American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

ENCRYPTED ONLINE EXAMINATION QUESTION PAPER DISTRIBUTION WITH ROLE-BASED ACCESS CONTROL

Akshitha Chamanthula, Ramesh G*
Vaagdevi Engineering College, Warangal, 506005, Telangana, India.
*Correspondence: Ramesh G (gadde.ramesh@gmail.com)

ABSTRACT

The rapid digitalization of academic and examination processes has increased the demand for secure mechanisms to handle sensitive examination question papers. The question paper distribution relies on manual methods such as physical transport, sealed envelopes, or basic electronic sharing, which offered limited security and were prone to leakage, unauthorized access, and human error. Even in semi-digital systems, question papers are often stored or transmitted in plaintext with weak access control, lacking proper authentication, authorization, and audit mechanisms. These limitations pose serious risks to examination integrity and confidentiality, especially in large-scale or remote examination environments. To address these challenges, this project presents a secure online examination question paper distribution framework that integrates strong cryptographic techniques with role-based access control. Examination content is protected using Advanced Encryption Standard Galois/Counter Mode (AES-GCM) symmetric encryption, while Rivest–Shamir–Adleman (RSA) public-key cryptography is employed for secure key generation and key exchange, and Secure Hash Algorithm-256 (SHA-256) hashing is used for secure password protection. Access to encrypted papers is strictly controlled through authentication and authorization checks, and decryption is performed dynamically only for authorized users, minimizing plaintext exposure and maintaining Role Based Access Control (RBAC). The system also maintains detailed audit logs to ensure accountability and traceability. By automating encryption, authorization, and access workflows using a lightweight web-based architecture, the proposed system enhances performance, reliability, and security. The significance of this work lies in providing a scalable, transparent, and robust solution that preserves examination integrity and strengthens trust in modern digital academic environments.

Keywords: Secure Question Paper Distribution, Advanced Encryption Standard Galois/Counter Mode (AES-GCM), Rivest–Shamir–Adleman (RSA), Secure Hash Algorithm-256 (SHA-256), Role-Based Access Control (RBAC), Examination Security

1. INTRODUCTION

In today's era of digitalization, the term information and communication technology (ICT) has expanded to encompass many aspects of computing technology and is more recognizable than ever before. The increasing use of ICTs in academic institutions is attributed to several factors. For instance, employing ICTs in education shall improve the quality of education. It shall facilitate the absorption and acquisition of knowledge and improve the effectiveness of implementing educational policies [1]. E-exam refers to a computerized exam through which the student uses a computer for taking his/her exam. It serves as an effective, unbiased, and exciting method for assessing students' academic level. Using e-exams for the assessment of students at the university level shall increase the objectivity of the assessment process [2,3].

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

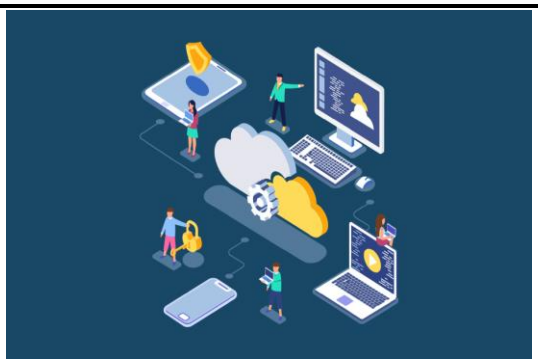


Fig. 1: Online Examination Question Paper Distribution

Now there arises a question that often confuses most of us, i.e., what is the difference between computer-based exam and online exam? The term computer-based exam (or computer-based test) encompasses online exam. Online exams (also known as e-exams) may be considered as a sub-class of computer-based exam, wherein the exam is conducted online. Online is used in the sense that the computer being used to take the test is connected to the intranet or the Internet, in a client–server environment. The computer being used for taking the test can be considered a client computer. The server computer is the one that is sitting somewhere on the Internet (or the intranet) and delivering the exam. Usually, in an online exam, there is some form of communication between the server and the client (not necessarily continuous). The exam results are uploaded to the server computer after the exam. The role of the client comes to an end as soon as he/she completes the exam and the results are uploaded. In technical terms, the session ends after the exam is completed.

As far as computer-based exam is concerned, it is a generic term used for any kind of exam or test given on a computer. The computer may or may not be online. In other words, the computer may or may not be connected to a server on the Internet (or intranet). After a computer-based exam (CBE) or computer-based test (CBT), the results may be stored locally on the computer's hard disk or transported online to the web server. Usually, standalone testing is referred to as CBT. Competitive exams are often referred to as online exams because they are delivered in real time simultaneously over the network to several students and the exams are conducted in a client–server environment. A CBT software exam engine may be viewed as an example of CBT. Here a candidate downloads the CBT software from the Internet and installs it on his/her own computer and appears in the exam. Here no server connection is required for appearing in the test/exam.

E-exam was introduced in the 1970s. It is used as an effective method for assessing one's level of knowledge, academic performance, and problem-solving skills. It is employed as a research tool by researchers to collect data or by trainers and educators to assess students. It enables teachers to save their efforts while assessing students. E-exam has been increasingly used by higher education institutions worldwide because it provides relatively more accurate results by employing stimuli that may be in an audio, text, graphic, or kinesthetic form [4].

E-exams facilitate the simplification of the conventional, paper-based exams. They are particularly beneficial when the class sizes are considerable, enabling ease in devising and renditioning the process. It includes marking and reporting the examination, later on storing, and performing statistical analysis [5,6]. Besides, they constitute an entirely computerized process, which helps ameliorate the assessment validity, which further comprises the examinee's performance, warranting a greater degree of skill and comprehension, for it employs enhanced question forms consolidating interactivity and multimedia. E-exams, furthermore, amend the authenticity of grading and the briskness of the exam results, promoting more extensive analysis and providing prompt feedback.

Compared to the conventional exam format, online examination substantially amends the efficacy of various data management responsibilities, comprising marking and

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

moderation of the data, followed by secure storing, which overall reduces the workload of the teachers while also lessening the burden of invigilating large student cohorts [7].

2. LITERATURE SURVEY

Vécsi Á et al. [8] proposed a secure electronic examination framework that balanced privacy, transparency, and communication. The system introduced a mechanism that allowed controlled communication between candidates and examiners during examinations, enabling clarification of ambiguous questions without compromising the integrity of the assessment process. To preserve participant privacy, the framework employed attribute-based certifications, ensuring that both candidates and examiners remained anonymous throughout registration, examination, evaluation, and result publication. Additionally, the system incorporated a revocation mechanism, allowing identities to be revealed only when fraudulent activities were detected during audits. This approach improved examination fairness, accountability, and resistance to identity-based attacks while maintaining confidentiality. Alharbe et al. [9] proposed a data-oriented Risk-Based Access Control (R-BAC) model that enhanced the traditional Attribute-Based Access Control (ABAC) framework by incorporating dynamic risk evaluation into authorization decisions. Instead of relying solely on predefined user attributes, the model assessed potential security risks associated with subject attributes, resource attributes, and environmental conditions before granting access. The authors developed a comprehensive set of risk assessment indicators and quantitatively evaluated them using the fuzzy consistency Analytic Hierarchy Process (AHP), which improved the accuracy of decision-making under uncertain conditions. Furthermore, the proposed framework was implemented using eXtensible Access Control Markup Language (XACML), demonstrating its compatibility with standardized access control policies and its suitability for real-world enterprise environments. Ren F et al. [10] developed a blockchain-enabled blended teaching evaluation management system integrated with searchable encryption to ensure secure storage, efficient retrieval, and privacy protection of educational data. The proposed architecture combined the Ethereum blockchain with the InterPlanetary File System (IPFS) through an on-chain and off-chain collaborative storage model, thereby supporting secure management of large volumes of student assignments while reducing blockchain storage overhead. To prevent unauthorized access, the authors implemented a smart contract-based Role-Based Access Control (RBAC) mechanism that assigned permissions according to user roles. The inclusion of searchable encryption enabled authorized users to retrieve encrypted data without exposing sensitive information, thereby enhancing both confidentiality and operational efficiency in educational environments.

Nyame G et al. [11] investigated the role of Role-Based Access Control (RBAC) in strengthening organizational knowledge security and identified several research directions for future exploration. The study proposed eight research propositions highlighting the evolving challenges associated with RBAC implementation in knowledge-intensive organizations. In addition, the authors developed a conceptual framework that integrated RBAC with three fundamental precursor constructs influencing effective role mining and role engineering. Their socio-technical analysis examined how organizational structures, human behavior, and technological factors collectively impacted access control policies. The study also emphasized the significance of status–role relationships in improving authorization decisions, thereby providing a comprehensive theoretical foundation for designing more adaptive and secure RBAC systems. Song H et al. [12] presented a blockchain-based access

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

control and behavior regulation framework designed for Internet of Things (IoT) environments. The proposed system adopted an Attribute-Based Access Control (ABAC) model in combination with blockchain smart contracts to achieve decentralized, fine-grained, and tamper-resistant authorization. Smart contracts automatically verified user identities and permissions before granting access to IoT resources, thereby eliminating dependence on centralized authentication servers. Additionally, the authors introduced an inter-domain communication mechanism based on the locator/identifier separation protocol, ensuring that network traffic between different IoT domains was securely authenticated and authorized. This architecture improved trust, scalability, and resistance to unauthorized access in distributed IoT ecosystems.

Al Lail M et al. [13] introduced an optimized cloud-based implementation of the Generalized Spatio-Temporal Role-Based Access Control (GSTRBAC) model specifically designed for modern Location-Based Services (LBS). The proposed framework extended conventional RBAC by incorporating spatial and temporal constraints into access decisions, enabling permissions to be granted based on both user location and access time. To support secure communication across cloud environments, the system employed two distinct communication protocols tailored to varying security requirements. Less-sensitive data were transmitted using a lightweight protocol to improve efficiency, whereas highly confidential information was protected through stronger cryptographic communication mechanisms. The proposed architecture enhanced flexibility, scalability, and security for cloud-based LBS applications. Figueroa-Lorenzo S et al. [14] addressed the security vulnerabilities of the Modbus industrial communication protocol by proposing an enhanced Role-Based Access Control (RBAC) model that secured both user authentication and message authorization. The framework extended the traditional RBAC approach by embedding role information into X.509v3 digital certificates, allowing secure authorization of clients before communication with industrial devices. In addition, the model introduced message-level authorization based on the Modbus Unit Identifier (Unit ID), ensuring that each communication frame originated from an authenticated and authorized source. This dual-layer authorization mechanism significantly improved the protection of industrial control systems against unauthorized access, message tampering, and cyberattacks while maintaining compatibility with existing Modbus infrastructures.

4. PROPOSED SYSTEM

The research introduces a secure and controlled framework for handling the creation, storage, distribution, and access of sensitive examination question papers in a digital environment. It emphasizes confidentiality, controlled accessibility, and accountability by integrating cryptographic techniques with role-based access policies. Sensitive content is encrypted before storage, ensuring protection even in the event of storage compromise, while access is granted only after strict authentication and authorization checks. Decryption is performed dynamically using secure keys, limiting plaintext exposure to authorized users and specific time frames. Continuous monitoring through detailed access logs records all critical activities, supporting traceability and compliance. The use of lightweight data storage and a web-based interface enable efficient data management and real-time interaction, making the framework reliable and scalable for modern examination systems.

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

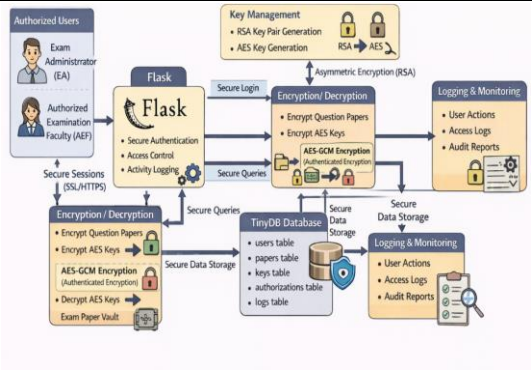


Fig. 2: System architecture of online examination.

User Authentication and Secure Session Establishment: The Fig. 2 Shows the Authorized users access the system through a secure web interface and authenticate using valid credentials. Upon successful login, secure sessions are established using encrypted communication, ensuring safe interaction throughout the workflow.

Request Handling and Access Control: All user requests are routed through the backend framework, where role-based access control policies are enforced. Only users with appropriate permissions are allowed to initiate sensitive operations such as paper access or decryption.

Cryptographic Key Management: Asymmetric cryptographic keys are generated and managed securely to protect encryption processes. These keys ensure that only authorized entities can encrypt or decrypt sensitive information, maintaining strict confidentiality.

Encryption and Secure Storage of Examination Data: Examination question papers are encrypted using symmetric encryption techniques before being stored. The encrypted data and protected keys are saved in a secure database, preventing unauthorized data exposure.

Controlled Decryption and Data Access: When authorized access is requested, decryption is performed dynamically using secure keys. Plaintext content is made available only temporarily to authorized users, minimizing the risk of data leakage.

Logging, Monitoring, and Audit Management: All critical actions, including login attempts, encryption, decryption, and data access, are recorded in detailed logs. These records support continuous monitoring, accountability, and audit analysis.

3.1 AES Encryption

AES is a symmetric block cipher used to securely encrypt and decrypt data using a single shared secret key as shown in Fig. 3. It operates on fixed-size data blocks and applies multiple transformation rounds to achieve strong confidentiality. AES is designed for high performance and is suitable for encrypting large volumes of data efficiently. The encryption process combines substitution, permutation, and key mixing operations to resist cryptographic attacks. Due to its speed and security, AES is widely adopted in secure storage and data transmission systems. Proper key handling and mode selection are critical to maintaining AES security.

Plain Data and Key Input: AES encryption begins with fixed-size plaintext blocks along with a secret symmetric key. The same key is later required for decryption, making secure key handling essential.

Key Expansion: The original AES key is expanded into multiple round keys using a deterministic key schedule. Each round key is unique and strengthens resistance against brute-force and cryptanalysis attacks.

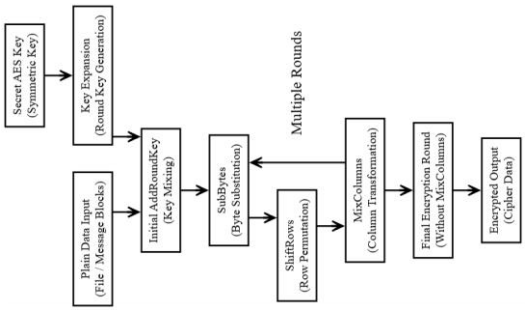


Fig. 3: Internal Workflow of AES Encryption

Initial Add Round Key Operation: The plaintext block is combined with the first-round key using a bitwise XOR operation. This step

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

immediately binds the data to the encryption key.

Core Transformation Rounds: Each encryption round applies Sub Bytes, Shift Rows, and Mix Columns operations to introduce confusion and diffusion. These transformations obscure statistical patterns in the original data.

Final Encryption Round: The final round performs substitution and permutation without the Mix Columns step. This ensures proper alignment for secure ciphertext generation.

Ciphertext Generation: After completing all rounds, the transformed data becomes ciphertext. The encrypted output is unintelligible without the correct AES key.

3.2 AES Decryption

AES decryption is the symmetric process of converting encrypted ciphertext back into its original readable form using the same secret key used during encryption as illustrated in Fig. 4. It applies a series of inverse mathematical transformations to undo the effects of encryption rounds. The decryption process follows the reverse order of encryption operations, ensuring accurate data recovery. Each round reverses substitution, permutation, and mixing applied during encryption. AES decryption guarantees data confidentiality by ensuring that only entities possessing the correct key can reconstruct the original data. Secure and correct key usage is essential for successful decryption.

Ciphertext and Key Input: AES decryption starts with the encrypted ciphertext, and the same secret key used during encryption. Without the correct key, decryption is computationally infeasible.

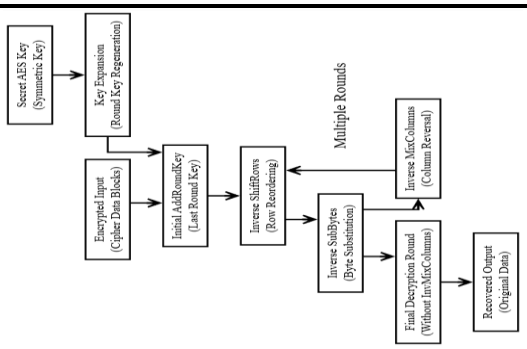


Fig. 4: Internal Workflow of AES Decryption

Key Expansion: The AES key is expanded into a set of round keys identical to those generated during encryption. These round keys are applied in reverse order during decryption.

Initial Add Round Key Operation: The ciphertext block is combined with the final round key using a bitwise XOR operation. This step initiates the reversal of encryption transformations.

Inverse Transformation Rounds: Each round applies inverse operations Inverse Shift Rows, Inverse Sub Bytes, and Inverse Mix Columns to systematically undo encryption effects. These steps restore the original data structure gradually.

Final Decryption Round: The final round excludes the Inverse Mix Columns operation and applies only inverse substitution and permutation. This completes the reversal process accurately.

Plaintext Recovery: After all rounds are executed, the original plaintext data is recovered. The output matches the original input provided before encryption.

3.3 AES-GCM

AES-GCM is a modern symmetric encryption technique that provides both data confidentiality and integrity in a single operation. It encrypts data using a counter-based encryption mechanism while simultaneously generating an authentication tag to detect any unauthorized modification. The use of a unique nonce for each encryption operation ensures protection against replay attacks. AES-GCM is computationally efficient and well-suited for securing sensitive digital

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

content in real-time systems. Its authenticated encryption property eliminates the need for separate hashing or message authentication mechanisms. Due to these characteristics, AES-GCM is widely adopted in secure storage and data protection applications.

Plaintext and Key Initialization: The Fig. 5 process begins with plaintext input and a securely generated symmetric key. A unique nonce is generated for each encryption session to ensure randomness. These elements form the foundation for secure encryption.

Counter Mode Encryption: The plaintext is encrypted block by block using AES in counter mode. A counter value is incremented for each block, ensuring that identical plaintext blocks never produce the same ciphertext. This step ensures strong confidentiality.

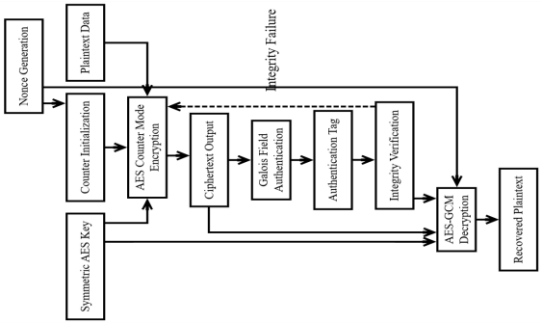


Fig. 5: Internal workflow of AES-GCM.

Authentication Tag Generation: Alongside encryption, Galois field operations are applied to the ciphertext and optional associated data. This process generates an authentication tag that represents the integrity state of the encrypted content. Any modification to the ciphertext results in tag mismatch.

Ciphertext and Tag Output: The final encrypted output consists of the ciphertext combined with the authentication tag and nonce. These components are stored or transmitted together. The authentication tag plays a critical role during decryption.

Decryption and Integrity Verification: During decryption, the ciphertext is decrypted using the same key and nonce. The authentication tag is recomputed and compared with the received tag. Decryption proceeds only if the tags match, ensuring data integrity.

3.4 RSA Key Generation

RSA key generation is a fundamental cryptographic process used to create a secure public–private key pair for asymmetric encryption. It relies on the mathematical difficulty of factoring large prime numbers, which makes the generated keys computationally infeasible to break. The process begins by selecting two large random prime numbers and computing their product to form the modulus. A public exponent is then chosen to support efficient encryption, while a private exponent is derived to enable secure decryption. The resulting public key can be safely shared, whereas the private key must be kept confidential. This mechanism forms the basis for secure key exchange and protected access in cryptographic systems.

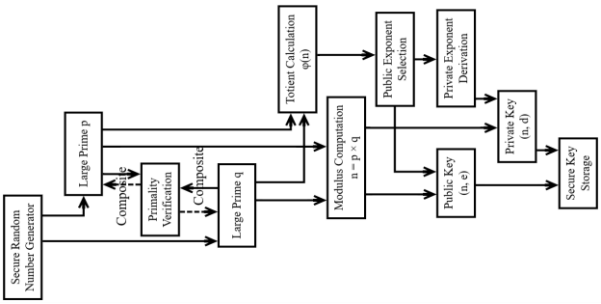


Fig. 6: Internal workflow of RSA key generation.

Prime Number Selection: The Fig. 6 process begins with the generation of two large random prime numbers. These primes are selected using probabilistic primality tests to ensure cryptographic strength. The secrecy of these prime values is essential for RSA security.

Modulus and Totient Computation: The two primes are multiplied to form a large modulus value. A totient value is then computed using the prime numbers, which plays a crucial role in determining key relationships. These values define the numerical space of the key pair.

Public Exponent Selection: A public exponent is selected such that it is relatively prime to the totient. This value is chosen to balance computational efficiency and security. The

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

public exponent becomes part of the publicly shared key.

Private Exponent Derivation: The private exponent is calculated as the modular inverse of the public exponent with respect to the totient. This step establishes the mathematical link between the public and private keys. The derived private exponent must remain confidential.

Key Pair Formation and Storage: The public key is formed using the modulus and public exponent, while the private key includes the modulus and private exponent. These keys are encoded and stored securely. Any compromise of the private key undermines system security.

4. RESULTS AND DISCUSSION

Fig. 7 illustrates the Administrator Dashboard, which acts as the central control panel for examination management. It provides an overview of system entities such as question papers, faculty members, authorization status, and encryption keys. The dashboard enables administrators to perform critical operations including paper creation, faculty authorization, and access monitoring. It supports centralized supervision and secure administration. This figure represents the operational backbone of the examination system.

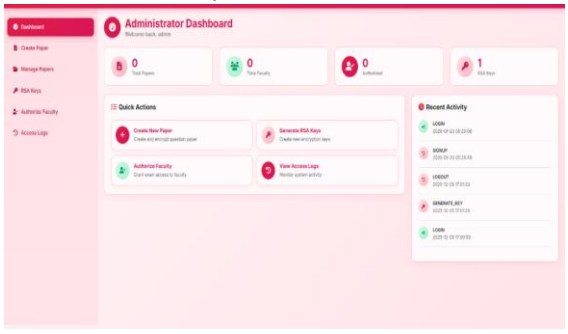


Fig. 7: Administrator Dashboard Screen

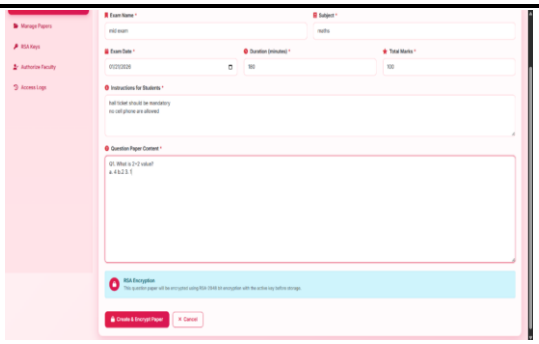


Fig. 8: Creating Question Paper Screen

Fig. 8 illustrates the Question Paper Creation screen used by administrators to prepare examination content. It allows structured input of examination metadata along with the question content. The screen integrates encryption functionality to secure the question paper before storage. This ensures confidentiality and prevents premature disclosure of exam materials. The figure highlights secure content generation within the examination lifecycle.

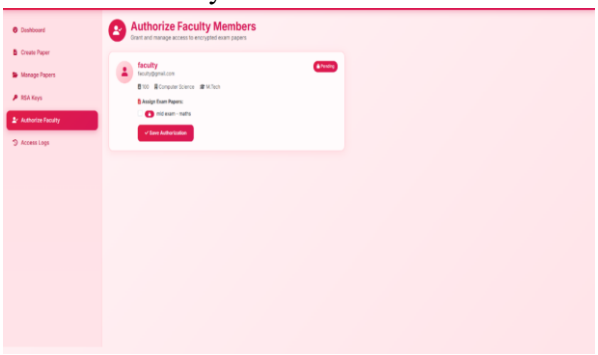


Fig. 9: Authorizing Faculty Members Screen

Fig. 9 illustrates the Authorizing Faculty Members screen that enables administrators to control faculty access to encrypted examinations. It displays faculty details along with their authorization status for specific exam papers. The screen supports selective permission granting based on institutional requirements. This mechanism enforces strict access governance and prevents unauthorized paper access. The figure reflects fine-grained role-based authorization control.

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

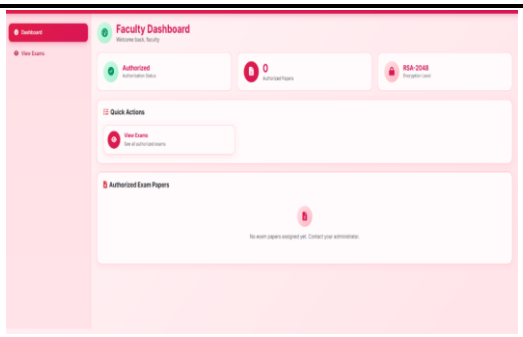


Fig. 10: Faculty Dashboard Screen

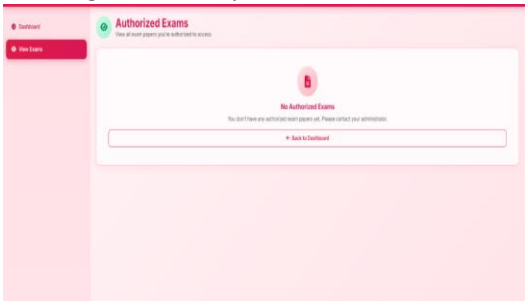


Fig. 11: View Exams Screen

Fig. 10 illustrates the Faculty Dashboard, which provides authorized faculty members with an overview of their access status. It confirms whether the faculty member is approved to view examination papers. The dashboard restricts access until explicit administrator authorization is granted. It ensures that faculty interactions remain within assigned permissions. This figure demonstrates controlled exam access from the faculty perspective.

Fig. 11 illustrates the View Exams screen that displays examination papers available to authorized faculty members. The screen enforces access validation by showing only exams assigned by the administrator. It prevents unauthorized viewing or downloading of question papers. This controlled visibility protects exam integrity and confidentiality. The figure represents the final secure access layer of the examination workflow

5. CONCLUSION

This research successfully demonstrates a secure and efficient framework for online examination question paper distribution by integrating encryption, role-based access control, and detailed activity logging. The implementation ensures that sensitive examination content remains confidential through strong cryptographic techniques while enabling controlled access for authorized users. By automating paper creation, encryption, authorization, and decryption workflows, the system significantly reduces manual intervention and associated security risks. Performance improvements are achieved through lightweight backend design, efficient cryptographic operations, and fast data access using a file-based database. The use of session-based authentication and modular routing enhances system responsiveness even under concurrent access. Dynamic decryption ensures that plaintext exposure is minimal, improving both security and operational efficiency. Audit logging further strengthens accountability and traceability across all system interactions.

REFERENCES

[1] Tinio, V.L. ICT in Education: UN Development Programme. Available online: http:www.eprmers.org

[2] Alsadoon, H. Students' perceptions of e-assessment at saudi electronic university. Turk. Online J. Educ. Technol. 2017, 16, 147–153.

[3] Nikolova, K. Data Mining in Brain Studies. IEETA. Available online: http://wiki.ieeta.pt/wiki/index.php/Nikolova-2012

[4] Daramola, O.; Oladipupo, O.; Afolabi, I.; Olopade, A. Heuristic evaluation of an institutional E-learning system: A Nigerian case. Int. J. Emerg. Technol. Learn. 2017, 12, 26–42.

[5] Osuji, U.S. The Use of e-Assessments in the Nigerian Higher Education System. Turk. Online J. Distance Educ. 2012, 13, 140–152. Available online: https://eric.ed.gov/?id=EJ1000419

[6] Farzin, S.; Dahlan, H.M. Proposing a model to predict students' perception towards adopting an e-assessment system. J. Theor. Appl. Inf.

Technol. 2016, 90, 144–153. Available online: www.jatit.org

[7] Joint Information Systems Committee (JISC). Effective Practice with e Assessment. Inf. Syst. J. , 1–52. Available online: https://www.webarchive.org.uk/wayback/archive/20140613220103/http://www.jisc.ac.uk/media/documents/themes/elearning/effpraceassess.pdf

[8] Vécsi, Á.; Pethő, A. Auditable Anonymous Electronic Examination. Cryptography 2024, 8, 19. https://doi.org/10.3390/cryptography8020019

[9] Alharbe, N.; Aljohani, A.; Rakrouki, M.A.; Khayyat, M. An Access Control Model Based on System Security Risk for Dynamic Sensitive Data Storage in the Cloud. Appl. Sci. 2023, 13, 3187. https://doi.org/10.3390/app13053187

[10] Ren, F.; Zhao, B.; Wang, J.; Zhou, J.-X.; Xie, T.-Y. Enhancing Blended Learning Evaluation Through a Blockchain and Searchable Encryption Approach. Electronics 2025, 14, 1039. https://doi.org/10.3390/electronics14051039

[11] Nyame, G.; Qin, Z. Precursors of Role-Based Access Control Design in KMS: A Conceptual Framework. Information 2020, 11, 334. https://doi.org/10.3390/info11060334

[12] Song, H.; Tu, Z.; Qin, Y. Blockchain-Based Access Control and Behaviour Regulation System for IoT. Sensors 2022, 22, 8339. https://doi.org/10.3390/s22218339

[13] Al Lail, M.; Moncivais, M.; Benton, R.; Perez, A.J. Cloud-Based Access Control Including Time and Location. Electronics 2024, 13, 2812. https://doi.org/10.3390/electronics13142812

[14] Figueroa-Lorenzo, S.; Añorga, J.; Arrizabalaga, S. A Role-Based Access Control Model in Modbus SCADA Systems: A Centralized Model Approach. Sensors 2019, 19, 4455. https://doi.org/10.3390/s19204455