Jurnal Mandiri IT
Vol. 14 No. 3, January (2026), pp. 381-391

ISSN 2301-8984 (Print), 2809-1884 (Online)
Published by Institute of Computer Science

Digital archiving using AES-256 encryption and role-based access control to strengthen data security at Pusdatin

Muhammad Naufal Arits Fikri[1], Nisrina Labiba Sarwoko[2], Sembada Denrineksa Bimorogo[3], Nadiza Lediwara[4], Aulia Khamas Heikhmakhtiar[5]
[1,2,3,4,5] Informatics, Republic of Indonesia Defense University, Bogor, Indonesia

A R T I C L E I N F O

Article history:

Received Dec 28, 2025
Revised Jan 20, 2026
Accepted Jan 13, 2026

Keywords:

AES 256;
Data Security;
Encryption;
Role-Based Access Control.

ABSTRACT

The rapid development of digital technology requires organizations, particularly government agencies, to implement robust and reliable data security systems. Data security is critical as the information managed is not only operationally valuable but also strategic and sensitive. The Center for Data and Information (Pusdatin) of the Ministry of Defense of the Republic of Indonesia plays a key role in managing and safeguarding defense-related data used for strategic decision-making. Based on observations and interviews, the existing data security system is considered adequate; however, several technical weaknesses remain, particularly in file management mechanisms and unstructured user access controls, which may lead to risks of data leakage and misuse. Therefore, this study aims to enhance data and file security through the implementation of Advanced Encryption Standard (AES-256) encryption and Role-Based Access Control (RBAC). This research employs the Waterfall method for system development, including analysis, design, implementation, and testing stages. System evaluation is conducted using functional testing and access control validation to assess the effectiveness of the implemented security mechanisms. The results indicate that AES-256 successfully ensures data confidentiality and integrity, while RBAC effectively restricts user access according to predefined roles, thereby reducing unauthorized access risks. The proposed system demonstrates improved data security and management efficiency, supporting a secure, efficient, and sustainable defense information system at Pusdatin

Corresponding Author:

Muhammad Naufal Arits Fikri,
Informatics,
Republic of Indonesia Defense University ,
Kawasan IPSC Sentul, Sukahati, Citeureup, Bogor Regency, West Java, 16810, Indonesia.
Email: naufalarits35@gmail.com

1. INTRODUCTION

In a connected digital era, data security has become an essential foundation for organizations and government institutions. The rapid flow of information and dependence on online systems present both opportunities and serious risks, such as data leaks and cyberattacks. These threats can cause financial loss, damage reputations, and disrupt stability. Therefore, a deep understanding of data security strategies and implementation is a crucial step to ensure that strategic information remains protected amidst dynamic technological developments. According to Ujung & Nasution (2023) Database security is a vital process in ensuring that data stored within a database remains protected and its availability is maintained. Furthermore, Mushtaq & Shah (2025) emphasize that online security has become one of the main pillars in the ever-evolving digital ecosystem, especially with the emergence of new media that enables faster and more widespread interaction and information exchange.

System security, information and data are the most important assets within an organization or company This view is consistent with cybersecurity resilience studies that identify organizational data and information systems as strategic assets requiring continuous protection through well-designed security mechanisms (Patterson et al., 2023). Such critical assets must have their security guaranteed and must possess a system that continuously protects them. Information and data are vital assets that must be protected through reliable security systems to remain safe from threats; In line with the findings of these researchers, data protection requires the implementation of structured and layered security to ensure information remains secure amidst technological developments (Arenas et al., 2023; Yousefnezhad et al., 2023). Strict database management is necessary to ensure every piece of information is properly stored and always available when needed. At the same time, the rapid growth of digital media and online interaction demands the strengthening of online security so that information exchange does not become a vulnerability for cyberattacks. Furthermore, Bumalod & Velasco (2024) state that as the most vital assets for an organization, information and data must be safeguarded through systems capable of guaranteeing confidentiality, integrity, and availability. With a comprehensive approach across all layers, threats of data leakage, manipulation, and misuse can be minimized even as the digital ecosystem continues to evolve .

The Center for Data and Information (Pusdatin) of the Ministry of Defense of the Republic of Indonesia is a working unit that plays a vital role in maintaining the security of defense information systems. Pusdatin is responsible for the development and management of defense information systems, the provision and maintenance of information and communication technology infrastructure, the security of information systems and cryptography, as well as the guidance of functional positions for computer administrators and cryptographers. With this mandate, Pusdatin has the obligation to maintain the availability, confidentiality, and integrity of data, which serves as the primary support in every strategic decision-making process. In today's digital era, the security of data and files is a critical aspect that cannot be ignored, especially as it concerns the protection of defense information that is critical and strategically valuable to the nation. Every piece of stored data is not only the basis for defense policy and operations but is also a vital asset that, if disrupted, leaked, or manipulated, could have serious impacts on the continuity of the defense system, organizational stability, and public trust. Therefore, the implementation of strict security standards, layered supervision, and increased awareness among all stakeholders is an absolute necessity to ensure that data integrity, availability, and confidentiality remain optimally maintained.

Based on interviews with employees at Pusdatin, the current data security is considered sufficiently secure. However, several technical aspects still need to be improved to maintain efficiency and minimize potential vulnerabilities in the future. Various challenges are still found in file and document management, such as insecure storage, vulnerability to data leaks, and the threat of cyberattacks. These conditions not only reduce operational efficiency but also potentially weaken the information defense system that should serve as the primary layer of protection. Furthermore, Logrippo (2025) states that interview results show that user access settings are not yet fully structured. Some authorization processes and the distribution of access rights are still carried out manually or inconsistently, creating loopholes that could be exploited by unauthorized parties. The lack of clarity in the distribution of access levels between user roles increases the risk of data leakage or misuse and complicates control when a security incident occurs. To address these access control challenges, Role-Based Access Control (RBAC) implemented within a centralized Identity and Access Management (IAM) system has been widely recognized as an effective solution. RBAC enables structured and consistent authorization by assigning access rights based on predefined user roles, thereby reducing human error and minimizing unauthorized access. The integration of RBAC into a centralized IAM framework also improves scalability, auditability, and security governance across organizational systems (Talluri et al., 2023).

One of the technologies proven effective for protecting confidential information in various applications is the Advanced Encryption Standard (AES). Comparative studies between asymmetric and symmetric cryptographic algorithms have shown that AES provides better efficiency and lower computational overhead compared to asymmetric algorithms such as RSA, particularly for large-scale data encryption (Parekh & Maru, 2025). The robustness of the Advanced Encryption Standard is further supported by comprehensive surveys that analyze its internal architecture, security strength, key management mechanisms, and extensive real-world applications, while also discussing its resilience and challenges in the post-quantum era, indicating that AES remains a reliable encryption standard for modern information systems (Ganesh et al., 2025). As a result, AES is widely

adopted in information systems that require high security without compromising system performance (Alvi Sholikhatin et al., 2022). Its implementation is extensively utilized in software to encrypt sensitive data, including support for smart industry-based systems such as smart manufacturing (Nasrullah, 2025). According Naimnule et al (2025) The AES algorithm is easy to implement, offers a high level of security, and uses minimal memory during its operation, thereby not overloading the processing or file size. In line with this Nirwan et al (2024), emphasize that encrypted files become significantly more secure from theft; even if the files are successfully taken, their contents remain inaccessible and cannot be manipulated. With these advantages, AES becomes a vital component in supporting the layered security strategy required to protect strategic information in the digital era.

Several previous studies confirm that the AES algorithm is proven effective in protecting sensitive data in various information systems. Furthermore Pandu Cahyo Sukoco & Afwan Anggara (2022) Implemented AES in the design of a web-based archive management application using the prototyping method. AES is used as an encryption mechanism for digital documents, ensuring that archives previously stored conventionally become secure, easy to search, and protected from the risk of loss or damage. Consequently, the resulting digital archive system is able to increase document management efficiency while closing data leakage gaps. Another study by Fatchur Shofyan & Rizky Tahara Shita (2024) utilized AES-256 CBC combined with Personal Access Token authentication on employee web services. Here, AES functions to encrypt every data exchange process and protect employee information from data theft as well as Distributed Denial of Service (DDoS) attacks. In addition, previous research has demonstrated that combining AES with message authentication mechanisms can further enhance system security. The combination of AES and HMAC SHA-256 has been successfully applied to secure URL parameters against SQL injection attacks, ensuring not only data confidentiality but also integrity and authenticity during transmission. These findings indicate that AES-based encryption can be strengthened through cryptographic validation mechanisms to mitigate common web-based attack vector(Gagan Akhmad Fauzi & Alam Rahmatulloh, 2025). The implementation results show that the system becomes more secure and can detect threats early through activity log monitoring.

Meanwhile, Nizamuddin Aulia Kafa & Dolly Virgian Shaka Yudha Sakti (2024) combining AES-256 with Huffman compression for the security of teacher, student, grade, and financial data at SMK Satria. AES is used to encrypt all school archives, while Huffman compression reduces file sizes, ensuring the resulting application not only maintains data confidentiality and integrity but is also efficient in terms of storage. A similar approach was also conducted by utilizing AES in e-learning site authentication tokens to close Cross-Site Scripting (XSS) vulnerabilities, with test results showing that two high-category vulnerabilities were successfully eliminated without overloading the processing or file size. Furthermore, Hussein & Naser (2025) implementing AES-256 in a web-based village information system to secure population data from threats such as SQL Injection, brute-force attacks, and sniffing. This implementation is proven to maintain the confidentiality, integrity, and availability of village data while simultaneously increasing public trust in village digitalization programs.

However, based on a review of previous studies, most existing research focuses on the implementation of AES-based encryption in general-purpose information systems such as educational platforms, village information systems, web services, and digital archives. These studies primarily emphasize data confidentiality through encryption mechanisms, while aspects of structured access control and role hierarchy management are often treated separately. Moreover, the integration of cryptographic security mechanisms with Role-Based Access Control (RBAC) in highly sensitive government defense environments remains limited. In particular, there is a lack of studies that specifically address the combined implementation of AES encryption and RBAC within defense-oriented government institutions, where data sensitivity, access hierarchy, and accountability requirements are significantly higher than in public or commercial systems.

This study emphasizes that data security is a primary pillar in maintaining the continuity and trust of an institution, particularly at the Center for Data and Information (Pusdatin) of the Ministry of Defense, which handles defense information of strategic value. Field observations indicate that although the current data security is classified as secure, there are still technical gaps that can be improved to increase system efficiency and resilience. The implementation of AES is seen as an appropriate step because it is proven to have a high level of security, good memory efficiency, and ease of integration without overloading system performance.

This study positions itself uniquely by proposing an integrated digital archiving security model that combines Advanced Encryption Standard (AES-256) encryption and Role-Based Access Control (RBAC) within the operational context of a government defense institution, namely the Center for Data and Information (Pusdatin) of the Ministry of Defense of the Republic of Indonesia. Unlike previous studies that implement encryption or access control mechanisms independently, this research emphasizes a layered security approach that simultaneously protects data confidentiality, integrity, and access authorization in a strategic defense environment. This integration is essential given the hierarchical structure, critical data sensitivity, and strict access requirements inherent in defense information systems.

Therefore, this study aims to enhance the security of digital files and documents at the Center for Data and Information (Pusdatin) of the Ministry of Defense of the Republic of Indonesia through the integrated implementation of AES-256 encryption and Role-Based Access Control (RBAC). The specific objectives of this research are to strengthen data confidentiality and integrity through encryption mechanisms, regulate user access privileges based on predefined roles, and improve the efficiency and accountability of digital archive management within a defense information system environment;The scientific contributions of this study include the development of an integrated security model tailored for government defense institutions, empirical evidence of the effectiveness of combining AES-256 and RBAC in protecting strategic data, and practical insights that can serve as a reference for other government agencies in designing secure and sustainable digital archiving systems; By adopting a structured and layered security approach, this research supports the strengthening of data integrity, confidentiality, and availability while contributing to the advancement of secure digital transformation initiatives in the public sector.(Arun Kumar Akuthota, 2025; Gunjal & Sonawane, 2023; Singh et al., 2024). With a structured and layered security approach, this study is expected to play a role in maintaining the integrity, confidentiality, and availability of strategic data, while supporting safe and sustainable digital transformation efforts for government agencies.

2. RESEARCH METHOD

2.1 Research Design

This research utilizes the Waterfall development model as a framework for system design.

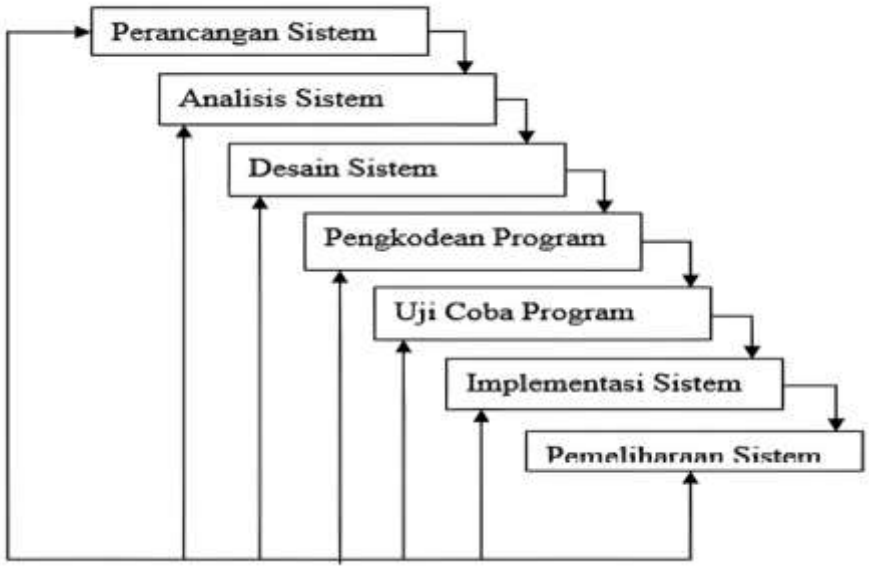

Figure 1. Waterfall Method
Source: Jurnal (Prahasti, 2022)

The Waterfall model describes a software development process that proceeds in a sequential and systematic manner, where each stage must be completed before moving on to the next. These stages include requirements analysis, system design, implementation, and testing, as shown in Figure 2.1. This approach is based on the assumption that system requirements can be clearly identified from the outset, allowing the development process to be more structured and

controlled. Modern simulation studies of the Waterfall lifecycle demonstrate how its staged progression enables project managers to estimate phase completion times and optimize resource allocation for higher predictability in software delivery (Saravanos & Curinga, 2023). Additionally, comparative analyses between structured and iterative methods confirm that while Waterfall's linear structure supports documentation and control, its rigid sequencing differs fundamentally from agile and hybrid frameworks, highlighting both strengths and limitations in practical application (Mishra & Alzoubi, 2023). By applying the Waterfall model, this research is expected to produce a system that is stable, well-documented, and easy to evaluate at each stage of its development.

2.2 Research Procedure

This research procedure applies a modified Waterfall model, which includes the stages of requirements analysis, system design, implementation, and testing. Requirements analysis was conducted through interview methods and direct observation to identify data security problems and access control issues at Pusdatin. Furthermore, during the system design stage, the primary focus was directed toward defining a secure file management architecture that integrates AES-256 encryption and Role-Based Access Control (RBAC) mechanisms. In this study, the Advanced Encryption Standard (AES) with a 256-bit key length is implemented using the Cipher Block Chaining (CBC) mode to ensure data confidentiality. Each file uploaded to the system is encrypted prior to storage, utilizing a randomly generated Initialization Vector (IV) for every encryption process to prevent pattern repetition. The encryption key is generated and managed securely at the application level and is only accessible to authorized system components. Decryption is performed dynamically when an authorized user requests access to a file, ensuring that plaintext data is never permanently stored on the server.

Role-Based Access Control (RBAC) is implemented as the primary authorization mechanism, where access rights are assigned based on predefined user roles. The RBAC mechanism operates by validating user roles during the authentication process and enforcing access restrictions before any file operation is executed. This integration ensures that encrypted files can only be accessed and decrypted by users with appropriate authorization.The implementation stage was realized through the development of a web-based prototype accompanied by the refinement of functional features, which then concluded with system testing to evaluate the performance of the functionality and the resulting security effectiveness.

2.3 Data Acquisition

Data were collected through interviews with Pusdatin staff, direct observation of existing data management processes, and documentation reviews. These methods were used to identify security gaps, workflow inefficiencies, and access control requirements.

2.4 System Modeling

The use case diagram in Figure 2.2 models the system functionality and user interactions within the file management system that implements the Role-Based Access Control (RBAC) mechanism.

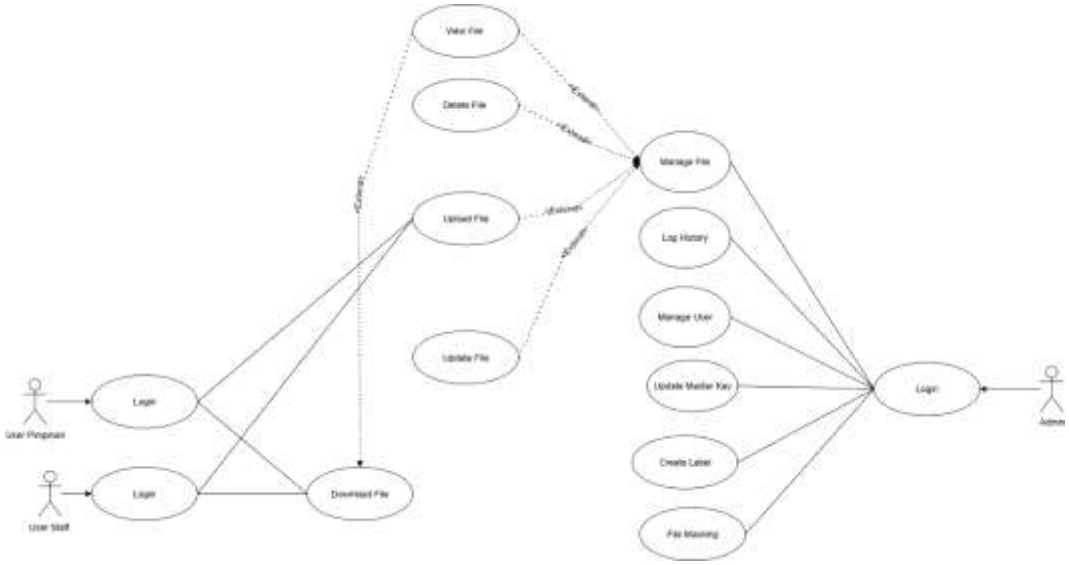

Figure 2. Usecase System
Source: Processed by the researcher

This modeling is used to describe the relationship between users and the primary system functions, such as the file upload process, access management, and file management based on user roles. The system involves three main actors: User Staff, User Pimpinan, and Admin, each having different roles and access rights. User Staff and User Pimpinan can log in, upload, download, and view files according to the granted authority, ensuring that data access remains controlled and aligned with the organizational structure. Meanwhile, the Admin has full access rights to manage the system, including the management of files, users, labels, encryption keys (master keys), and activity monitoring through log history. The extend relationship in the Manage File function indicates that the file management process consists of several derivative operations, such as creating, updating, deleting, and reviewing files. Overall, this use case modeling aims to ensure that each system function can only be accessed by authorized users, thereby enhancing the security, orderliness, and accountability of data management within the Pusdatin Kemhan RI environment.

The authorization flow within the system follows a structured RBAC mechanism. After a successful login process, the system identifies the user role and maps it to predefined access privileges. Every request to access, upload, modify, or delete files is validated against the user's assigned role. If the requested action does not match the authorized access rights, the system automatically denies the request and records the event in the system activity log. This authorization flow ensures that access control enforcement is consistent, auditable, and aligned with the organizational hierarchy of Pusdatin.

2.5TESTING METHOD

System testing was conducted to verify functional correctness and security mechanisms, including the implementation of access control and the file encryption process. This testing ensures that only authorized users can access encrypted files according to their predefined roles.

3. RESULTS AND DISCUSSIONS

3.1 SYSTEM IMPLEMENTATION RESULTS

The data management and security system was successfully implemented as a web-based application by applying AES-256 encryption and Role-Based Access Control (RBAC), as shown in Figure 3.1.

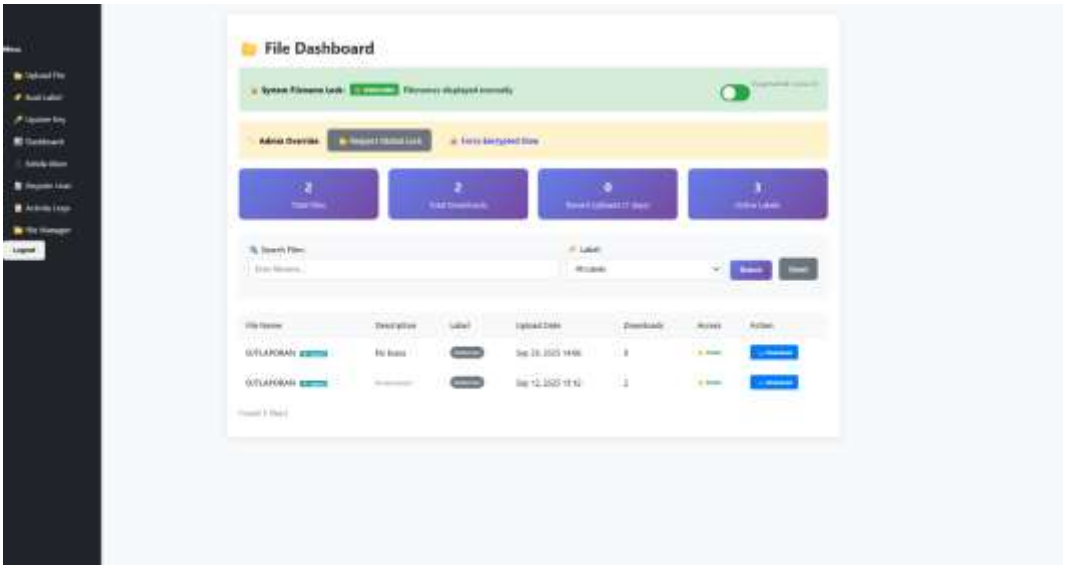

Figure 3. Dashboard
Source: Processed by the researcher

Every uploaded file undergoes an automatic encryption process before being stored in the database, ensuring that the file cannot be read without a valid decryption process. The system differentiates user access rights based on the roles of Admin, Pimpinan, and Staff, so that each user can only access features and data according to their authority.

Figure 4. Database
Source: Processed by the researcher

After the upload process, in figure 3.2 each file is automatically encrypted before being stored in the database to ensure data confidentiality and prevent unauthorized access. As illustrated in Figure X, the original file is transformed into an encrypted format using the Advanced Encryption Standard (AES) algorithm, resulting in unreadable ciphertext. The encrypted file data are then stored in the database as a Binary Large Object (BLOB), while metadata such as filename, MIME type, uploader identity, access level, and encryption status are stored in separate database fields.

This approach ensures that sensitive files are never stored in plaintext form within the database. Even if unauthorized parties gain access to the database storage layer, the file contents remain protected due to the encryption mechanism. Decryption is only performed dynamically when an authorized user with the appropriate access level requests the file, and the system verifies the user's role through the RBAC mechanism before granting access. This design strengthens data security by combining cryptographic protection with structured access control, ensuring confidentiality, integrity, and controlled availability of stored files.

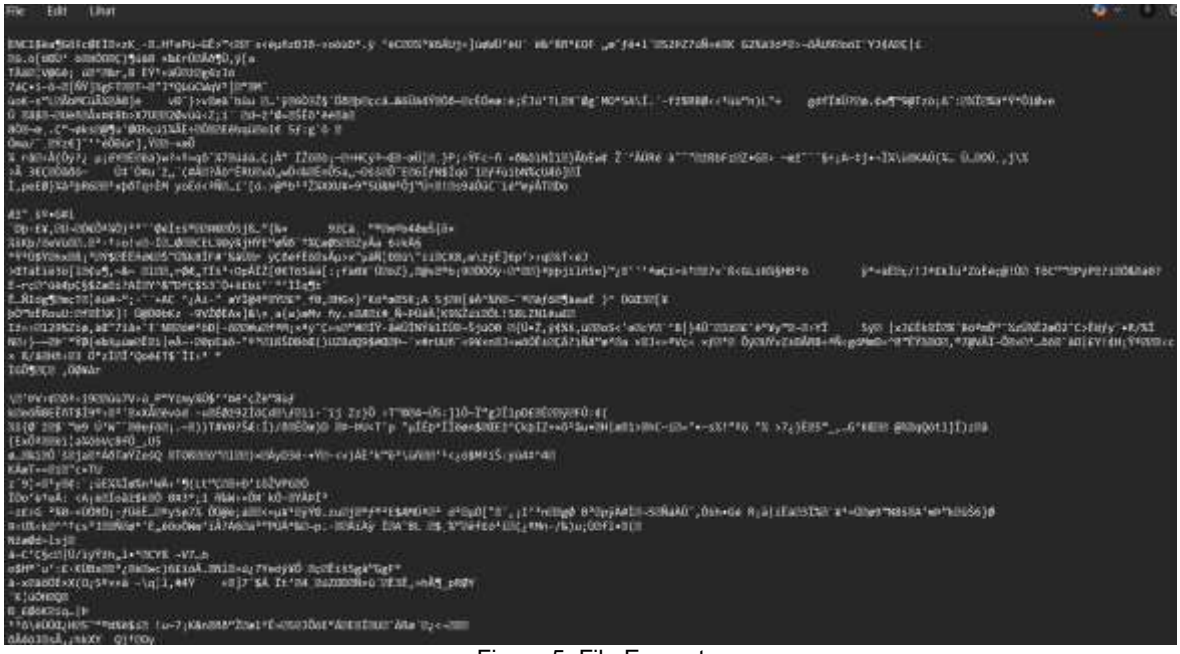

Figure 5. File Encrypt
Source: Processed by the researcher

A Figure 3.3 illustrates the output of a file after the encryption process has been applied using the Advanced Encryption Standard with a 256-bit key (AES-256). The original plaintext file is transformed into ciphertext, which appears as a sequence of random and unreadable characters when opened using a standard text editor. This visual representation confirms that the encryption process has been successfully executed, as the file content no longer preserves any recognizable structure or readable information from the original data. The encrypted file cannot be interpreted or reconstructed without the corresponding cryptographic key, thereby ensuring data confidentiality. This implementation prevents unauthorized users from accessing or manipulating the file contents, even if the encrypted file is obtained directly from the storage medium. Decryption is only performed by the system when a legitimate request is made by an authenticated and authorized user, whose access rights are validated through thel RBAC mechanism. The result demonstrates that AES-256 effectively protects sensitive documents by converting them into secure ciphertext, supporting a layered security architecture within the digital archiving system.

3.2 Database And Access Control Analysis

The system database structure is designed based on the Entity Relationship Diagram (ERD), which reflects the relationships between the main entities, namely Users, Files, Labels, Access Levels, Activity Logs, and System Settings, as shown in Figure 3.3.

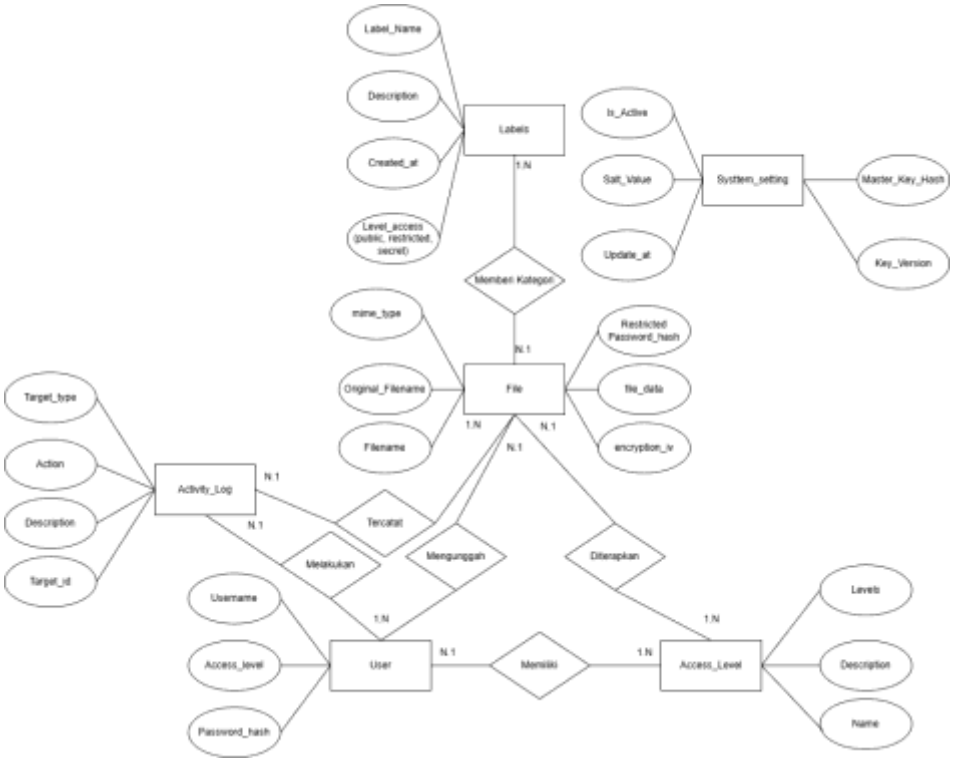

Figure 6. ERD
Source: Processed by the researcher

The relationships between tables are designed to support role-based access control mechanisms, where each file is associated with the uploading user and a specific access level. Additionally, the Activity Logs table is used to record all user activities as part of the system security audit. This database design ensures data consistency and activity traceability, while supporting the implementation of layered security.

3.3 System Testing Results

System testing was conducted using the black box testing method for all user roles, namely Admin, Pimpinan, and Staff. The testing results show that all primary system functions operate in accordance with the predefined requirements.

Tabel 1 System Testing Result

Role	Tested Features	Result
Admin	Login, File Management, Key Update, User Management, Log History, File Masking, Create Label, Update Master Key	Passed
Pimpinan	Login, Upload,Download File	Passed
Staff	Login, Upload, Download	Passed

Source: Processed by the researcher

The authentication process successfully validates user credentials, file format validation functions effectively, and the role-based access restriction mechanism is capable of preventing unauthorized access. This indicates that the system is functioning stably and securely.

3.4 Discussion

The implementation of AES-256 encryption and Role-Based Access Control (RBAC) in the file management system is proven to be capable of enhancing security and data access control. These results are consistent with previous research stating that the combination of symmetric encryption and role-based access control is effective in preventing data leaks and the misuse of access rights. With the presence of audit logs and encryption key updates, the system possesses a layered security level that meets the requirements for strategic data management.

4. CONCLUSION

This research successfully implemented a web-based digital data management system integrating AES-256 encryption and Role-Based Access Control (RBAC) to enhance information security at the Pusdatin of the Ministry of Defense of the Republic of Indonesia. The results demonstrate that the proposed system effectively ensures data confidentiality through symmetric encryption mechanisms and enforces structured authorization through role-based access control, thereby preventing unauthorized data access. From a scientific perspective, this study contributes to the field of information security by demonstrating the practical integration of cryptographic encryption and access control mechanisms within a government defense environment, which has been limitedly addressed in previous studies. Practically, the developed system supports improved data security governance by strengthening confidentiality, integrity, accountability, and access control management in government agencies handling sensitive information. IAM Despite its effectiveness, this study has several limitations. Performance evaluation was conducted on a limited-scale environment, and integration with national identity and access management () systems has not yet been implemented. Therefore, future research is recommended to include large-scale performance testing, deeper security threat simulations, integration with centralized government IAM infrastructures, and the exploration of post-quantum cryptography algorithms to enhance long-term security resilience. These directions are expected to ensure the sustainability and scalability of secure digital data management systems within government institutions.and serves as a foundational reference for high-level security implementations within government agencies.

ACKNOWLEDGEMENTS

The authors would like to express their gratitude to the Center for Data and Information (Pusdatin), Ministry of Defense of the Republic of Indonesia, for providing facilities, data access, and technical support during the research process. The support and cooperation greatly contributed to the successful completion of this study.

REFERENCES

Alvi Sholikhatin, S., Prayogo Kuncoro, A., Lutfia Munawaroh, A., & Gilang Aji Setiawan, dan. (2022). Comparative Study of RSA Asymmetric Algorithm and AES Algorithm for Data Security. *Edu Komputika Journal*, *9*(1), 60–67. http://journal.unnes.ac.id/sju/index.php/edukom

Arenas, L. A., Yactayo-Arias, C., Quispe, S. R., & Sandoval, J. L. (2023). Leveraging Security Modeling and Information Systems Audits to Mitigate Network Vulnerabilities. *International Journal of Safety and Security Engineering*, *13*(4), 763–771. https://doi.org/10.18280/ijsse.130420

Arun Kumar Akuthota. (2025). Role-Based Access Control (RBAC) in Modern Cloud Security Governance: An In-depth Analysis. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *11*(2), 3297–3311. https://doi.org/10.32628/cseit25112793

Bumalod, M. C., & Velasco, R. M. A. (2024). Synergistic Information Security Design Implementation based on Role-Based Access Control, Information Classification, and AES Cryptographic Encryption. *International Journal in Information Technology in Governance, Education and Business*, *6*(1), 68–85. https://doi.org/10.32664/ijitgeb.v6i1.136

Fatchur Shofyan, & Rizky Tahara Shita. (2024). Implementasi Web Service Restful API dengan Autentikasi Personal Access Tokens dan Algoritma AES 256. *Jurnal Ticom: Technology of Information and Communication*, *12*(3), 108–114. https://doi.org/10.70309/ticom.v12i3.130

Gagan Akhmad Fauzi, & Alam Rahmatulloh. (2025). Kombinasi AES dan HMAC SHA-256 untuk Pengamanan Parameter URL dari Serangan SQL Injection. *Jurnal Informatika Dan Multimedia*, *17*(1), 46–59. https://doi.org/10.33795/jtim.v17i1.6596

Ganesh, R., Khan, B. U. I., Khan, A. R., & Kamsin, A. Bin. (2025). A panoramic survey of the advanced encryption standard: from architecture to security analysis, key management, real-world applications, and post-quantum challenges. In *International Journal of Information Security* (Vol. 24, Issue 5). https://doi.org/10.1007/s10207-025-01116-x

Gunjal, M. B., & Sonawane, V. R. (2023). International Journal of INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING Multi Authority Access Control Mechanism for Role Based Access Control for Data Security in the Cloud Environment. *International Journal of Intelligent Systems and Applications in Engineering IJISAE*, *2023*(2s), 250–264. www.ijisae.org

Hussein, Z. A., & Naser, O. A. (2025). Evaluation of AES-256 encryption and machine learning for securing GSM communications against sniffing attacks. *Egyptian Informatics Journal*, *32*(July), 100832. https://doi.org/10.1016/j.eij.2025.100832

Logrippo, L. (2025). Data flow security in Role-based access control. *Journal of Information Security and Applications*, *90*(April), 103997. https://doi.org/10.1016/j.jisa.2025.103997

Mishra, A., & Alzoubi, Y. I. (2023). Structured software development versus agile software development: a comparative analysis. *International Journal of System Assurance Engineering and Management*, *14*(4), 1504–1522. https://doi.org/10.1007/s13198-023-01958-5

Mushtaq, S., & Shah, M. (2025). Threats to the Digital Ecosystem: Can Information Security Management Frameworks, Guided by Criminological Literature, Effectively Prevent Cybercrime and Protect Public Data? *Computers*, *14*(6). https://doi.org/10.3390/computers14060219

Naimnule, F. A., Hanoe, F. A. L., Banusu, M. N., Mano, M. O., Studi, P., Informasi, T., & Timor, U. (2025). Implementation of AES Encryption for Data Security on Web-Based Information Systems in Fafinesu A Village. *Sistem Kendali & Jaringan) E-ISSN*, *4*(3), 2808–3520. https://doi.org/10.58982/krisnadana.v4i3.836https://ejournal.sidyanusa.org/index.php/jkdn/index

Nasrullah, A. H. (2025). Secure Web-Based File Encryption Using AES-128. *Journal of Embedded Systems, Security and Intelligent Systems*, *6*(2), 146–155. https://doi.org/10.59562/jessi.v6i2.8436

Nirwan, S., Hamidin, D., & Azzalea, S. E. (2024). Implementation of AES-256 Algorithm for Encryption on Chatting Platforms. *Internet of Things and Artificial Intelligence Journal*, *4*(4), 616–624. https://doi.org/10.31763/iota.v4i4.804

Nizamuddin Aulia Kafa, & Dolly Virgian Shaka Yudha Sakti. (2024). Implementasi Kriptografi Berbasis Web dengan Algoritma Advanced Encryption Standard (AES) 256 dan Kompresi Huffman untuk Pengamanan File di SMK Satria. *Jurnal Ticom: Technology of Information and Communication*, *12*(2), 50–55. https://doi.org/10.70309/ticom.v12i2.109

Pandu Cahyo Sukoco, & Afwan Anggara. (2022). Web-Based Payroll Data Security Application Using the AES Cipher Method at the Mangga Dua Store Kebumen. *International Journal of Engineering Technology and Natural Sciences*, *4*(1), 42–51. https://doi.org/10.46923/ijets.v3i2.143

Parekh, S., & Maru, M. J. (2025). AES, DES, and RSA in Data Security: A Review. *International Journal of Scientific Research and Engineering Development*, *8*(5). www.ijsred.com

Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers and Security*, *132*. https://doi.org/10.1016/j.cose.2023.103309

Prahasti. (2022). Aplikasi Pelayanan Antrian Pasien Menggunakan Metode FCFS Menggunakan PHP dan MySQL. *Jurnal Media Infotama*, *18*(1), 341139.

Saravanos, A., & Curinga, M. X. (2023). Simulating the Software Development Lifecycle: The Waterfall Model. *Applied System Innovation*, *6*(6). https://doi.org/10.3390/asi6060108

Singh, J., Rani, S., & Kumar, V. (2024). Role-Based Access Control (RBAC) Enabled Secure and Efficient Data Processing Framework for IoT Networks. *International Journal of Communication Networks and Information Security (IJCNIS)*, *16*(2). https://doi.org/10.17762/ijcnis.v16i2.6697

Talluri, S., Anne, V. P., & Chadalavada, V. S. (2023). Role-Based Access Control (Rbac) in a Centralized Identity and Access Management (Iam) System. *International Journal of …*, *4*(1), 88–95. https://iaeme.com/Home/editorial_board/IJIT

Ujung, A. M., & Nasution, M. I. P. (2023). Pentingnya Sistem Keamanan Database Untuk Melindungi Data Pribadi. *Jurnal Sistem Informasi Dan Informatika*, *1*(2), 44–47. https://doi.org/10.47233/jiska.v1i2.929

Yousefnezhad, N., Malhi, A., Keyriläinen, T., & Främling, K. (2023). A Comprehensive Security Architecture for Information Management throughout the Lifecycle of IoT Products. *Sensors*, *23*(6), 1–21. https://doi.org/10.3390/s23063236