

Synergistic Information Security Design Implementation based on Role-Based Access Control, Information Classification, and AES Cryptographic Encryption

Marjay C. Bumalod

marjay.bumalod24@gmail.com

Isabela State University, Philippines

Rose Mary A. Velasco

rosemary.a.velasco@isu.edu.ph

Isabela State University, Philippines

Abstract: Security technology has undergone significant development and research in response to increasing cyber threats. The Intranet Document Management System (IDMS) was created to centralize documents within organizations, ensuring efficiency and streamlining processes. Given the critical nature of document management in organizational workflows, secure and safe management is paramount. This study aims to develop a secure IDMS using Advanced Encryption Standard (AES) encryption, Role-Based Access Control (RBAC), and an Information Classification Model. We also provide a comprehensive overview of the key characteristics and performance metrics of each access control model and cryptographic algorithm, facilitating decision-making for system design and implementation. The system offers high granularity, ease of administration through role assignments with document classification, high flexibility with customized permissions, and scalability with roles and classification. AES is chosen for its high security and fast performance, making it a widely used encryption standard.

Keywords: Advanced Encryption Standard (AES), Access Control, Cryptographic Algorithm, Document Management System, Information Classification

INTRODUCTION

In this era of digitization, where digital data overwhelms organizations and individuals, there is a greater need than ever for effective, secure, and well-organized documentation. The IDMS, a crucial tool that revolutionizes how we create, save, access, and distribute information in new ways, ushers in a new era of effective document handling. According to (Imen & Belhassen, 2018), digital document management, or DMS, is a computer application-based method for measuring, managing, storing, and minimizing paper use. With the integration of the AES encryption method, IDMS is a sophisticated software solution created to centrally manage, secure, share, and arrange digital data. NIST held a competition 2000 to find a robust encryption/decryption method, and the AES algorithm emerged victorious. There are no known security weaknesses, and it will take years for computers to achieve the processing capacity required for brute-force attacks (Garcia, 2015).

Due to the vast volumes of information organizations generate and receive, including emails, reports, contracts, and more, the digital age has resulted in a data overload by the company. This volume may be too much to handle. These days, it is necessary to protect sensitive and confidential data. Unauthorized access, accidental disclosures, and data breaches can all have negative consequences. There needs to be more version control to make it easier for organizations to identify the most recent version of a document. Nevertheless, ensuring that only authorized personnel access specific information can be challenging while maintaining the ease of sharing with those who need it. Permission and access control are relevant here. Keeping track of who has viewed and read the papers you provide to end users is crucial. Achieving the ideal balance between security and accessibility is crucial.

Analytical applications are the core of the Big Data phenomenon, as they extract significant value in information and knowledge from the data acquired and archived with the techniques described above (Fugini & Finocchi, 2018). This result can be achieved through business intelligence or more exploratory techniques, defined as advanced analytics. However, Lee and Iio (2015) volunteered to work in several small-scale archives, and almost all the institutions need help introducing information systems to fulfill the needs of their clients and staff. The problem is that both staff and users need help with time-consuming procedures. It is reasonable to close the shelves to protect valuable information resources in a traditional way of storing documents. On the other hand, (Reddy & Gopu, 2017) developed an EDRM system that protects documents in a corporate environment using cryptographic primitives, RSA, and AES encryption. The EDRM also displays the decrypted contents in a secure Viewer, restricting the operations that can be performed on the content. However, (Abang et al., 2022) analyzed the DMS for private HEIs in the Philippines; there are some problems arising during the manual requisition of documents, such as (1) a Hard time accommodating a large number of requestors entering the school premises; (2) Misplaced request forms; (3) Hard time in checking the request documents if it is already in process or already for release; (4) Hard time to go to school for request process and claiming the documents and; (5) Misplaced claim stub and receipt.

An Intranet Document Management System (IDMS) with AES encryption, Role-Based Access Control (RBAC), and information classification is crucial to address the issues of data overload, protecting sensitive information, and the requirement for effective version control and access permissions. AES encryption shields sensitive papers from unwanted access and data breaches, guaranteeing they are encrypted before storage. RBAC allows businesses to set access rights according to employee responsibilities, guaranteeing that only persons with the proper authorization may access specific data. Furthermore, information classification makes it possible to group documents according to their level of sensitivity, which facilitates the use of suitable security measures and turns them into structured information. Moreover, through automated reports such as document trails and user actions, organizations may strike a balance between security and accessibility by including these three security measures in the IDMS. This will guarantee that confidential data is safeguarded while preserving effective internal sharing and collaboration.

REVIEW OF RELATED LITERATURE

The median cost of a single data breach in 2015 was \$3.8 million, increasing 23% from the previous year. Many companies have transitioned to electronic methods of collecting, storing, and exchanging data to save costs, streamline operations, and reorganize internal divisions to deliver services more successfully and economically (Joseph, 2018). Furthermore, as network technology has advanced, malicious computer viruses and hacker attacks have become common. Password cracking is used in these attacks to steal user information, compromise databases, erase or modify data, and carry out other criminal tasks. Even worse, it could compromise the computer system's security, putting the online library at serious risk. Users' and licensees' interests are compromised, and they are at risk. Many users distribute digital libraries, limiting the uniformity of information security expertise (Hao, 2015).

However, encrypting documents at the file level can provide data security and protect data transfer or storage safety (Lin et al., 2021). Document security is ensured via encryption, done with a key or password. Only those with the correct decryption keys may view the encrypted documents. For example, in some exceptional cases, it is necessary to securely share the password with the recipient after sending the encrypted file. According to Raigoza and Jituri (2016), the previous ten years have mainly benefited the Advanced Encryption Standard (AES) industry standard. Formerly known as Rijndael, the AES completed a five-year standardization process. The National Standards and Technology Institute (NIST) selected it as the AES after competing with fifteen other designs.

According to Imen and Belhassen (2018), when information and data are stored on a drive or documents, they are essential for organizing company activities. However, the present business process languages and models do not clearly explain the link between data flow and access control. A recent development in business process management is the artifact-centric and data-aware approach. They aim to provide a comprehensive process flow and increase the usage of data-driven processes in BPM systems by utilizing modeling, data, or documentation. Moreover, according to a study by (Liu, 2021), colleges and other educational institutions must develop an electronic document organization system that keeps up with the expansion of big data. The current situation of electronic information documents in higher education institutions is concerning when looking at data. The main problems are a shortage of full-time employees, bad administration, and inattention. To effectively tackle these difficulties, leadership emphasis

and resource integration are required to handle the platform issue, encourage using electronic documents in academic institutions, and address basic and complicated issues.

Despite the valuable insights provided by existing literature, several gaps and areas for further research have been identified. Firstly, while the median cost of a single data breach was highlighted in previous studies, there is a lack of recent data and analysis on the current trends and costs associated with data breaches. This gap presents an opportunity for future research to provide updated insights into the financial impacts of data breaches on organizations. Additionally, the transition of many companies to electronic methods for data collection, storage, and exchange has been noted. However, there is a need for further research to explore the specific challenges and benefits of this transition, particularly in terms of cost savings, operational efficiency, and organizational restructuring. Furthermore, while the literature acknowledges the prevalence of malicious computer viruses and hacker attacks, there is a gap in understanding the specific techniques used in these attacks, such as password cracking, and their potential impact on data security. Future research could delve deeper into these areas to enhance our understanding of cybersecurity threats and mitigation strategies.

Objective of the Study

This study aims to design and develop an Intranet Document Management System that centralizes the company's different types of documents and implements three information security measures: Role-Based Access Control (RBAC), Information Classification, and AES-128 document encryption.

Specific Objectives

1. Analyze the encryption and decryption process of the Advanced Encryption Standard (AES)-128 algorithm.
2. Determine the document file size after encryption.
3. Evaluate different access control models: Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC) based on Granularity, Ease of Administration, Flexibility, Scalability, Security, and Adaptability.
4. Compare various cryptographic algorithms, such as AES, DES, 3DES, RSA, Blowfish, Twofish, and RC4, based on key size, block size, security, performance, and usage.

METHODOLOGY

As stated in the earlier section, the development of IDMS with the implementation of AES-128 encryption, RBAC, and Information Classification is the primary purpose of this study. However, some preparations were needed before getting started with this project.

Data Collection

At this point, data was collected by identifying different papers of the company that needed to be centralized. The author will be able to learn about document management systems, accessibility, and security systems from the early literature as the author gathers and examines reliable data from multiple sources in this first stage and assesses potential results for creating this system.

Requirement Specification

The Software Requirements Specification (SRS) serves as the basis of software development, exhibiting influence over all succeeding stages. Accordingly, a high-quality SRS may increase the likelihood of excellent software quality (Osman & Zaharin, 2018). At this point, the author determined the information needs and requirements for constructing the system, as well as the system goals and objectives of the stakeholders to be designed. When creating the DMS, the authors should adhere to ISO 27001's four (3) levels of information classification: restricted (accessible to most employees), internal (accessible to all employees), confidential (accessible only to senior management), and public (accessible to everyone).

System Analysis and Design

System analysis and design is a problem-solving technique that entails looking at a more extensive system, disassembling its component pieces, and figuring out how it functions to achieve a specific goal. At this point, the authors investigate the issues, pinpoint the goals and specifications, and then create the best solution to meet those demands. This may entail reviewing the procedure to satisfy end users' basic needs. The system's overall model design process, which includes inputs into the design process, process activities, and process outputs, is shown in Figure 1. The design process's activities are independent and interconnected, influencing earlier design choices. Knowledge of the platform is essential to the design process to prevent long-term procedures, as most software design process rework is unavoidable.

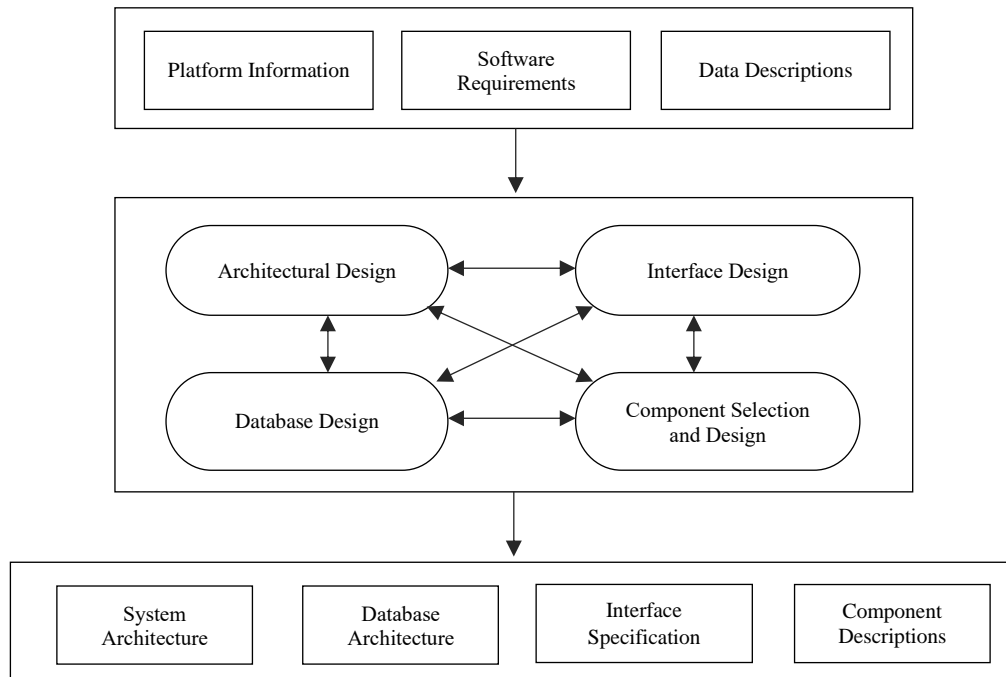


Figure 1. General Model Design Process

Architectural Design

Therefore, an architectural design decision results from a design process at the earliest stages of building or during the software system's evolution. The application domain of the system, the architectural styles and patterns employed in the system, the COTS components and other infrastructure options, as well as other elements required to satisfy the system, may all be taken into consideration when making architectural design decisions (Bosch & Jansen, 2005). Figure 2 illustrates the platform's layered architecture design and encompasses the system's overall structure, components, and interactions. It defines how the software components will be organized, how they will communicate, and how the system will be deployed and maintained. The presentation layer includes a web interface that provides users access to the platform through a web browser using a computer, tablet, or mobile device. The application layer contains the platform's business logic, user authentication, content management, and communication features. The business logic layer implements role-based access control (RBAC) to manage user permissions and access levels and uses AES-128 encryption to encrypt documents and prevent unauthorized access. The database layer stores and manages the platform's data, including user profiles, documents, and other content. Monitoring and logging functions monitor user activities within the platform and provide reports for the system administrator. Deployment involves

implementing cloud-based hosting and domain services load balancing and auto-scaling to handle varying traffic levels.

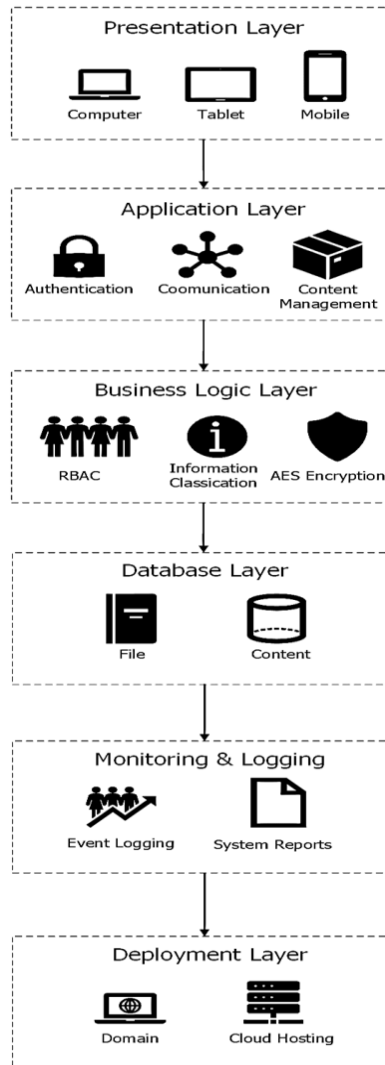


Figure 2. Layered Architecture

Database Design

The cornerstone of application system design is database architecture. A data flow diagram, data dictionary, or other appropriate tools should be used to define user requirements in the database design process precisely. According to Juxiang and Zhihong (2012), it involves removing redundant data and rewriting, deleting, and introducing anomalous material while adhering to standard form theory. The authors created the system's database structure using the data they had collected during the requirements definition and SAD stages. The Entity Relationship Diagram (ERD) depicted in Figure 3 thoroughly examines, comprehends, and produces the system's data structures. Moreover, the database architecture design was derived by examining the relationships between each attribute of the provided database. The ERD is a visual representation of the relationships between entities in the database. It helps design and model data structures and is critical to database design. The ERD consists of several key components: entities, attributes, a primary key, relationships, and a foreign key.

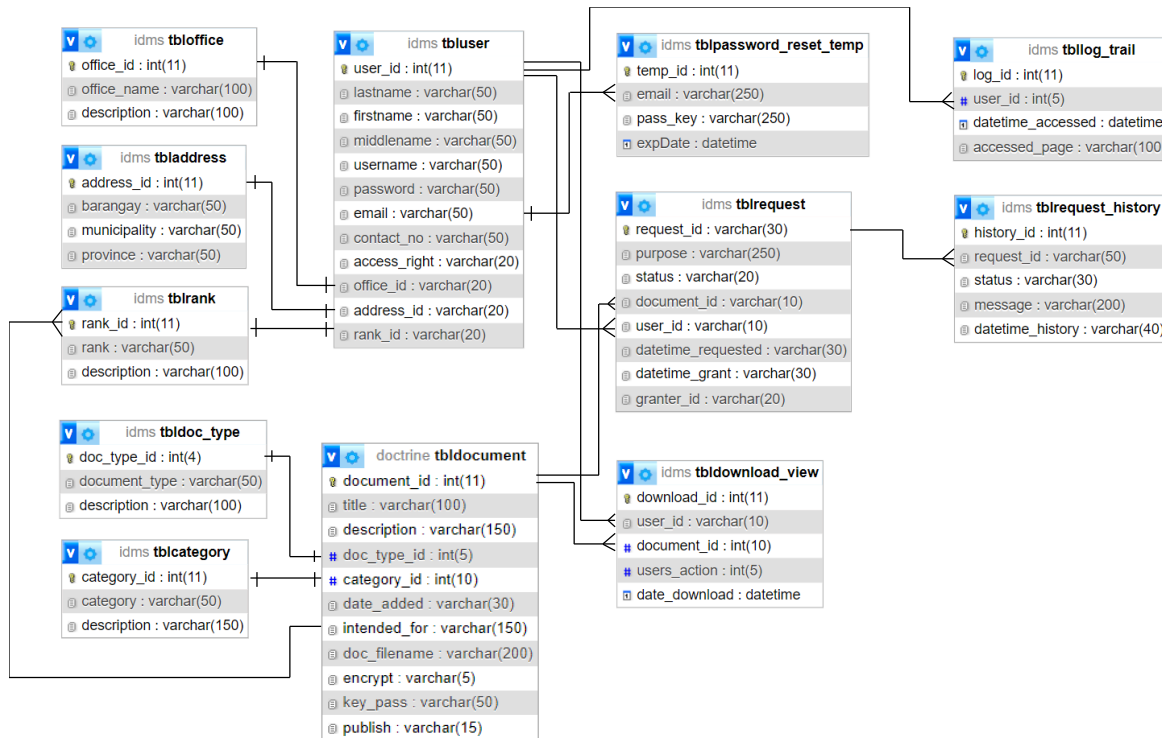


Figure 3. Entity Relationship Diagram (ERD) of the IDMS.

Interface Design

The User interface (UI) design is the asset that helps users interact with the product's interface for services. For example, the User Interface consists of visual design elements, including colors and typography (Sharma & Tiwari, 2021). The user interface is also used to look at the functionality of the screens or unconventional systems like voice-based processes. The author came up with the design of the system interface. The author initialized the interface design using Figma and developed it into a web-based platform using HTML, CSS, JavaScript, Bootstrap Framework, JQuery, and PHP Programming.

Component Selection and Design

Before designing a combination of components for an application, it is highly significant for practitioners to define the requirements of performance very clearly. The system components have a significant impact on the system's performance. The number of combinations could be considerably large, and practitioners could feel no place to start when facing such a large dataset (Cao et al., (2014). The author integrated an AES-128 encryption and decryption process using php implementation and role-based access control as a mechanism to grant access to the different documents displayed in the intranet and uses an information classification model to classify the documents by safeguarding the company's information. Email integration was added as a feature for users' password recovery. It utilized a web push library and notification API as a system notification for the newly added documents or information and new incoming messages between each type of user.

Use the Case Diagram of the Encryption and Decryption and the System Flowchart of the three Information Security

Figure 4 provides a behavioral or use case diagram representing user interactions and system interactions to achieve a specific goal. It visually depicts the encryption functional requirements of a system and shows the various use cases (functions or services) that the system performs in response to actors. The System admin will be responsible for uploading or adding a document, and the IDMS will respond to the user request by passing it to the Key

Management to generate the AES Key. The AES will process the document's encryption, and after the encryption process, the document and its metadata should be stored in the database. Once the document is available to the specified users, the decryption process will occur before rendering it to the client.

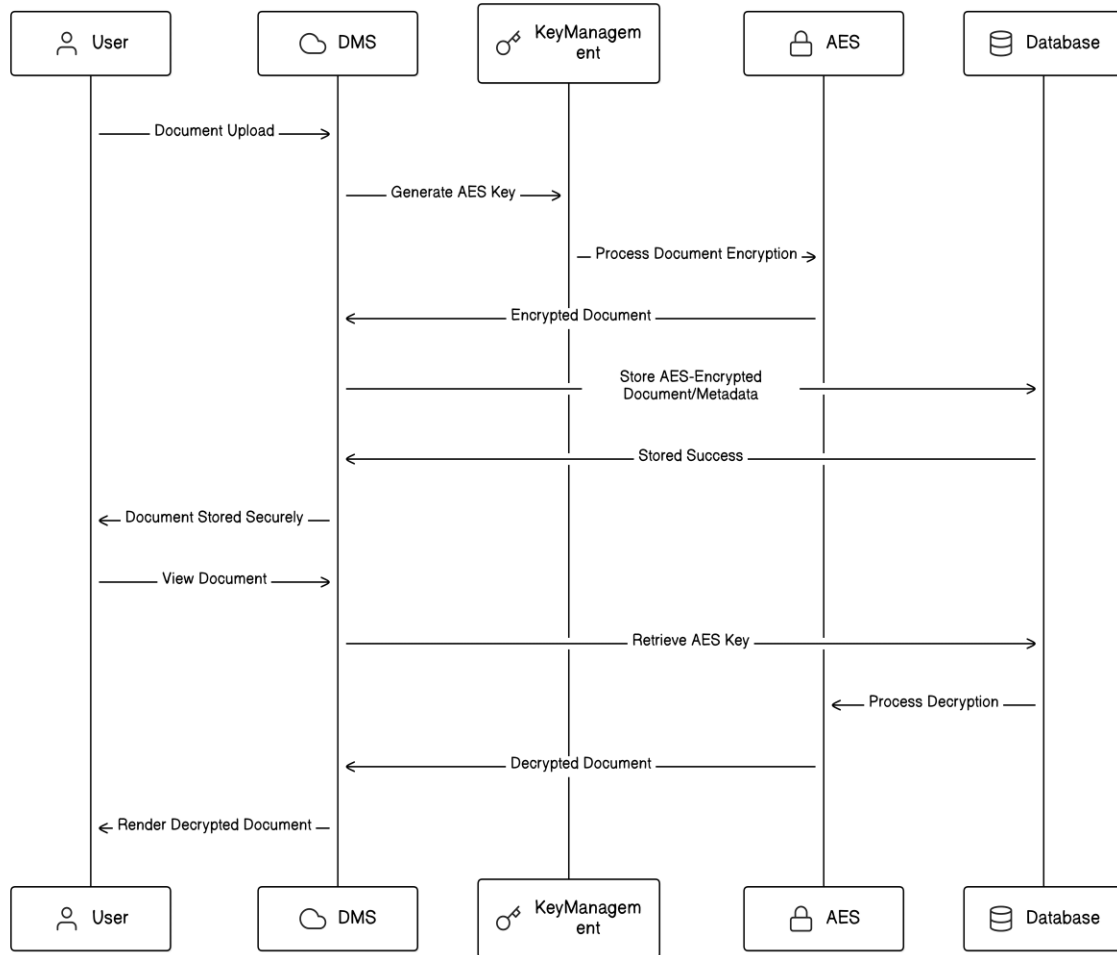


Figure 4. Conceptual Diagram of Intranet Document Management with AES

Figure 5 illustrates the workflow for accessing and decrypting documents within an information security implementation system. The process begins with the user authentication step, where users must authenticate themselves to gain access to the system, ensuring that only authorized users can proceed.

After successful authentication, the user's role is retrieved, determining their access level and permissions. The user then attempts to access documents within the system, with access control managed by Role-Based Access Control (RBAC) policies, ensuring that users can only access documents appropriate to their roles.

Once the user attempts to access the documents, the system classifies them into three categories: Confidential, Restricted, and Internal, each representing different levels of information sensitivity and security requirements. Regardless of the classification, all documents undergo AES-128 decryption, which decrypts the document using the Advanced Encryption Standard (AES) with a 128-bit key, ensuring secure access to the content.

Upon successful decryption, the document is available in its readable form, allowing the user to access the information. The process concludes with an end node, indicating the completion of the document access and decryption workflow.

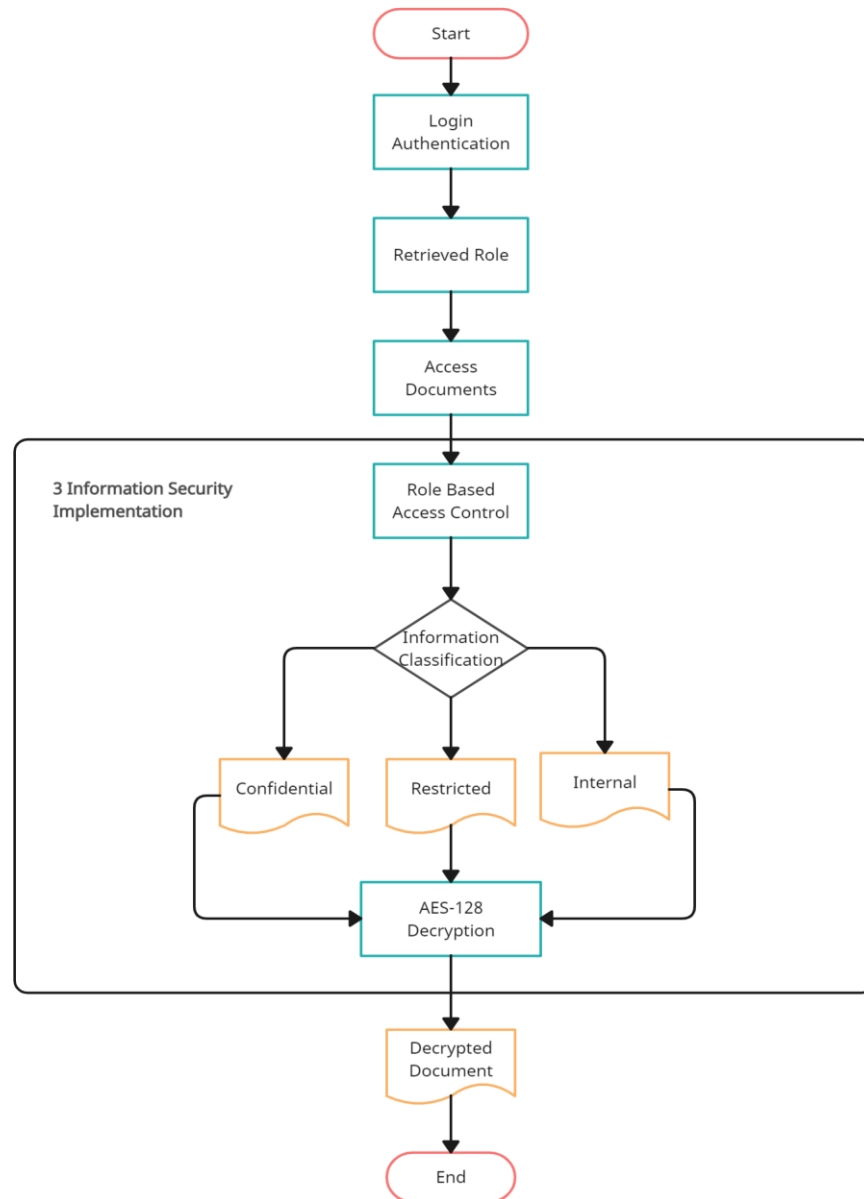


Figure 5. Flowchart of RBAC, Information Classification, and AES.

Structural Features of AES Algorithm

AES takes a 128-bit data block as input and performs several transformations to generate output cipher text. Each 128-bit data block is processed in a 4-by-4 array of bytes called the state (Chen et al., 2019). The Round Key size can be 128, 192, or 256 bits (Kuai & Li, 2020). The number of rounds repeated in the AES, N_r , is defined by the key length, which is 10, 12, or 14 for key lengths of 128, 192, or 256 bits, respectively.

The AES algorithm encryption and decryption are shown in Figure 6. The number of rounds of transformations (Nr) is given by:

$$Nr = \frac{SK}{32} + 6, \text{ where } SK = \text{Key size}$$

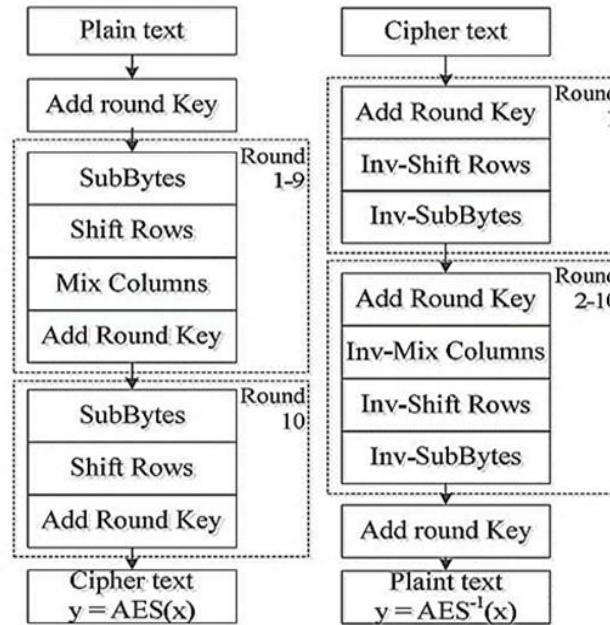


Figure 6. AES Algorithm flow for Encryption and Decryption

The AES 128 bits secret key algorithm results in a total of 10 rounds, out of which from 1 to Nr rounds have four transformations AddRoundKey, SubBytes using S-Box, ShiftRows, and MixColumns except the Nr round have only three transformations Sub Bytes, Shift Row and Add Round Key. The input bits are arranged in a 4×4 matrix of bytes known as a state array, and each column and row are known as a word.

Add Round Key

The round cipher keys are generated in the key expansion by bitwise XOR operation. After the key schedule in key expansion, the key can be divided into 11 groups of 4-byte words. The first 4-byte word is the initial 128-bit secret key, and subsequent keys are generated in the key expansion using SubWord, Rotation Word (RotWord), and Rcon.

SubWord means a nonlinear transformation of each key byte using S-Box (Gangadari & Ahamed, 2016). The RotWord is a cyclic left shift of each byte in a word-by-one byte. Rcon is an array of constant words, and the leftmost byte in a word is non-zero, involved in direct XOR operation with the plain text, and the rest of the ten rounds use subsequent four words to generate ARKs.

Bytes Substitution using S-Box

S-box transformation replaces each element (byte) of input data with another data (byte) using precomputed LUTs, as seen in Figure 7. AES defines an S-box of 256 values for the substitution. You work through the 16 bytes of the state matrix and use each byte as an index into the 256-byte S-Box (Reddy & Gopu, 2017).

Y																	
x		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	F
	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	Be	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	Cf
	6	d0	ef	aa	fd	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	C6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	Df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	Bb	16

Figure 7. Look-up Table (LUT) S-Box

Shift Rows

The transformation moves elements by one byte, which produces diffusion in the encrypted text. As seen in Figure 8, the first row's bytes stay the same while the second, third, and fourth rows are shifted 1, 2, and 3 to the left, respectively.

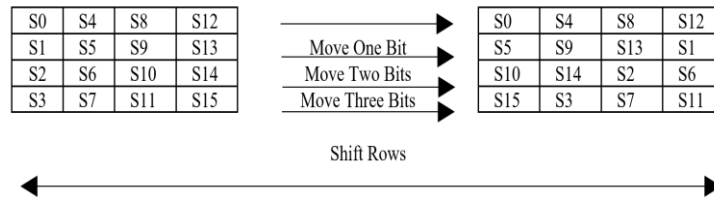


Figure 8. Shift Rows

Mix Column

It is also a linear transition. This layer mixes each column of the state matrix, and each transformation causes a byte to affect three other bytes in the same column. During MixColumns and InvMixColumns, a linear transformation is applied to the input state matrix to form the output state matrix (Fang et. al., 2017). This transformation consists of a matrix multiplication over the Galois Field (GF(28)) between a fixed matrix and the input state matrix (see Figure 9).

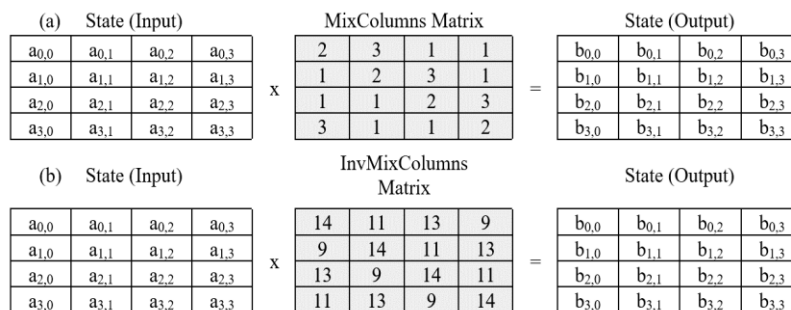


Figure 9. MixColumns (a) MixColumns and (b) InvMixColumns steps of AES-based encryption and decryption.

Information Classification Model

Information classification assists in resolving problems by determining and allocating sensitivity levels to an organization's shared information. It is, therefore, essential to maintaining information security. It is the procedure for categorizing or classifying data to safeguard critical information.

The author classified the various firm papers into three categories: internal information, restricted information, and confidential information. For an organization with many systems/processes, it is imperative to understand that classification of all information will take considerable time. It is wise to start with an initial subjective classification of the most critical systems/applications or business processes based on the information in the inventory (Bergstrom et al., 2021).

This is crucial since it facilitates data retrieval, manipulation, and eliminating duplicate information to contribute to the efficiency of storage and maximizing data security measures. Everyday activities may be managed more effectively with the help of well-organized information. Information classification is based on security, which protects sensitive data and raises security awareness inside the organization. The responsibility of protecting the information lies with everyone handling the documents and information. The system ensures that employees understand the value of information they work with and safeguards that information.

However, based on the data gathered, Table 1 shows the information classified in the company's documents that needs to be displayed on the web application. Each type of document can fall into three categories depending on the purpose or subject of the document given by the company to its users.

Table 1

Information Classification of Documents

Type of Documents	Confidential	Restricted	Internal
Department Administrative Order	No	Yes	Yes
Announcements/Events	No	No	Yes
Mission/Vision/Goals	No	No	Yes
Job Objectives	No	No	Yes
Process Flow Diagram	No	No	Yes
Policy	Yes	Yes	Yes
OSDA	No	No	Yes
Trainee Module	No	No	Yes
Contract	No	No	Yes
Forms	No	Yes	Yes
Directories	No	No	Yes
Company Profile	No	No	Yes
Government Guidelines/Implementation	No	Yes	Yes

Role Based Access Control (RBAC)

RBAC is a security mechanism that controls access to system resources. It protects sensitive information and ensures employees can only access the information they need for their jobs. Figure 10 illustrates role-based security, which determines permissions to grant access to documents on the information classification model, particularly restricted and confidential information.

Admission of new members into roles and revocation of old members depends on the competencies and responsibilities of users assigned to roles (Nyame & Qin, 2020). For restricted information, the admin user will select roles to manage a particular document, and other unselected roles will automatically request permission from the admin to access records. In the confidential information category, all documents will be requested in the admin role to access them. If accessing information is acceptable, the admin role will grant access to them.

The benefits of RBAC include improving operational efficiency, particularly in changing a user's role; RBAC lets the system quickly implement access control on the entire system and cuts down on potential errors when assigning permissions to the user.

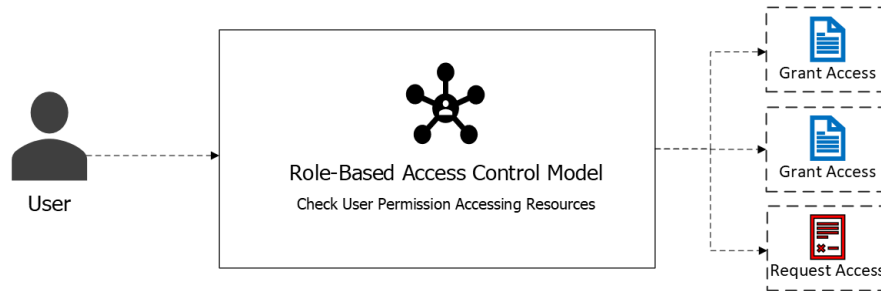


Figure 10. Role-Based Access Control of the system.

RESULTS AND DISCUSSION

Organizations typically categorize information according to confidentiality, and people are allowed access to view it. Classification information model is a method by which organizations evaluate the data they contain and the degree of protection they should receive based on ISO 27001 criteria (Irwin, 2022). Figure 11 shows the interface design with three options for classifying documents. The classification information field is internal, restricted, and confidential. End users will request access to all confidential levels, and restricted levels are linked to specific roles or titles. The documents are viewable by all workers or users at the internal level.

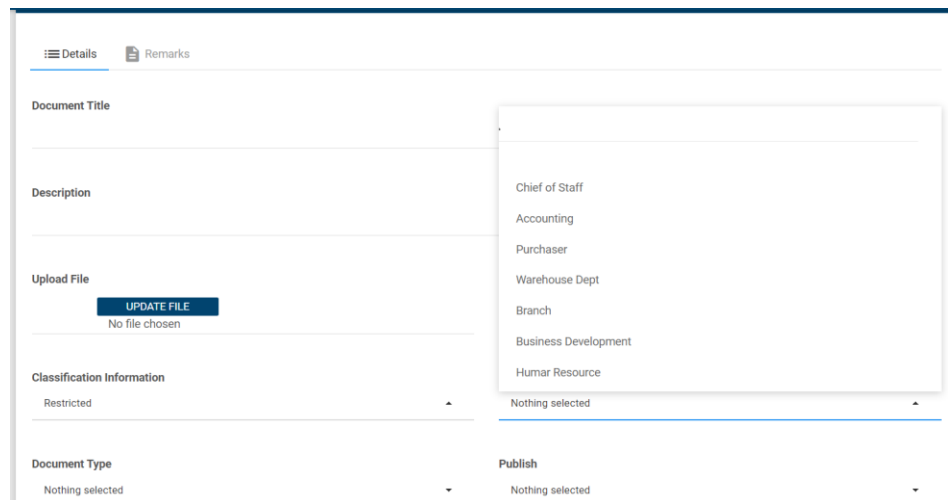


Figure 11. Uploading of Document

In the process of adding the documents, before saving them, the backend encrypts the file and locates it in the file database. Figures 12 and 13 illustrate the result and the algorithm of the encrypted document.

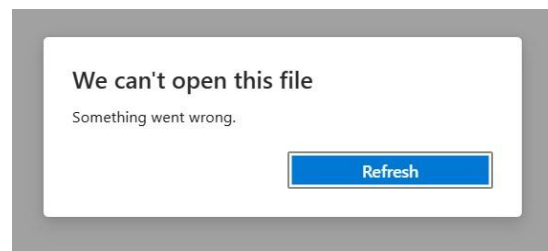


Figure 12. Output of Encrypted Document

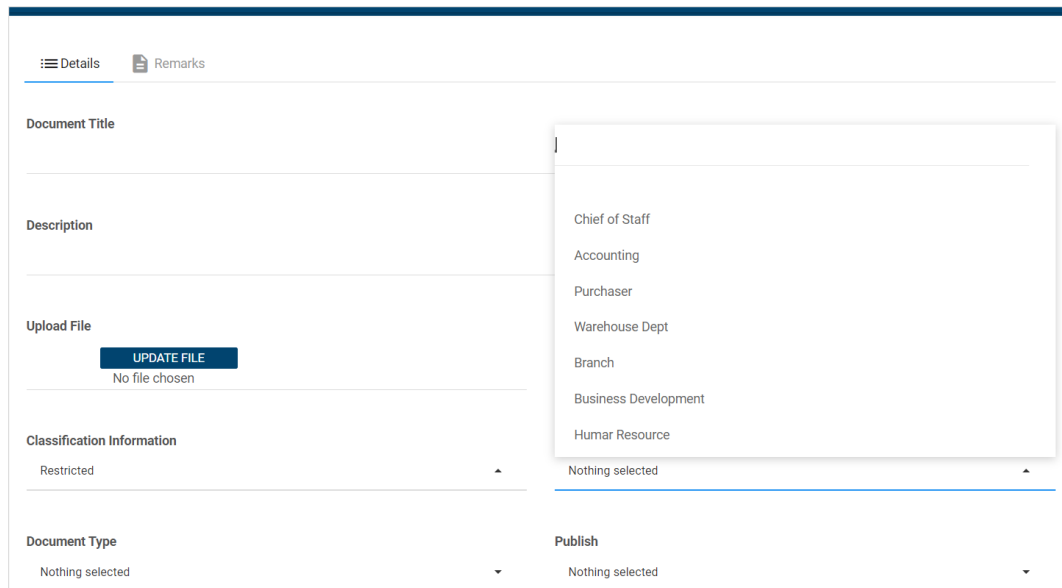
The author implied a PHP function for file encryption and decryption that takes the file name, source, or input file as input and returns the key used during the procedure (see Figure 13). The code was developed using the AddRoundKey, SubBytes, ShiftRows, and MixColumns functions in conjunction with the AES library and AES-CTR or counter mode library. One way that block ciphers operate is through the AES-Counter Library. This method allows the encryption and decryption procedures to run in parallel and allows for random access to the encrypted data. The pseudo-random values generated by a counter in the AES-CTR mode are XORed with the plaintext to create the ciphertext.

```
<?php
require 'lib/aes.php';
require 'lib/aesctr.php';

function encrypt($pdfName, $inputFile, $key) {
    $nameFile = file_get_contents($inputFile);
    $encFile = AesCtr::encrypt($nameFile,$key,128);
    $enkrip = file_put_contents("../file_store/".$pdfName), $encFile);
}

function decrypt($pdfName, $inputFile, $key){
    $nameFile = file_get_contents($inputFile);
    $encFile = AesCtr::decrypt($nameFile,$key,128);
    $senkrip = file_put_contents("file_store/decrypt/".$pdfName), $encFile);
}
?>
```

Figure 13. AES Encryption and Decryption Sample Function Algorithm using PHP Programming



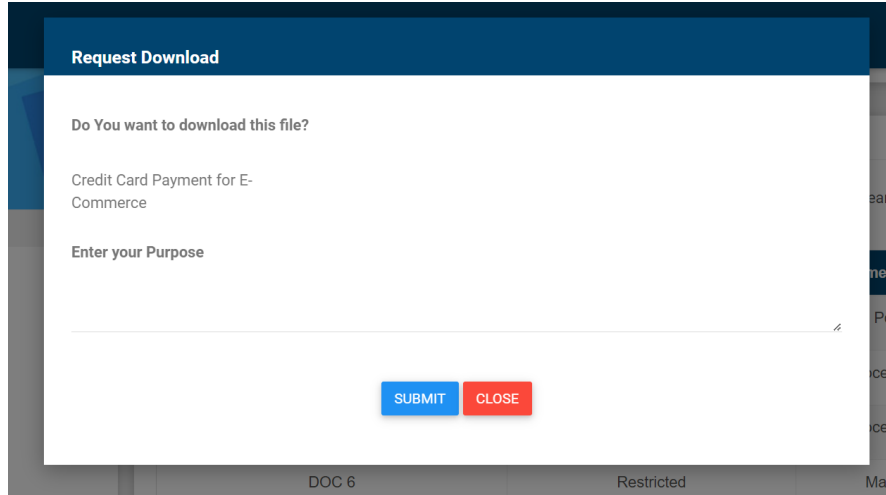
The screenshot displays a web-based 'Access Control' form. It includes sections for 'Details' and 'Remarks'. The form fields are: 'Document Title' (text input), 'Description' (text input), 'Upload File' (with an 'UPDATE FILE' button and 'No file chosen' status), 'Classification Information' (a dropdown menu currently showing 'Restricted' and a list of roles/designations), and 'Document Type' (a dropdown menu showing 'Nothing selected'). A secondary dropdown menu is open next to 'Classification Information', listing roles: 'Chief of Staff', 'Accounting', 'Purchaser', 'Warehouse Dept', 'Branch', 'Business Development', and 'Humar Resource' (sic). Below this list is a 'Nothing selected' option.

Figure 14. Access Control

From Figure 14 access control, we have three options in the classification information: confidential, restricted, and internal. When the admin selects a restricted type, the system will show a drop-down list of designations. The user can select which designation is intended for a specific document. Multiple selections of roles or designations will be saved as an array type in the database. The system will convert the retrieval of multiple roles given in one

document to an array so that the system can check whether the authenticated user has permission to access the document.

The document is assigned in confidential and restricted types, and the system will allow the users to request a particular document, as shown in Figure 15. It should be submitted with their intention on the documents or their purpose. After request submission, the system admin can view and evaluate their request.



Request Download

Do You want to download this file?

Credit Card Payment for E-Commerce

Enter your Purpose

SUBMIT **CLOSE**

DOC 6 Restricted Man

Figure 15. Permission Control

The system administrator can view analytics in the dashboard depending on the user's action (see Figure 16). The system provided a communication module for them to follow up on a specific document, which is counted when the system has received user messages. However, in the card New Request, the system will count how many pending document requests have been received by the system. On the Approved request and Declined Request, the system will count how many documents have been approved or declined by the system administrator. The system can also provide a trend line chart for the downloaded files based on today's, yesterday's, and last week's downloaded files. The top document type card is based on the files requested by the users. On the other hand, the Visited Users card will show the number of users who visited the IDMS based on Today, Yesterday, Last week, Last month, Last Year, and All Visited Dates.

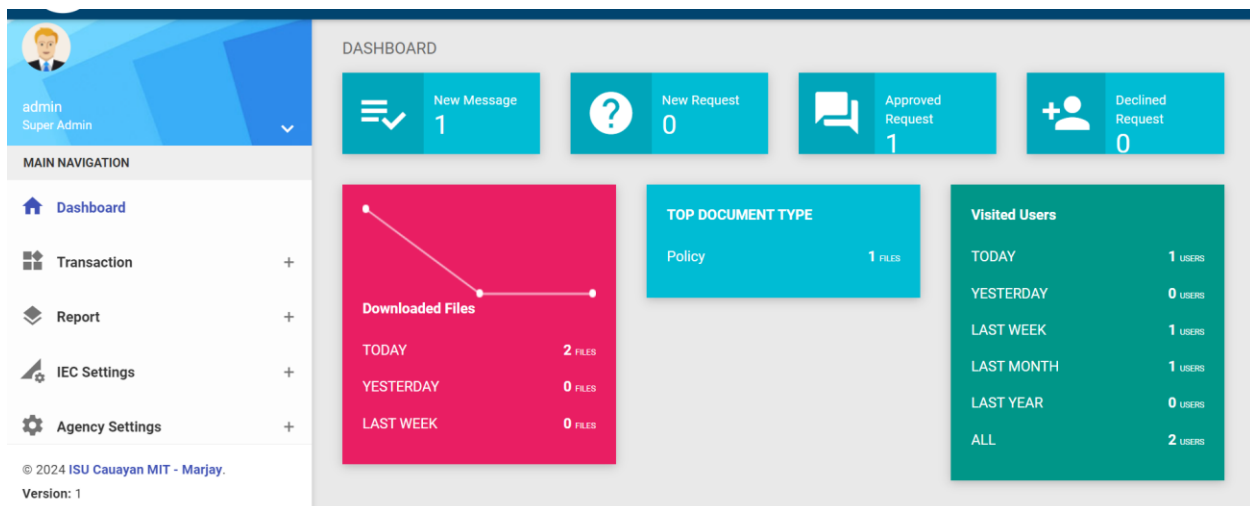
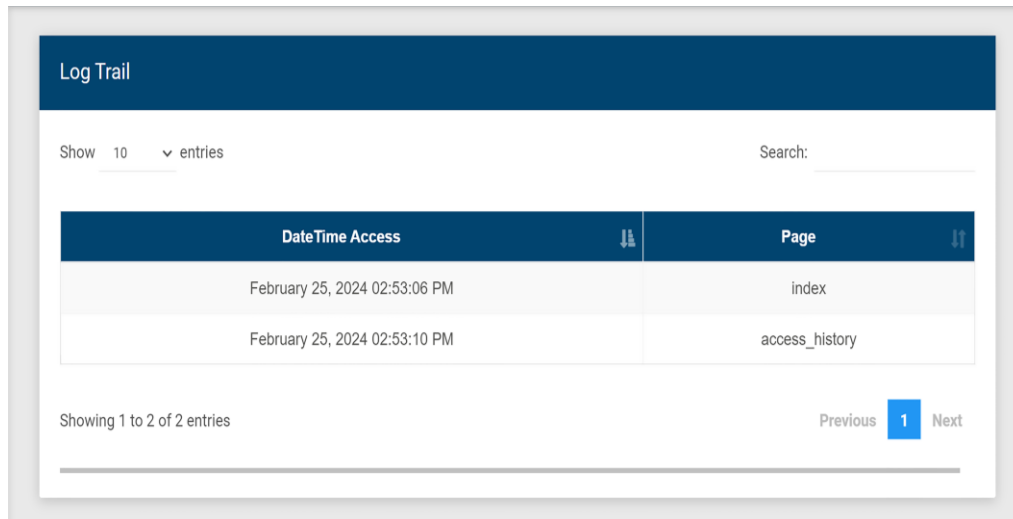


Figure 16. Dashboard

Figure 17 displays the user interface of a log trail module designed to track and record user activity within a system. The log trail module organizes data in a table format, providing a clear and accessible layout. It includes a "Show Entries" dropdown, allowing users to customize the number of entries displayed per page, and a search box for finding specific log entries quickly. The table features two columns: "DateTime Access," which records the exact date and time of page accesses, and "Page," which lists the specific pages visited.



The screenshot shows a web interface titled "Log Trail". At the top, there is a "Show 10 entries" dropdown and a "Search:" input field. Below this is a table with two columns: "DateTime Access" and "Page". The table contains two rows of data. At the bottom of the interface, it says "Showing 1 to 2 of 2 entries" and has "Previous", "1", and "Next" navigation links.

DateTime Access	Page
February 25, 2024 02:53:06 PM	index
February 25, 2024 02:53:10 PM	access_history

Figure 17. Users Log Trail

Security Analysis

A comparison of all encrypted files based on their output size in Table 2 reveals no significant differences. Compared to their initial size, every file has grown by around 33%. The 116 kb original file size was raised by 32.76% to 154 kb in comparison. Also enlarged by 33% over the initial size are 510 kb, 1075 kb, and 1710 kb.

Table 3 displays a comparative study of each access control model. Each model exhibits varying levels of granularity, ease of administration, flexibility, scalability, security, and adaptability. Each model has its strengths and weaknesses, highlighting the importance of selecting the most suitable model based on specific organizational needs and requirements.

Table 4 displays a comparative study of every cryptographic method. Upon analyzing the characteristics of various encryption algorithms, including AES, DES, 3DES, RSA, Blowfish, Twofish, and RC4, it is evident that each algorithm offers unique features and trade-offs in terms of key size, block size, security, performance, and usage. Each algorithm has its strengths and weaknesses, making it crucial to select the most suitable algorithm based on the application or system's specific security and performance requirements.

Table 2

AES-128 encrypted output file size

Original File Size	Output Size	Increase File Size
116kb	154kb	32.76%
510kb	679kb	33.14%
1075kb	1433kb	33.30%
1710kb	2279kb	33.27%

Table 3

Comparative analysis of each Access control model

Criteria	DAC (Golightly et. al., 2023)	MAC (Parkinson & Khan, 2022)	RBAC (Karatas & Akbulut, 2018)
Granularity	High	Very High	High
Ease of Administration	Easy(Managed by resource owners)	Challenging(Requires label Management)	Easy(Managed by role assignments)
Flexibility	Highly(Customized Permission)	Low(Rigid Security Labels)	Moderate(Structured roles)
Scalability	Limited Scalability in large systems	More scalable with a hierarchy	Good scalability with roles
Security	Depends on resource owners' discretion	High (Strict enforcement)	Good(Structured role-based)
Adaptability	Adaptable with effective management	Less adaptable due to rigid labels	Adaptable with well-defined roles

Table 4

Comparative analysis of each cryptographic algorithm

Algorithm	Designed by	Key Size	Block Size	Security	Performance	Usage	Reference
AES	Vincent Rijmen, Joan Daemen in 2001	128/192/256 bits	128 bits	High	Fast	Secure	(Smid, 2021)
DES	IBM in 1975	56 bits	64 bits	Low	Slow	Legacy	(Al-hazaimeh et. al., 2023)
3DES	IBM in 1978	112/168 bits	64 bits	Medium/Fair	Slow	Legacy	(Gurpreet & Supriya, 2023)
RSA	Ron Rivest, Adi Shamir, Leonard Adleman In 1978	Variable	Variable	High	Slow	Public Key	(Patil et al., 2016)
Blowfish	Bruce Schneier in 1993	32-448 bits	64 bits	Medium/Fair	Fast	Secure	(Malika, 2020)
Twofish	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson in 1998	128/192/256 bits	128 bits	High	Fast	Secure	(Gaur et al., 2019)
RC4	Ronald Rivest 1987	Variable	Variable	Low	Fast	Stream Cipher	(Jindal & Singh, 2015)

CONCLUSION

Integrating Cryptography, Role-Based Access Control (RBAC), and Information Classification models provides a robust defense against data breaches. The proliferation of extensive data has amplified the need for adequate information security and encryption techniques. This study has focused on enhancing an Intranet Document Management System (IDMS) with Advanced Encryption Standard (AES) encryption to fortify the security and integrity of sensitive data. AES encryption significantly enhances the security of private documents by utilizing its controlled 128-bit key strength. Moreover, secure key management practices and encryption technologies ensure protection against unauthorized access. RBAC further enhances security by simplifying access control administration

and ensuring users access only necessary resources for their roles. The information classification model is a crucial component in the security framework, providing a structured approach to categorizing and handling information based on its sensitivity and importance. These measures are crucial in environments where privacy and document security are paramount.

REFERENCES

- Abang, K. R., Gatmaitan, D. V., Manalo, F. R., Torcelino, M. R., Rodriguez, R. L., & Serrano, E. A. (2022). CCT Online Request of Students Credentials, A Document Management System for Private HIEs in the Philippines. In *2nd International Conference in Information and Computing Research (iCORE)*. <https://doi.org/10.1109/iCORE58172.2022.00024>
- Al-hazaimeh, O. M., Al-Shannaq, M. A., Bawaneh, M. J., & Nahar, K. M. (2023). Analytical Approach for Data Encryption Standard Algorithm. *International Journal of Interactive Mobile Technologies (IJIM)*, 17(14), 126–143. <https://doi.org/10.3991/ijim.v17i14.38641>
- Bergstrom, E., Karlsson, F., & Åhlfeldt, R. (2021). Developing an information classification method. *Information and Computer Security*, 29(2), 209-239. <https://doi.org/10.1108/ICS-07-2020-0110>
- Bosch, J., & Jansen, A. (2005). Software architecture as a set of architectural design decisions. In *5th Working IEEE/IFIP Conference on Software Architecture (WICSA'05)*. <https://doi.org/10.1109/WICSA.2005.61>
- Cao, J., Ren, L., Shi, W., & Yu, Z. (2014). A framework for component selection in collaborative sensing application development. In *2014 International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*. <https://doi.org/10.4108/icst.collaboratecom.2014.257552>
- Chen, S., Hu, W., & Li, Z. (2019). High performance data encryption with AES implementation on FPGA. In *2019 IEEE 5th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC) and IEEE International Conference on Intelligent Data and Security*. <https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2019.00036>
- Fang, J., Li, L., Jiang, J., Gan, L., Zheng, W., Fu, H., & Yang, G. (2017). SW-AES: Accelerating AES algorithm on the Sunway TaihuLight. In *2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC)*. <https://doi.org/10.1109/ISPA/IUCC.2017.00181>
- Fugini, M., & Finocchi, J. (2018). Innovative big data analytics: A system for document management. In *2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. <https://doi.org/10.1109/WETICE.2018.00058>
- Gangadari, B. R., & Rafi Ahamed, S. (2016). Design of cryptographically secure AES like S-Box using second-order reversible cellular automata for wireless body area network applications. *Healthcare Technology Letters*, 3(3), 177–183. <https://doi.org/10.1049/htl.2016.0033>
- Garcia, D. (2015). Performance evaluation of Advanced Encryption Standard algorithm. In *2015 Second International Conference on Mathematics and Computers in Sciences and in Industry (MCSI)*. <https://doi.org/10.1109/MCSI.2015.61>
- Gaur, S. S., Kalsi, H. S., & Gautamm, S. (2019). A Comparative Study and Analysis of Cryptographic Algorithms: RSA, DES, AES, BLOWFISH, 3-DES, and TWOFISH. *International Journal of Research in Electronics and Computer Engineering*, 7(1), 996-999.
- Golightly, L., Modesti, P., Garcia, R., & Chang, V. (2023). Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN. *Cyber Security and Applications*, 1, 100015. <https://doi.org/10.1016/j.csa.2023.100015>
- Gurpreet, S., & Supriya. (2023). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. *International Journal of Computer Applications*, 67(19), 33-38. <https://doi.org/10.5120/11507-7224>
- Hao, T. (2015). The information security analysis of digital library. In *2015 8th International Conference on Intelligent Computation Technology and Automation (ICICTA)*. <https://doi.org/10.1109/ICICTA.2015.250>
- Imen, A., & Belhassen, Z. (2018). A semantic model for document management in business processes. In *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*. <https://doi.org/10.1109/WAINA.2018.00107>

- Irwin, L. (2022, August 30). What is ISO 27001 information classification. IT Governance. <https://www.itgovernance.co.uk/blog/what-is-information-classification-and-how-is-it-relevant-to-iso27001>
- Jindal, P., & Singh, B. (2015). RC4 encryption-a literature survey. In *International Conference on Information and Communication Technologies (ICICT 2014)*. <https://doi.org/10.1016/j.procs.2015.02.129>
- Joseph, R. (2018). Data breaches: Public sector perspectives. *IT Professional*, 20(4), 57-64. <https://doi.org/10.1109/MITP.2017.265105441>
- Juxiang, R., & Zhihong, N. (2012). Taking database design as trunk line of database courses. In *2012 Fourth International Conference on Computational and Information Sciences*. <https://doi.org/10.1109/ICCIS.2012.310>
- Karataş, G., & Akbulut, A. (2018). Survey on access control mechanisms in cloud computing. *Journal of Cyber Security and Mobility*, 7(1), 1-36. <https://doi.org/10.13052/2245-1439.731>
- Kuai, J., & Li, L. (2020). File encryption system based on the hybrid LPC coefficient and AES algorithm. In *2020 International Conference on Wireless Communications and Smart Grid (ICWCSG)*. <https://doi.org/10.1109/ICWCSG50807.2020.00008>
- Lee, T., & Iio, J. (2015). Document management system based on ISAD(G). In *2015 18th International Conference on Network-Based Information Systems (NBIS)*. <https://doi.org/10.1109/NBiS.2015.103>
- Lin, Y., Xia, X., & Yang, J. (2021). Document encryption method with mechanism of Enigma machine. In *2021 International Conference on Artificial Intelligence, Big Data and Algorithms (CAIBDA)*. <https://doi.org/10.1109/CAIBDA53561.2021.00061>
- Liu, F. (2021). Analysis on the information management of university electronic document in the big data era. In *2021 International Conference on Internet, Education and Information Technology (IEIT)*. <https://doi.org/10.1109/IEIT53597.2021.00037>
- Malika, A. (2020). Comparative study of Blowfish. *International Journal of Innovative Science and Research Technology*, 5(2), 235-238. <https://www.ijisrt.com/assets/upload/files/IJISRT20FEB013.pdf>
- Nyame, G., & Qin, Z. (2020). Precursors of Role-Based Access Control Design in KMS: A Conceptual Framework. *Information*, 11(6), 334. <https://doi.org/10.3390/info11060334>
- Osman, M., & Zaharin, M. (2018). Ambiguous Software Requirement Specification Detection: An Automated Approach. In *2018 IEEE/ACM 5th International Workshop on Requirements Engineering and Testing (RET)*. <https://www.computer.org/csdl/proceedings-article/ret/2018/574901a033/13bd1sx4ZsU>
- Parkinson, S., & Khan, S. (2023). A survey on empirical security analysis of access control systems: A real-world perspective. *ACM Computing Surveys*, 55(6), 123. <https://doi.org/10.1145/3533703>
- Patil, P., Narayankar, P., D.G., N., & S.M., M. (2016). A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. In *Proceedings of the International Conference on Computer Science*. <https://doi.org/10.1016/j.procs.2016.02.108>
- Raigoza, J., & Jituri, K. (2016). Evaluating performance of symmetric encryption algorithms. In *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*. <https://doi.org/10.1109/CSCI.2016.0258>
- Reddy, R., & Gopu, S. (2017). Enterprise digital rights management for document protection. In *2017 31st International Conference on Advanced Information Networking and Applications: Workshops (WAINA)*. <https://doi.org/10.1109/WAINA.2017.48>
- Sharma, V., & Tiwari, A. K. (2021). Study on User Interface and User Experience Designs and Its Tools. *World Journal of Research and Review*, 12(6), 41-43. https://www.wjrr.org/download_data/WJRR1206016.pdf
- Smid, M. E. (2021). Development of the Advanced Encryption Standard. *Journal of Research of the National Institute of Standards and Technology*, 126, 126024. <https://nvlpubs.nist.gov/nistpubs/jres/126/jres.126.024.pdf>