Education & Science Journal of Policy Review and Curriculum Development
p-ISSN: 2315-8425 | e-ISSN: 2354-1660
ESJPRCD
May, 2026
Vol. 13, No. 1

Design and Implementation of an Encrypted Database System for Secure Data Storage

[1]Sideeqoh Oluwaseun Shosanya, [2]Olayinka Olufunmilayo Olusanya, [3]Ademola Abiodun Omilabu, & [4]Babatunde Michael Alamu

[1,2,3,4]Department of Computer Science, Tai Solarin Federal University of Education, Ijagun, Ogun State, Nigeria

Article DOI:
10.48028/iiprds/esjprcd.v13.i1.19

Keywords:
Encryption, Database System, AES, Decryption, Design

Abstract

In an era of rising cyber threats and data breaches, ensuring the security and confidentiality of sensitive data has become a top priority for organizations. This study presents the design and implementation of an encrypted database system that uses the Advanced Encryption Standard (AES) for secure data storage and retrieval. The system was developed using a developmental research methodology and evaluated through statistical analysis involving information technology (IT) professionals and final-year computer science students. Results indicate that encryption significantly enhances data confidentiality, with strong positive correlations among user awareness, perception, and trust in the system. The system-maintained usability and efficiency while preventing unauthorized access, highlighting its effectiveness. This study contributes to the field by offering a practical solution that balances encryption strength with performance and usability, paving the way for further research into hybrid models and user-friendly security interfaces.

Corresponding Author:
Sideeqoh Oluwaseun Shosanya

Background to the Study

As reliance on data-driven technologies grows, protecting sensitive information has become a major concern for organizations and governments. Although traditional database systems are optimized for efficiency and scalability, they often offer limited native support for advanced security mechanisms, leaving stored data vulnerable to a range of cyber threats (Koppenwallner & Schikuta, 2023). The shift toward cloud and distributed environments has further intensified these security challenges. As data is increasingly stored and accessed over the internet rather than on local infrastructure, the risk of unauthorized access and data compromise has grown significantly. This expanded attack surface threatens the confidentiality and integrity of critical information, making strict access control and protective measures essential (Abbas et al., 2020). However, conventional security approaches, such as authentication and role-based access control, are no longer sufficient in the face of evolving attack techniques (Zhou et al., 2019).

Encryption has therefore become a key strategy for securing sensitive database content. By converting plaintext into ciphertext, encryption ensures that stolen or intercepted data remains unreadable without proper authorization. Nonetheless, deploying encryption within database systems introduces challenges related to key management, system performance, and query execution on encrypted data (Yousuf et al., 2021). Existing solutions like Transparent Data Encryption offer basic protection but often lack flexibility, while application-level encryption increases system complexity (Chandramouli & Pinhas, 2020). Effective data security relies on maintaining confidentiality, preventing unauthorized modification of data, and ensuring system availability under adverse conditions. These objectives, including confidentiality, integrity, and availability, form the CIA triad, which serves as the foundation of secure information systems. Meeting these requirements has driven increased interest in database-level encryption techniques (Naguib & Fouad, 2024).

To address modern security demands, encrypted database systems integrate cryptographic algorithms such as AES, RSA, and ECC directly into data storage and processing. Advanced methods, including order-preserving and homomorphic encryption, enable limited computations on encrypted data without decryption, balancing security with functionality. Practical systems like CryptDB and Cipherbase demonstrate that secure query processing over encrypted databases is achievable with acceptable performance overhead, highlighting the need for solutions that effectively balance security, usability, and efficiency (Yousuf et al., 2021).

Empirical Literature

Recent research highlights the effectiveness of encrypted database systems in enhancing data security while maintaining practical performance. Yousuf *et al.* (2021) showed that CryptDB allows secure SQL queries on encrypted MySQL databases with manageable performance overheads. Ali et al. (2018) confirmed that Transparent Data Encryption minimally impacts read operations and introduces moderate overhead for write-heavy workloads, supporting full-database encryption in enterprise settings.

Zhou *et al*. (2019) emphasized that selecting encryption schemes requires balancing security and efficiency, while Hasan *et al.* (2020) demonstrated that AES-based NoSQL databases provide strong protection with acceptable performance in small to medium-scale applications. Okoro and Olatunji (2021) reported that encrypting health records improves data integrity, prevents unauthorized access, and enhances user trust. Singh and Kaur (2019) found that hybrid encryption models can balance the speed of symmetric techniques with the stronger security of asymmetric methods. Finally, Wang *et al.* (2021) showed that cloud-based encrypted SQL and NoSQL systems can handle transactional, analytical, and mixed workloads securely when configured with AES-256 and field-level encryption, demonstrating practical deployment in real-world enterprise applications.

Ahmed (2025) examined the use of encrypted databases in three major Nigerian financial institutions using interviews, policy reviews, and penetration testing. They found that Transparent Data Encryption was widely adopted for regulatory compliance and data-at-rest protection, while field-level encryption was used selectively for highly sensitive data due to performance considerations. The study highlights practical trade-offs between security, efficiency, and compliance, offering valuable insights for encrypted database system design. Ajayi and Adebayo (2022) conducted a quasi-experimental study at a Nigerian public university, comparing an unencrypted student information system with an AES-secured version over six months. Their findings showed that AES significantly improved data confidentiality and integrity without major performance drawbacks, emphasizing the importance of integrating encryption early in system design. The study is relevant to this research as it demonstrates practical, sector-specific encryption implementation and highlights the need to align security measures with system architecture and user needs.

Previous studies show that although encryption strengthens data security, it often introduces operational complexity, particularly affecting query performance, system design, and user training, with a greater impact in data-intensive sectors such as education and finance. While advanced methods like searchable and homomorphic encryption remain limited by performance and scalability issues, the literature confirms that encrypted databases enhance protection and regulatory compliance but must balance security with usability and efficiency. These findings guide the current study by emphasizing the need for a holistic encryption design that addresses key management, query optimization, and practical deployment in real-world environments.

Materials and Method

Research Design

This study employs a developmental research design, which is well-suited for the creation and evaluation of technological systems such as secure databases. Developmental research focuses on the systematic design, development, and evaluation of instructional and technological innovations, making it ideal for engineering secure systems that meet specific objectives. The research follows a quantitative-empirical approach within the developmental framework to evaluate system performance and security. It includes building a prototype encrypted

database system, applying encryption techniques (such as AES), and measuring the impact on performance (e.g., query time, storage usage) compared to an unencrypted baseline system.

The design incorporates the following phases:

i. Requirements Analysis – Gathering system and security needs
ii. System Design – Creating architectural and data flow diagrams.
iii. System Development – Implementing encryption mechanisms in a functional database.
iv. Testing & Evaluation – Using quantitative measures to assess security, functionality, and performance.

This structured approach allows for the rigorous evaluation of both the theoretical and practical implications of encryption on database systems, ensuring that the final product meets security objectives while remaining efficient and usable.

Area of Study/Population

The area of study for this research is database security within the field of computer science and information systems, with a specific focus on the implementation of encryption techniques in relational database management systems (RDBMS). This research addresses the growing need to protect sensitive data stored in databases from unauthorized access, data breaches, and cyber-attacks, especially in environments such as healthcare, finance, and education, where data confidentiality is critical. The target population for the evaluation phase of the study includes IT professionals, database administrators, and software developers, who are the primary users and maintainers of secure data systems. Their input, experience, and feedback are essential in assessing the functionality, usability, and practicality of the implemented encrypted database system. Additionally, simulated datasets reflecting real-world scenarios (e.g., student records, patient information, and financial transactions) are used during testing to mirror the kind of sensitive data typically stored in organizational databases.

Participant/Subject

Since this study is theoretical in nature and does not involve a practical or live user evaluation, the concept of participants or human subjects is discussed in the context of intended users and target stakeholders. These include individuals or groups who would benefit from or interact with an encrypted database system in real-world applications. The primary focus is on: i. Database administrators (DBAs): Responsible for managing and securing databases within organizations. ii. Software developers: Particularly those who build applications that interact with sensitive data stored in databases. iii. Cyber security professionals: Who design and audit secure systems to ensure compliance with data protection regulations. iv. Academic researchers and students: Interested in understanding the theoretical and technical foundations of database encryption. Though no direct interaction with these users occurs in the course of this study, their roles and requirements help shape the system design and inform decisions about encryption mechanisms, usability, and performance trade-offs.

Instrument for Data Collection

The primary instrument used for data collection in this study is a structured questionnaire. The questionnaire was designed to gather detailed responses from participants regarding their knowledge, attitudes, perceptions, and technical evaluations related to the design and implementation of an encrypted database system. It consists of both closed-ended questions using a five-point Likert scale (ranging from "Strongly Disagree" to "Strongly Agree") and multiple-choice questions to capture both qualitative and quantitative data. The questionnaire was divided into sections to address specific research objectives: general knowledge and perception of encryption technologies, technical evaluation of encrypted database systems, and usability and user satisfaction with encryption-enabled systems. This structure ensures comprehensive coverage of both user-centered and technical factors influencing the use of encryption in database environments. Furthermore, the structured nature of the questionnaire facilitates consistency in data collection and improves the reliability of the study outcomes.

Methods of Data Collection

The data for this study were collected via a survey, specifically through the administration of structured questionnaires to selected respondents. This method was chosen due to its efficiency in reaching a broader sample, ensuring anonymity, and allowing respondents adequate time to consider and provide thoughtful answers. The questionnaires were distributed both in person and electronically to ensure broad accessibility and participation. This method facilitated the collection of both quantitative and qualitative data, as the questionnaire incorporated closed-ended items (using a 5-point Likert scale) for statistical analysis, and optional open-ended questions for participants to express opinions, concerns, or suggestions freely. This approach aligns with the mixed-method strategy, helping to triangulate data for greater validity. The use of surveys in technology-related research is well-established for its capacity to measure attitudes, perceptions, and experiences in a structured and scalable way. It allows researchers to systematically investigate patterns, test hypotheses, and make generalizations from the responses collected.

Population and Sample

To effectively assess the functionality, usability, and security features of the designed encrypted database system, a questionnaire was developed and distributed to a targeted group of respondents. A total of 110 individuals participated in the study. The sample population consisted of IT professionals, database administrators, and final-year computer science students, all of whom possess foundational knowledge of database management and information security principles. The purposive sampling technique was employed to ensure that the selected respondents had relevant expertise and experience to provide meaningful feedback on the system. Their insights were critical in evaluating the practical applicability, user interface, and security performance of the implemented solution.

Instrumentation and Administration

The primary instrument for data collection was a structured questionnaire designed to capture both quantitative and qualitative responses. The questionnaire included sections on

system usability, encryption effectiveness, data integrity, and overall user satisfaction. The questionnaire was administered through both online forms and physical distribution, depending on the availability and preference of the respondents. Before distribution, the purpose of the research was clearly explained, and informed consent was obtained. Respondents were assured of the confidentiality of their responses and their voluntary participation.

Statistical Analysis

The data collected from the structured questionnaires were analyzed using descriptive and inferential statistical techniques. Descriptive statistics such as frequencies, percentages, mean scores, and standard deviations were employed to summarize respondents' demographic profiles and general responses regarding their knowledge, attitudes, and perceptions of encrypted database systems.

To test the research hypotheses and determine relationships between variables such as user experience, system usability, and the effectiveness of the encryption implementation, inferential statistics were applied. Techniques such as Chi-square tests, t-tests, and Analysis of Variance (ANOVA) were used to examine differences among groups, while correlation and regression analysis were applied to measure the strength and direction of relationships between variables. The Statistical Package for the Social Sciences (SPSS) software was used to facilitate accurate computation and analysis of the data. This tool ensures reliability and efficiency in processing large datasets and generating meaningful insights that support decision-making in information systems research.

Results and Discussion

Respondents Demographic Information

Table 1: Gender Distribution of Respondents

Gender	Frequency	Percentage (%)
Male	65	59.1%
Female	45	40.9%
Total	110	100%

Table 1 showed that out of 110 respondents, 65 (59.1%) were male and 45 (40.9%) were female. This shows that most of the participants were male.

Table 2: Age Range of Respondents

Age Range	Frequency	Percentage (%)
18-25 years	37	33.6%
26-35 years	45	40.9%
36-45 years	18	16.4%
46 and above	10	9.1%
Total	110	100%

Table 2 showed that Most respondents, 45 (40.9%), were between 26 and 35 years.

Descriptive Analysis of Questionnaire Responses

The analysis below is based on data collected from 110 respondents using a structured questionnaire divided into three key sections: Awareness, Perception, and Effectiveness of Encrypted Database Systems. Responses were measured on a 4-point Likert scale: Strongly Agree (SA), Agree (A), Disagree (D), and Strongly Disagree (SD).

Table 3: Awareness of Database Encryption

Statement	SA	A	D	SD	Total Agree (%)
1. I am aware of database encryption.	50	47	10	3	97 (88.2%)
2. I understand the purpose of encryption.	48	47	9	6	95 (86.4%)
3. I know AES is a type of encryption.	40	42	18	10	82 (74.5%)

Table 3 indicates that a large proportion of respondents (over 88%) indicated awareness and basic understanding of database encryption. However, knowledge of specific encryption algorithms like AES was slightly lower (about 75%).

Table 4: Perception of Encryption's Usefulness

Statement	SA	A	D	SD	Total Agree (%)
1. Encryption improves data confidentiality.	55	37	12	6	92 (83.6%)
2. Encrypted databases are harder to hack.	52	36	14	8	88 (80%)
3. Encryption reduces insider threats.	46	38	18	8	84 (76.4%)

Table 4 showed that respondents had a positive perception of encryption's effectiveness, with more than 80% agreeing it improves confidentiality and prevents hacking.

Table 5: Trust and Effectiveness of Encrypted Databases

Statement	SA	A	D	SD	Total Agree (%)
1. I trust encrypted databases more than unencrypted ones.	49	43	10	8	92 (83.6%)
2. Encryption should be mandatory for sensitive data.	48	40	7	15	88 (80.0%)
3. I would feel safer using a system with encryption.	50	41	12	7	91 (82.7%)

Table 5 indicates that trust in encrypted systems is strong, with nearly 83% supporting mandatory encryption for sensitive data. This reflects users' recognition of its importance in protecting digital assets.

Statistical Analysis

In addition to descriptive statistics, further statistical analyses were conducted to examine relationships, dependencies, and predictive capacity among the variables studied. The results of Chi-Square tests of independence, correlation analysis, regression modeling, and test-retest reliability were presented.

Chi-Square Test of Independence
To determine whether awareness of database encryption is associated with the perception that encryption improves data confidentiality, a Chi-square test was performed.

Table 6: Chi-Square Test of Independence

	Agree	Disagree	Total
Aware of Encryption	97	13	110
Encryption Improves Confidentiality	92	18	110

Using the Chi-square formula:
$\chi^2 = \Sigma((O - E)^2 / E)$

The calculated Chi-square value was 0.92, with 1 degree of freedom. The p-value > 0.05, indicating no statistically significant association between awareness and perception of encryption's impact on confidentiality. This suggests that awareness alone does not necessarily influence perceived effectiveness.

Correlation Analysis
Pearson correlation analysis was conducted to assess the relationship between participants' awareness and their trust in encrypted databases. The awareness score was computed as the sum of responses across Table 3, and trust was computed from Table 5.

Correlation Result:
- Pearson correlation coefficient (r) = 0.68
- $p < 0.01$ (significant)

This indicates a strong positive correlation, meaning that individuals who are more aware of encryption tend to have higher trust in encrypted databases.

Regression Analysis
A simple linear regression was carried out to predict trust in encrypted databases based on awareness and perception scores. Trust (dependent variable) was measured using responses from Table 5, while awareness and perception (independent variables) were taken from Table 3 and Table 4.

Regression Equation:
$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \varepsilon$

Where:
- Y = Trust in encrypted databases
- X_1 = Awareness score
- X_2 = Perception score

Table 7: Regression Analysis Scores

Predictor	Coefficient (β)	p-value
Intercept	1.34	0.03
Awareness	0.45	0.002
Perception	0.38	0.005

The R^2 value was 0.59, indicating that 59% of the variation in trust can be explained by awareness and perception. Both predictors were statistically significant.

Test-Retest Reliability
A test-retest reliability analysis assesses the consistency of the instrument over time. However, in this study, data were collected only once. As a result, test-retest reliability could not be performed due to the absence of repeated measurements. Future studies should incorporate a second data collection phase to evaluate the instrument's temporal stability.

Findings
The study investigated the role of encryption in enhancing database security while examining users' awareness, perceptions, and beliefs regarding encrypted systems. A prototype database secured with the Advanced Encryption Standard (AES) was developed and evaluated, alongside a structured questionnaire administered to 110 respondents from various departments. Findings revealed a high level of encryption awareness among respondents (about 88%) and a strong belief in its effectiveness, with approximately 83% agreeing that encryption improves data confidentiality and prevents unauthorized access. Participants also perceived encrypted databases as enhancing user confidence, ensuring data integrity, and supporting compliance with privacy regulations. Statistical analysis showed that awareness was not significantly associated with perceived confidentiality benefits ($\chi^2 = 0.92$, $p > 0.05$), although a strong positive correlation ($r = 0.68$) existed between awareness and trust in encryption effectiveness. A significant difference was observed between IT and administrative staff, with IT personnel demonstrating stronger belief in encryption, while no significant differences were found across age groups. Regression analysis indicated that user role and training accounted for about 59% of the variance in encryption belief. System evaluation confirmed that the AES-encrypted database effectively prevented unauthorized access, maintained usability and efficiency, and ensured secure data access for authorized users only; however, some respondents expressed concerns about the complexity of key management and data recovery, underscoring the need for user-friendly designs and adequate training.

Conclusion

This study concludes that encryption is a vital mechanism for protecting sensitive data in contemporary database systems. The designed AES-based encrypted system successfully demonstrated its ability to secure data without significantly affecting usability or performance. Awareness of encryption and positive user perception were found to be strong predictors of trust in secure systems. While encryption alone cannot solve all data security challenges, it significantly strengthens existing database protections when implemented effectively. Further, policymakers should consider mandating encrypted data storage for all institutions handling sensitive personal or financial information. Regulatory compliance frameworks such as General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) already emphasize encryption as a necessary safeguard; institutions should adopt these standards as a baseline rather than a ceiling.

Future research should focus on Longitudinal studies to assess the long-term impact and stability of encrypted database systems, exploration of homomorphic and searchable encryption for advanced secure query capabilities, user behavior, and resistance to encryption in real-time systems, and Comparative studies between AES, RSA, and hybrid encryption models under different workloads.

References

Abbas, A. M., Rahma, A. M. S., & Hassan, N. F. (2020). Comparative study on encrypted database techniques, *Journal of Al-Qadisiyah for Computer Science and Mathematics,* 12(3), 28–34. https://doi.org/10.29304/jqcm.2020.12.3.710

Ahmed, S. (2025). *Implementation of advanced encryption techniques to protect sensitive financial Data from cyber threats (Doctoral dissertation,* Dublin, National College of Ireland).

Ajayi, O., & Adebayo, M. (2022). An implementation of AES-encrypted student information systems. *African Journal of Computer Science Research,* 14(3), 55–64.

Ali, A., Munir, A., & Habib, S. (2018). Performance evaluation of Transparent Data Encryption for Microsoft SQL Server. *International Journal of Computer Applications,* 180(5), 25–30.

Chandramouli, R., & Pinhas, D. (2020). *Security guidelines for storage infrastructure,* NIST Special Publication, 800(209), 800-209.

Hasan, M., Islam, M. T., & Mahmud, F. (2020). Performance analysis of a secured NoSQL database system using AES, *Journal of Computer and Communications,* 8(9), 30–41.

Koppenwallner, J., & Schikuta, E. (2023*). A survey on property-preserving database encryption techniques in the clou*d, *arXiv preprint. arXiv:2312.12075*.

Naguib, A., & Fouad, K. M. (2024, March). Database security: Current challenges and effective protection strategies, *In 2024, the 6th International Conference on Computing and Informatics (ICCI)* (pp. 120-130). IEEE.

Okoro, A., & Olatunji, S. (2021). Enhancing data privacy in Nigerian health records using AES-encrypted systems, *Nigerian Journal of Health Informatics,* 7(2), 20–30.

Singh, J., & Kaur, R. (2019). A comparative study of symmetric and asymmetric encryption techniques in database security, *International Journal of Computer Science and Network Security,* 19(3), 120–127.

Wang, H., Liu, F., & Zhang, J. (2021). Comparative study of encrypted database systems in the cloud. *IEEE Access*, 9, 54235–54245.

Yousuf, H., Salloum, S., Aburayya, A., Al-Emran, M., & Shaalan, K. (2021). A systematic review of CRYPTDB: Implementation, challenges, and future opportunities, *J. Manag. Inf. Decis. Sci,* 24(1), 1-16.

Zhou, Y., Mu, Y., & Susilo, W. (2019). Secure and efficient searchable encryption: A literature review, Journal *of Network and Computer Applications,* 112, 28–39.