International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Literature Review on Secure Examination Question Paper & Answer Key Management Using Encryption, Digital Signatures, and Access Control

R. K. Taware[1], Vaishnavi Jagtap[2], Shraddha Menkudale[3], Deeksha Yadav[4], Siddhi Gatade[5]

[1]Professor, Department of Computer Engineering, SVPM's College of Engineering, Malegaon (BK), Maharashtra, India
Email: *rututaware11[at]gmail.com*

[2]Department of Computer Engineering, SVPM's College of Engineering, Malegaon (BK), Maharashtra, India
Email: *jagtapvaishanavi21[at]gmail.com*

[3]Department of Computer Engineering, SVPM's College of Engineering, Malegaon (BK), Maharashtra, India
Email: *menkudaleshraddha0912[at]gmail.com*

[4]Department of Computer Engineering, SVPM's College of Engineering, Malegaon (BK), Maharashtra, India
Email: *yadavdeeksha.06[at]gmail.com*

[5]Department of Computer Engineering, SVPM's College of Engineering, Malegaon (BK), Maharashtra, India
Email: *siddhigatade2004[at]gmail.com*

Abstract: ***Examination question papers and answer keys contain confidential information, and their exposure before the examination can affect fairness and institutional trust. This review examines approaches used to protect examination documents, including conventional password-protected files, encryption, digital signatures, access-control mechanisms, and blockchain-based architectures. The reviewed work includes the SecureQ blockchain-and-IPFS approach, the Secured Question Paper Management System proposed by Rahman et al., and relevant NIST guidance on authenticated encryption and digital signatures. The comparison indicates that no single control addresses every risk: encryption protects confidentiality, signatures help verify authenticity and detect modification, and role-based access control limits who can perform particular actions. Blockchain can provide distributed records and tamper-evident coordination, but it may introduce additional infrastructure and operational requirements that are not necessary for every centralized college workflow. Based on these observations, the review discusses ExamGuard, a centralized question-paper and answer-key management system that combines AES-256-GCM, RSA-based key wrapping, RSA-PSS digital signatures, SHA-256 integrity checks, backend-enforced role and resource authorization, private file storage, timed access, notifications, and audit logging. The paper presents the rationale and design of this combined approach rather than claiming that it is universally superior. Further independent security testing, deployment validation, and comparative performance measurements are needed before making quantitative claims.***

Keywords: Examination security; AES-256-GCM; digital signature; role-based access control; question paper management; answer-key protection

1. Introduction

Examinations are an important part of academic assessment. Their credibility depends not only on the quality of the questions but also on keeping question papers confidential until the permitted release time. If a paper is accessed early, modified without permission, or delivered to the wrong person, the institution may face unfairness, loss of trust, and the need to conduct another examination. Traditional handling methods such as printed copies, shared folders, and password-protected documents can be useful, but they do not by themselves provide a complete process for controlling access, checking document integrity, and recording sensitive actions.

Digital management can make document handling more traceable, but moving a file online does not automatically make it secure. A suitable system must consider confidentiality, integrity, authenticity, authorization, release timing, and accountability together. Encryption makes stored content unreadable without the required key. Digital signatures allow the system to verify whether signed data has changed and whether it was signed by the holder of a particular private key. Access control determines which authenticated user may carry out a particular action. These controls solve related but different problems and should not be treated as interchangeable [2], [3].

This review examines selected work on secure question-paper management and relevant cryptographic guidance. It then identifies a practical design direction for ExamGuard, which is intended for a centralized educational institution and includes both question papers and post-examination answer keys.

2. Review Scope and Method

This paper adopts a focused narrative review approach to examine selected research and technical standards relevant to secure examination question-paper and answer-key management. The literature selection focused on sources directly related to examination-document confidentiality, integrity, authenticity, encryption, digital signatures, and secure document handling. Two research publications were

selected: Rahman et al.'s 2021 study on a secured question-paper management system and Solomon Raju, Sowmya, and Chennamma's 2024 SecureQ study. These were supplemented by two official technical standards published by the National Institute of Standards and Technology (NIST): Special Publication 800-38D, which specifies AES-GCM, and Federal Information Processing Standards Publication 186-5, which addresses digital signatures. The sources were selected because they provide relevant examination-security approaches and established cryptographic guidance applicable to the design discussed in this paper.

The selected sources were examined according to their security objectives, principal mechanisms, contributions, and limitations in the context of centralized college examination workflows. The two research publications provide application-level approaches to examination security, whereas the NIST documents provide technical guidance for cryptographic mechanisms rather than examination-management systems. This review is limited to these four selected sources and does not claim exhaustive literature coverage. No systematic database search, formal screening protocol, quality assessment, or meta-analysis was conducted. Bibliographic details were checked against publisher, repository, or standards-provider records where available [1]–[4].

The sources were compared according to the security problem addressed, principal techniques, likely operational requirements, and limitations relevant to a college examination workflow. This is not a systematic review: no exhaustive database search, formal screening protocol, quality-scoring framework, or meta-analysis was performed. The conclusions should therefore be read as a structured comparison of selected sources, not as a complete inventory of every published examination-security system.

3. Background: Security Requirements

3.1 Confidentiality through encryption

Confidentiality means that a question paper or answer key should not be readable by an unauthorized person. ExamGuard's documented design uses AES-256-GCM to encrypt each document with a fresh 32-byte data-encryption key. The initialization vector and authentication tag are retained with the protected data. GCM is an authenticated-encryption mode, so it provides confidentiality and a cryptographic check on the encrypted content when used correctly [3]. As with any cryptographic design, key protection and correct IV handling remain essential.

3.2 Authenticity and integrity through signatures

A document can be encrypted and still require a way to detect replacement or unauthorized modification. A digital signature supports verification that the signed bytes correspond to the version signed by the holder of the signing private key. NIST's Digital Signature Standard explains the use of digital signatures for detecting unauthorized modification and authenticating the signatory [4]. In ExamGuard, the documented design uses RSA-PSS with SHA-256 for signing protected document data and checks the signature before decryption. A valid signature does not, by itself, prove that a requester is authorized to view the document.

3.3 Access control and accountability

Role-based access control (RBAC) assigns permissions according to roles, such as teacher, examination coordinator, and administrator. However, role checks alone may be insufficient for confidential papers. The system also needs resource-level rules—for example, whether a teacher owns a paper, whether a coordinator has been assigned to it, and whether the release time has arrived. Audit records can help administrators investigate who performed actions such as login, submission, access, or role changes. Audit logging is useful only when sensitive values such as passwords, tokens, and document keys are excluded from logs.

4. Literature Review

4.1 Secured Question Paper Management System (2021)

Rahman, Iftekhar, Alam, Gafur, and Nandi proposed a secured question-paper management approach published in the AIUB Journal of Science and Engineering in 2021. The paper identifies question leakage as a weakness of traditional handling and proposes a model involving blockchain, digital signatures, hashing, encryption/ decryption, one-time authentication code (OTAC), and randomization [1]. Its contribution is the combination of multiple security mechanisms around question-paper preparation and delivery rather than relying only on a password-protected file.

For the ExamGuard review, this paper is relevant because it treats examination security as an end-to-end workflow. At the same time, the approach relies on blockchain-related components and other mechanisms that must be integrated and maintained. The available publication record confirms the methods described in its abstract, but this review does not infer a measured cost or performance penalty because comparable benchmark results were not established from the bibliographic record alone.

4.2 SecureQ: Security of Examination Question Paper Through Blockchain (2024)

Solomon Raju, Sowmya, and Chennamma presented SecureQ at the 2024 International Conference on Innovation and Novelty in Engineering and Technology. The publication describes a blockchain- and IPFS-based approach intended to make examination-paper handling more secure and tamper-resistant [2]. The separation of distributed file storage and blockchain records can support content-addressed retrieval and an auditable record of relevant actions.

This direction is useful when an institution needs distributed coordination or wants records to be verifiable across parties that do not fully trust one central operator. However, a decentralized design also introduces additional components to configure, monitor, and govern. For a

college that already operates a central examination cell, the design question is whether those distributed properties are necessary for the actual threat model. A centralized system may be more straightforward to operate, provided that access controls, key management, logging, backups, and administrative privileges are handled carefully.

4.3 NIST guidance on AES-GCM (2007)

NIST Special Publication 800-38D specifies Galois/Counter Mode (GCM) as an authenticated-encryption mode for an approved block cipher [3]. This guidance is not an examination-management application, but it provides a technical foundation for selecting an encryption mode that protects document confidentiality while also authenticating encrypted data. Its relevance is that document protection should not depend on encryption alone; the implementation must also validate the authentication tag and use the mode correctly.

4.4 NIST Digital Signature Standard (2023)

NIST FIPS 186-5 describes digital-signature algorithms and their role in detecting unauthorized modification and authenticating the signatory [4]. Applied to examination documents, this supports checking a signature before delivering a protected file. It also reinforces an important distinction: signature verification establishes a cryptographic property of the signed data, while the application's authorization logic decides whether the current user may receive that data.

4.5 Comparative summary

Source / approach	Main technique	Contribution	Consideration for ExamGuard
Rahman et al. (2021) [1]	Blockchain, signatures, hashing, encryption, OTAC, randomization	Multi-control approach to question-paper security	Useful workflow precedent; assess whether all components are needed in a centralized setting
SecureQ (2024) [2]	Blockchain and IPFS	Distributed storage and tamper-resistant records	Potentially useful where decentralized trust is required; operational needs must be evaluated
NIST SP 800-38D [3]	AES-GCM guidance	Authenticated encryption foundation	Supports confidential document storage with tag validation
NIST FIPS 186-5 [4]	Digital signatures	Authenticity and modification detection	Supports verification of signed content; does not replace authorization

5. Research Gap

The selected literature demonstrates that examination-paper security can be strengthened using combinations of cryptography, access controls, and auditable workflows. However, the reviewed sources do not by themselves establish one universally best architecture for every institution. A practical need in centralized college examination systems is the integration of the following security controls into a unified and understandable operational workflow:

- Confidential storage of question papers and answer keys using authenticated encryption.
- Signature and integrity verification before any protected document is decrypted or delivered.
- Backend-enforced role permissions combined with paper ownership, recipient assignment, and release-time checks.
- Separate, controlled handling of question papers and answer keys, including a post-examination upload window.
- Private object storage, audit logging, and notifications without exposing keys or internal storage paths.
- A design that avoids distributed-ledger infrastructure when its decentralization benefits are not required by the institution's threat model.

This gap is a design-oriented conclusion from the selected sources, not proof that no other system has implemented the same combination. A broader systematic search would be required to make a universal novelty claim.

6. ExamGuard: Proposed Integrated Approach

ExamGuard is a web-based system designed to manage examination question papers and answer keys through a centralized workflow. The supplied project documentation records a React and Vite frontend, a Node.js and Express backend, Supabase PostgreSQL for metadata, and a private Supabase Storage bucket for protected documents. The security design includes bcrypt password hashing, JSON Web Tokens (JWT), backend role and resource authorization, AES-256-GCM, RSA-OAEP key wrapping, RSA-PSS signatures, SHA-256 digest checks, notifications, and audit logs.

6.1 Question-paper workflow

A teacher logs in, prepares or uploads a question paper, and selects the intended recipient. The backend validates the uploaded PDF and checks the teacher's authority to submit it. The document is encrypted with AES-256-GCM using a per-document data-encryption key. The system records integrity and signature information, protects the AES key using RSA-OAEP, and stores the encrypted object in private storage. Paper metadata and recipient assignment are stored in the database. An in-app notification informs the assigned recipient that a paper has been scheduled.

6.2 Verify-before-decrypt access

When an eligible user requests a paper, the backend authenticates the account and checks the current role, resource ownership or assignment, and delivery timing. It retrieves the protected object and validates its SHA-256 digest and RSA-PSS signature. Only after these checks pass does the backend unwrap the AES key and perform AES-GCM decryption. If verification fails, the request must stop and the document must not be delivered.

6.3 Answer-key workflow

ExamGuard also includes answer-key management. According to the supplied project documentation, the teacher who owns the question paper may upload the corresponding answer key within the configured post-examination window. Duplicate submissions are blocked by the documented business rule, and coordinator access is restricted to authorized or assigned workflows. The answer key is independently encrypted and signed, and its download follows the same verification-before-decryption principle. Exact timing rules should be aligned with the institution's official examination policy before deployment.

6.4 Roles, audit, and current implementation status

The documented roles are ADMIN, TEACHER, and EXAM_COORDINATOR. Teachers submit papers and related answer keys; coordinators access assigned or authorized materials; administrators manage accounts and review security activity. The backend enforces permissions rather than relying only on hidden buttons or frontend routing. The current ExamGuard implementation includes role-based access management, question-paper and answer-key workflows, cryptographic protection, secure document verification, notifications, and audit-related functionality. The backend enforces role-based permissions and resource-level authorization rather than relying solely on frontend restrictions. Functional and regression testing has been conducted to evaluate the implemented workflows. However, these project-level test results should not be interpreted as an independent security audit or proof of production readiness. Further validations, including security testing and live deployment configuration checks, remains necessary.

7. Discussion

The literature and the ExamGuard design point to a layered approach: no single algorithm solves every security requirement. AES-256-GCM protects document confidentiality and authenticates encrypted content; RSA-OAEP protects the document-encryption key; RSA-PSS and SHA-256 support signature and integrity verification; RBAC and resource-level rules decide who may access a paper; and audit logs support later review. The layers complement one another, but their benefits depend on correct implementation and operational controls.

Compared with a blockchain-based design, ExamGuard chooses centralized storage and backend-controlled access. This may reduce the number of distributed components an institution must operate, but it also means the central service, database privileges, private keys, backups, and administrator accounts become important trust points. Therefore, the paper should not claim that a centralized design is inherently more secure or always faster. Its suitability depends on institutional needs, the threat model, the quality of key management, and evidence from testing. A further distinction is that an encrypted file is not automatically safe if the decryption key is exposed, and a signed file is not automatically private if an unauthorized person can obtain plaintext. Similarly, a correct role assignment is not enough if a user can bypass the backend or guess another resource identifier. ExamGuard's verify-before decrypt flow and its combination of role, assignment, ownership, and timing checks are intended to address these risks in a single process.

8. Conclusion

This review considered selected examination-security research and cryptographic standards relevant to confidential question-paper handling. The reviewed approaches show the value of combining document protection with authenticity checks and controlled access. Blockchain and IPFS can be appropriate where decentralized storage or shared tamper-evident records are required, while a centralized architecture may be suitable for institutions whose workflows are managed by a trusted examination cell.

ExamGuard applies this centralized direction by combining AES-256-GCM encryption, RSA-OAEP key wrapping, RSA-PSS digital signatures, SHA-256 integrity checks, backend-enforced role and resource authorization, private storage, timed access, answer-key controls, notifications, and audit logging. Its central design principle is to verify authorization and document integrity before decryption. The approach is a practical design proposal, but broader literature coverage and independent security and performance evaluation are required before drawing general conclusions about superiority or production readiness.

References

[1] S. M. T. Rahman, M. N. Iftekhar, R. Alam, S. M. R. Gafur, and D. Nandi, "Secured Question Paper Management System," AIUB Journal of Science and Engineering, vol. 20, no. 1, pp. 25–32, Apr. 2021, doi: 10.53799/ajse.v20i1.121.

[2] G. Solomon Raju, K. N. Sowmya, and H. R. Chennamma, "Security of Examination Question Paper Through Blockchain—SecureQ," in Proceedings of the 2024 International Conference on Innovation and Novelty in Engineering and Technology (INNOVA), 2024, doi: 10.1109/INNOVA63080.2024.10847055.

[3] M. Dworkin, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, NIST Special Publication 800-38D, National Institute of Standards and Technology, 2007. doi: 10.6028/NIST.SP.800-38D.

[4] National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-5, 2023. doi: 10.6028/NIST.FIPS.186-5.