Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th October 2025. Vol. 5. No. 1; e-ISSN: 2808-4519

Implementation of an Executive Information System for Thesis Document Submission with the Addition of AES-256-CBC Cryptography Algorithm

Taqiyuddin Ahmad Al Aufa[1]*, Adriano Femaz Rivaldy[2], Amalia Anjani Arifiyanti[3], Agung Brastama Putra[4]

[1, 2, 3, 4] UPN Veteran Jawa Timur

23082010135@student.upnjatim.ac.id [1], 23082010139@student.upnjatim.ac.id [2], amalia_anjani.fik@upnjatim.ac.id [3], agungbp.si@upnjatim.ac.id [4]*

Abstract

The rapid digitalization of higher education demands secure and efficient management of academic documents such as thesis submissions. This study aims to develop an Executive Information System (EIS) for Thesis Document Submission integrated with AES-256-CBC cryptographic security to ensure data confidentiality, integrity, and controlled access. The system is implemented as a web-based platform using the Laravel framework and MySQL database, where each uploaded thesis document is automatically encrypted, and only authorized users with a valid Master Key can decrypt it. The AES-256-CBC algorithm generates unique ciphertexts for every encryption process, supported by randomized Initialization Vectors and separate key management to prevent unauthorized access or data leakage. Furthermore, the EIS dashboard implements the drill-down method, presenting real-time analytical information. This allows academic leaders to navigate hierarchically from high-level summaries to specific, detailed data, enhancing their ability to monitor thesis submissions and make informed decisions effectively. The results indicate that the integration of cryptography and executive information management enhances both document security and administrative efficiency, providing a reliable and transparent solution for safeguarding academic data within higher education institutions.

***Keywords**: AES-256-CBC; Cryptography; Drill-down; Executive Information System; Information Security*

1. Introduction

In the era of higher education digitalization, the management of academic documents such as thesis submissions demands high levels of efficiency, speed, and security. Thesis documents, which contain students' scholarly work, are confidential academic assets of significant value to the institution. However, in practice, many document submission systems still lack adequate data security mechanisms, leading to potential risks such as unauthorized access, data manipulation, and leakage of sensitive information.

One approach to addressing this issue is the implementation of cryptographic algorithms within information systems. Cryptography serves to maintain the confidentiality, authenticity, and integrity of data through encryption and decryption processes. The Advanced Encryption Standard (AES) algorithm is one of the most widely used cryptographic methods due to its high level of security and processing efficiency[1]. The AES-256-CBC (Cipher Block Chaining) variant provides stronger protection through a 256-bit key length and a chained encryption mechanism that produces unique ciphertexts even when the plaintexts are identical.

While cryptography addresses data confidentiality issues, the submission process itself still presents managerial challenges, specifically, the limited accessibility of executive information for faculty or program leaders in monitoring thesis submission activities. Submission data dispersed across different departments often complicates strategic decision-making processes, such as determining graduation rates, supervision productivity, or thesis completion trends. An Executive Information System (EIS) is fundamentally a category of information system specifically designed to meet the needs of executives [2]. Unlike daily operational systems, an EIS focuses on presenting summarized (aggregate) and high-level data, often in the form of visual dashboards. Its purpose is to consolidate data from various sources to support performance monitoring, trend identification, and strategic decision-making. Therefore, an Executive Information System (EIS) is needed to present integrated, real-time, and visual information that supports data-driven decision-making[3].

A previous relevant study on the implementation of Executive Information Systems (EIS) was conducted by Tanjung and Wahyuni [4] in the context of mail delivery at PT Pos Indonesia DC Medan Denai. The study highlighted issues where the mail delivery reporting process was still semi-computerized, making it difficult for management to access historical data and proof of delivery. The proposed solution was a web-based EIS capable of presenting information on delivery status, courier data, and on-time delivery reports in visual formats such as

charts. The purpose of implementing this EIS was to provide better data storage and to facilitate strategic decision-making by management in addressing delivery delay issues.

To enhance the data analysis capabilities of the executive dashboard, the proposed system also implements the drill-down method. The drill-down method is an approach that allows users to analyze data in greater depth by presenting information hierarchically. This approach enables executives to navigate from summarized (high-level) data to more specific and detailed information.

Relevant research on the implementation of the drill-down method in Executive Information Systems (EIS) has been conducted by Dewi et al. [5] in a case study on television performance at PT. Jawa Pos Media Televisi (JTV). The implemented solution was a web-based EIS utilizing the drill-down method, which presents data hierarchically, from high-level summaries to highly detailed information. Functionally, the system allows executives to zoom in or drill down within data visualizations, such as clicking on a "Genre" bar chart to display a breakdown of "Sub-Genre," and further clicking to view specific "Program" details. The study's results showed that this method effectively supports executives in analyzing data from an overview to detailed levels, enabling faster and more responsive decision-making

This study proposes the development of an Executive Information System for Thesis Document Submission equipped with AES-256-CBC-based security features. The system is implemented as a web-based application that allows students to upload thesis documents with an automatic encryption process, while providing an executive dashboard for faculty members to monitor submission status, the number of accepted theses, and supervision activity.

2. Methods

2.1. Executive Information System Architecture

The Executive Information System (EIS) developed in this study is designed to support a secure and integrated thesis document submission process. The system architecture is web-based and consists of three main layers: the presentation layer, the application layer, and the data layer.

This architecture operates in an integrated manner. The presentation layer functions as the user interface accessible to three types of actors: students (for uploading documents), thesis supervisors (for validation processes), and program heads (for monitoring the analytical dashboard). This interface connects to the application layer, which serves as the main controller for all business processes. This layer not only manages submission data but, most importantly, performs automatic file encryption using the AES-256-CBC algorithm when documents are uploaded, ensuring that files cannot be accessed without a valid decryption mechanism. In turn, the data layer encompasses the database that stores essential metadata (such as file name, upload time, and encryption status), user data, and aggregate data required by the EIS. This layered architecture enables the executive dashboard to efficiently retrieve data and present visual information, such as charts and submission trend tables, providing comprehensive visibility for faculty leadership in strategic decision-making.

This system is developed using the Laravel framework, which manages both the backend and frontend of the application in an integrated manner. The database used is MySQL, which stores all user information, document metadata, and encryption process results. The selection of Laravel and MySQL is based on their ease of implementation, strong security features, and extensive ecosystem support for web-based application development.

2.2. Drill-down Method

To support the analytical functionality of the Executive Information System (EIS), this study implements the drill-down method. The drill-down method is an approach that presents data using a hierarchical concept, allowing users to navigate from a summary (high-level) view to more detailed data levels[6]. In this system, the drill-down method is specifically implemented on the Head of Study Program's (Kaprodi) dashboard. The administrator can directly interact with visual elements, such as clicking on a bar in the chart displaying the total number of thesis submissions. This action triggers the system to "drill down" and display a detailed data table that presents the breakdown of the aggregated data. This functionality enables administrators to gain deeper insights from summary data in a direct and interactive manner.

Previous studies have demonstrated the implementation of the drill-down method as an effective solution in Executive Information Systems (EIS) to address issues related to manual and unstructured operational data. For example, a study on the new student admission system at SMK Tritech Informatika Medan [7], identified problems where manual data archiving made it difficult for executives to search for information. The drill-down method was implemented to enable executives to view summarized data in detail, such as displaying charts of new student admissions by year or major. Similarly, research conducted at J&T Express Belawan [8], found that executives received too many lengthy expedition reports, making it difficult to take action. An EIS with a drill-down feature was applied to break down summarized data into more detailed information, for instance, by sorting transaction data for analysis. In both case studies, the drill-down method proved to assist executives in interpreting reports more concisely and effectively, thereby supporting strategic decision-making.

2.3. Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric cryptographic algorithm that uses a single key for both encryption and decryption processes[9]. This study employs the AES-256 variant, which has a 256-bit key length and offers the highest level of security among the AES variants.

The AES encryption process divides data into 128-bit blocks and performs several main stages (SubBytes, ShiftRows, MixColumns, and AddRoundKey) over 14 rounds of encryption[10]. These stages transform the original data into ciphertext that is extremely difficult to decrypt without the correct key. AES-256 was chosen because it provides an optimal balance between high security and processing efficiency for protecting digital documents[11].

2.4. Cipher Block Chaining (CBC)

This study employs the Cipher Block Chaining (CBC) mode of operation to enhance encryption security. In this mode, each plaintext block is XORed with the ciphertext of the previous block, making the encryption result of each block dependent on the one before it[12].

The first block uses a randomly generated Initialization Vector (IV) to ensure that each encryption process produces a unique ciphertext[13], even when the plaintext is identical. The IV is stored along with the process metadata for decryption purposes. Through this mechanism, the CBC mode prevents the emergence of patterns that could be exploited by unauthorized parties, making it more secure for use in thesis document submission systems.

2.5. Key Management and System Implementation

Key management in this system utilizes user login information, specifically the combination of student ID (NPM) and password, to dynamically generate an encryption key using the SHA-256 hash function. The key is unique to each user and is not stored in the database, thereby enhancing the overall system security[14].

In addition, the system generates a random Initialization Vector (IV) for each file encryption process and stores it in the MySQL database along with the document metadata[15]. All encryption and decryption processes are executed on the server side using the AES-256-CBC algorithm, implemented within the Laravel framework. Uploaded thesis documents are automatically encrypted, and they can only be decrypted by authorized parties (the student, thesis supervisor, or program head) after entering the student's “Thesis Master Key,” which must be shared by the student out-of-band (outside the system).

3. Results and Discussion

3.1. System Interface and Functionality

The developed system is designed to facilitate secure thesis document submission through a web-based interface. On this page, students can upload their thesis documents by providing information such as the title, supervisor’s name, year of enrollment, and creating a Master Key that will be used in the document encryption process. This Master Key serves as the main password that must be kept confidential and shared out-of-band with the thesis supervisor so they can decrypt the file.

Fig. 1: Thesis document upload page interface for students

Once all data is completed, the system automatically performs encryption using the AES-256-CBC algorithm and stores the encrypted file on the server. Through this mechanism, the confidentiality of the thesis document is ensured, as only those possessing a valid Master Key can access it. The interface display of the thesis document upload page for students is shown in Figure 1.

Fig. 2: Document decryption interface for thesis supervisors

The interface for thesis supervisors is designed to allow them to securely access students' thesis documents through the decryption process. On this page, supervisors can view basic submission information—such as the thesis title and student identity—before entering the Master Key that has been shared by the student out-of-band.

The decryption process is carried out using the AES-256-CBC algorithm, where the Master Key functions to unlock and download the previously encrypted thesis document. Only those possessing a valid Master Key can perform this process, ensuring that the document's confidentiality is maintained. This design guarantees that the thesis supervision process is secure, controlled, and accessible only to authorized parties. The supervisor's decryption interface is shown in Figure 2.

Fig. 3: Executive Information System dashboard for the head of the study program

Figure 3 shows the Executive Information System (EIS) dashboard used by the head of the study program to monitor thesis submission activities. The dashboard displays charts of the number of theses based on student cohorts and a summary of the total uploaded documents. The data presented is dynamic and updated in real-time from the system database.

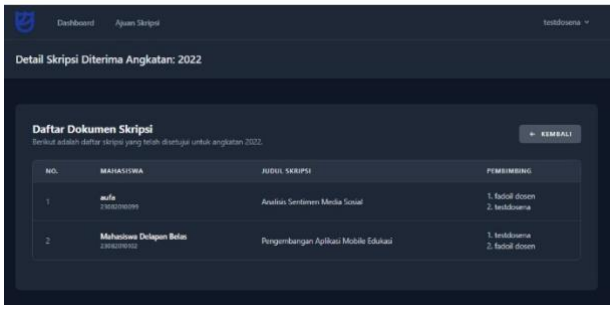


Fig. 4: Display of Drill-Down Results

Figure 4 demonstrates the results of implementing the drill-down method on the executive dashboard. This view appears after the executive (Head of Study Program) interacts with the main dashboard—for instance, by clicking on the aggregated data labeled "Class of 2022" in a chart. In accordance with the described method, the system then "drills down" from a summary view to a detailed view, as indicated by the page title "Accepted Thesis Details for Class of 2022." On this page, a table titled "List of Thesis Documents" is presented, containing detailed operational data, including specific information such as student names, student IDs (NPM), thesis titles, and the list of assigned supervisors. This functionality demonstrates the system's ability to present data hierarchically, transitioning from strategic summaries to individual data details.

Through this interface, the program head can easily monitor thesis submission trends over the years and identify student activity by cohort. This information assists leadership in making strategic decisions, such as scheduling thesis supervision or evaluating academic performance. The integration of AES-256-CBC–based document security with the executive dashboard demonstrates that the system not only ensures data confidentiality but also enhances managerial efficiency.

3.2. Database View

The system's database component is used to store metadata information for each thesis document uploaded by students. This metadata includes the thesis title, year of enrollment, submission status, original file name, encrypted file name, as well as the Initialization Vector (IV) value and master key hash generated during the encryption process. All of this data is stored in the system's main table, as shown in Figure 5.

Fig. 5: Database table structure for storing encrypted document metadata

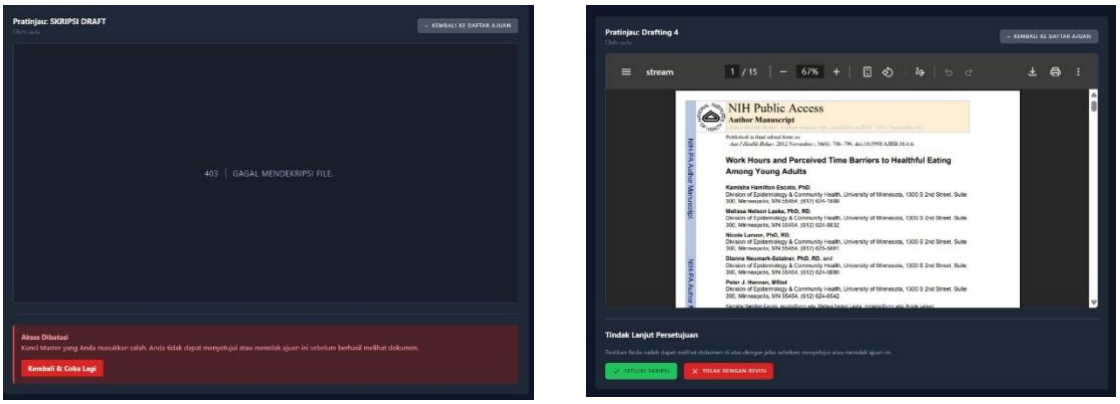
The presence of the iv and master_key_hash columns indicates that the system implements key management separately from the encrypted document. The master_key_hash value does not store the original key but rather the hashed result of the Master Key entered by the student. This ensures that no encryption keys or passwords are stored directly in the database, thereby minimizing the risk of data leakage.

In addition, each entry includes created_at and updated_at timestamp columns to facilitate user activity tracking and security auditing. This design supports the principles of data confidentiality and integrity, ensuring that only non-sensitive information is stored while confidential data remains protected on the user's side.

3.3. Encryption and Decryption Test Results

The system includes a validation mechanism to ensure that the decryption process can only be performed using the correct Master Key. When a user enters an invalid key, the system rejects the decryption process and displays an error message, "403 | GAGAL MENDEKRIPSI FILE," along with a notification that access is restricted. Users cannot proceed with document approval or download until successful decryption is performed using a valid key.

This decryption failure demonstrates that the AES-256-CBC algorithm functions as intended. Without a valid Master Key, the ciphertext cannot be reverted to its plaintext form, ensuring that the document's contents remain protected even when stored on the server. In addition, providing an informative error message helps users understand the cause of failure and take corrective action, such as requesting the key again out-of-band. To further enhance system security, it is recommended that each failed decryption attempt be logged, including the timestamp, user identity, and related document. The failed decryption condition is shown in Figure 5a.



(a) (b)

Fig. 6: a) Failed decryption display, b) Successful thesis document decryption display

Figure 6b illustrates the successful decryption condition, where the previously encrypted thesis file can be displayed again after the user enters a valid Master Key. Once decryption is successful, the system presents the document in its original form on the preview page, allowing the thesis supervisor to make a decision on the submission through the Approve Thesis or Reject with Revision buttons.

The comparison between Figures 6a and 6b demonstrates that the system has effectively implemented the AES-256-CBC algorithm. When an incorrect key is entered, the decryption process is denied (Figure 6a), while with the correct key, the file is successfully restored to its plaintext form (Figure 6b). This mechanism ensures the confidentiality and integrity of documents during storage and transmission.

By allowing successful decryption only under valid authentication conditions, the system upholds the principles of data security based on confidentiality and controlled access, while simultaneously facilitating an efficient and secure academic supervision process.

4. Conclusion

This study successfully developed an Executive Information System for Thesis Document Submission equipped with AES-256-CBC–based cryptographic security. The system provides a secure environment where thesis documents are automatically encrypted during upload and can only be decrypted by authorized users possessing a valid Master Key. By integrating encryption at the system level and managing keys independently from the database, the proposed design ensures data confidentiality, integrity, and resistance against unauthorized access.

In addition to its security features, the system enhances managerial efficiency through a real-time executive dashboard. This dashboard successfully implements the drill-down method, which presents submission data in a structured, hierarchical format. This functionality enables program heads to navigate from high-level visual summaries (such as graphs) to specific, detailed tables of information (such as lists of student submissions) with a single click. This deep-level analysis capability empowers leaders to monitor academic activity, evaluate supervision performance, and make data-driven decisions more effectively. Overall, the system demonstrates how the integration of robust cryptography and advanced information analysis can simultaneously strengthen information security and support strategic academic administration in higher education.

References

[1] R. Mulyo Liauren, B. Zaman, S. Bahri, T. Informatika, and S. Kharisma Makassar, "IMPLEMENTASI ALGORITMA AES DAN BCRYPT UNTUK PENGAMANAN DATA PENGGUNA PADA WEBSITE JAHITKU", [Online]. Available: https://jahitku.my.id/.

[2] M. P. Maliky, L. Tanti, F. Teknik, D. I. Komputeruniversitas, and P. Utama, "Sistem Informasi Eksekutif (SIE) Untuk Memantau Keluar Masuk Kapal Pada Kantor Otoritas Pelabuhan Utama Belawan Executive Information System (Eis) To Monitor Entry And Exit Of Ships At The Belawan Main Port Authority Office)," 2023. [Online]. Available: http://kti.potensi-utama.ac.id/index.php/JUREKSI/index|

[3] S. Safrodin, C. Chotimah, and I. Junaris, "Pemanfaatan Aplikasi Evaluasi Diri Madrasah sebagai Sistem Informasi Eksekutif dalam Pengambilan Keputusan Strategis di Madrasah Ibtidaiyah Al-Muhtaduun," *Jurnal Penelitian Inovatif*, vol. 4, no. 3, pp. 1297–1306, Jul. 2024, doi: 10.54082/jupin.498.

[4] A. Tanjung and L. Wahyuni, "Sistem Informasi Eksekutif Pengiriman Surat Pada Pt Pos Indonesia Dc Medan Denai Berbasis Online," 2023. [Online]. Available: http://kti.potensi-utama.ac.id/index.php/JID

[5] M. Salma Wajendra Dewi *et al.*, "SISTEM INFORMASI EKSEKUTIF PERFORMA TELEVISI PT. JAWA POS MEDIA TELEVISI MENGGUNAKAN METODE DRILL DOWN."

[6] J. Jureksi, A. Pratama, and A. Syahputra, "Penerapan Metode Drill Down Dalam Sistem Informasi Laporan Kunjungan Kolektor Pada PT Mitsui Leasing Application of the Drill Down Method in the Collector Visit Report Information System at PT Mitsui Leasing," 2024.

[7] S. Paulina and L. Wahyuni, "Sistem Informasi Eksekutif Penerimaan …," 2024.

[8] J. Jureksi, D. Kurniawan, and B. Triandi, "Sistem Informasi Eksekutif Expedisi Produk Pada J&T Express Menggunakan Metode Drill Down Berbasis Web (Studi Kasus: J&T Express Belawan)," 2023.

[9] R. M. Hilmy Hernandi and J. C. Chandra, "Implementasi Algoritme AES-256 dan AES-GCM untuk Mengamankan Dokumen Pada Sistem Data Rekam Medis Klinik Mulya Implementation of Aes-256 dnd AES-GCM Algorithms to Secure Documents in The Medical Record Data System at Mulya Clinic," *KRESNA: Jurnal Riset dan Pengabdian Masyarakat*, vol. 4, pp. 12–22, 2024, [Online]. Available: https://jurnaldrpm.budiluhur.ac.id/index.php/Kresna/

[10] R. Rahman, A. R. Zahirah, and S. Artikel, "Keamanan data terenkripsi: studi kasus enkripsi AES dalam pengembangan web formulir aduan PPKS ITH INFORMASI ARTIKEL ABSTRAK," 2024.

[11] Asep Rizal Nurjaman and Agus Tinus Turnip, "COMBINATION OF AES-256 AND SHA3-512 CRYPTOGRAPHIC ALGORITHMS TO ENHANCE PDF DOCUMENT SECURITY".

[12] S. Manullang, Allwine, and Jakaria Sembiring, "Pengamanan Data File Dokumen Menggunakan Algoritma Advanced Encryption Standard Mode Chiper Block Chaining," *Antivirus : Jurnal Ilmiah Teknik Informatika*, vol. 17, no. 1, pp. 53–67, Jun. 2023, doi: 10.35457/antivirus.v17i1.2811.

[13] M. Wildan and W. M. Ashari, "Text Data Security Using LCG and CBC with Steganography Technique on Digital Image," 2024. [Online]. Available: http://jurnal.polibatam.ac.id/index.php/JAIC

[14] Iwan Setiadi, Santi Widianti, and I Putu Prachanda Kayuan, "Implementasi Kriptografi Pengamanan Data Soal Ujian di Lingkungan Perguruan Tinggi Menggunakan Algoritma AES-256 dan SHA-256," *Jurnal Penelitian Rumpun Ilmu Teknik*, vol. 3, no. 4, pp. 153–178, Dec. 2024, doi: 10.55606/juprit.v3i4.4569.

[15] F. Sabila, R. Maulana, A. Trisna Sari, A. Anjani Arifiyanti, and A. Brastama Putra, "Implementasi Algoritma AES-256-CBC untuk Pengamanan Dokumen Berbasis Kriptografi", [Online]. Available: https://ejurnal.itats.ac.id/snestikdanhttps://snestik.itats.ac.id