Express.js and implements key logic for:

- Storing encrypted exam papers on the internet.
- Creating a symmetric encryption key, which is subsequently divided into n equal parts using SSS.
- Safely transferring these components to the protectors via email. Reconstructing the key using any t threshold parts for authorized decryption.
- Security tokens and authentication middleware safeguard API endpoints. JWT (JSON Web Tokens) are utilized for managing sessions and controlling access.

C. User and Management Interface

The frontend, based on React, offers users with two distinct interface options.

- Admin dashboard: facilitates the uploading of question papers, setting key split parameters, assigning guardians, and monitoring the delivery process.
- The Guardian panel enables the retrieval, verification, and contribution of key information during the reconstruction process.
- Responsive design and basic role-based access control guarantee ease of use across various devices.

D. Implementation Plan

The system is now operational at https://safepaper.in, hosted on a secure cloud platform. The production database was hosted on MongoDB Atlas. By using a custom domain with SSL encryption, you can guarantee secure HTTPS access. Email services are verified using OAuth2 to prevent spam filtering and guarantee the successful delivery of important emails.

Fig. 1. Architecture Diagram of the SafePaper

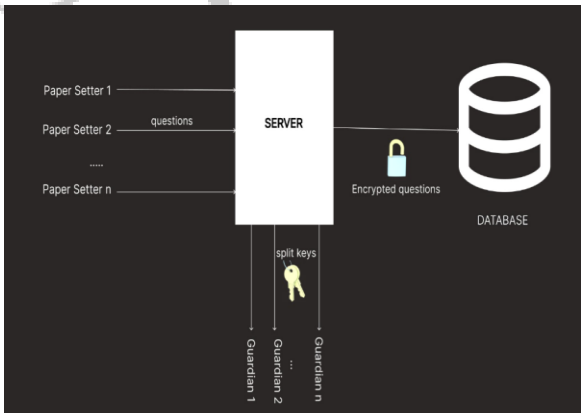

Fig.1. The safepaper platform's system architecture showcases the secure workflow, starting from encrypting the question papers and storing them in the cloud, and finally decrypting them using Shamir's secret sharing. This guarantees that only individuals possessing the key shares can reconstruct the decryption key, thereby eliminating any single point of failure or unauthorized disclosure.

Fig. 2. Question Paper Retrieval Architecture

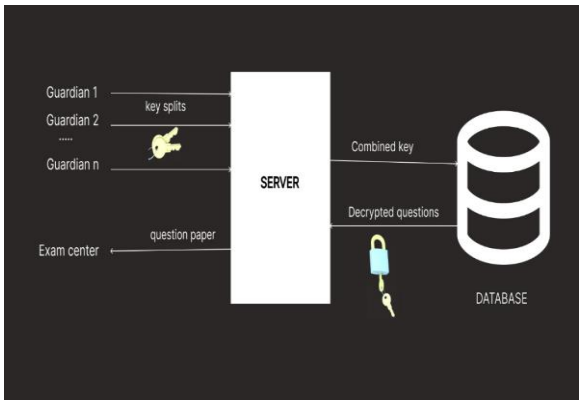

Fig. 2. The diagram depicts a secure system where encrypted question papers are stored in a database and retrieved through a server that reconstructs a secret key using shares from multiple guardians. Once the predetermined number of key splits is obtained, the combined key decrypts the questions for authorized exam centers, guaranteeing the privacy and restricted access of the exam content.

V. Result

The Safepaper system provides a dependable and secure approach to distributing digital examination papers, effectively addressing the problems of question paper leakage and unauthorized access. By implementing Shamir's secret sharing (SSS) algorithm, distributed key management, and secure server-based decryption, the system ensures that question papers remain confidential until the designated exam period. The integration of tools like nodemailer for automated communication greatly enhances operational efficiency and transparency. The architecture not only ensures high reliability and scalability but also adheres to the current security standards required in educational institutions. Future enhancements may include integrating blockchain technology, adopting biometric authentication methods, and introducing real-time audit logging to improve the security and dependability of the system.

References

[1] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[2] K. Devi and M. R. B. Raju, "A secure framework for question paper leakage prevention using cryptographic techniques," *Int. J. Comput. Appl.*, vol. 176, no. 29, pp. 6–11, 2020.

[3] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[4] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed. Boca Raton, FL: CRC Press, 2014.

[5] A. Wadhwa, A. Lamba, and P. Singh, "A secure cloud-based question paper generation and distribution system," *Proc. Int. Conf. Comput., Commun. Autom.*, pp. 1090–1095, 2017.

[6] A. K. Yadav and A. Gaur, "Security of confidential documents using Shamir's secret sharing," *Int. J. Comput. Sci. Mob. Comput.*, vol. 8, no. 6, pp. 42–48, 2019.

[7] R. K. Kodali and A. R. A. Rajesh, "Blockchain-based question paper delivery system for secure exams," *Proc. IEEE Int. Conf. IoT*, pp. 1–5, 2021.

[8] A. Mishra, "A survey on cryptographic techniques in digital question paper security," *Int. J. Adv. Res. Comput. Sci.*, vol. 9, no. 5, pp. 32–36, 2018.

[9] M. Naor and A. Shamir, "Visual cryptography," in *Adv. Cryptol. – EUROCRYPT '94*, Springer, 1995, pp. 1–12.

[10] M. H. Dehkordi and S. Mashhadi, "New schemes on threshold multi-secret sharing," *Comput. Stand. Interfaces*, vol. 30, no. 4, pp. 237–241, Jun. 2008.

[11] P. D. Zambre and V. P. Pawar, "A secure online examination system using secret sharing scheme," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 4, no. 3, pp. 384–389, Mar. 2014.

[12] P. Sharma and A. Sethi, "Secure and reliable email transmission using NodeMailer in web applications," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 6, no. 1, pp. 12–16, 2020.

[13] M. Bellare and P. Rogaway, "Entity authentication and key distribution," *Adv. Cryptol. – CRYPTO'93*, Springer, 1994, pp. 232–249.

[14] A. Das, A. Chatterjee, and S. Sen, "Design and implementation of secure question paper distribution using hybrid cryptography," *Proc. Int. Conf. Inf. Syst. Design Intell. Appl.*, Springer, 2018, pp. 315–323.

[15] R. L. da Silva and T. de Melo, "Improving exam paper security using distributed key sharing in cloud systems," *Int. J. Inf. Manage.*, vol. 55, p. 102215, 2020.

[16] M. T. Goodrich and R. Tamassia, *Introduction to Computer Security*. Boston, MA: Pearson, 2011.

[17] J. Kelsey, B. Schneier, and D. Wagner, "Modelling cryptographic protocols with logic and secrecy properties," *IEEE Secur. Priv.*, vol. 2, no. 2, pp. 16–23, Mar./Apr. 2004.

[18] NodeMailer, "NodeMailer documentation," [Online]. Available: https://nodemailer.com/about/ [Accessed: May 10, 2025].

[19] S. Patil and V. Jadhav, "Threshold-based secure question paper delivery using image steganography and encryption," *Int. J. Comput. Appl.*, vol. 975, pp. 8887–8891, 2016.

[20] D. Boneh and X. Boyen, "Secure identity-based encryption without random oracles," in *Adv. Cryptol. – EUROCRYPT 2004*, Springer, 2004, pp. 443–459.