International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 09 Sept. 2025, pp: 219-231 www.ijaem.net ISSN: 2395-5252

A Web-Based Lecture Delivery Modules and Students' Database Privacy using Strong Encryption Schemes and Blockchain Techniques for Tertiary Institutions in Kogi Central

Yunisa Sunday[1], Emmanuel Eturpa Salami[2], Ekundayo Onimisi Kayode[3], Yahaya Nurudeen Yusuf[4], Attah Joshua[5]

Department of Computer Science, Confluence University of Science and Technology, Osara
Department of Software Engineering, Confluence University of Science and Technology, Osara
Department of Computer Science, Confluence University of Science and Technology, Osara
Department of Computer Science, Confluence University of Science and Technology, Osara
Department of Computer Science, Confluence University of Science and Technology, Osara

Date of Submission: 05-09-2025 Date of Acceptance: 15-09-2025

ABSTRACT
This study develops and evaluates a secure web-based lecture delivery module designed for tertiary institutions in Kogi Central.The increasing concerns regarding unauthorized access, data breaches, and manipulation of academic records in conventional web-based platforms has become one of great concern. The system integrates students' academic database with strong encryption schemes and blockchain techniques to ensure data confidentiality, integrity, and accountability. The research adopt the Secure System Development Life Cycle (SSDLC) while a multi-layered architecture that comprises of three layers was used.The proposed framework combines a user-friendly interface for lecture delivery with a backend architecture that secures student information through encryption and blockchain-supported logging. Empirical testing was conducted to assess system performance, security resilience, and scalability under realistic workloads. The findings demonstrate that the integration of encryption and blockchain enhances trust, prevents tampering, and ensures robust access control. This work contributes to the development of secure educational technologies for data-sensitive environments and provides a model that can be extended across similar academic settings.
(Keywords: Encryption, Blockchain, Privacy,**)**

I. INTRODUCTION

According to Timothy Prewitt (2006) discuss extensively on history of distance learning, traditionally a peripheral university activity, is briefly traced. The advent, first of the British Open University with its renovated philosophy of distance learning, and then of the new information and communication technologies and their application to distance education, has led to a revalorization of open and distance education. These technologies are rapidly blurring the distinction between traditional higher education and distance learning. Various techniques of distance learning are described, particularly the electronic classroom and the electronic library. The advent of online learning has transformed the education landscape, offering unparallel flexibility and accessibility. However, this shift has also introduced significant security risks, particularly concerning students' personal data and intellectual property.

Ishara et al.,(2010) point out that, the Real Time Interactive Lecture Delivery System (RTILDS) project is motivated by the need to increase students' interaction with the lecturer in real time during a lecture. The completed system comprises of a website that maintains profiles of lecturers and lecture material (presentations, quizzes, student feedback, etc.). Online lecture delivery systems, which store and transmit sensitive information, have become prime targets

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 09 Sept. 2025, pp: 219-231 www.ijaem.net ISSN: 2395-5252

for cyber threats. Students' personal data, including names, addresses and financial information is vulnerable to unauthorized access, identity theft, and exploitation. Moreover, lecture modules and educational contents are valuable intellectual properties that require protection from theft, plagiarism, and unauthorized use. Student data privacy refers to the protection of personal and sensitive information collected, stored, and transmitted by educational institutions. This includes demographic data, academic records, login credentials, and other sensitive information. The increasing reliance on online lecture delivery systems has created new vulnerabilities, making student data more susceptible to cyber threats, data breaches, and unauthorized access.

Yoshiyasu Takefuji (2021) demonstrate how to build a resilient secured education system for online lectures against malicious attacks. Online lecture delivery has become an essential tool for educational institutions in Kogi Central which enable them to: Reach a broader audience, provide high-quality educational content, enhance student engagement and participation, offer personalized learning experiences. However, these systems also pose significant risks to student data privacy. Traditional security measures, such as firewalls and passwords, which are no longer sufficient to safeguard against sophisticated cyber threat, the need for robust security solutions has become paramount. Therefore, strong encryption algorithms offer a reliable means of protecting data in transit and at rest with the help of blockchain technology with its decentralized nature.

II. LITERATURE REVIEW

This research work by Cui et al (2023) presents a novel framework for classifying secret keys in symmetric encryption algorithms by applying deep transfer learning technique. It addresses the problem of security vulnerabilities which arise from side-channel attacks that exploit leaked electromagnetic signals from cryptographic devices. Traditional attacks depend on exhaustive key-guessing, which is computationally expensive. The method proposed by Cui et al (2023) uses a divide-and-conquer strategy, breaking down long encryption keys into semi-byte units and using a deep residual convolutional neural network for classification. Transfer learning optimizes model training and improves the efficiency; it also reduces the key search space while maintaining very high accuracy. The results show an attack accuracy of up to 91%, demonstrating the effectiveness of the framework in extracting encryption keys from leaked signals with limited data.Saket et al (2024) presents a novel symmetric key encryption algorithm based on the Extended Modified Substitution Algorithm method to improve data security. Saket et al (2024) proposed an algorithm that generates a random key matrix (256x256x2) and applies sequential randomization techniques such as, shifting, cycling and also character position-based encryption. The encryption process ensures high randomness, while conversely the decryption process effectively reverses these steps taken before. Results obtained by the researchers demonstrate the algorithm's efficiency, robustness against cryptographic attacks, and scalability across different forms of data, including text, images, and videos. The study shows the suitability of the algorithm for secure data transmission and storage.Jurayev et al (2025) introduces an algorithm for generating round keys in symmetric block encryption, aiming to improve security and randomness. The method proposed by Jurayev et al (2025) evaluates the degree of randomness using a key and an initialization vector, making sure it passes all 15 NIST statistical tests. The approach includes key expansion techniques like the S-box permutations, circular shifts, and XOR operations, commonly used in AES, DES, and GOST encryption standards. Results confirm that the generated keys show strong randomness and resistance to cryptanalysis, making the algorithm very suitable for secure cryptographic applications.Mondal et al (2024) explores the implementation of the RSA algorithm for encryption and decryption of text messages to enhance security in communication. It shows how RSA, an asymmetric encryption method, secures digital communication by using a public key for the encryption and a private key for the decryption. The researchers discuss the mathematical foundation of RSA, stating its reliance on large prime numbers for key generation, making it resistant to brute-force attacks. Examples demonstrate the encryption and decryption processes, showing RSA's effectiveness in safeguarding sensitive text messages. Mondal et al (2024) conclude by emphasizing the relevance of RSA in modern secure communication despite computational issues.Shankar (2022) introduces RSA+, a modified version of the RSA algorithm designed to improve security while maintaining its computational complexity. The newly proposed algorithm adds an additional layer of encryption by abstracting the encryption exponent, making decryption more difficult without knowing the private key. RSA+ is shown to be at least as secure

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 09 Sept. 2025, pp: 219-231 www.ijaem.net ISSN: 2395-5252

as RSA, with its security relying on the difficulty of factoring large numbers. Shankar (2022) also explores potential vulnerabilities, computational black boxes, and alternative cryptosystems related to RSA. Ibharalu et al (2024) presents an improved approach for accelerating RSA key generation by improving the process of finding large prime numbers. Since RSA encryption relies on generating large prime numbers, the proposed method by the researchers incorporates efficient prescreening techniques and Fermat's Little Theorem to reduce the computational complexity. The study shows that the new approach significantly lowers key generation time, achieving a 66.8% speed increase for 2048-bit keys compared to conventional methods. By refining the process of prime selection and testing, the researchers were able to enhances the overall efficiency of RSA cryptography, making it more practical for real-time applications.

Fundamentally, a distributed ledger maintaining immutability, transparency, and security by recording transactions across numerous nodes is what blockchain is. By using a peer-to-peer network instead of traditional centralized databases, blockchain lowers the danger of fraud, data manipulation, and illegal access while doing away with the need for middlemen. The technology uses smart contracts, consensus processes, and cryptographic hashing to improve the efficiency and trust of online transactions.An "Anonymous State Pinning" strategy is put out by Robinson and Brainard (2019) to improve the security of private blockchains by thwarting consortium member cooperation. The method preserves anonymity and privacy by "pinning" the state of a private blockchain to a public blockchain, like Ethereum. In contrast to current techniques, it stops transaction rate leakage and enables users to contest faulty pins without disclosing their identities. An estimated $508 is spent on pinning each year, according to the authors' formal security proof and cost analysis. In order to enhance scalability and lessen Ethereum MainNet congestion, they also present a hierarchical pinning architecture (Robinson & Brainard, 2019).

To improve security and trust in cloud environments, Pourmajidi et al. (2020) suggest Logchain, a blockchain-based system for immutable log storage. The technology ensures log integrity without depending on a single trusted party by integrating with both public (Ethereum) and private (IBM Blockchain) blockchains. By employing a hierarchical ledger topology, Logchain enhances scalability while lowering computing expenses and blockchain congestion. The study offers a thorough implementation, complete with IBM Blockchain and Ethereum smart contracts, as well as a cost and performance analysis. According to the findings, Logchain efficiently maintains log integrity while maximizing blockchain utilization (Pourmajidi et al., 2020). The challenges, approaches, and future trends of forensic analysis techniques for private blockchains in the public sector are examined by Feltovic (2025). Private blockchains improve access control and data protection in contrast to public blockchains, which complicates forensic investigations. Access control verification, block structure analysis, and cryptographic evidence analysis are important forensic techniques. In order to handle changing risks, the study highlights the necessity of improved legal frameworks, international cooperation, and AI integration. To guarantee blockchain integrity and transparency, future studies should concentrate on improving forensic instruments and legal frameworks (Feltovic, 2025). The relationship between private blockchains and deterministic databases is examined by Lai et al. (2023), who emphasize how these two systems share the concepts of replica consistency and deterministic transaction execution. In order to improve disk-oriented blockchain performance, the paper presents Harmony, a revolutionary deterministic concurrency control protocol. Blockchain throughput is greatly increased by harmony, which reduces transaction abort rates, enhances hotspot resilience, and permits inter-block parallelism. The authors demonstrate HarmonyBC's improved performance over current private blockchain designs by implementing a relational blockchain based on PostgreSQL. According to experimental findings, HarmonyBC outperforms state-of-the-art private blockchains in terms of throughput, achieving 2.0× to 3.5× higher throughput (Lai et al., 2023).

In order to increase the effectiveness of smart contracts in blockchain-based financial transactions, Ferrari et al. (2025) investigate optimization strategies. Key inefficiencies are identified in the study, including expensive gas expenses, latency, and security flaws. Gas optimization, Layer 2 solutions, and zero-knowledge proofs are suggested as remedies. Results show that customized smart contracts can minimize security concerns, increase transaction throughput, and cut gas expenses by up to 40%. The study emphasizes the necessity of balanced optimization tactics by highlighting the trade-offs between efficiency and security. These revelations

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 09 Sept. 2025, pp: 219-231 www.ijaem.net ISSN: 2395-5252

enhance financial blockchain applications' overall scalability, affordability, and dependability. Emma (2024) investigates how smart contracts and blockchain improve security and transparency in online transactions in a range of sectors. The study emphasizes how blockchain's decentralized and unchangeable characteristics lower fraud and boost confidence in industries like supply chains, legal services, healthcare, and finance. By automating contracts, smart contracts ensure real-time execution and do away with middlemen. In addition to discussing issues including interoperability, scalability, and regulatory problems, the paper suggests solutions like cross-chain protocols, Layer 2 scaling, and regulatory improvements. Blockchain integration with AI, IoT, and machine learning is a future trend that will improve automation and security.

A semantic interoperability framework for blockchain-based smart contract generation with Knowledge Graphs is proposed by Van Woensel and Seneviratne (2024). The study focuses on Health 3.0, where blockchain serves as a neutral middleman for decentralized healthcare data administration, ensuring safe and open decision-making. By combining knowledge Graph-based rules into smart contracts, a hybrid on-/off-chain strategy is presented, enhancing automation, effectiveness, and reliability. The model's accuracy and cost-effectiveness in blockchain implementation were demonstrated during testing in the processing of health insurance claims. For wider applications, the paper recommends more improvements utilizing Large Language Models (LLMs) and extended rule sets. A thorough analysis of security flaws in Ethereum blockchain smart contracts is given by Kushwaha et al. (2021), who point out important flaws that could result in monetary losses. The report divides vulnerabilities into three main categories: Ethereum Virtual Machine restrictions, Solidity programming errors, and Ethereum blockchain architecture faults. Alongside detecting technologies like Oyente, Mythril, and Securify, real-world attacks like the DAO hack and Parity Multisig wallet exploit are examined. Better smart contract coding techniques, more thorough security audits, and formal verification techniques are some of the preventive actions the authors suggest. The study highlights how urgently strong security mechanisms are needed to reduce vulnerabilities in decentralized apps built on Ethereum.

III. METHOD

The research adopt a hybrid method of Secure System Development Life Cycle (SSDLC) and design implementation evaluation approach. SSDLC was used that enable the integration of strong encryption and blockchain techniques in system design. To develop each phase of the system, Agile Methodology was used because it allows for iteration in the whole process of the design. The methodology was structured into four phases which are; System Design, System Integration, Implementation and Evaluation. A three layered architecture was used in the design of the system.

System Design

The system architecture was designed to combine a lecture delivery module with a secured student database. The lecture delivery interface included course uploads, live streaming, and recorded sessions. The student database stored academic records, authentication credentials, and attendance logs. While the Strong encryption algorithms were applied to protect data in storage and during transmission. Blockchain techniques were embedded to create immutable records of database transactions such as grade entries, attendance updates, and course registrations. This ensured traceability and eliminated the possibility of unauthorized alterations. A web-based prototype was developed using widely adopted programming frameworks. The encryption layer secured communication between client and server, while the blockchain ledger was deployed as a private permissioned chain to log academic transactions.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 09 Sept. 2025, pp: 219-231 www.ijaem.net ISSN: 2395-5252

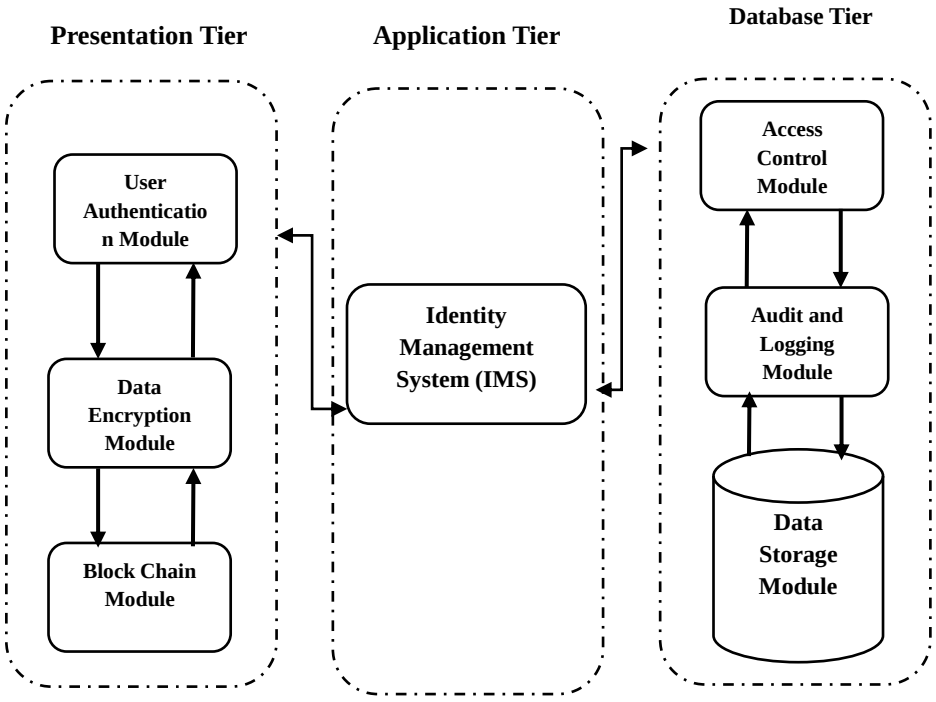

Figure 1: System Architecture for A Web-Based Lecture Delivery Modules and Students' Database Privacy using Strong Encryption Schemes and Blockchain

Architecture Components:

The User Authentication Module is responsible for authenticating users (students, faculty members, administrators), it utilizes strong encryption algorithms and integrates with Identity Management System. While the Data Encryption Module is responsible for encrypting sensitive data (student records, lecture modules), and it utilizes strong encryption algorithms integrates with Data Storage Module

The Data Storage Module is responsible for storing encrypted data, it utilizes secure storage solutions (e.g., encrypted databases, secure file systems) and integrates with Data Encryption Module. While the Blockchain Module is responsible for implementing blockchain-based security schemes and utilizes blockchain platforms (e.g., Hyperledger, Ethereum) as well as integrates with Data Encryption Module and Data Storage Module. The Access Control Module is responsible for controlling access to sensitive data, it utilizes role-based access control (RBAC) and attribute-based access control (ABAC) and it Integrates with User Authentication Module Data Encryption Module. The Audit and Logging Module is responsible for logging and auditing all system activities and it utilizes secure logging mechanisms (e.g., encrypted logs, secure log storage) as well as integrates with all modules. The Identity Management System (IMS) is responsible for managing user identities and access credentials which integrates with User Authentication Module.

Data Flow Diagram:

Figure 2 shows the how data flows withing the system from the point users interacts with the system to the point where audit control module keeps track of the entire actions of users.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 09 Sept. 2025, pp: 219-231 www.ijaem.net ISSN: 2395-5252

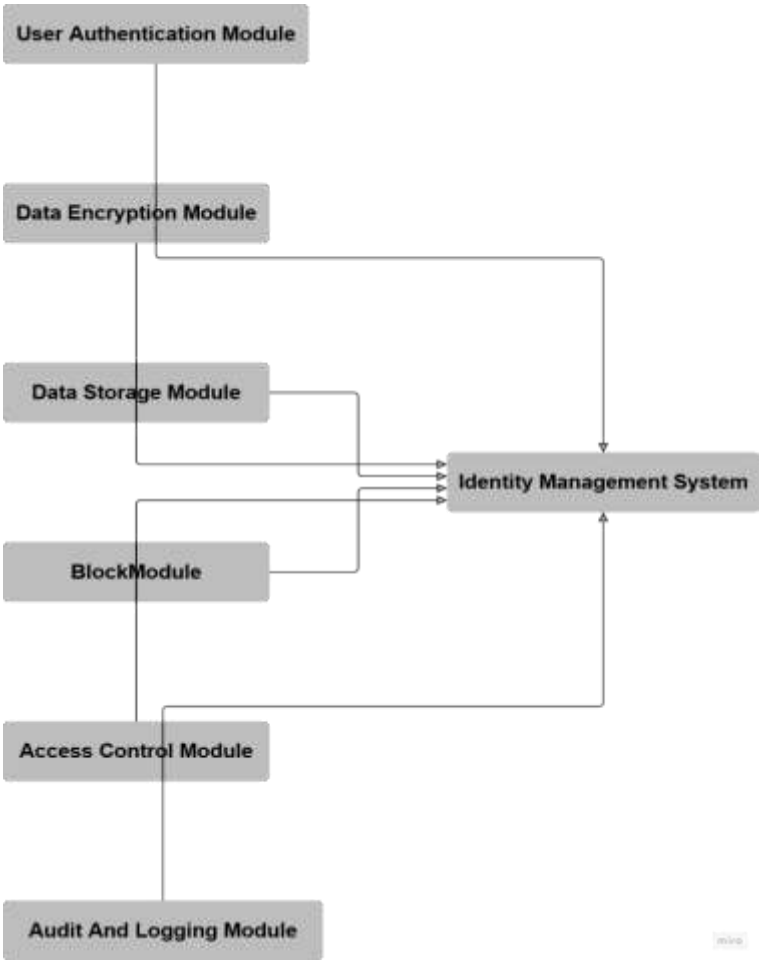

Figure 2: Data Flow Diagram Web-Based Lecture Delivery Modules and Students' Database Privacy using Strong Encryption Schemes and Blockchain

Sequence Diagram:

The sequence diagram of the Web-Based Lecture Delivery Modules and Students' Database Privacy using Strong Encryption Schemes and Blockchain show the various sections that makes us the entire system as shown in figure 3.

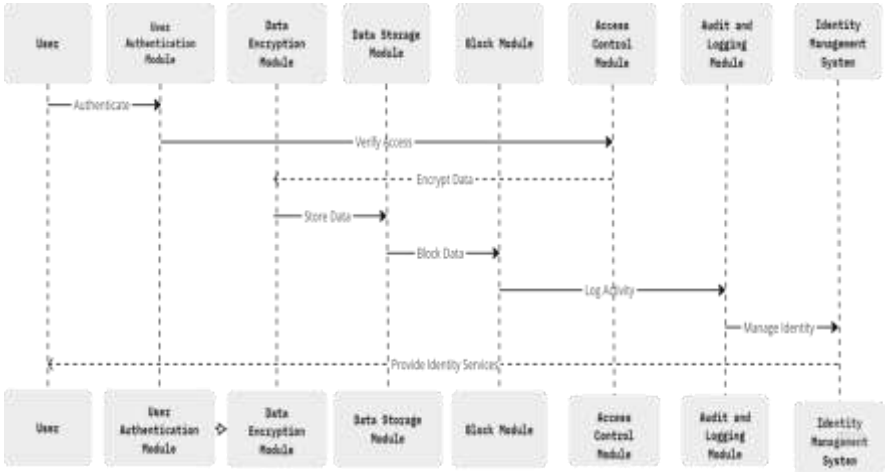

Figure 3: Sequence Diagram of Web-Based Lecture Delivery Modules and Students' Database Privacy using Strong Encryption Schemes and Blockchain

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 09 Sept. 2025, pp: 219-231 www.ijaem.net ISSN: 2395-5252

RBAC Matrix

Table 1: Summary of the Role Base Access Control Matric

Action	Student	Lecturer	Dept Admin	Registry	Auditor	SysAdmin
View own courses/lectures	✔	✔	✔	✔	✖	✔
Upload lecture	✖	✔	✔	✖	✖	✔
Grade submissions	✖	✔	✔	✖	✖	✔
Finalize grades (step-up)	✖	✔	✔	✔	✖	✔
Issue transcript	✖	✖	✖	✔	✖	✔
View audit trails	✖	✖	✖	✔	✔	✔

IV. RESULTS

System Integration and Implementation:

Integration and Implement of the system was done using tools such as Apache JMeter and Wireshark were used for load testing and traffic inspection.Performance and security tests were conducted using simulated workloads with varying numbers of concurrent users. Performance metrics included encryption/decryption time, transaction throughput, latency, and storage overhead. Security tests focused on resilience against tampering, replay attacks, and unauthorized access.

The performance evaluation showed that the system maintained acceptable response times under increasing user load. Encryption and decryption times averaged within milliseconds, with minimal impact on system throughput. The blockchain ledger recorded all database operations without significant delays, and storage overhead remained within manageable limits.Security testing confirmed the system's resistance to unauthorized access and tampering. Replay attack attempts were blocked by the system's authentication and transaction timestamping mechanisms. Unauthorized access tests demonstrated that encrypted records could not be read or altered without valid credentials.Scalability tests revealed that the system was able to handle concurrent user sessions effectively, maintaining stable performance up to the tested thresholds.

Table 1. System Performance Results

Concurrent Users	Avg. Encryption Time (ms)	Avg. Decryption Time (ms)	Throughput (transactions/sec)	Latency (ms)	Storage Overhead (MB)
50	2	2	500	120	5
100	3	3	480	135	10
200	4	4	460	150	18
400	5	6	430	180	35
800	7	8	400	220	60

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 09 Sept. 2025, pp: 219-231 www.ijaem.net ISSN: 2395-5252

Table 1 provides summarizes of the performance results obtained under varying numbers of concurrent users. The evaluation focused on four key metrics: encryption/decryption time, system throughput, latency, and blockchain storage overhead.

Encryption and Decryption Time.

The encryption and decryption times increased gradually as the number of concurrent users grew as shown in the graph in Figure 4. At 800 concurrent users, encryption time averaged 7 ms, and decryption time averaged 8 ms. This indicates that the cryptographic scheme scales reasonably well under high load conditions without introducing significant delays.

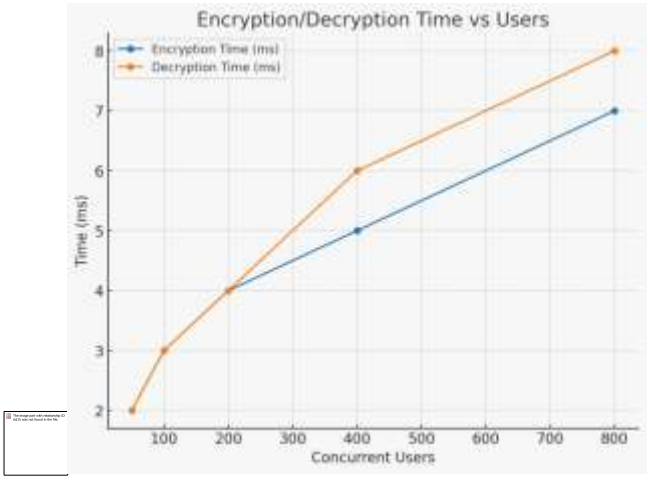

Figure 4. Encryption/Decryption Time vs. Users

System Throughput.

Figure 5 shows that throughput decreased slightly as user numbers increased, dropping from 500 transactions per second at 50 users to 400 transactions per second at 800 users. Despite this decline, the system maintained acceptable throughput levels even under heavy loads, confirming its scalability.

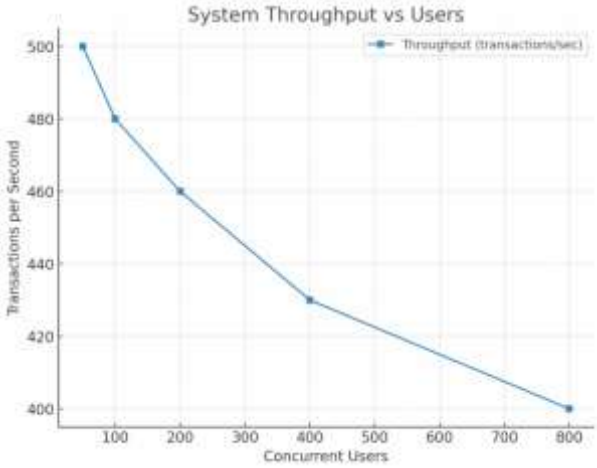

Figure 5: System Throughput vs Users

System Latency.

The Latency values increased steadily as concurrent users scaled up as shown in Figure 6 from 120 ms at 50 users, latency rose to 220 ms at 800 users. Although the increase is expected in multi-user environments, latency remained within acceptable thresholds for web-based educational applications.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 09 Sept. 2025, pp: 219-231 www.ijaem.net ISSN: 2395-5252

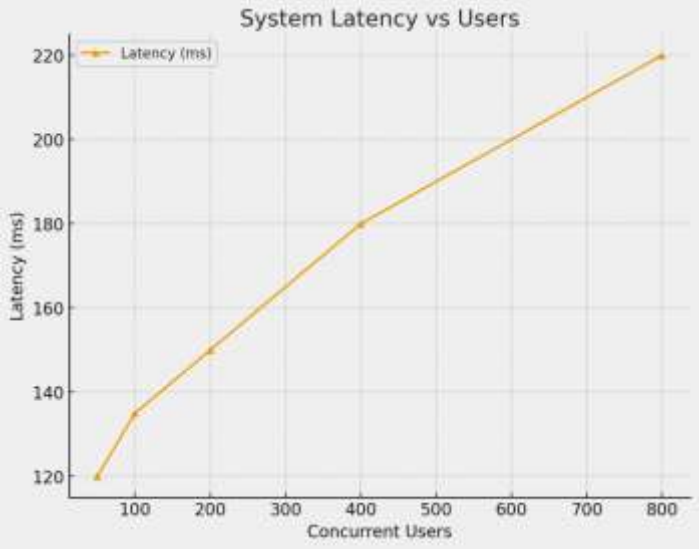

Figure 6: System Latency vs Users

Storage Overhead.

The Blockchain integration introduced storage overhead due to the immutable recording of academic transactions as shown in the graph in Figure 7. Storage requirements grew from 5 MB at 50 users to 60 MB at 800 users. While overhead increases with usage, the results demonstrate that the blockchain-based logging mechanism remains manageable in academic settings.

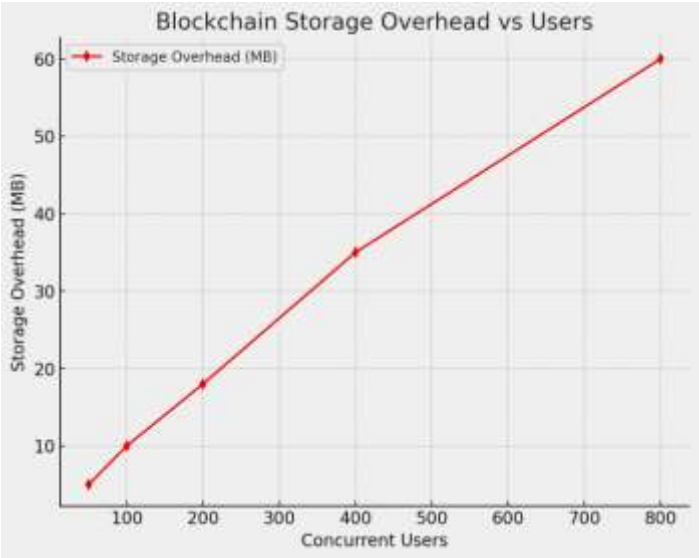

Figure 7: Blockchain Storage Overhead vs Users

V. DISCUSSION

The results indicate that combining strong encryption with blockchain techniques significantly enhances the security and trustworthiness of web-based educational systems. Encryption ensures that sensitive student records remain confidential, while blockchain provides accountability through immutable logging of academic activities. Unlike conventional systems where data tampering or unauthorized changes may go unnoticed, the blockchain ledger guarantees transparency and verifiability.The modest overhead introduced by encryption and blockchain integration did not compromise the system's usability, making it suitable for deployment in resource-constrained academic environments such as those in Kogi Central. Furthermore, the user-friendly design of the lecture delivery module ensures accessibility

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 09 Sept. 2025, pp: 219-231 www.ijaem.net ISSN: 2395-5252

for both staff and students, aligning with the growing demand for digital learning platforms.This study demonstrates that secure, scalable, and transparent digital infrastructures can be successfully adopted in tertiary institutions to address data privacy concerns. Future extensions could focus on interoperability with national education data platforms and the integration of adaptive learning features to further enhance the digital learning ecosystem.

Proposed Framework

The proposed framework integrates a user-friendly lecture delivery interface with a secure backend architecture that protects student data through encryption and blockchain supported logging. The design is structured into four main layers, as shown in Figure 8 (conceptual illustration to be inserted).Presentation Layer (User Interface) which provides an intuitive web-based platform for both students and lecturers as well as enables access to lectures, course materials, assignments, and discussion forums. The design emphasizes simplicity, responsiveness, and accessibility to ensure that students and staff can use the system with minimal technical challenges. Application Layer (Lecture and Student Services) that manages core educational services such as; Lecture Management(uploading, streaming, and storing lectures),Assessment Management (assignments, quizzes, and grading.) and Student Records(enrollment, attendance, and academic history.).These services operate under a role-based access system to ensure that users can only perform actions appropriate to their roles (e.g., student, lecturer, administrator).Security Layer (Encryption and Privacy Control)which ensures the confidentiality and integrity of student data. All sensitive information, such as academic records and grades, is encrypted during storage and transmission. Authentication mechanisms, such as strong passwords and optional multi-factor authentication, provide controlled access. This layer also enforces data minimization, ensuring that only necessary information is collected and processed.Blockchain Logging Layer (Integrity and Accountability)that strengthen trust, a private permissioned blockchain is integrated for logging academic transactions such as grade entries, attendance updates, and transcript requests. Each action is recorded as an immutable log entry, preventing tampering and ensuring transparency. Rather than storing full personal details on the blockchain, only hashed references of transactions are recorded, guaranteeing both integrity and privacy.

Key Features of the Framework

User-Friendly Design: Easy navigation and mobile compatibility for accessibility.

Confidentiality: Strong encryption schemes secure student records and communication.

Integrity: Blockchain provides tamper-proof logs of academic activities.

Scalability: The modular design allows the system to support large numbers of users typical of tertiary institutions.

Accountability: Immutable records enable reliable auditing of institutional processes.

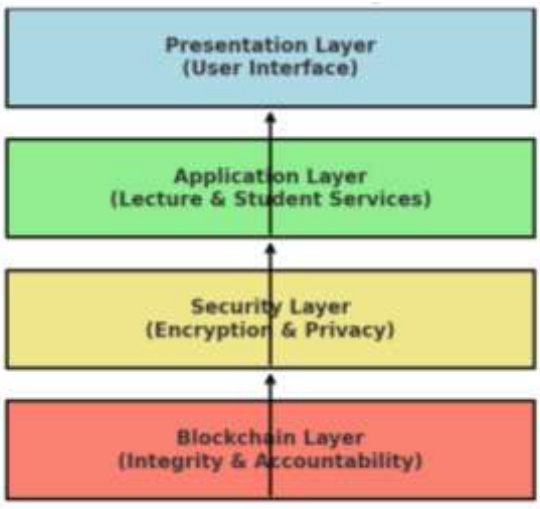

Figure 8: Proposed Framework for Web-Based Lecture Delivery Modules and Students' Database Privacy using Strong Encryption Schemes and Blockchain

The framework demonstrates how educational technology can be designed to combine usability with robust data protection. By integrating encryption and blockchain, the system ensures privacy, integrity, and accountability in managing student data while maintaining a seamless lecture delivery experience. This model provides a practical solution for tertiary institutions in Kogi Central and similar educational contexts.

VI. CONCLUSION

In conclusion, this research successfully designed, implemented, and evaluated a secure and scalable web-based lecture delivery system that integrates strong encryption and blockchain technology. The system directly addresses pressing concerns of data privacy, integrity, and trust in tertiary institutions and offers a sustainable model for secure digital learning in Nigeria and beyond. However, there is the need to conduct a comparative evaluation of different blockchain platforms and their impact in educational contexts. Cost-benefit analysis of implementing privacy-preserving academic systems in low-resource institutions and investigation of student perceptions of trust, adoption, and acceptance of blockchain-backed lecture systems. How all of these innovations can be effectively and efficiently adopted in learning.

VII. ACKNOWLEDGEMENT

I acknowledge the support provided by the Tertiary Education Trust Fund (TETFUND) through the Institutional Based Research (IBR) Grant with the reference number CUSTECH/DRID/ADMIN/IBR/TETF/ VOL .2.15 that was given in carrying out the entire research work. Also, my appreciation goes to the Management team of Confluence University of Science and Technology Osara, Kogi State as well as the office of the Directorate of Research, Innovation and Development (DRID) for facilitating the process and approval of the fund disbursed in conducting this research work.

REFERENCES:

[1]. Timothy Prewitt (2006). The Development of Distance Learning Delivery Systems, High Education in Europe, The Development of Distance Learning Delivery Systems: Higher Education in Europe: Vol 23, No 2 (tandfonline.com)

[2]. W Ishara Udeshika Cooray; D M Pathmasiri Abhayawickrama; G Ragel Roshan (2010). Real time interactive lecture delivery system, Real time interactive lecture delivery system | IEEE Conference Publication | IEEE Xplore

[3]. Yoshiyasu Takefuji (2021). Resilient Secured Education System for Online Lectures During the Pandemic, Resilient Secured Education System for Online Lectures During the Pandemic: Journal of Applied Security Research: Vol 17, No 4 (tandfonline.com)

[4]. Liang Xue, Renxuan Fu, Dan Lin, Kailan Kuok, Chufeng Huang, Junyu Su and Wei Hong (2021). Exploring the Innovative Blockchain-Based Application of Online Learning System in University, Exploring the Innovative Blockchain-Based Application of Online Learning System in University | SpringerLink

[5]. Ali Ikhwan[1,2], Rafikha Aliana A. Raof[1], Phaklen Ehkan[1], Yasmin Yacob[1] and M. Syaifuddin[3],(2020). Data Security Implementation using Data Encryption Standard Method for Student Values at the Faculty of Medicine, University of North Sumatra.Published under license by IOP Publishing Ltd, Journal of Physics: Conference Series, 5th International Conference on electronic design. Volume 1755,DOI: 10.1088/1742-6596/1755/1/012022,

[6]. Almogren, A., Mohiuddin, I., Din, I. U., AlMajed, H., & Guizani, N. (2020). FTM-IoMT: Fuzzy-based Trust Management for Preventing Sybil Attacks in Internet of Things. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2020.3027440

[7]. Alfa, Abraham Ayegba., Alhassan, J. K., Olaniyi, O. M., & Olalere, M. (2021). Blockchain technology in IoT systems: current trends, methodology, problems, applications, and future directions. Journal of Reliable Intelligent Environments, 7(2), 115–143. https://doi.org/10.1007/s40860-020-00116-z

[8]. B. Al Samarai (2023).Use Of Blockchain Technology In Educational International Journal on "Technical and Physical Problems of Engineering" (IJTPE)Published by International OrganizationSSN 2077-3528,IJTPE Journalwww.iotpe.comijtpe@iotpe.com, Issue 57, Volume 15, Number4, page 140-151

[9]. R. Kirubakaramoorthi, D. Arivazhagan and D. Helen(2015). Survey on Encryption Techniques used to Secure Cloud Storage System, Indian Journal of Science and Technology, Vol 8(36), DOI: 10.17485/ijst/2015/v8i36/87861 ISSN (Print) : 0974-6846 ISSN (Online) : 0974-5645

[10]. L. Arockiam1 , S. Monikandan (2013)Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm. International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, ISSN (Print) : 2319-5940 ISSN (Online) : 2278-1021

[11]. Anna McFadden, Barrie Jo Price (2000) An Overview of Online Educational Delivery Applications. Society for Information Technology & Teacher Education International Conference, 2000 ISBN 978-1-880094-37-2

[12]. Rajkumar Kannan and Frederic Andres (2010), Towards automated lecture capture, navigation and delivery system for web lecture on demand, International Journal of Innovation in EducationVol. 1, No. 2 pp 204-212 https://doi.org/10.1504/IJIIE.2010.03686

[13]. Yunisa Sunday, Yahaya Yusuf, and Abdulkadir Naafisat (2024), A web-based expert System for Online medical diagnoses. Interntional organisation of Scientific research (IOSR JOURNALS)

[14]. Chris Obrien. Richard and Luann (2011)A Comparison of Large Lecture, Fully Online, and Hybrid Sections of Introduction to Special Education,Volume 30, Issue 4https://doi.org/10.1177/875687051103000404

[15]. Ouariach, F. Z., Nejjari, A., & Khaldi, M. (2023). Communication tools and e-learning: A revolution in the research methodology of communication for a pedagogical scenario. RA Journal of Applied Research, 9(4), 170-177. https://doi.org/10.47191/rajar/v9i4.03

[16]. Ouariach, F. Z., Nejjari, A., & Khaldi, M. (2024). Communication tools between learning activities and e-learning. In M. Khaldi et al. (Eds.), Proceedings of the E-Learning and Smart Engineering Systems (ELSES 2023) (pp. 453-459). Atlantis Highlights in Social Sciences, Education and Humanities. https://doi.org/10.2991/978-94-6463-360-3_42

[17]. Kesiena, E., Nwobodo-Nzeribe, H., & Chibueze, K. (2024). Advancements in e-learning: Design and implementation of a virtual classroom and text-based environment. Exploremetics Journal, 5(2), 10-20. https://doi.org/10.5281/zenodo.13382442

[18]. Enakrire, R. T. (2024). The usefulness of computer skills for enhanced teaching and learning among lecturers in an open-distance e-learning (ODEL) environment. Education and Information Technologies, 29, 16597–16612. https://doi.org/10.1007/s10639-024-12519-z

[19]. Biswas, K., Sridharan, B., & Chowdhury, M. J. M. (2023). Impacts of integration of learning activities with video modules in asynchronous learning. Proceedings of AAEE 2023, Griffith University, Gold Coast, Qld, Australia. Retrieved from https://www.researchgate.net/publication/376686475

[20]. Hallie, F., Jose, H., James, A., & Eric, T. (2024). Enhancing student engagement in mathematics through online problem-based learning. International Journal on Studies in Education, 6(1), 51-66. https://doi.org/10.46328/ijonse.175

[21]. Turyamureeba, S. (2024). Blended learning in higher education: Models and effectiveness. Eurasian Experiment Journal of Arts and Management, 5(3), 5-10. https://www.researchgate.net/publication/383544478

[22]. Siriwardena, B. P., Abeywickrama, L. M., Sandika, A. L., & Vidanapathirana, N. P. (2024). Exposing the Technological Acceptance Model in Blended Learning for Undergraduate Agricultural Entrepreneurs. Journal of the University of Ruhuna, 12(2), 70-92. https://doi.org/10.4038/jur.v12i2.8043

[23]. Jailani, N., Rosli, R., & Mahmud, M. S. (2025). Factors influencing mathematics teachers' blended learning: A systematic review. International Journal of Learning, Teaching and Educational Research, 24(1), 397-419. https://doi.org/10.26803/ijlter.24.1.20

[24]. Tanjung, Y. I., Festiyed, F., Diliarosta, S., Asrizal, A., Arsih, F., & Fadillah, M. A. (2025). Developing the Physics Learning Management System (PLMS) to support blended learning models. International Journal of Information and Education Technology, 15(1), 18-29. https://doi.org/10.18178/ijiet.2025.15.1.2214

[25]. Jamali, N., Uzma, U., & Dahraj, M. A. (2025). Assessing and analyzing significant differences among junior elementary school teachers' readiness and responsiveness towards blended learning. International Journal of Social Sciences and Business, 3(2), 115-125. https://doi.org/10.5281/zenodo.14835667

[26]. Liu, P., Li, M., Zhang, F., & Li, H. (2025). The effect of blended learning on the English students' course performance. Journal of English Language Teaching and Applied Linguistics, 15(1), 19-35. https://doi.org/10.32996/jeltal.2025.7.1.3