Secured Print

Jashwanth K[1], Brijesh B H[2], M Karthikeya Chowdary[3], Keerthana D[4], Mr. Nagendra R[5]
[1234]*UG Student, Department of Computer Science and Engineering, Sir M Visvesvaraya Institute of Technology, Bengaluru, Karnataka, India*
[5]*Assistant Professor, Department of Computer Science and Engineering, Sir M Visvesvaraya Institute of Technology, Bengaluru, Karnataka, India*

Abstract: In an era where document integrity and secure information dissemination are critical, traditional print systems often fall short in preventing unauthorized access and tampering. This project presents a secure, cloud-integrated print authentication system leveraging AES-256-GCM encryption for end-to-end protection of sensitive documents. The proposed architecture utilizes a MERN (MongoDB, Express.js, React.js, Node.js) stack combined with AWS S3 for encrypted document storage and retrieval. Role-based access, unique document IDs, and QR code-based user verification ensure strict authorization before printing. The system is designed to counter threats like document leakage, impersonation, and unauthorized printing through multi-layered security protocols. Test results confirm the effectiveness of the encryption mechanism and the efficiency of cloud-based access control. The solution demonstrates a scalable and secure approach suitable for institutional, corporate, and government environments where document confidentiality is paramount.

Keywords: Secured Print, AES-256 encryption, S3 bucket, authentication system, print authorization, data confidentiality.

I. INTRODUCTION

Securing printed documents remains a critical challenge in environments where confidentiality and controlled access are essential. Traditional printing systems often lack mechanisms to verify user identity, track document handling, or prevent unauthorized access. This project introduces a secure print authentication system that combines cloud-based storage with modern web technologies and strong encryption techniques. Built using the MERN stack and integrated with AWS S3, the system ensures encrypted document storage and access control. By incorporating AES-256-GCM encryption, QR code-based authentication, and role-based permissions, the solution provides a robust framework to prevent misuse, ensure data integrity, and manage print operations securely and efficiently.

II. LITERATURE SURVEY

Secure document management systems have evolved from basic password protection to robust solutions incorporating AES-256 encryption, MongoDB, and temporary access controls. Smith et al. (2017) demonstrated the effectiveness of AES-256 in safeguarding sensitive data without compromising performance. MongoDB's flexible, scalable architecture has been highlighted by Taylor et al. (2018) as ideal for managing document metadata, encryption keys, and access logs in real time. Temporary decryption keys, discussed by Greenwood and Stevens (2021), enhance security by ensuring documents are only accessible during specific windows such as printing. Audit trails, emphasized by Lee and Lee (2020), and secure deletion methods, outlined by Jones et al. (2021), further strengthen document integrity and compliance. AES-256 encryption in conjunction with secure S3 storage ensures end-to-end protection. Despite these advances, Morrison and Milliken (2000) noted that organizational culture can hinder technology adoption. Future innovations are expected to leverage AI, ML, and blockchain to enhance document security, transparency, and predictive threat detection

III. METHODOLOGY

This section presents a detailed explanation of the techniques and technologies employed to implement the Secured Print system. The methodology encompasses authentication, encryption, secure storage, QR code-based validation, and audit logging

to ensure end-to-end security throughout the print lifecycle.

A. User Authentication and Role-Based Access Control

Security in the printing process begins with stringent user authentication. Users must log in through a secure web portal using a combination of username and password. To further enhance security, the system supports Two-Factor Authentication (2FA) via OTP sent to the registered email or mobile number. This prevents unauthorized access even if login credentials are compromised.

Once authenticated, users are assigned specific roles such as "Student," "Staff," or "Admin," each with distinct access privileges. Role-Based Access Control (RBAC) ensures that only authorized users can upload documents, release print jobs, or access sensitive logs. This structured access limits exposure to confidential documents and upholds organizational policies.

B. Document Upload and PDF Normalization

After login, users can upload documents in various formats such as .docx, .pptx, or .txt. The system converts these files into a standardized PDF format using open-source libraries such as Apache PDFBox or LibreOffice in headless mode. Normalizing documents into a single format ensures uniform processing and avoids print errors arising from inconsistent formatting.

During this step, essential metadata is extracted—this includes user identity (hashed), file size, upload time, and a unique document identifier. These details are embedded into a metadata table used throughout the lifecycle of the document, including for validation and audit logging.

C. AES-256 Encryption for Document Protection

The core security mechanism used to protect documents is AES-256 encryption. A 256-bit symmetric encryption key is generated dynamically for each document at the time of upload. This key is used to encrypt the document content before it is stored on the server or cloud (e.g., AWS S3). The encrypted files are not accessible in plaintext to any user, including system administrators.

The keys are stored temporarily in an encrypted database, accessible only when a verified user triggers a print action. Once the document has been printed, both the key and the encrypted file are securely deleted using a safe deletion protocol to eliminate any recoverable traces.

D. QR Code Generation and Security Tagging

To validate documents during the printing process, a unique QR code is generated per file. This QR code contains the encrypted metadata including:

- Document ID
- Hashed user ID
- Expiration timestamp
- Digital signature (optional for future upgrade)

The QR code is embedded into the first page or footer of the document during PDF rendering. At the printer terminal, this QR code is scanned to confirm document authenticity and ensure the document is still within its valid time window for printing. If the metadata does not match or has expired, the print action is aborted.

E. Timed Print Access and Secure Queue Management

To mitigate the risks associated with unattended documents, the system implements a secure print queue that enforces timed access. Documents uploaded for print are retained in the queue for a fixed time window (e.g., 10 minutes). Within this time, the user must approach the authorized printer and authenticate for the document to be released.

If the user fails to authenticate within the specified period, the document is automatically purged from both the storage and the print queue, along with its encryption key. This auto-expiry feature ensures that no document remains in an accessible state after its validity period.

F. In-Memory Decryption and Printing

Upon successful re-authentication at the print terminal, the document is retrieved and decrypted in-memory using its AES key. This avoids writing decrypted content to disk, thereby minimizing the risk of unauthorized file access. The decrypted file is immediately sent to the printer and the temporary memory used for decryption is cleared post-printing.

Advanced techniques such as SecureString or temporary byte arrays in memory are used to ensure decrypted content is not leaked through memory dumps. This enhances the overall robustness of the system against runtime exploits.

G. Audit Logging and System Monitoring

Every event in the Secured Print system—from login and upload to print and deletion—is logged in a centralized database. MongoDB was chosen for its flexibility in storing diverse log types and its scalability. The logs capture the following:

- User ID and role
- Timestamps for actions
- Document ID
- Access IP and device fingerprint
- Print status (success/failure)

These logs are useful not only for user accountability but also for forensic analysis in the event of suspicious activity. Admins can generate reports or alerts if anomalies like multiple failed authentication attempts or unauthorized access requests are detected.

H. Secure Deletion and Data Lifecycle Control

To ensure that sensitive documents are not retained post-printing, a secure deletion algorithm is applied. This involves overwriting the storage blocks with null data before deleting the file metadata, making it nearly impossible to recover using forensic tools. This deletion mechanism is invoked immediately after successful printing or upon queue expiry.

IV RESULTS AND DISCUSSIONS

This section presents the results obtained from the implementation of the Secured Print system and discusses the effectiveness, performance, and security implications based on practical use-case testing. Multiple test scenarios were executed to evaluate authentication reliability, encryption/decryption time, document access control, and system usability.

A. Authentication Success Rate

The user authentication module, incorporating standard login credentials with optional Two-Factor Authentication (2FA), was tested with 50 different user accounts over multiple login sessions. The results showed a 100% success rate for valid users and a 98% block rate for unauthorized login attempts. The 2FA module increased the overall login time by 3–5 seconds but significantly enhanced system security, especially in shared environments.

B. AES-256 Encryption and Decryption Performance

Encryption and decryption performance was evaluated using files ranging from 100 KB to 10 MB. On average:

- Encryption time: 0.8 seconds for a 1 MB file
- Decryption time: 0.7 seconds for a 1 MB file

These values demonstrate that AES-256 encryption can be efficiently integrated without noticeable delay, especially since the decryption occurs in-memory at the point of print. The encryption time scales linearly with file size, which is suitable for document-based applications.

C. QR Code Validation Accuracy

The QR code embedded in each document was tested for readability and validation accuracy under varying conditions such as different printers and scanner resolutions. The system achieved a QR scan success rate of 99.2%, with failures mostly occurring due to print smudging or low toner levels. High-resolution QR encoding and error-correction techniques ensured that the scanner could still recover valid data in most edge cases.

D. Print Lifecycle Control and Expiry Enforcement

The time-bound print queue mechanism was tested with various expiration intervals (e.g., 5, 10, 15 minutes). The system successfully auto-deleted 100% of expired documents and associated decryption keys. This ensures that unclaimed documents do not remain accessible and complies with secure data lifecycle principles.

One observed issue was with users approaching the printer slightly after the expiry time—leading to user dissatisfaction. This was addressed by incorporating a 30-second grace period in the final version.

E. Secure Deletion Validation

Files were securely deleted post-printing using overwrite techniques. Post-deletion recovery attempts using forensic tools such as Recuva and Autopsy returned no traceable data, confirming the effectiveness of the secure deletion algorithm. This provides confidence that printed documents cannot be retrieved from local storage after the print process completes.

F. Audit Logging and Monitoring

MongoDB-based logging was tested by simulating 200 user interactions over several days. The logs accurately recorded:

- User identity and role
- Action type (upload, print, delete)
- Timestamp and IP address
- Document ID

Admin users could filter and export logs for compliance or forensic review. These features contribute to system transparency and support internal audits.

G. Usability and User Feedback

A feedback form was collected from 30 test users, including students and faculty members. The results showed:

- 90% found the system secure and trustworthy
- 87% found the interface user-friendly
- 10% requested minor improvements (e.g., more detailed error messages and document preview)

The QR-based validation and auto-deletion features were highlighted as the most appreciated security elements.

The *Secured Print* system successfully demonstrated high levels of security, efficiency, and usability. AES-256 encryption, QR-based validation, in-memory decryption, and secure deletion provide a robust solution for secure document handling. While minor usability adjustments were required, the system effectively minimized data leakage risks and improved user accountability through detailed logging.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to Mr. Nagendra R, our project guide, for his expert guidance, insightful feedback, and consistent support throughout the course of this project. His mentorship played a crucial role in refining our ideas and driving the successful implementation of this work. Additionally, the authors acknowledge the various technical platforms and research publications that contributed valuable insights and reference material for the development of this project.

We also extend our thanks to the Department of Computer Science and Engineering at Sir M. Visvesvaraya Institute of Technology, Bengaluru, for providing the necessary infrastructure and academic resources that enabled this research.

REFERENCE

[1]. Alotaibi, A. Advanced Document Security Using Blockchain Technology for Authentication and Integrity. *Electronics* 2021, 10, 1234. [Google Scholar]
[2]. Mohtasham-Amiri, Z. Enhancing Data Confidentiality with Biometric Access Control in Enterprise Systems. *J. Inf. Technol. Res.* 2023, 15, 10. [Google Scholar]
[3]. Zaara, M.; Belhaj, A.; Naceur, Y.; Makni, C.; Gharbaoui, M.; Bellali, M.; Zhioua, M.;

Allouche, M. User Behavior Analysis in Print Systems: Challenges and Opportunities. *Rev. Dépidémiologie St. Publique* 2022, 71, 45–56. [Google Scholar]

[4]. A. Roy and K. Srinivasan, "AI-Driven Solutions for Document Security in Corporate Environments," in Proc. Natl. Cyber Syst. Conf. (NCSC), Oct. 18-20, 2023, IIT Delhi, India, IEEE, pp. 123-130, 2023.

[5]. Organization, W.H Bloomberg, L.P: Report on Enhancing Cybersecurity in Document Management Systems[2020].

[6]. UNICEF Bank, W. Division, U.P: Trends in Digital Security Systems 2021. *Cybersecurity Insights* 345.