IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

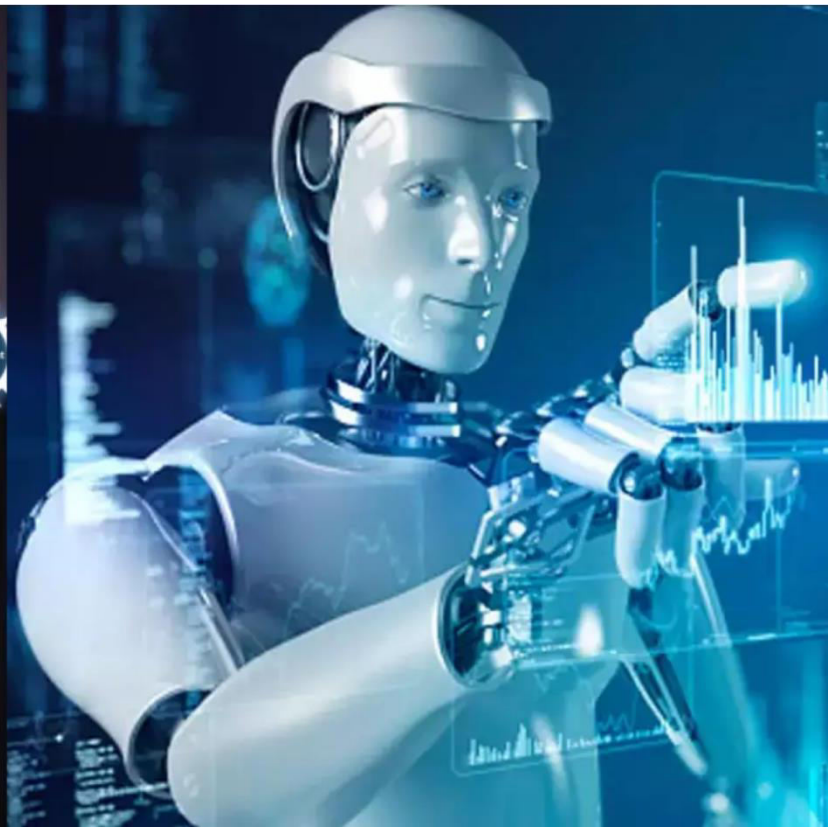
ISSN(O): 2319-8753
ISSN(P): 2347-6710



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





Impact Factor: 9.935

Volume 15, Issue 10, October 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 10, October 2026

|DOI: 10.15680/IJIRSET.2026.1510105|

SecureQ: A Secure, Time-Locked Question Paper Distribution and Leakage Prevention System

Ms. Amruta Biradar, Ms. Sakshi Bandgar, Ms. Sanika Taralkar, Ms . Vaishnavi Mali,

Prof. Shobhana Raichurkar

Department of Computer Science And Engineering, MAEER'S MIT CORER, Barshi. Dt., Solapur, India

Guide, Department of Computer Science And Engineering, MAEER'S MIT CORER, Barshi. Dt., Solapur, India

ABSTRACT: SecureQ is a secure digital system designed to protect examination question papers from unauthorized access and premature leakage. The system aims to improve the confidentiality and security of question paper distribution through authentication, encryption, role-based access control, and time-locked access. It allows authorized administrators to upload and manage question papers while ensuring that eligible users can access them only during the permitted time period. The system can also include multi-factor authentication, digital watermarking, and audit logging to enhance security and traceability. By combining these security mechanisms, SecureQ aims to reduce the risk of question paper leakage, prevent unauthorized distribution, and improve transparency in the examination process. The proposed system provides a structured and reliable approach to secure digital question paper management.

KEYWORDS: SecureQ, Question Paper Security, Question Paper Leakage Prevention, Encryption, Time-Locked Access, Multi-Factor Authentication, Role-Based Access Control, Digital Watermarking, Audit Logging, Examination Management System.

I. INTRODUCTION

The SecureQ system is designed to provide a secure and reliable method for distributing examination question papers digitally. In traditional examination systems, question papers may be exposed to unauthorized individuals during preparation, storage, or distribution. Such incidents can compromise examination integrity, create unfair advantages, and reduce trust in the examination process.

SecureQ aims to address these challenges by implementing security mechanisms such as user authentication, encryption, role-based access control, and time-locked access. The system allows authorized administrators to upload and manage question papers securely while restricting access to eligible users until the scheduled examination time. Additional features, such as multi-factor authentication, digital watermarking, and audit logging, can further improve security and accountability.

The main objective of SecureQ is to minimize the risk of question paper leakage and prevent unauthorized access before the examination. By combining digital technologies with controlled access mechanisms, the proposed system aims to improve confidentiality, transparency, and efficiency in examination management.

Overall, SecureQ provides a structured approach to secure question paper handling and distribution, helping educational institutions maintain the integrity and fairness of examinations.

II. LITERATURE SURVEY

A literature survey is an important part of the SecureQ project because it helps identify existing methods, technologies, **and security** mechanisms used to protect confidential examination question papers. Traditional question paper distribution methods may face challenges such as unauthorized access, information leakage, and limited tracking of document access. By studying existing security techniques, SecureQ aims to develop a more secure and reliable system for digital question paper management.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 10, October 2026

|DOI: 10.15680/IJIRSET.2026.1510105|

1. Traditional Question Paper Distribution Systems: Traditional systems often depend on physical transportation, printed documents, and manual handling. These methods require careful supervision and may be vulnerable to unauthorized copying, loss, or disclosure of confidential papers.
2. Encryption-Based Security Systems: Encryption is used to protect confidential information by converting readable data into an encoded format. Only authorized users or systems with the appropriate decryption capability can access the protected information. SecureQ proposes using encryption to improve the confidentiality of question papers during storage and distribution.
3. Authentication Systems: Authentication verifies the identity of users before allowing access to sensitive information. Password-based authentication and multi-factor authentication can help prevent unauthorized individuals from accessing examination materials.
4. Role-Based Access Control Systems: Role-based access control assigns permissions according to the responsibilities of users. In SecureQ, administrators and authorized examination staff can be assigned different permissions to ensure that only permitted users can upload, manage, or access question papers.
5. Time-Locked Access Systems: Time-based access control restricts access to information until a specified date and time. This approach can help ensure that examination question papers remain inaccessible to authorized recipients until the scheduled release time.
6. Digital Watermarking and Audit Logging: Digital watermarking can help identify the source of a distributed document, while audit logging records activities such as uploads, access attempts, and downloads. These techniques can improve traceability and support investigations into suspected unauthorized distribution.
7. Proposed SecureQ System: Based on these security concepts, SecureQ proposes combining authentication, encryption, role-based access control, time-locked access, and audit logging in a single system. Additional features, such as digital watermarking and multi-factor authentication, may further strengthen protection when implemented. The proposed system aims to reduce the risk of question paper leakage and improve the confidentiality and reliability of examination management.

III. METHODOLOGY

The methodology of the SecureQ system describes the step-by-step process used to protect examination question papers from unauthorized access and leakage. The system follows a secure digital workflow,beginning with user authentication and question paper uploading and ending with controlled access at the scheduled examination time. It uses security mechanisms such as encryption, role-based access control, and time-based restrictions to maintain the confidentiality of examination materials.

The proposed system allows authorized administrators to upload question papers and configure their release schedules. Before providing access, the system verifies the user's identity, checks the assigned permissions, and confirms whether the scheduled access time has been reached. Audit logging can record important activities for monitoring and security review.

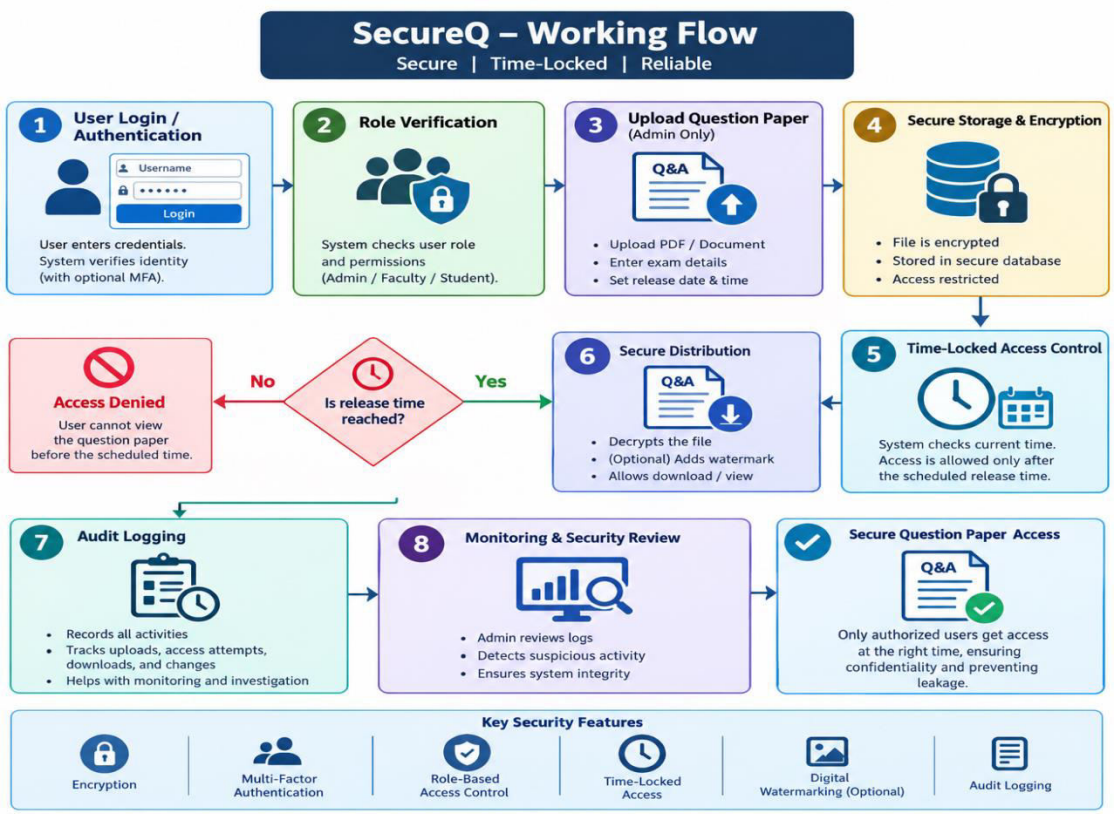
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 10, October 2026

|DOI: 10.15680/IJIRSET.2026.1510105|



Working Steps of the SecureQ System

1. User Authentication: Users log in using their registered credentials. Additional authentication methods can be used if implemented.
2. . Role Verification: The system checks the user's role and permissions before allowing access to specific functions
3. Question Paper Upload: Authorized administrators upload examination question papers and enter relevant details, such as subject name, examination date, and release time.
4. Secure Storage: The question papers are stored using appropriate security mechanisms. Encryption can be applied to protect confidential files.
5. Time Scheduling: The administrator sets the date and time when the question paper is permitted to become accessible.
6. Time-Locked Access Control: The system checks the current server time and verifies whether the permitted access period has started. Early access attempts are rejected.
7. Secure Question Paper Distribution: Once the scheduled time is reached, eligible users can access or download the question paper according to their assigned permissions.
8. Digital Watermarking: If implemented, a recipient-specific watermark can be added to help trace unauthorized redistribution.
9. Audit Logging: The system records important activities, including uploads, access attempts, successful access, and administrative changes.
10. Monitoring and Security Review: Administrators can review recorded activities and test the system to identify potential security weaknesses.

IV. HARDWARE AND SOFTWARE REQUIREMENTS

The SecureQ system requires suitable hardware and software resources to develop, run, and manage the secure distribution of examination question papers. The system uses digital security mechanisms to support user authentication, protected question paper storage, and time-based access control.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 10, October 2026

|DOI: 10.15680/IJIRSET.2026.1510105|

A. Software Requirements

1. Operating System: Windows 10/11 or Linux.
2. Frontend: HTML, CSS, JavaScript, or React.js, depending on the implementation.
3. Backend Programming Language: Python, Java, or another supported language.
4. Backend Framework: Flask, Django, FastAPI, or an equivalent framework.
5. Database: MySQL, SQLite, or PostgreSQL for storing user details, question paper information, schedules, and access logs.
6. Security Libraries: Established cryptographic libraries for encryption and secure password handling.
7. Code Editor: Visual Studio Code or another suitable development environment.
8. Web Browser: Google Chrome, Microsoft Edge, or Mozilla Firefox.
9. Version Control: Git and GitHub for source code management.
10. Network: A reliable network connection for accessing the web application.

B. Hardware Requirements

1. Processor: Intel Core i3 or equivalent and above.
2. RAM: Minimum 4 GB; 8 GB recommended.
3. Storage: Sufficient disk space for the application, database, and encrypted question paper files.
4. Display: Standard monitor or laptop display.
5. Input Devices: Keyboard and mouse.
6. Server: A local computer or cloud server capable of running the application and database.

C. Functional Requirements

1. Secure login and user authentication.
2. Role-based access permissions.
3. Question paper uploading and management.
4. Encryption and protected file storage.
5. Scheduled release of question papers.
6. Restriction of unauthorized or premature access.
7. Activity logging and administrative monitoring.
8. Optional multi-factor authentication and digital watermarking.

V. EXPERIMENTAL RESULTS



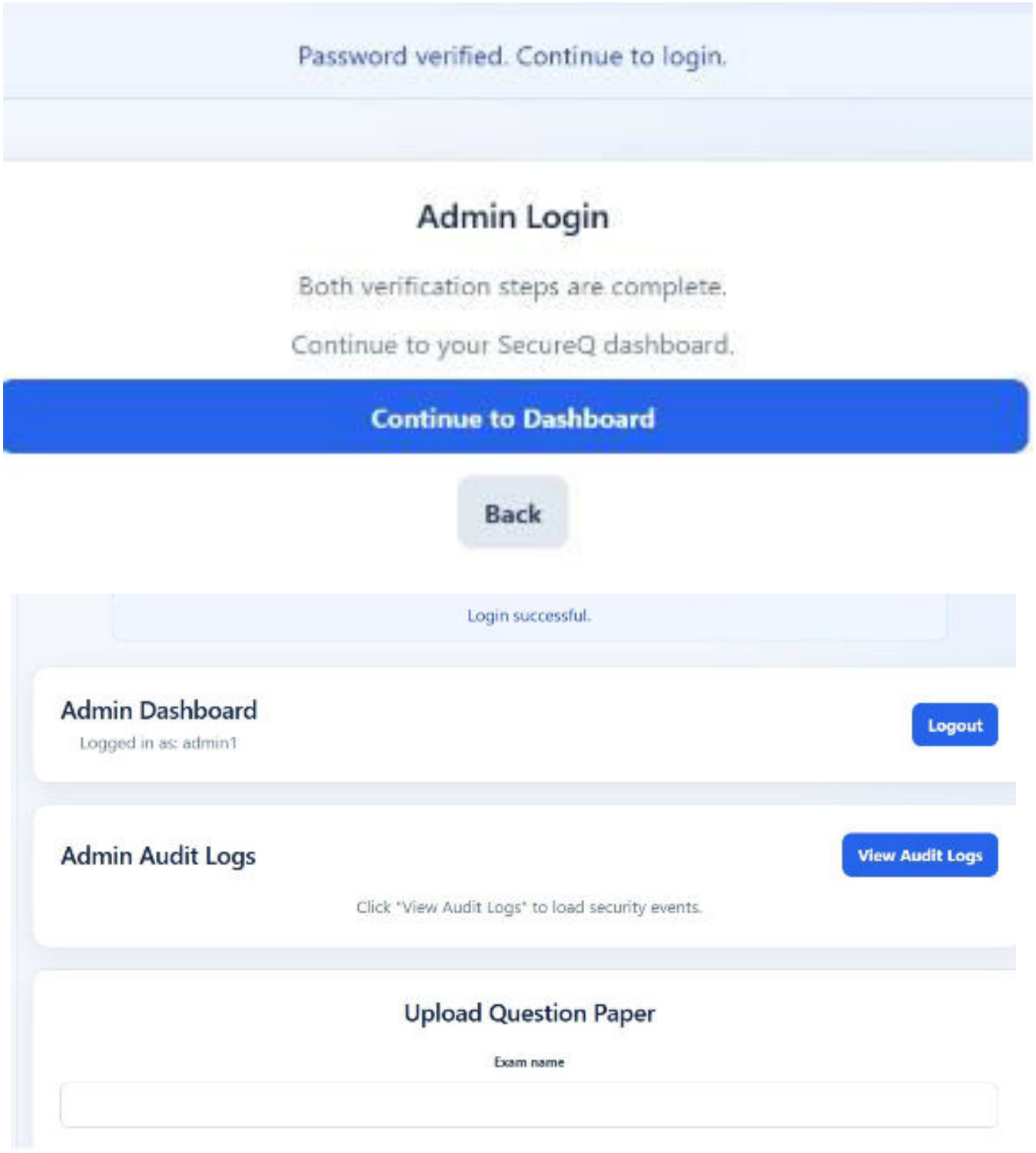
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 10, October 2026

|DOI: 10.15680/IJIRSET.2026.1510105|



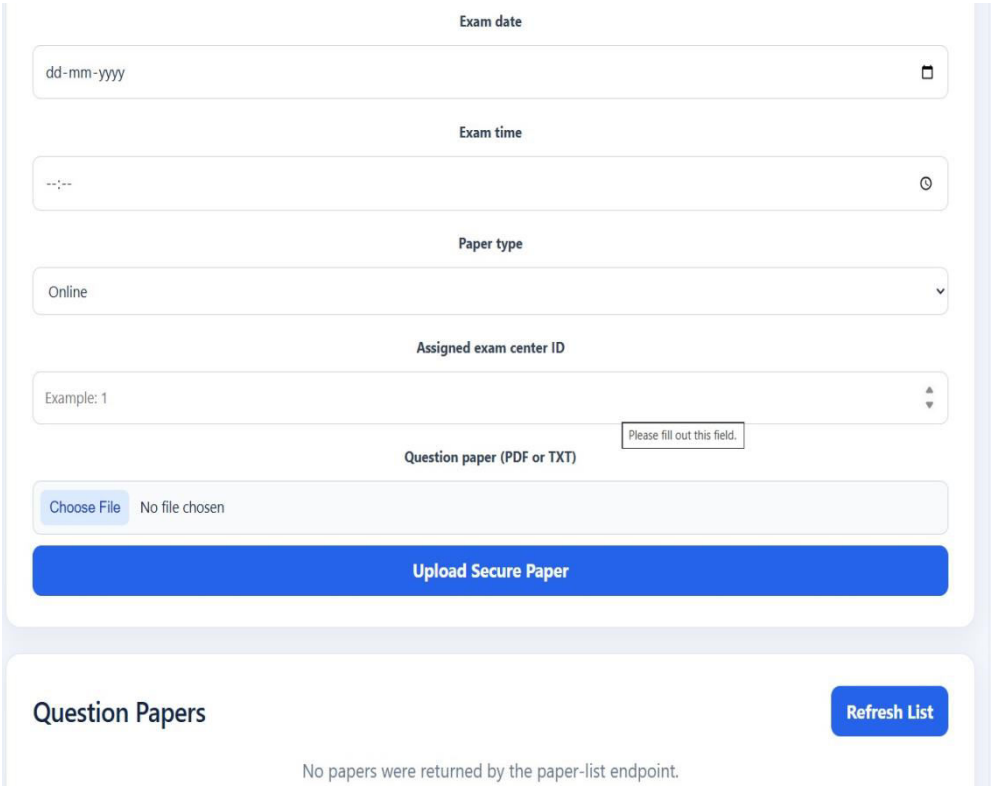
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

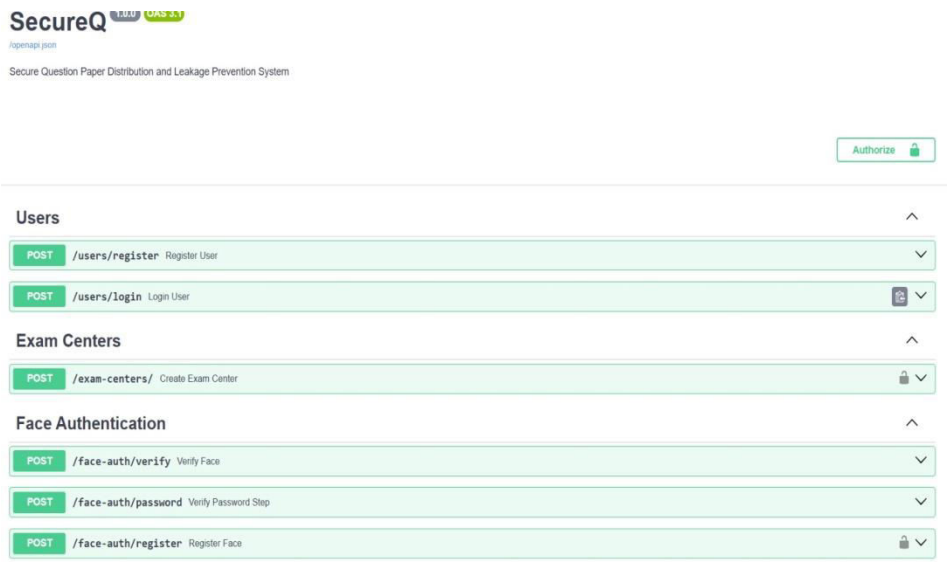
Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 10, October 2026

|DOI: 10.15680/IJIRSET.2026.1510105|





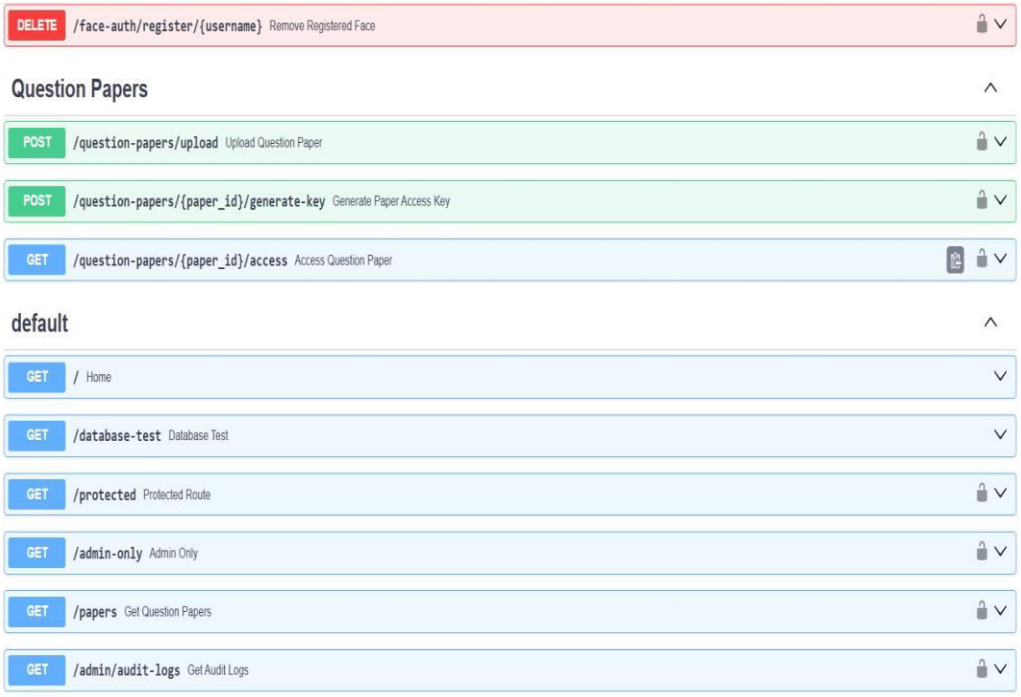
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 10, October 2026

|DOI: 10.15680/IJIRSET.2026.1510105|



VI. CONCLUSION

SecureQ is a proposed secure digital system designed to protect examination question papers from unauthorized access and leakage. The system combines security mechanisms such as user authentication, encryption, role-based access control, and time-locked access to improve the confidentiality and reliability of question paper distribution.

The system allows authorized administrators to upload and manage question papers while restricting access to eligible users according to predefined permissions and examination schedules. Additional features, such as multi-factor authentication, digital watermarking, and audit logging, can further strengthen security and improve traceability when implemented.

SecureQ aims to reduce the risks associated with traditional question paper distribution methods and support a more transparent and controlled examination process. Its effectiveness depends on proper implementation, configuration, and security testing. Although no digital system can guarantee complete prevention of leakage, SecureQ can help minimize common security risks through multiple layers of protection.

In conclusion, SecureQ provides a promising approach to secure examination question paper management and distribution. Future improvements may include stronger identity verification, enhanced monitoring, tamper-resistant audit records, and integration with institutional examination management systems.

REFERENCES

1. D. Temoshok et al., “Digital Identity Guidelines,” NIST Special Publication 800-63-4, National Institute of Standards and Technology (NIST), July 2025. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-63-4. CSRC+1
2. M. J. Dworkin et al., “Advanced Encryption Standard (AES),” Federal Information Processing Standards Publication 197 (FIPS 197-upd1), National Institute of Standards and Technology, 2023. [Online]. Available: https://doi.org/10.6028/NIST.FIPS.197-upd1. NIST
3. OWASP Foundation, “OWASP Application Security Verification Standard (ASVS),” Version 5.0.0, May 2025.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 10, October 2026

|DOI: 10.15680/IJIRSET.2026.1510105|

[Online]. Available: https://owasp.org/www-project-application-security-verification-standard/. OWASP Application Security Verification Standard+1

4. OWASP Foundation, "Password Storage Cheat Sheet." [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html. OWASP Cheat Sheet Series
5. OWASP Foundation, "Authorization Cheat Sheet." [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html.
6. D. Temoshok et al., "Digital Identity Guidelines: Authentication and Authenticator Management," NIST Special Publication 800-63B-4, National Institute of Standards and Technology, July 2025. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-63B-4. NIST



INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details