Journal of Information Systems and Informatics
Vol. 6, No. 4, December 2024 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v6i4.940 Published By DRPM-UBD

Design and Build a Notary MIS Using the AES 256 Algorithm at a Web-Based Notary Office

Arya Pratama Damanik[1], Suendri[2]

[1,2]Information Systems Study Program, State Islamic University of North Sumatra, Medan, Indonesia
Email: [1]aryapratamadmk@gmail.com, [2]suendri@uinsu.ac.id

Abstract

This research aims to design and develop a web-based Notary Management Information System (MIS) incorporating the AES 256 encryption algorithm to enhance data management and security in notary offices. Utilizing the Rapid Application Development (RAD) methodology, the system was developed through iterative collaboration between developers and users to meet both functional and non-functional requirements. Key features of the system include the management of order data, client records, notarial protocols, and user activity logs. The innovative application of the AES 256 algorithm ensures high-level data security, with validation tests confirming its effectiveness in protecting sensitive information. Performance testing demonstrated significant improvements, including a 40% reduction in data retrieval time and seamless encryption processes, compared to previous manual methods. The system also enhances accessibility and work efficiency through its web-based architecture. This research not only provides a practical solution for notary offices but also serves as a scalable model for secure MIS development in other industries.

Keywords: Notary, R&D, AES256

1. INTRODUCTION

In the era of modern world development, digitalization has become a key element in increasing the efficiency of various jobs. Many applications and systems have been developed to support the operations of companies, organizations and agencies, both on a small and large scale[1]. However, despite this progress, significant challenges arise regarding data security. The recent national data leak case shows that data that is not properly protected can be accessed by irresponsible parties. Therefore, every information system requires reliable data protection to prevent the risk of data theft or damage[2].

One area that really needs secure data management is the world of notary law. Notaries play an important role in providing legality and legal value to important documents, such as deeds, agreements and contracts[3]. Based on Article 1 number

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

1 of Law Number 2 of 2014 concerning the Position of Notaries, a notary is a public official who has the authority to make authentic deeds and is responsible for notarial protocols as state archives. This protocol must be stored properly because it is the lifetime responsibility of a notary (Article 65 UUUJN)[4].

In practice, managing notarial protocols which are still done manually creates a few problems, such as the ever-increasing accumulation of documents, the risk of losing documents due to disorganized storage, and vulnerability to physical damage to documents. This situation shows the need for a more modern, efficient and secure data management system.

The proposed solution is the development of a web-based management information system capable of digitizing the management of notarial protocols. This system not only makes recording, archiving and searching for documents easier, but also improves data security aspects through the application of the Advanced Encryption Standard (AES) 256 algorithm. This algorithm is known for its high level of security and uses a symmetric encryption method through four main stages: Sub Byte, Shift Rows, Mix Columns, and Add Round Key[5].

Previous research has discussed the development of management information systems in the notarial field. For example, research by Mutia Putri Nabila Lubis and Nur Ahmadi Rahmani developed a desktop-based information system to support notary office administration. However, this research is limited to local access without online features[6]. On the other hand, Aldi Maulana Akbar's research developed a mobile-based document management application that offers flexibility, but is still lacking in terms of security and the ability to handle large amounts of documents[7].

In contrast to previous research, this research will develop a web-based system that can be accessed online with tighter security features through the implementation of the AES 256 algorithm. This system is designed to answer the need for document management that is safe, efficient, and can be accessed from various locations with a connection. Internet.

Through this research, it is hoped that an effective and secure web-based management information system can be realized using the CodeIgniter framework, PHP programming language, and MySQL database. This system will be tested for its feasibility to ensure that the system can be the right solution to support the digitization of notary data management, while increasing protection for the confidentiality of managed documents.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

2. METHODS

This research uses the Rapid Application Development (RAD) method to build a web-based management information system, as shown in Figure 1. Rapid Application Development is a software development model that emphasizes speed and flexibility through an iterative and collaborative approach [8]. With its incremental (multi-layered) characteristics, the RAD method allows rapid system development with prototypes that are continuously refined until they reach the desired final result.

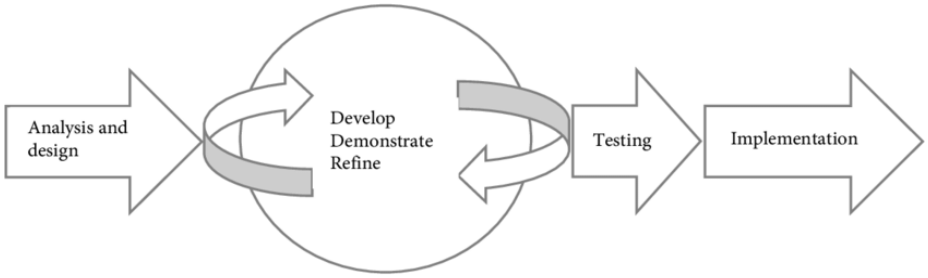

Figure 1. Rapid Application Development (RAD) Method

The RAD approach facilitates iterative collaboration between developers and users, so that user needs and input can be accommodated dynamically throughout the development process [9]. The following are the stages of implementing the RAD method in this research:

1) Requirements Planning

This stage involves identifying the application objectives and required information needs through observations and interviews. In this stage, intensive collaboration between researchers and end users (notaries) is very important to clearly understand user problems and needs. This activity aims to produce a comprehensive system requirements specification as a basis for the following stages.

2) Workshop Design RAD

At this stage, system modeling is carried out to analyze the needs that have been identified. An initial prototype of the system was developed using modeling tools such as Unified Modeling Language (UML) to visualize the system processes and structure. This prototype will be tested on users to get feedback. This process takes place repeatedly (iteratively) until the resulting system design meets user needs. This approach allows users to actively participate in system development thereby increasing the chances of successful implementation [9].

3) Implementation
This stage involves coding the system based on the agreed design. A web-based archiving information system was developed to simplify document grouping, file storage and data security. The system built is tested using the black-box testing method to ensure that each function runs according to predetermined specifications. This test compares the results of manual calculations with system output to ensure the validity and accuracy of system functionality[10].

2.1. Algorithm Advanced Encryption Standard 256

This research uses the Advanced Encryption Standard (AES) 256 algorithm to improve data security in web-based management information systems. AES was chosen as the encryption algorithm because of its proven reliability in various data security applications[10]. AES 256 is the strongest variant of this algorithm, with a 256-bit key length that provides very high protection against brute force attacks[11]. Several main reasons for choosing AES 256 over other encryption algorithms. First, AES 256 has the largest key length among AES variants (128-bit and 192-bit), thereby offering a higher level of security. Second, AES is an encryption standard that is widely adopted by governments, organizations, and industry around the world, including by the National Institute of Standards and Technology (NIST). Finally, despite offering a very high level of security, AES 256 is designed to remain efficient in terms of speed and resource consumption, both for hardware and software[12].

Table 1. AES Key Length

	Key length (Nk Words)	Block Size (Nb Words)	Number of Spins (Nr)
AES 128	4	4	10
AES 192	6	4	12
AES 256	8	4	14

After the system has been developed, testing is carried out to ensure that encryption runs correctly and all system features function according to specifications. The testing method used is Encryption and Decryption Phase Testing. This stage aims to ensure the data can be encrypted and decrypted correctly using AES 256.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

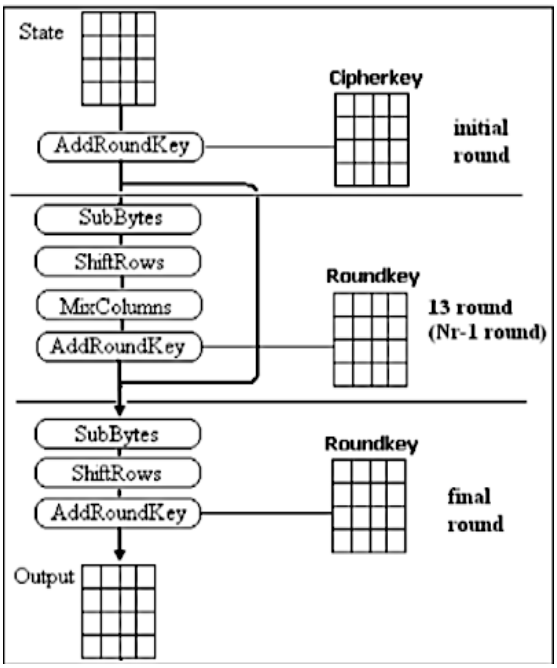

Figure 2. AES Encryption Process

The flowchart illustrates the AES 256 encryption process. First, enter the data and key. The key is 256 bits. Perform the AddroundKey process, which XOR as the plaintext and key. Encryption involves changing SubBytes, ShiftRows, MixColumns, and addRound-Key. At Round = 0, apply Ad-droundKey. Then, apply SubBytes, ShiftRows, MixColumns, and addRound-Key for Round = 13. For Round = 14, implement SubBytes, ShiftRows, and addRoundKey to generate ci-phertext[13].

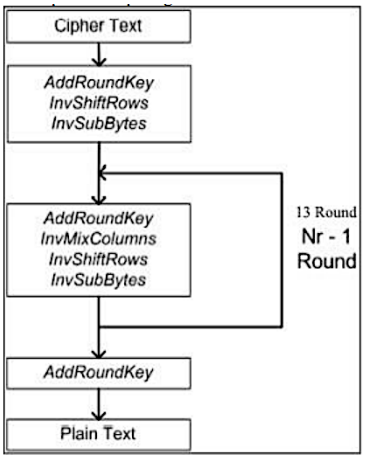

Figure 3. AES Description Process

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

The flowchart describes the AES 256 decryption process. First, enter the chipertext. Combine keys with chipertext using the AddroundKey process. Decryption has 4 types of changes: inverseSubbyte, inverseShiftRows, InverseMixColumn, and addRoundKey. At Round = 0, the state undergoes an addroundKey change. In the next round, implement inverseSubbytes, inverseShiftRows, inverseMixColumns, and addRoundKey. After Rounds = 13, do inverseSubbytes, inverseShiftRows, and addRoundKey to get the plaintext[14].

3. RESULTS AND DISCUSSION

Results In this study, the author carried out the steps contained in the stages of the RAD method. Here are the steps taken by the author.

3.1. Requirements Planning

This stage focuses on the identification and collection of system requirements as a whole[15] In the context of a web-based notary management system, a team of developers and stakeholders (e.g., notaries and staff) collaborate to formulate functional and non-functional requirements. At this stage, the notary office's business processes related to the creation, storage, and management of notary documents are mapped. Problems in manual systems or previous systems are identified, such as the length of the filing process or the lack of information accessibility, which will later become the basis for designing a new system. The main goal of this stage is to confirm that all requirements have been clearly understood before proceeding to the design stage[15].

3.2. Workshop Design RAD

After the requirements were approved, the team entered the design workshop phase. In the RAD method, the design does not need to be too detailed at the beginning, but rather is built iteratively and quickly[16] At this stage, the team held several workshop sessions that involved prototyping and direct feedback from users. This stage involves the planning of UML. It consists of use cases, activity diagrams, and class diagrams.

1) Use case Diagram

The Use Case diagram illustrates the interaction between two actors, namely employees and admins, with a web-based notary management information system. Employees and admins have access to log in to the system, as well as manage data such as order data and client data, shown in Figure 4. However, there is a difference in access rights between the two. Admins have full control, including managing protocol data, user data, as well as activity logs that record all interactions in the system. While employees only have access to manage order data and client data

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

without access rights to protocol, user, and activity log modules. This diagram shows how the system restricts access rights based on roles to maintain the security and efficiency of data management in a notary office.

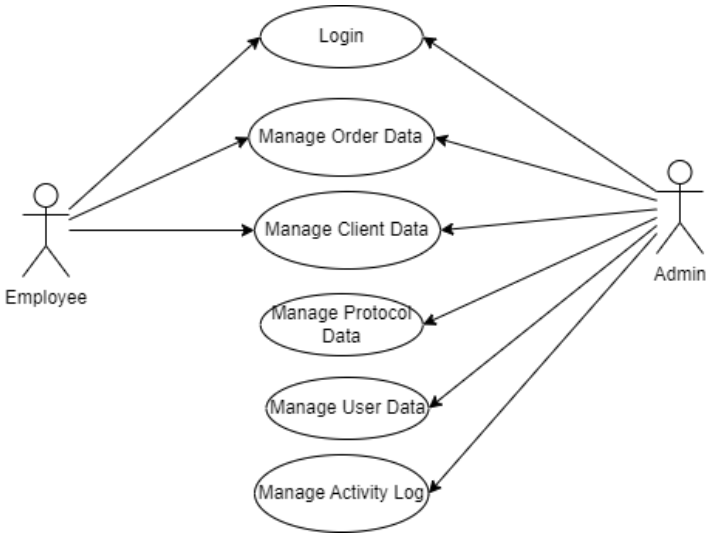

Figure 4. Use Case Diagram

2) Activity Diagram

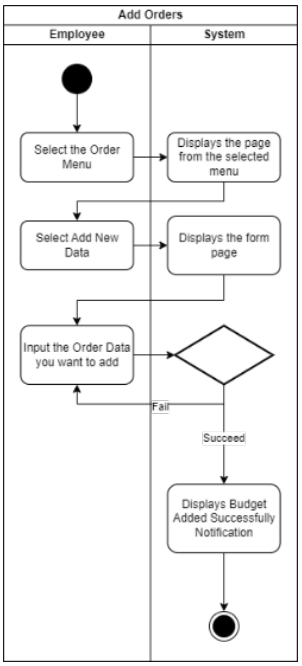

Figure 5. Activity Diagram

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

The diagram above is an Activity Diagram that illustrates the flow of the process of adding orders in the information system. The process starts from the staff who select the Order menu on the system interface. The system then responds by displaying the selected page. After that, the staff selects the option to add new data, and the system displays a form page for filling in the data. The staff then inputs the order data that they want to add. After the data is inputted, the system checks the validity of the data. If the process fails (e.g. invalid data), the staff will be asked to repeat the filling process. If successful, the system will display a notification that the order has been successfully added. This process ends the order addition activity. This diagram illustrates the collaboration between staff and the system in the process of managing order data.

3) Class Diagram

The class diagram as illustrates in Figure 6 the structure of a web-based notary management information system through class representation and relationships between classes. Each class has attributes that are relevant to its function in the system.

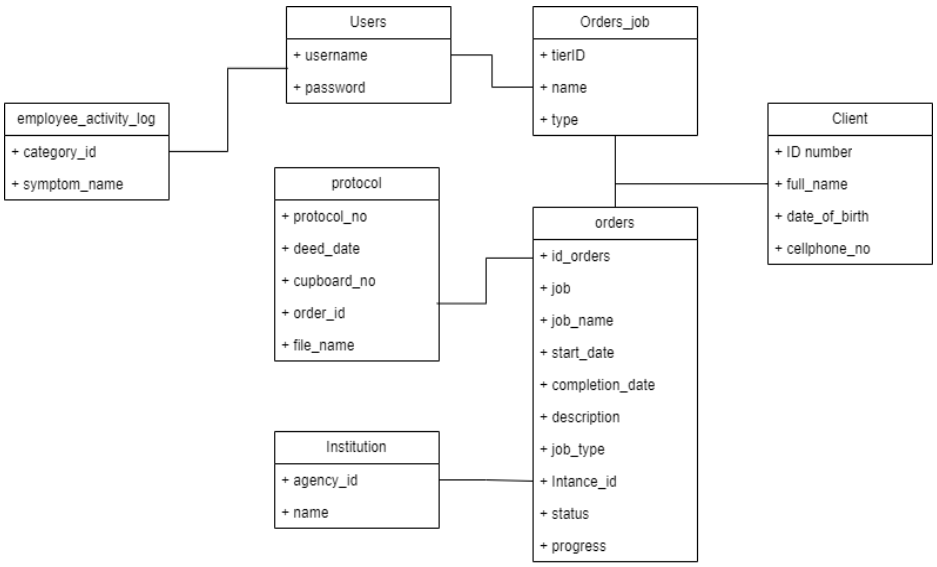

Figure 6. Class Diagram

3.3. Implementation of AES 256 Algorithm

In the first implementation of the code, which is to create a helper code to initiate encryption using AES 256, the code consists of an encryption and decryption process.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

```
<?php
defined('BASEPATH') OR exit('No direct script access
allowed');
if (!function_exists('encryptData')) {
    function encryptData($data)
    {
        $key = 'arya2024'; // Kunci rahasia
        $iv =
openssl_random_pseudo_bytes(openssl_cipher_iv_length('AES-
256-CBC')); // Membuat IV acak
        $encrypted = openssl_encrypt($data, 'AES-256-CBC',
$key, 0, $iv); // Enkripsi
        return base64_encode($iv . '::' . $encrypted); //
Menggabungkan IV dengan ciphertext
    }
}
if (!function_exists('decryptData')) {
    function decryptData($data)
    {
        $key = 'arya2024'; // Kunci rahasia
        list($iv, $encrypted) = explode('::',
base64_decode($data), 2); // Memisahkan IV dan ciphertext
        return openssl_decrypt($encrypted, 'AES-256-CBC',
$key, 0, $iv); // Dekripsi
    }
}
```

Code 1. Encryption using AES 256

In the pseudocode in as shown in Code 1 is the process of invoking the encryption and description functions that were previously created in the helper image 12. The process is that when saved to the database, the data will turn into random words that cannot be understood. Meanwhile, the process of invoking the decryption function that had previously been encrypted on the database to be displayed in the system in the form of data that should or should not be random words that are difficult to understand. Code 2 is the process of it. Next is Figure 8 of the data stored in the database as a result of encryption using AES 256 where the data has been turned into random letters that cannot be understood**.**

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

```
public function editklien($ktp)
    {
        $data['username']=$this->user['nama'];
        $data['mode']=$this->user['log'];
        $data['klien']=$this->klien->getKlien($ktp);
        $this->form_validation->set_rules('nama', 'Nama',
'required');
        // Contoh DecryptData
        $data['klien']['nama_lengkap'] =
decryptData($data['klien']['nama_lengkap']);
        $data['klien']['nomor_HP'] =
decryptData($data['klien']['nomor_HP']);
        $data['klien']['nomor_KTP'] =
decryptData($data['klien']['nomor_KTP']);
        if ($this->form_validation->run() === FALSE)
        {
            $this->load->view('header');
            $this->load->view('nav',$data);
            $this->load->view('v_editKlien',$data);
            $this->load->view('footer');
        }
        else
        {
            // Contoh EncryptData
            $_POST['nomor_ktp'] = encryptData($this->input-
>post('nomor_ktp'));
            $_POST['nama'] = encryptData($this->input-
>post('nama'));
            $_POST['nomor_hp'] = encryptData($this->input-
>post('nomor_hp'));
            $this->klien->ubah($ktp);
            redirect(base_url('klien'),'refresh');
        }
    }
```

Code 2. Encrypted on the database

The login Page as shown in Figure 7 is the first page that users will see when accessing the system. This page is designed to ensure secure access to the system. Users, including notaries or employees must enter a username and password that has been registered beforehand. After logging in, the user will be redirected to the dashboard that corresponds to their access rights (e.g., notary or employee).

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

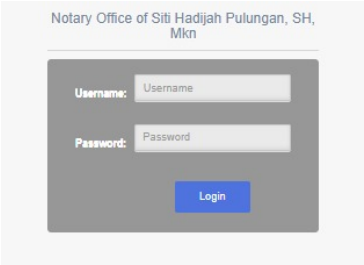

Figure 7. Login Page

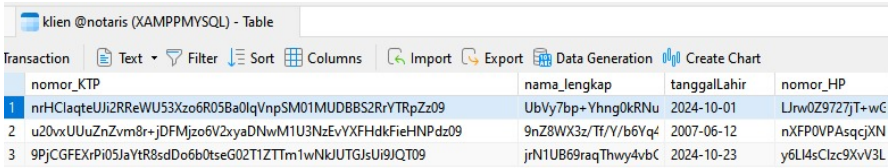

Figure 8. Encryption Results

3.4. Implementation

The following is the implementation in this study that is presented in the form of the system display.

1) Data Admin Client

In this view, admins can view, manage, and update the information of clients who have dealt with the notary office. Client data typically includes basic information such as full name, date of birth, phone number, and NIK. This page also supports efficient search of client data, allowing admins to quickly find the information they need. Admins can also add new clients, edit existing data, or delete data that is no longer needed.

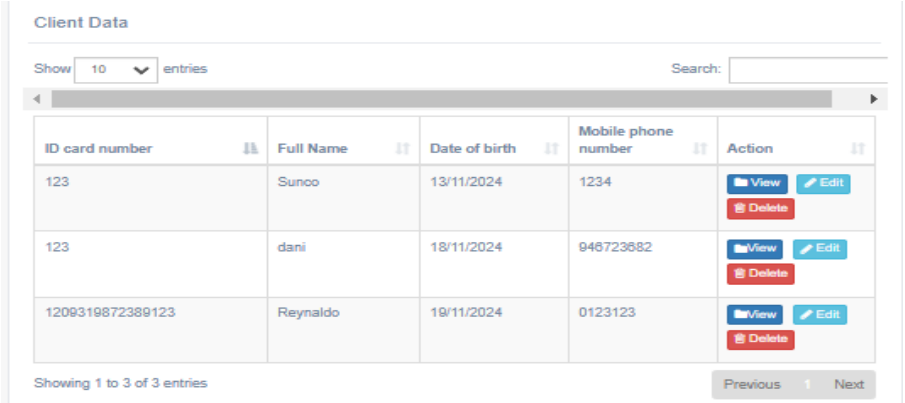

Figure 9. Admin client view

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

2) Order Data Display Picture

This view provides access to admins or employees to manage order or transaction data related to notary services. Each order contains de-tail information such as the type of legal document requested by the client (e.g., sale and purchase deed, land deed, etc.), start & finish date, and process status (e.g., completed, in progress, or pending approval). This function facilitates overall order monitoring and management and ensures that each transaction runs according to the expected procedures.

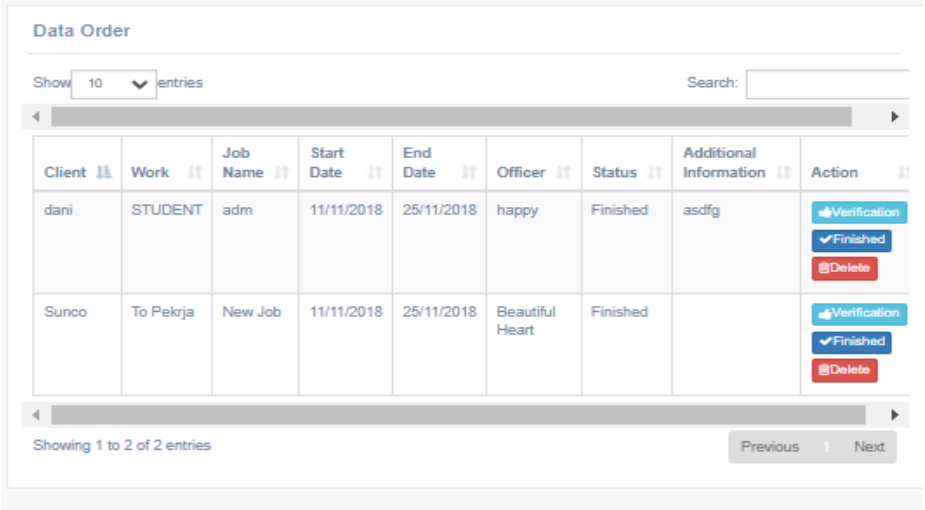

Figure 10. Order data

This page displays a list of orders that includes important information such as order number, client name, service type, order date, and completion status. Users can easily search, add, edit or delete order data through an intuitive interface**.**

3) Notarial Protocol Data

Admins or employees to manage order data or transactions related to the Memorandum - 409 RIS service. Each order contains detailed information such as the type of legal document requested by the client (e.g., sale and purchase deed, land deed, etc.), start & finish date, and process status (e.g., completed, in progress, or pending approval). This function makes it easier to monitor and manage orders as a whole and ensures that each transaction goes according to the expected procedures. The account data view provides functionality for admins to manage user accounts within the system. Each user of the system has an account with a different level of access, 410 e.g. notary (owner) or employee. Admins can add, edit, or delete accounts, and define the access rights or roles of each user. This ensures that sensitive data can only be accessed by people who have authority according to their position in the notary office.

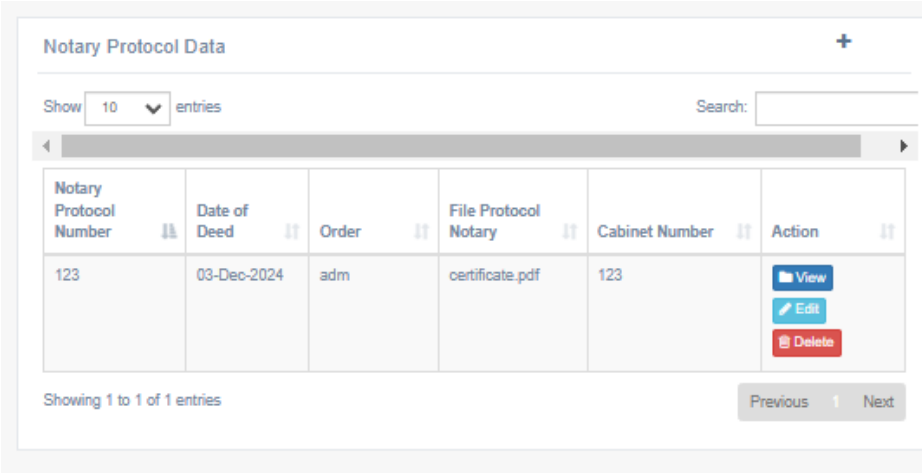

Figure 11. Notary Protocol Data

4) Account data

The Account Data view is designed to manage system user account information, including admins and employees. This view enables structured account management, supports access control, and ensures the system is only accessed by authorized parties.

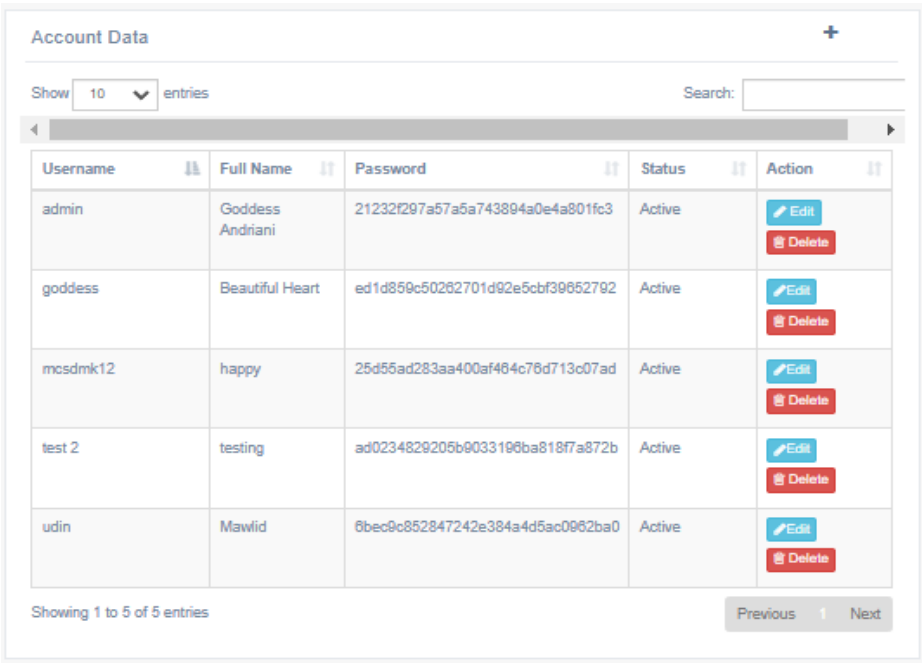

Figure 12. Account data view

5) Employee productivity data

This page presents data such as the number of tasks completed, completion time, and the level of productivity of each employee in a certain period. This view helps management identify high performers and areas that need improvement**.**

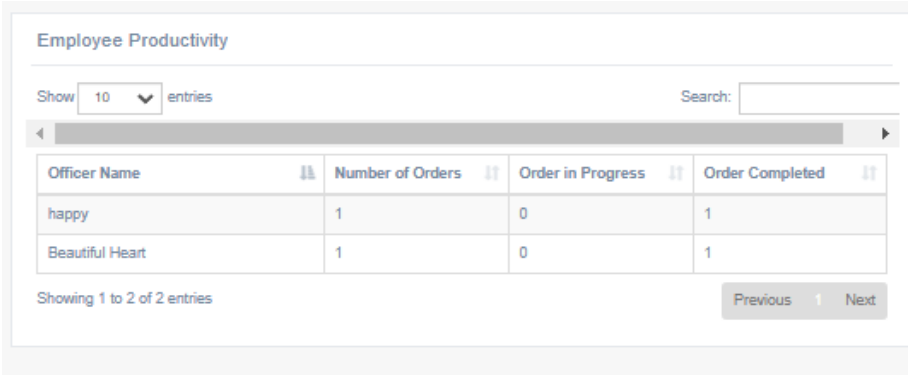

Figure 13. Employee Productivity Data Display

6) Work monitoring data

This display records and displays the activity log of each employee while working in the system. The information logged includes the time of login, the activities performed (e.g., management of client data, orders, or protocol archiving), as well as the time of logout. This activity log function is essential for maintaining transparency and accountability, allowing admins or management to keep track of who performed a particular action and when it was performed. It can also be used as the basis for audits in case of problems or errors in the work process.

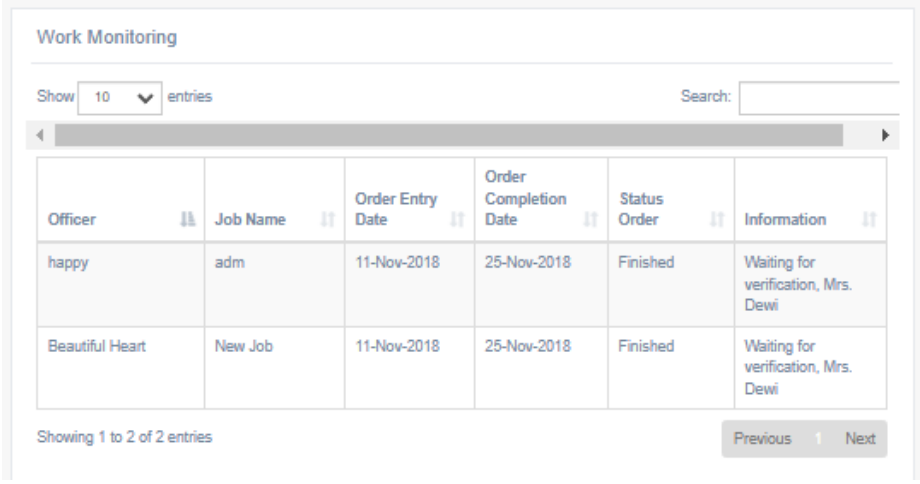

Figure 14. Work Monitoring Data Display

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

3.5. Black-Box Testing of a Web-Based Notary Management Information System with the AES 256 Algorithm

Black-box testing is used to verify whether each menu in the system works according to the expected specifications without checking the program code. The focus of this testing is to ensure that the input provided produces the appropriate output for each system function. The following is an explanation of black-box testing for each menu:

Table 2. Black Box Testing

Testing	Desired realization	Test Results	Comclusion
Login	Enter a valid username and password, the system displays the dashboard page	The system only grants access to registered users	Valid
Data Admin Client	Enter the new client data (name, address, phone number), the system saves the data to the database	Client data successfully added, changed, or deleted	Valid
Order Data	Enter the new client data (name, address, phone number), the system saves the data to the database	Order data is added or deleted correctly	Valid
Notarial Protocol Data	Upload protocol related documents, the system saves and displays successful upload status	The document was successfully uploaded and searched	Valid
Account Data	Enter new account data, the system saves the data.	Account data was successfully added, changed, or deleted	Valid
Employee Productivity Data	Enter employee productivity data (name, completed tasks, work time).	Employee productivity data has been successfully saved and searched	Valid
Work Monitoring Data	Enter new work data (work title, status, deadline), the system saves the data.	Work data added or updated successfully	Valid

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

3.6. Discussion

This study's application of the Rapid Application Development (RAD) method in creating a web-based notary management system underscores the effectiveness of RAD in complex software projects requiring significant user interaction and fast-paced iterations. The RAD approach's adaptability to changing requirements and its focus on user feedback are reflected in several critical aspects of the system's

The use of iterative design and prototyping sessions facilitated an environment where user feedback was actively solicited and promptly integrated. This ongoing engagement helped tailor the system specifically to the needs of the notaries and their staff, ensuring that the final product was not only functional but also user-friendly. This approach likely increased user satisfaction and reduced resistance to adopting the new system, a common hurdle in implementing new technology solutions in professional settings.

The integration of the AES 256 encryption algorithm during the early stages of system development demonstrates a proactive approach to addressing data security concerns. In the context of notarial work, where document confidentiality is paramount, embedding high-level encryption into the system architecture without affecting user experience is a significant achievement. This security measure ensures that sensitive information remains protected, enhancing trust in the system's reliability and compliance with legal standards.

The outcomes from the black-box testing phase reflect the system's robustness and the effectiveness of the RAD method in achieving a design that meets specified requirements without the need for extensive revisions. This testing not only confirmed the system's functional capabilities but also demonstrated its stability and readiness for deployment, crucial for systems handling sensitive legal documentation.

The success of the RAD approach in this project offers valuable insights for future software development projects, particularly those requiring rapid development cycles and high levels of customization. It suggests that RAD can significantly enhance project outcomes through its emphasis on user-cantered design and iterative feedback, making it a suitable choice for projects where user requirements are complex and evolving.

The deployment of the RAD method in this project highlights its strengths in fostering a collaborative, flexible, and user-focused development environment. By effectively integrating user feedback, ensuring high data security, and demonstrating system efficacy through targeted testing, the project not only met but potentially exceeded the initial project goals and user expectations.

4. CONCLUSION

This research succeeded in designing a web-based management information system for notary offices with data security using the AES 256 algorithm, which protects data from misuse even if an attack occurs. This system increases work efficiency and productivity with integrated features, such as management of client data, protocols and user activity, as well as easy accessibility. The RAD approach allows for rapid, user-specific development. As well as being relevant for notaries, this system could be a model for other sectors requiring secure data management, with potential for further developments such as blockchain integration for additional security, expansion to mobile platforms, and the use of AI to automate data analysis.

REFERENCES

[1] A. Mutriadi, "Implikasi Perdata Terhadap Integritas Jabatan Notaris," *Juripol*, vol. 4, no. 1, pp. 348–352, 2021, doi: 10.33395/juripol.v4i1.11135.

[2] J. Jozan Adolf and W. Handoko, "Eksistensi Wewenang Notaris Dalam Pembuatan Akta Bidang Pertanahan," *Notarius*, vol. 13, no. 1, pp. 181–192, 2020, doi: 10.14710/nts.v13i1.29313.

[3] Y. P. Rahman, "Pengaturan Penyerahan Protokol Notaris Yang Telah Meninggal Dunia Dan Prakteknya Di Provinsi Sumatera Barat," *JCH (Jurnal Cendekia Hukum)*, vol. 5, no. 1, p. 1, 2019, doi: 10.33760/jch.v5i1.120.

[4] L. Clara and A. Budi, "Implementasi Metode Algoritma AES Pada Perlindungan Data Sistem Login," *J. Inform. dan Bisnis*, vol. 10, no. 2, pp. 1–14, 2021.

[5] H. Wulandari, J. Karman, and E. Elmayati, "Implementasi Algoritma Aes (Advanced Encryption Standard) Pada Penjualan Alat – Alat Elektronik Berbasis Web (Studi Kasus Toko Sonia Elektronik)," *J. Teknol. Inf. Mura*, vol. 15, no. 1, pp. 41–51, 2023, doi: 10.32767/jti.v15i1.2049.

[6] M. P. N. Lubis and N. A. B. I. Rahmani, "Analisis Dan Perancangan Sistem Informasi Kwitansi Berbasis Desktop Pada Kantor Notaris Mangatas Nasution SH," *Musytari Neraca Manajemen, Akuntansi, dan Ekonomi*, vol. 2, no. 10, pp. 123–133, 2023.

[7] A. M. Akbar, "Pembuatan Program Aplikasi Management Administrasi Pada Kantor Notaris Vika Kartika SH, M. Kn Berbasis Mobile APPS," *Kohesi J. Sains dan Teknol.*, vol. 4, no. 3, pp. 91–100, 2024.

[8] Suendri and Anggika Wardani, "Implementation of the WASPAS Method in Selection Librarian FST UIN Sumatera Utara," *J. Sist. Cerdas*, vol. 7, no. 1, pp. 38–44, 2024, doi: 10.37396/jsc.v7i1.385.

[9] H. Irfansyah, S. Suendri, and A. Ikhwan, "Sistem Monitoring Aktivitas Karyawan Lapangan Dengan Metode Lock GPS Berbasis Cloud Pada PTPN II," *JISTech (Journal of Islamic Science and Technology)*, vol. 6, no. 2, pp. 94–106, 2021, doi: 10.30829/jistech.v6i2.11436.

[10] A. Hartono, S. Suendri, and A. M. Harahap, "Penggunaan Algoritma Extreme Learning Machine Berbasis Android Untuk Mengidentifikasi Daging Sapi dan Babi," *J-SISKO TECH (Jurnal Teknol. Sist. Inf. dan Sist. Komput. TGD)*, vol. 6, no. 1, p. 127, 2023, doi: 10.53513/jsk.v6i1.7409.

[11] A. A. Permana, J. Maulindar, and D. Hartanti, "Implementasi Sistem Kriptografi Algoritma AES (256-bit) Berbasis Web API untuk Mengamankan Data Pribadi di CV. Elang Cahaya Sukses Surakarta," *Pros. Semin. Nas.*, pp. 707–711, 2022.

[12] I. Fitriani and A. B. Utomo, "Implementasi Algoritma Advanced Encryption Standard (AES) pada Layanan SMS Desa," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 5, no. 3, pp. 153–163, 2020, doi: 10.14421/jiska.2020.53-03.

[13] N. A. Fadhlurrohman, "Penerapan Kriptografi Dengan Algoritma AES-128 Implementation Of Aes-128 Cryptography For Enhanced Digital Document Security At Bpjs Kesehatan," *Semin. Nas. Mhs. Fak. Teknol. Inf.*, vol. 3, no. September, pp. 1–9, 2024.

[14] N. Putu, A. Astriyani, D. Rimbawa, and B. Raharjo, "Studi Perbandingan AES 128 dan 256 untuk Pengamanan Sistem Informasi Manajemen Rumah Sakit Dr. Mintoharjo," *J. Educ.*, vol. 06, no. 02, pp. 13293–13300, 2024.

[15] R. H. Sukarna, A. M. Januriana, H., and M. Hilman, "Implementasi Algoritma Enkripsi Pada Sistem Informasi Manajemen Helpdesk Berbasis Desktop," *J. Inform. dan Ris.*, vol. 1, no. 2, pp. 31–39, 2023, doi: 10.36308/iris.v1i2.535.

[16] A. Ignasius and D. V. Shaka Yudha Sakti, "Penerapan Algoritma Aes (Advance Encryption Standard) 128 Untuk Enkripsi Dokumen Di Pt. Gunung Geulis Elok Abadi," *Skanika*, vol. 5, no. 1, pp. 1–10, 2022, doi: 10.36080/skanika.v5i1.2118.