

Blockchain Framework for Securing and Distributing Exam papers

Srivalli N

Department of Information Science

Engineering and

RV College of Engineering

Bengaluru, Karnataka, India

Prof. Sushmitha N

Department of Information Science and

Engineering

RV College of Engineering

Bengaluru, Karnataka, India

ABSTRACT – The increasing reliance on digital technologies for educational processes has heightened concerns regarding exam paper leakage, compromising academic integrity and fairness. To address this issue, this proposal introduces a Blockchain-Powered Exam Paper Leakage Prevention System that leverages the inherent transparency, immutability, and decentralized nature of blockchain technology. Traditional exam management systems often involve manual handling and centralized storage of examination materials, making them vulnerable to unauthorized access, human error, and insider threats. These weaknesses have led to instances of exam paper leakage, undermining the credibility of academic institutions and eroding stakeholder trust. There is a critical need for a secure, automated, and tamperproof system that mitigates these risks while ensuring accountability and transparency. The proposed system integrates smart contracts and cryptographic security mechanisms to ensure secure storage, controlled access, and tamper-proof transmission of examination materials. Smart contracts automate key processes such as access authorization and time-bound release of exam papers, removing the dependency on manual operations. Cryptographic techniques, including encryption and digital signatures, safeguard sensitive data from unauthorized access and verify data authenticity.

This approach builds the trust among stakeholders—administrators, educators, and students—while reducing the chances of data breaches. The system is designed to be scalable, auditable, and adaptable to various educational settings, setting a new standard for secure academic examination management.

KEYWORDS - Blockchain-Powered Exam System, Exam Paper Leakage Prevention, Smart Contracts, Interplanetary File System, Tamper-Proof Transmission, Digital Signatures

INTRODUCTION

The integration and security of exam papers are critical concerns for educational institutions worldwide. With increasing instances of exam paper leaks, ensuring the confidentiality of examination content has become a pressing issue. Traditional systems for handling exam papers, including physical distribution and centralized digital storage, are vulnerable to various security breaches, such as unauthorized access, tampering, and insider threats. To address these challenges, a Blockchain-Powered Exam Paper Leakage Prevention System offers a promising solution. Blockchain, a decentralized and immutable distributed ledger technology, provides a secure framework for managing exam papers. By using blockchain, institutions can ensure that exam papers are stored in a tamper-proof environment, with all interactions recorded on an unalterable ledger. Smart contracts, integrated within the blockchain, enable automated enforcement of access policies to ensure that exam papers are only accessible to authorized personnel at specified times. Additionally, cryptographic techniques safeguard the confidentiality and integrity of the exam papers during storage and transmission. This system doesn't only prevent unauthorized access and tampering but also enhances the transparency and accountability of the entire examination process. By leveraging the advantages of blockchain, smart contracts, and cryptography, educational institutions can safeguard their examination data from leaks, ensuring a more secure and trustworthy exam environment.

II LITERATURE REVIEW

[1]. Blockchain for Secure Data Management:

Blockchain provides decentralized, immutable, and transparent data storage, ensuring exam papers' integrity and preventing tampering. Blockchain ensures secure, auditable access and protects sensitive exam data from breaches (Zohar & Hammer, 2024).

[2]. Blockchain in Educational Security Systems:

Blockchain is used to secure exam papers, preventing unauthorized access and ensuring data integrity. It helps reduce fraud and misconduct in academic settings (Ramakrishnan et al., 2020).

[3]. Smart Contracts for Automated Control:

Smart contracts automate the process of exam paper release, ensuring access is granted only to authorized users at the right time. They eliminate human errors and help prevent leaks (Zhang et al., 2023).

[4]. Cryptography for Securing Exam Papers:

Cryptographic techniques, like encryption and digital signatures, protect exam papers during storage and transmission. Blockchain combined with cryptography ensures exam papers remain confidential and unaltered (Wang et al., 2020).

[5]. Reducing Insider Threats:

Blockchain reduces the risks posed by insider threats in centralized systems by decentralizing data management (Dastjerdi et al., 2022). It provides an immutable audit trail for all access to exam papers.

[6]. Blockchain and IoT Integration for Exam Security:

Blockchain combined with IoT sensors ensures the physical security of exam papers during transport and storage (Li et al., 2022). It provides real-time monitoring and additional layers of security.

[7]. Transparency and Auditability in Exam Processes:

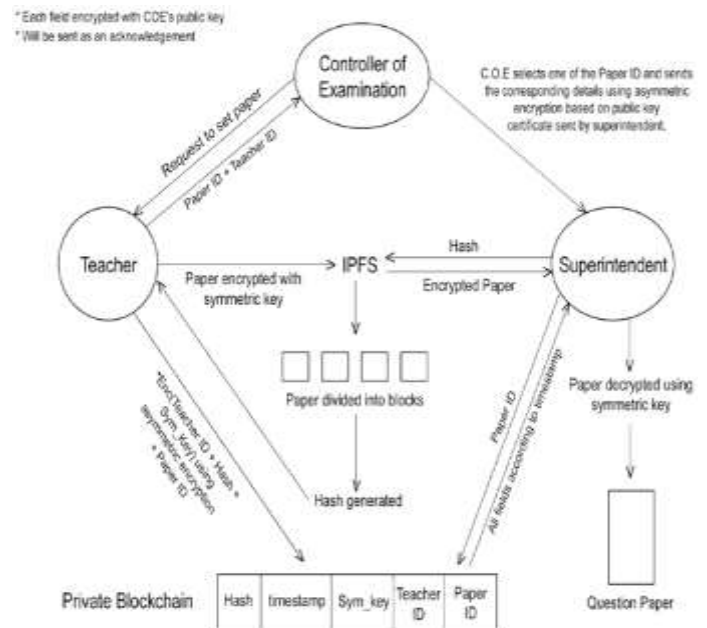
Blockchain's transparent ledger ensures full traceability of all actions on exam papers, making unauthorized access detectable (Christidis & Devetsikiotis, 2023).

[8]. Blockchain in Securing Digital Identities:

Blockchain manages digital identities, provides only authorized access.

(Makhdoom et al., 2024). It uses public-private key encryption for secure authentication.

III SECURITY ARCHITECTURE



Database will be maintained at each actor's end which will hold the required values.

Fig 1: Blockchain-Based Exam Paper Workflow

The process begins with the Controller of Examinations (COE), who refers to the official date sheet and initiates a secure request to selected subject teachers for question paper creation. This request is sent through a protected digital interface, ensuring that only authorized educators are involved.

Each teacher, upon receiving the request, drafts the exam paper on their local device in PDF format. To maintain confidentiality from the very beginning, the document is encrypted using a symmetric encryption algorithm—a method that locks the file with a secret key known only to the sender and authorized recipients.

Once encrypted, the file is uploaded to the InterPlanetary File System (IPFS), a decentralized storage network. IPFS breaks the file into smaller chunks, each of which is hashed (converted into a unique digital fingerprint). These hashes are then combined into a single root hash, which serves as a permanent, tamper-proof reference to the entire document.

This root hash, along with metadata such as the paper ID, timestamp, and an anonymized teacher ID, is recorded on the blockchain ledger. This ensures that a verifiable, immutable record of the submission exists—without revealing the paper’s content or the identity of the teacher. The COE’s portal is then updated to reflect the new submission, but all identifying details remain hidden to preserve fairness and prevent bias. Upon receiving this, the superintendent accesses the blockchain to verify the hash and validate their credentials. Once authenticated, a smart contract or automated access protocol triggers a secure retrieval request to IPFS. The system reconstructs the encrypted file using the stored chunk hashes, ensuring that the paper is exactly as it was submitted—untouched and unaltered. This lifecycle not only ensures confidentiality, integrity, and traceability, but also builds trust in the examination process by eliminating manual handling, reducing insider threats, and enabling full auditability.

IV SECURITY CHALLENGES

As educational institutions transition toward digital platforms for exam administration, the confidentiality and integrity of exam papers face a growing number of threats. These issues come from both internal actors and external adversaries, exploiting vulnerabilities in centralized systems, manual workflows, and unsecured communication channels.

Identifying and understanding these potential attack vectors is critical for designing a system that upholds academic integrity. By identifying and addressing these threats, institutions can design a resilient, transparent, and tamper-proof exam management system.

Blockchain, when used with smart contracts and strong cryptographic practices, offers a powerful foundation to protect the integrity of academic assessments.

Insider Threats Authorized: Even in a secure system, the greatest risk often comes from within. Authorized personnel—such as examiners, administrators, or IT staff—may misuse their access to leak or manipulate exam content. These actions might be driven by personal gain, coercion, or negligence. A robust system must therefore enforce strict role-based access controls, audit trails, and accountability mechanisms to deter and detect such behavior.

If someone gains access to the paper—even minutes before the scheduled release—it can compromise the entire process. Attackers might try to bypass time locks or exploit system loopholes to decrypt files early. Smart contracts and time-based access controls are essential to ensure that no one, not even authorized users, can access the content before the designated time.

Key Leakage or Weak Key Management: Encryption is only as strong as the protection of its keys. If symmetric or private keys are stored insecurely, shared carelessly, or managed poorly, they can be intercepted or stolen. This would allow unauthorized decryption of exam papers. Secure key vaults, multi-factor authentication, and key management protocols are critical to safeguarding these keys.

Tampering with File Storage: Even if the exam paper is encrypted and stored off-chain (e.g., in IPFS), attackers might attempt to replace the file or manipulate its hash to point to a different version. This could go undetected if hash verification is not enforced. Blockchain’s immutability and hash-based verification mechanisms ensure that any tampering attempt is immediately flagged and rejected.

V MITIGATION TECHNIQUE

To address the identified risks, the proposed system employs a multi-layered defense strategy combining cryptographic safeguards, decentralized validation, and smart contract automation.

These techniques ensure that only save users can access sensitive content, that transactions are tamper-evident, and that every interaction is immutably recorded for forensic traceability.

To protect sensitive exam content from leaks, tampering, and unauthorized access, the system integrates several layers of defense—each reinforcing the other to create a resilient security framework.

For example, a teacher can upload a paper but cannot view others’ submissions. This principle of least privilege minimizes the risk of misuse and makes every action traceable.

Strong Encryption and PKI Integration: Before any paper is uploaded, it’s encrypted using AES-256, a military-grade encryption standard.

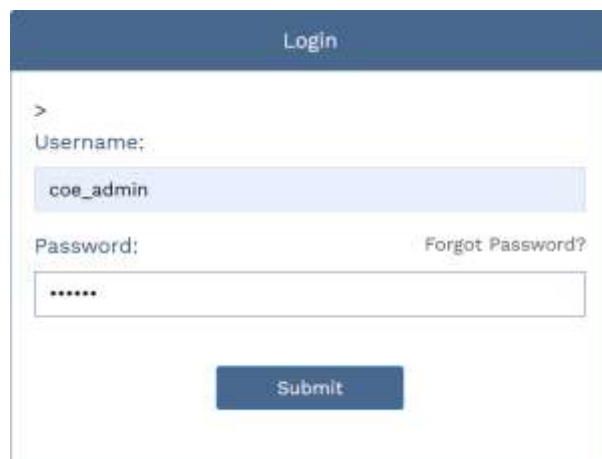
The decryption keys are managed through Public Key Infrastructure (PKI) or blockchain-based digital identities, ensuring that only verified users can unlock the content. This protects the paper both in storage and during transmission Key Infrastructure (PKI) or blockchain-based identity.

Hash Verification: To ensure the file hasn't been tampered with, the system compares the cryptographic hash of the retrieved file with the original hash stored on the blockchain. If even a single byte has changed, the mismatch is detected instantly, and the file is rejected. This guarantees data integrity.

Multi-Signature Validator Protocol: No single person can authorize sensitive actions—like releasing a paper or changing access permissions. Instead, a group of independent validators must approve the action. This multi-signature protocol prevents collusion and ensures that decisions are made transparently and collectively.

VI RESULT AND ANALYSIS

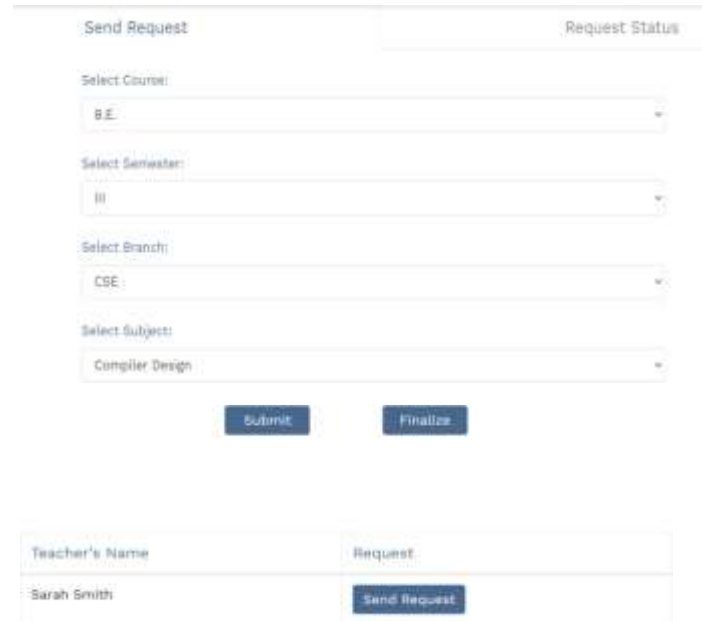
To better understand system behavior, a range of visual dashboards and log views were developed



The screenshot shows a login form with a dark blue header labeled 'Login'. Below the header, there are two input fields: 'Username:' with the value 'coe_admin' and 'Password:' with masked characters '*****'. A 'Forgot Password?' link is next to the password field. A 'Submit' button is at the bottom.

Fig 2: Login Page

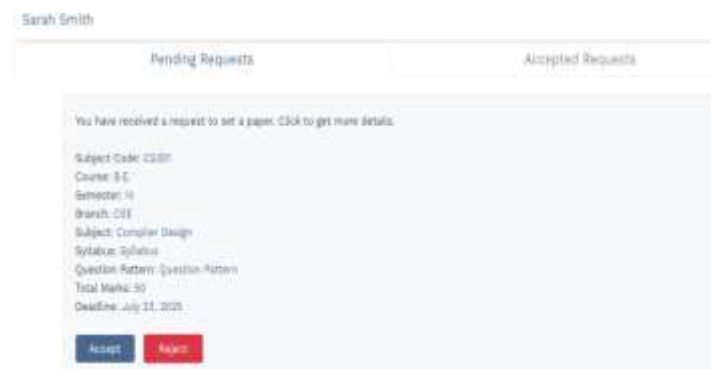
Figure 2 showcases the Controller of Examinations (COE) Dashboard, a secure portal for initiating exam paper assignments. After logging in, the COE reviews the academic datasheet and sends encrypted paper-setting requests to subject-specific faculty based on scheduled exams.



The screenshot shows the COE dashboard. It has a 'Send Request' button and a 'Request Status' tab. Below, there are dropdown menus for 'Select Course:' (B.E.), 'Select Semester:' (III), 'Select Branch:' (CSE), and 'Select Subject:' (Compiler Design). There are 'Submit' and 'Finalize' buttons. Below this, there is a table with 'Teacher's Name' (Sarah Smith) and a 'Request' column with a 'Send Request' button.

Fig 3: Controller of Examination Dashboard

Figure 3 illustrates the COE's interface for initiating paper-setting requests. After entering academic details like course, semester, branch, and subject, the dashboard displays eligible faculty. The COE selects one and submits a digitally signed request with syllabus, pattern, and deadline—all securely transmitted via the blockchain portal.



The screenshot shows the faculty dashboard for Sarah Smith. It has tabs for 'Pending Requests' and 'Accepted Requests'. A message says 'You have received a request to set a paper. Click to get more details.' Below, there is a list of request details: Subject Code: C300, Course: B.E., Semester: III, Branch: CSE, Subject: Compiler Design, Syllabus: Syllabus, Question Pattern: Question Pattern, Total Marks: 30, and Deadline: July 11, 2025. There are 'Accept' and 'Reject' buttons.

Fig 4: Faculty Dashboard

Figure 4 depicts the faculty dashboard displaying incoming paper-setting requests from the COE. Each request includes key academic details—subject code, course, semester, branch—along with syllabus, paper format, total marks, and the submission deadline needed to draft the question paper.

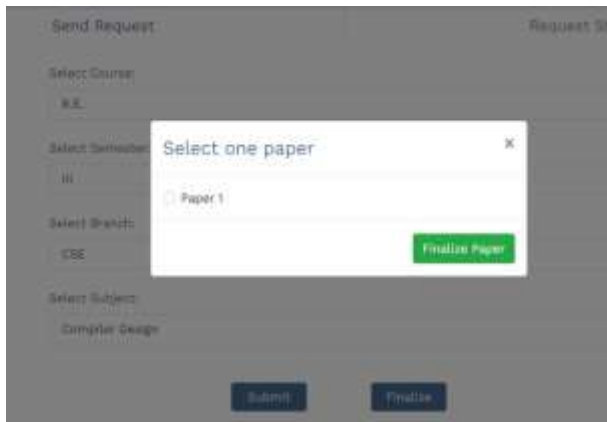


Fig 5: COE Finalization of paper

Figure 5 shows the COE's dashboard where uploaded question papers from faculty are retrieved and reviewed. After verifying academic details, the COE finalizes the paper, which is then securely forwarded to the Superintendent of Examinations for authorized distribution.

The Superintendent receives each completed paper and prepares to distribute them to the respective examiners as shown in the Fig 8.6. To maintain clarity and organization, each paper is accompanied by its corresponding subject code, which helps examiners immediately identify the relevant course or subject.

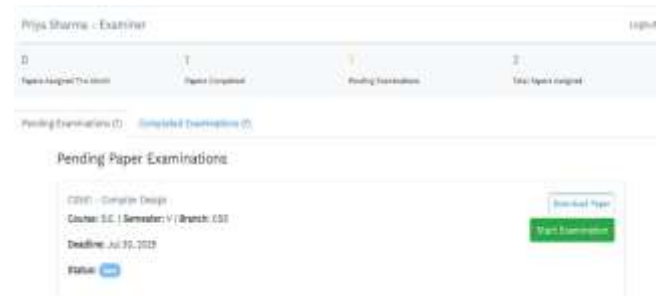


Fig 7: Examiner Dashboard

The dashboard in the Fig 8.7 presented to the examiner serves as a centralized and intuitive interface following the receipt of the question paper from the Superintendent. It prominently displays essential information including the course name, the associated subject code, and the current status of the examination process— whether the paper is pending review, accepted, or in preparation for activation.



Fig 6: Superintendent Dashboard

Figure 6 displays the Superintendent's dashboard, showing all finalized question papers approved by the COE. Each entry includes course details, subject metadata, and is securely stored for download by authorized personnel, ensuring accurate distribution through the blockchain-enabled portal.



Fig 8.6: Distribution of Paper

Once the Controller of Examinations has finalized the question papers, the responsibility shifts to the Superintendent, who plays a pivotal role in ensuring smooth and secure coordination.



Fig 8: Examiner Feedback

Figure 8.8 illustrates the structured feedback interface presented to examiners upon receiving the finalized question paper.

This form serves as a critical checkpoint in the examination workflow, allowing examiners to assess and document the paper's quality and relevance before proceeding to the next phase.

The form prompts the examiner to evaluate multiple dimensions of the question paper, including the difficulty level (to ensure the paper is balanced and suited to the intended academic standard), the extent of syllabus coverage (to verify alignment with prescribed curricula), and the overall question quality—such as clarity, logical flow, and the depth of concepts tested. Another essential field captures the appropriateness of the question paper, enabling the examiner to judge whether the paper reflects both fairness and relevance to the target course.

VII DISCUSSION

As educational universities look for online platforms for exam administration, the shift brings not only convenience but also new responsibilities—particularly around safeguarding the confidentiality and integrity of exam papers. Blockchain technology offers a transformative approach, but its impact goes far beyond technical implementation.

At the heart of this transformation is the concept of decentralized trust. Unlike traditional systems that rely on central authority to manage and secure exam content, blockchain distributes trust across a network. Every action, whether uploading a paper or accessing it—is recorded immutably, creating a transparent and tamper-proof audit trail.

This fundamentally reshapes administrative workflows, reducing the need for manual oversight and enabling real-time verification of every step in the process. Automation plays a critical role in this ecosystem. Smart contracts enforce rules such as access timing and role-based permissions without human intervention. This minimizes the risk of errors or intentional breaches, ensuring that exam papers are only accessible to the right people at the right time.

It also reduces the administrative burden, allowing staff to focus on oversight rather than micromanagement. Equally important is how this shift affects stakeholder perception. Everyone involved can see that the process is fair and verifiable, which strengthens the credibility of the examination system as a whole. However, successful implementation requires more than just deploying the technology. A system is only as strong as its weakest link, and even the most advanced cryptographic protection can be undermined by poor practices or lack of awareness.

Ultimately, the integration of blockchain into exam paper distribution represents a significant leap forward. It offers a powerful blend of transparency, automation, and security—but it must be implemented thoughtfully, with attention to both technical robustness and human usability. Balancing these elements is key to building a system that not only works but earns the trust of everyone it serves.

VIII CONCLUSION

This final section synthesizes the insights gained from the system's design, implementation, and security analysis. It reaffirms the value of blockchain technology in securing exam processes and highlights how the proposed framework sets a new precedent for transparent, secure, and scalable academic operations. The conclusion also reflects on the system's adaptability and potential for future integration across broader educational workflows.

By layering encryption, enforcing time-locked access through smart contracts, and storing sensitive content off-chain in secure, decentralized environments, the system addresses many of the vulnerabilities that plague traditional exam workflows. It offers a scalable and auditable model that aligns with the evolving needs of digital education.

It introduces a new standard for fairness and integrity in academic operations. Automation reduces the risk of human error, consensus mechanisms prevent unilateral control, and verifiable logs foster trust among stakeholders.

The strength of the system ultimately depends on how well these human and operational factors are managed.

As education continues to digitize, blockchain-enabled exam systems are poised to become foundational to secure academic governance. They don't just protect data—they redefine how institutions build and maintain trust in a digital world.

IX FUTURE SCOPE

1. Integration with National Education Systems –

Collaborate with government bodies to implement blockchain-based exam security across schools, universities, and certification authorities.

2. **Enhanced Biometric Security** – Incorporate advanced biometric verification methods like iris scans or voice recognition for stronger multi-factor authentication.

3. **AI-Powered Anomaly Detection** – Use AI to monitor blockchain logs for unusual patterns, identifying security breaches in real-time.

4. **Decentralized Identity Management** – Implement decentralized identity solutions to enhance user privacy and secure authentication without relying on centralized databases.

5. **Cross-Institution Collaboration** – Develop a shared blockchain network for multiple educational institutions to securely manage exams and prevent leaks on a larger scale.

6. **Smart Grading and Certification** – Extend the system to include automated grading, certification issuance, and verification through smart contracts to reduce manual errors and fraud.

7. **Mobile and IoT Integration** – Enable secure mobile access and integrate with IoT devices like biometric scanners for a more seamless examination experience.

REFERENCE

[1]. Wen, H., Sun, S., Huang, T., & Xiao, D. (2024). An intrinsic integrity driven rating model for a sustainable reputation system. *Expert Systems with Applications*, 249, 123804.

[2]. A. Badr, L. Rafferty, Q. H. Mahmoud, K. Elgazzar and P. C. K. Hung, "A permissioned blockchain-based system for verification of academic records", *2019 10th IFIP International Conference on New Technologies Mobility and Security NTMS 2019 - Proceedings and Workshop*, pp. 1-5, 2019.

[3]. S. Guerreiro, J. F. Ferreira, T. Fonseca and M. Correia, "Integrating an academic management system with blockchain: A case study", *Blockchain: Research and Applications*, vol. 3, no. 4, pp. 1-10, 2022.

[4]. M. Turkanović, M. Hölbl, K. Košič, M. Heričko and A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform", *IEEE Access*, vol. 6, pp. 5112-5127, Jan. 2018.

[5]. Canessane, R. A., Srinivasan, N., Beuria, A., Singh, A., & Kumar, B. M. (2019, March). Decentralized applications using Ethereum blockchain. In 2019 fifth international conference on science technology engineering and mathematics (ICONSTEM) (Vol. 1, pp. 75-79). IEEE.

[6] V. Hegde, S. D and L. S, "Randomized Online Question Paper Generation through SQL query and JEE," 2019 International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 8, no. 8, pp.1438-1442.

[7] M. Imran, A. Uddin, F. Rafath, M. Osman, A. Sultana and K. Srikanth, "Real Time Application of Advanced Exam Paper Leakage Detection and Alert System with Theft Protection," 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI) (48184), Tirunelveli, India, 2020pp421-427.doi: 10.1109/ICOEI48184.2020.9142950

[8] P. Nalajala, P. Madhuri, M. Bhavana, B. Godavarthi, and G. Reddy, "RFID based security for exam paper leakage using electromagnetic lock system," 2019 International journal of pure and applied Mathematics, vol. 117, no. 20, pp.845-852.

[9] I. Nurhaida, D. Ramayanti and R. Riesaputra, "Digital signature & encryption implementation for increasing authentication, integrity, security and data non-repudiation," 2019 International Research Journal of Computer Science (IRJCS), vol. 4, no. 4, pp.4- 14.

[10] M. A. Sadikin and R. W. Wardhani, "Implementation of RSA 2048-bit and AES 256-bit with digital signature for secure electronic health record application," 2020 International Seminar on Intelligent Technology and Its Applications (ISITIA), Lombok, 2016, pp. 387-392, doi: 10.1109/ISITIA.2016.7828691.

[11] Canessane, R. A., Srinivasan, N., Beuria, A., Singh, A., & Kumar, B. M. (2019, March). Decentralised applications using ethereum blockchain. In 2019 fifth international conference on science technology engineering and mathematics (ICONSTEM) (Vol. 1, pp. 75-79). IEEE.

- [12] Wen, H., Sun, S., Huang, T., & Xiao, D. (2024). An intrinsic integritydriven rating model for a sustainable reputation system. *Expert Systems with Applications*, 249, 123804.
- [13] Tasic, I., & Cano, M. D. (2024). An orchestrated IoT-based blockchain system to foster innovation in agritech. *IET Collaborative Intelligent Manufacturing*, 6(2), e12109.
- [14] Alagheband, M. R., & Mashatan, A. (2022). Advanced encryption schemes in multi-tier heterogeneous internet of things: taxonomy, capabilities, and objectives. *The Journal of Supercomputing*, 78(17), 18777-18824.
- [15] Choudhury, S., Lenka, R. K., Barik, R. K., & Panda, N. C. (2019, July). Security Protocols in Internet of Things (IoT)-A Review. In *2019 International Conference on Intelligent Computing and Remote Sensing (ICICRS)* (pp. 1-6). IEEE.