IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 11, November 2023

DOI: 10.17148/IJARCCE.2023.121109

Data Security Implementation with Advanced Encryption Standard 256 in Notary Mobile Applications

Tegar Rangga Nur Ridawan[1], RR Hajar Puji Sejati[2]

Department of Informatics, Yogyakarta University of Technology, Yogyakarta, Indonesia[1]

Department of Informatics, Yogyakarta University of Technology, Yogyakarta, Indonesia [2]

Abstract: The widespread use of mobile devices, especially in Indonesia where 67% of the population owns a mobile device, underscores the rapid advancement of mobile technology. Google's Android, with its open-source nature and extensive application support, has become the leading choice. In the context of increasing reliance on public services, including those provided by notaries and land deed officials, data security is of paramount importance. The development of a mobile notary application addresses this need, offering ease of interaction and reliable data security. This research implements the AES 256 encryption and decryption method, ensuring secure data exchange through the app. The AES algorithm, recognized as a Federal Information Processing Standard, secures data stored in an encrypted MySQL database. This Android-based notary app successfully uses AES-256 in document encryption, making files unreadable to unauthorized parties. The app also aims to build trust between users and notaries while preventing potential misuse of documents. Further development is expected to increase interaction between users and notaries, improving efficiency and accessibility of public services.

Keywords: Cryptography, Mobile Applications, Data Security, Notary.

I. INTRODUCTION

The use of mobile devices has become a widespread trend among the global community, especially in Indonesia. According to Databook's, as many as 67 percent of the Indonesian population already owns a mobile device (Hidayat, 2022), This information is taken from the Central Bureau of Statistics. As evidenced by the rapid advances in mobile device technology, these advances have had a significant impact, especially in improving the effectiveness of mobile devices (Aceto et al., 2018) and efficiency (Szymkowiak et al., 2021), especially as a communication tool that supports various daily activities. Google's mobile operating system, Android, is the main choice of many users today because of its Open-Source operating system (Sharma, 2018), extensive application support and integration with Google services (Adekotujo et al., 2020), to user flexibility (O'Reilly-Shah & MacKey, 2016). The advantages of mobile devices with the Android operating system are not only limited to communication functions but have evolved into personal assistants capable of taking photos, recording video and sound, creating documents, and storing data efficiently.

This is related to the current community cannot be separated from the need for public services. Public services themselves have various types, such as licensing services, general services, population administration, and land and building tax services (Ramadhani, 2017). One type of crucial public service is that provided by notaries and land deed officials. Their job involves a series of very important steps and responsibilities to ensure the legality and validity of property transactions. The security of data or documents in the land deed process is a very crucial aspect. It is important to build trust between the parties involved, so that there are no doubts regarding the process of obtaining a land deed. To facilitate public interaction with notaries or land deed officials, the development of mobile notary applications is an effective solution. This application not only brings benefits in terms of ease of interaction but is also designed with trustworthy data security.

This research designs and implements the AES 256 encryption and decryption method, which has been tested for reliability, providing assurance that the data and information exchanged through this application remains safe and secure. Cryptography is a discipline that aims to maintain the confidentiality of messages by encrypting them so that they cannot be understood by unauthorized parties (Azhari et al., 2022), (Nurrahmi et al., 2020). The cryptographic process involves two main stages, namely encryption and decryption. One of the most popular cryptographic algorithms, the Advanced Encryption Standard (AES), incorporates the principles of the symmetric algorithm (Kamarudin & Mohammad, 2011) and asymmetric (Mulud Muchamad & Pambudi, 2023) by using a specially developed model.

DOI: 10.17148/IJARCCE.2023.121109

The AES algorithm, issued by the National Institute of Standards and Technology (NIST), is based on the Rijndael algorithm which was recognized as Federal Information Processing Standard (FISP) 197 in 2001 (Smid, 2021). In addition, the inputted data will be stored in an encrypted database, with MySQL as the database management system used. Then, the administrator can access it through the website. Thus, the implementation of the mobile notary application not only provides practical benefits, but also provides certainty regarding the security of information that is very important in the process of making land deeds.

II. RESEARCH METHOD

The main problem with hard file data storage media is the lack of special protection for document files. This weakness raises concerns because if the document is lost, the important data contained therein may not be recoverable, or may even be widely disseminated by irresponsible parties. Therefore, in this research, an Android-based application will be developed to enhance the security of clients' important documents. In addition, the admin interface will be created in a website version to make it easier to use, by applying the AES 256 algorithm method.

2.1 Document

In this research, documents are divided into two types: notarial documents and documents of land deed officials. Although both have official authority from the government, the difference is very clear. Notarial documents are legal statements made by authorized notaries, public officials with the task of making, certifying, and storing legal deeds such as agreements, buying and selling, and inheritance (Afifah, 2017). This document has strong evidentiary power in the eyes of the law (Widodo & Purnomo, 2020).

Meanwhile, a document of a land deed maker is a land deed made by a person authorized to administer land deeds, including the purchase, sale, granting of rights, and registration of land rights (Kusuma Wardhini, 2022). This document clearly records transactions or legal events related to land and property (Juridical et al., 2023).

2.2 Cryptography

The word cryptography comes from the Greek language, consisting of two words, namely crypto which means secret, and graphia which means writing (Hassan & Abbas Majeed, 2023). Cryptography is the discipline that studies how to hide messages. In its implementation, cryptography becomes a method for encrypting or encoding data that can only be understood or has special meaning to a specific group of users (Azhari et al., 2022; Nurrahmi et al., 2020). Some terms that are often used in cryptography are as follows (Adi Putra et al., 2023; Bancin et al., 2023; Widodo & Purnomo, 2020):

TABLE I TERM IN CRYPTOGRAFI

Term	Description
Plaintext	Represents the original clear text or information before encryption.
Ciphertext	Is the result of the encryption process or random information derived from plaintext that has been cryptographed.
Decryption	It is the opposite of encryption which is the process of returning ciphertext to plaintext.
Encryption	It is a cryptographic process from plaintext to ciphertext.

2.3 Algorithm Advanced Encryption Standard 256 (AES)

The Advanced Encryption Standard (AES) algorithm is a symmetric block cipher algorithm that uses symmetric keys for encryption and decryption. Introduced as the latest cryptographic standard by NIST in 2001, AES replaced the deprecated DES algorithm.

The AES encryption process involves a series of rounds whose number depends on the chosen key length, which can be 128, 192, or 256 bits. Each round requires a round key and input from the next round, with the round key generated based on the given key. The AES algorithm can encrypt and decrypt data with varying key lengths. The key length affects the number of rounds, the difference when the key can be described in Table 2 AES Key Comparison.

DOI: 10.17148/IJARCCE.2023.121109

TABLE II AES KEY COMPARISON

	Key (NK Words)	**Block (Nb Words)**	**Putaran (Nr)**
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

The encryption process involves four types of byte transformations, namely SubBytes, ShiftRows, MixColumns, and AddRoundKey (Selvapriya & Suganthi, 2023). In the initial stage of encryption, the input that has been copied into the state will go through AddRoundKey byte transformation. After that, the state will undergo SubBytes, ShiftRows, MixColumns, and AddRoundKey transformations repeatedly as many as Nr (Dhansukhbhai Patel & Desai, 2023). This stage is known as the round function in the AES algorithm. The last round is different from the previous rounds, in that in the last round, the state does not undergo the Mix Columns transformation. The decryption process uses the reverse algorithm of AES encryption, applying the inverse transformation on all the basic steps used in the encryption algorithm.

2.3.1 AES Algorithm Encryption Process

The encryption process of the AES algorithm consists of four types of bytes transformation, namely SubBytes, ShiftRows, Mixcolumns, and AddRoundkey such as (Selvapriya & Suganthi, 2023; Widodo & Purnomo, 2020).

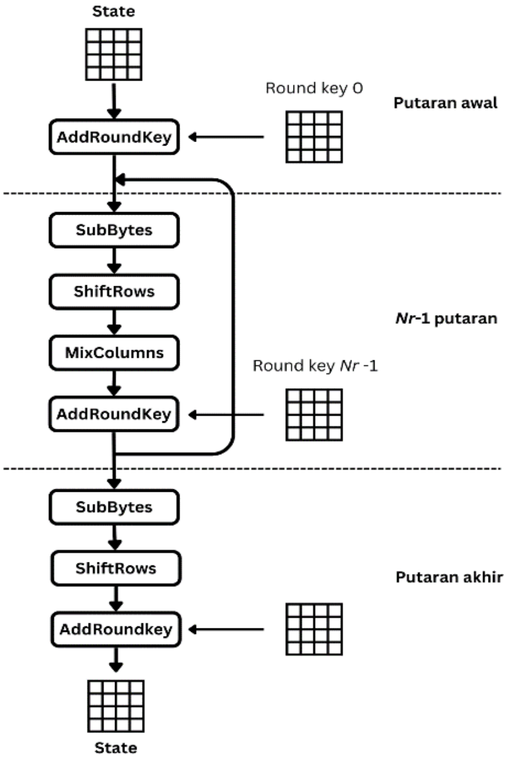


Fig. 1 AES Algorithm Encryption Process

The encryption process of the AES algorithm consists of three main stages, as follows:

1. The initial stage, called Initial Round, involves copying the input into a state that will undergo the AddRoundKey transformation. This AddRoundKey transformation involves an XOR operation between the plaintext and the chipkey.

2. The next stage is the Round Function which is repeated Nr-1 times. At each literation, the process includes:
- SubBytes: Replacement of bytes using a substitution table (S-Box).
- ShiftRows: Shifting the rows of the statre array in order.
- MixColumns: Randomization of data in each column of the state array.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁎ Peer-reviewed journal & Refereed journal ⁎ Vol. 12, Issue 11, November 2023
DOI: 10.17148/IJARCCE.2023.121109

- AddRoundKey: XOR operation between the current state and the round key.

3. The last stage is called Final Round, which occurs in the last round. The last round has a difference in that the state does not undergo the MixColumns transformation. At this stage, the process still involves SubBytes, ShiftRows, and AddRoundKey as in the previous rounds.

2.3.2 AES Algorithm Decryption Process

The decryption process is applied in the opposite way to encryption to produce the inverse cipher. The byte transformations applied to the inverse cipher involve ShiftRows, Inverse SubBytes, Inverse MixColumns, and AddRoundKey. While the key usage remains the same, the order of the decryption process in AES is not simply the reverse of encryption, but rather the order is swapped.

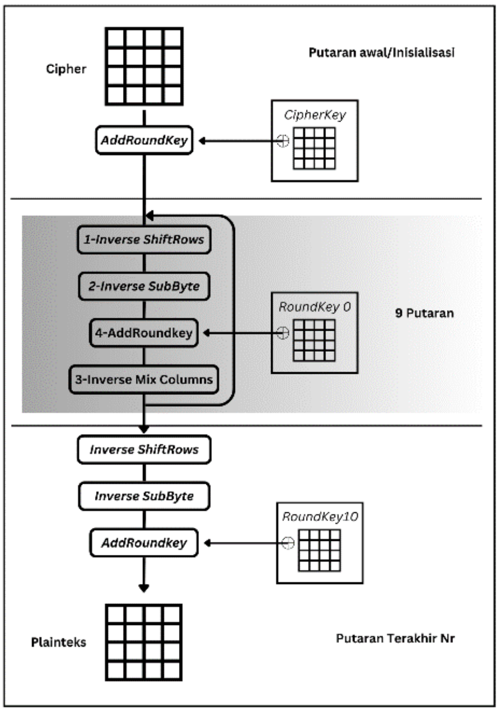


Fig. 2 AES Algorithm Decryption Process

2.4 System Design

Creating a good application requires a good design, from the appearance to the system inside. By doing conceptual design, the application can be well organized and can avoid mistakes in making it. In addition, if there is an error, it will be easier to find the point of error. The following is the design of the application system architecture.

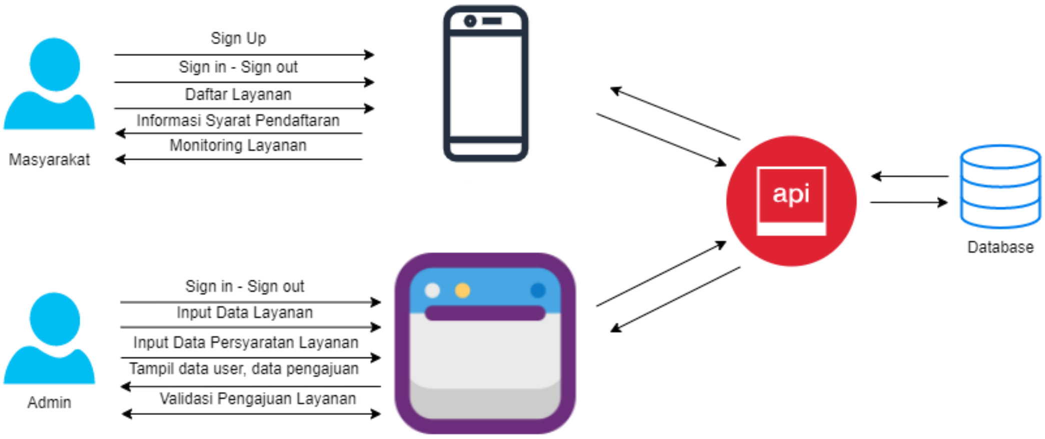


Fig. 3 Application Design Architecture

2.4.1 Flowchart

Flowchart is a form of diagram used to describe a process, system, planning flow, or various other things (Cellina et al., 2022). This diagram uses graphical symbols to describe steps or activities in sequence, making it easier to understand the process flow (Zhang et al., 2023). In the system to be created, there are several application features such as Login, dashboard page, service input, service requirement input, and service submission data validation.

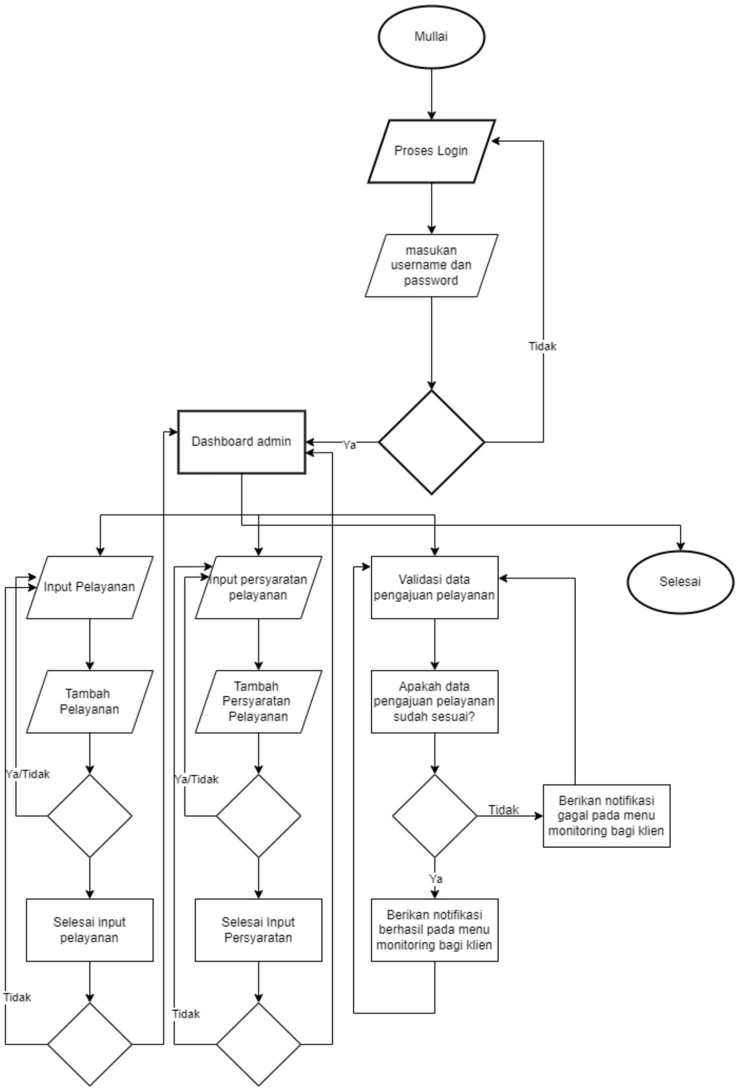

Mullai
Proses Login
masukan username dan password
Tidak
Ya
Dashboard admin
Selesai
Input Pelayanan
Input persyaratan pelayanan
Validasi data pengajuan pelayanan
Tambah Pelayanan
Tambah Persyaratan Pelayanan
Apakah data pengajuan pelayanan sudah sesuai?
Ya/Tidak
Ya/Tidak
Tidak
Berikan notifikasi gagal pada menu monitoring bagi klien
Ya
Selesai input pelayanan
Selesai Input Persyaratan
Berikan notifikasi berhasil pada menu monitoring bagi klien
Tidak
Tidak

Fig. 4 Application Flowchart

III. RESULT AND DISCUSSION

The application being developed is an Android-based cryptography application by applying the Advanced Encryption Standard (AES-256) method. In the early stages of implementation, an interface design is carried out which is then implemented using the Kotlin programming language. After that, the application is connected to the REST API, and for data storage purposes, MySQL is used as a database to store encrypted documents.

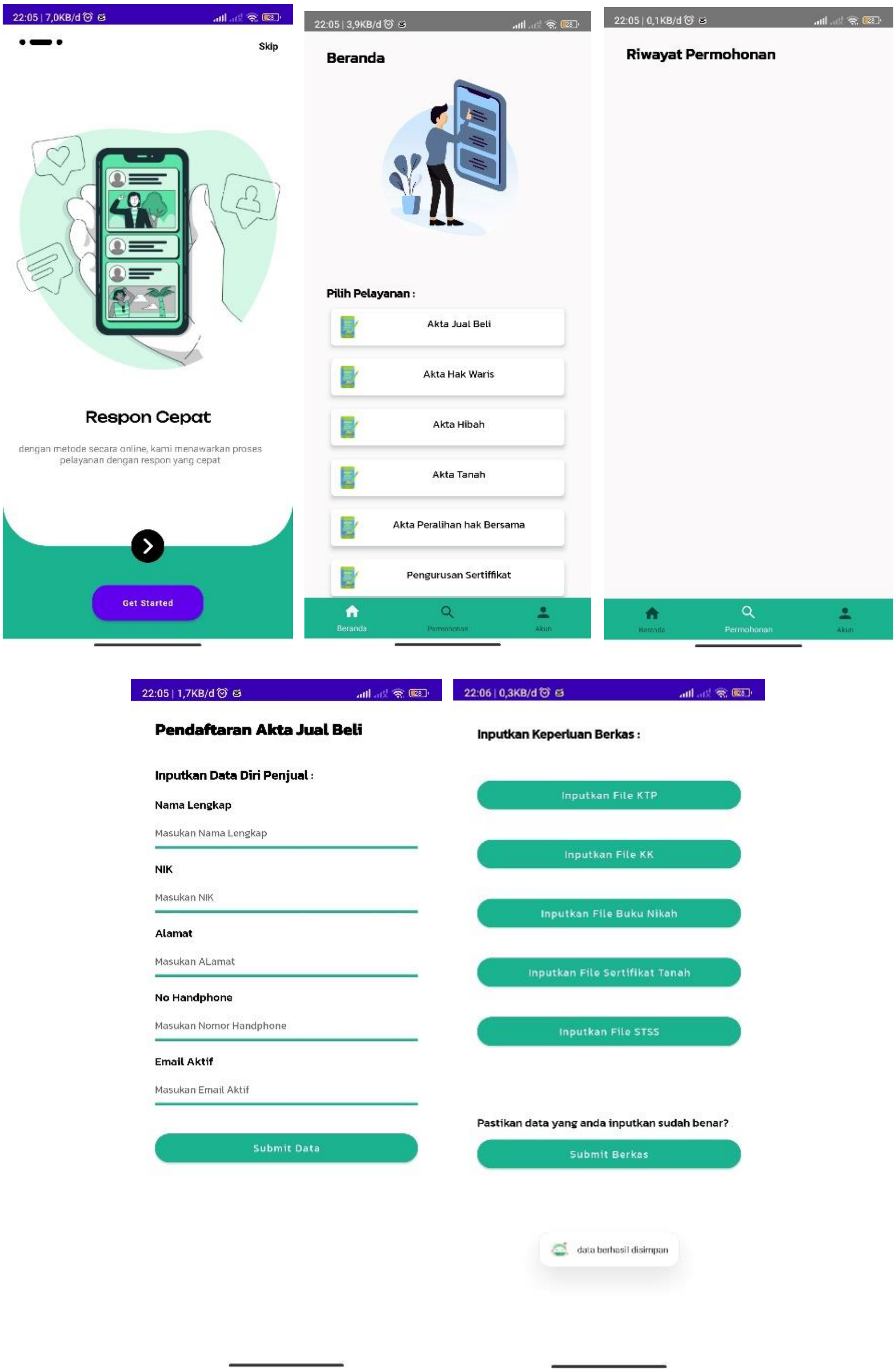
In this application, users are given roles to be able to input or open files, so as to prevent potential misuse. This application supports ebrkass with extensions such as docx, doc, xls, xlsx, pdf, and txt, with a maximum size limit of 2 Mb.

3.1 App View

This page will be displayed to users starting from the splash screen page, home page, application history, file registration, and document input. On the home page there are several features such as sale and purchase deeds, inheritance rights deeds, grant deeds and so on. Furthermore, the application history section will display a history of applications that have

DOI: 10.17148/IJARCCE.2023.121109

been submitted and are awaiting a decision or verification process from a land deed official or notary. The following is a view of the notary mobile application.



Respon Cepat

dengan metode secara online, kami menawarkan proses pelayanan dengan respon yang cepat

Beranda

Pilih Pelayanan :

Riwayat Permohonan

Pendaftaran Akta Jual Beli

Inputkan Data Diri Penjual :

Nama Lengkap: Masukan Nama Lengkap

NIK: Masukan NIK

Alamat: Masukan ALamat

No Handphone: Masukan Nomor Handphone

Email Aktif: Masukan Email Aktif

Inputkan Keperluan Berkas :

Pastikan data yang anda inputkan sudah benar?

data berhasil disimpan

Fig. 5 Mobile App View

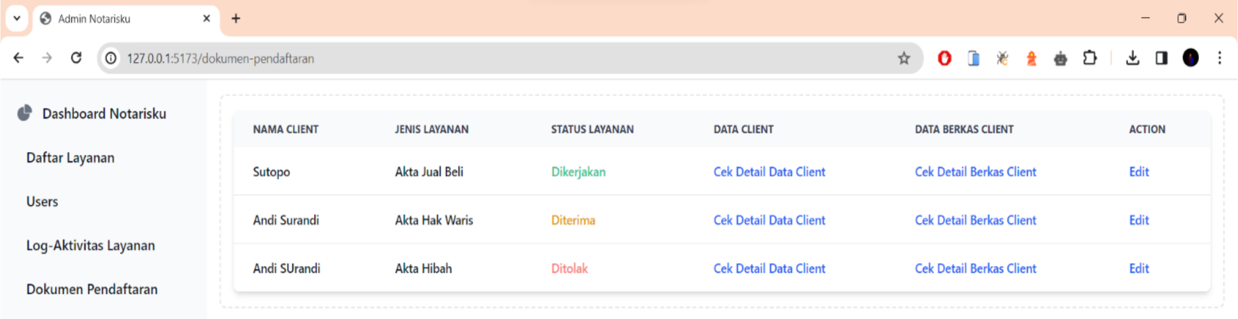
DOI: 10.17148/IJARCCE.2023.121109

3.2 Encryption process

Once the user inputs the required document, an automatic encryption process will take place, and the document will be stored in the database.

If the user has a role that allows access to the document, then the document can be downloaded and viewed. Otherwise, if the user does not have a role that allows access to the document, the system will give a warning that you do not have permission to access the document.

The following is a display of documents that are included in the website.



Admin Notarisku

127.0.0.1:5173/dokumen-pendaftaran

Dashboard Notarisku

Daftar Layanan

Users

Log-Aktivitas Layanan

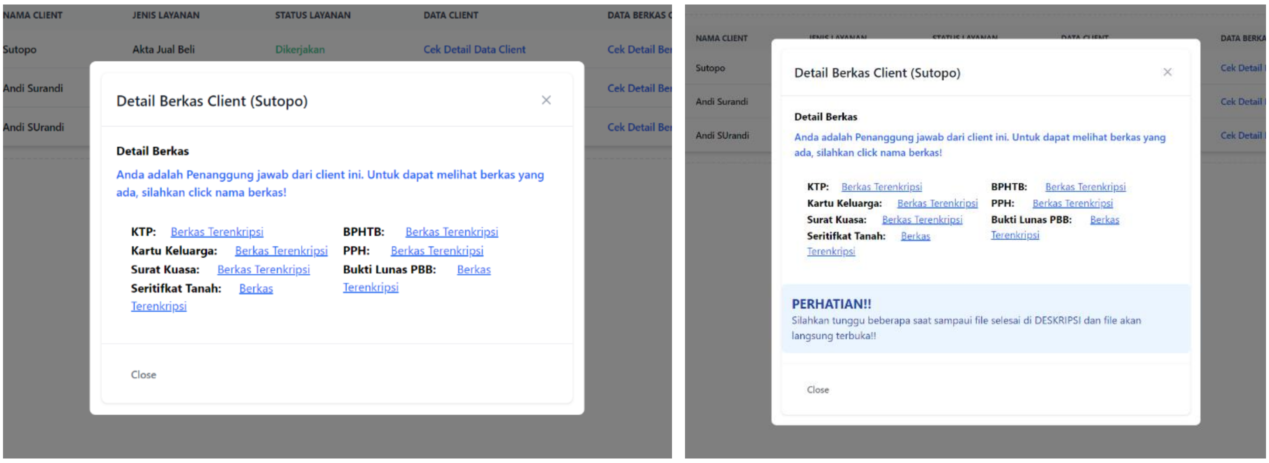
Dokumen Pendaftaran

NAMA CLIENT	JENIS LAYANAN	STATUS LAYANAN	DATA CLIENT	DATA BERKAS CLIENT	ACTION
Sutopo	Akta Jual Beli	Dikerjakan	Cek Detail Data Client	Cek Detail Berkas Client	Edit
Andi Surandi	Akta Hak Waris	Diterima	Cek Detail Data Client	Cek Detail Berkas Client	Edit
Andi SUrandi	Akta Hibah	Ditolak	Cek Detail Data Client	Cek Detail Berkas Client	Edit

Fig. 6 Encyption Process On the Admin Website

This is the view that appears when the user has access rights to the document.

If the user decides to download the document, keep in mind that there will be a warning stating to be patient for a few moments, as a decryption process is in progress to complete the download of the document.



Detail Berkas Client (Sutopo)

Detail Berkas

Anda adalah Penanggung jawab dari client ini. Untuk dapat melihat berkas yang ada, silahkan click nama berkas!

KTP: Berkas Terenkripsi

Kartu Keluarga: Berkas Terenkripsi

Surat Kuasa: Berkas Terenkripsi

Seritifkat Tanah: Berkas Terenkripsi

BPHTB: Berkas Terenkripsi

PPH: Berkas Terenkripsi

Bukti Lunas PBB: Berkas Terenkripsi

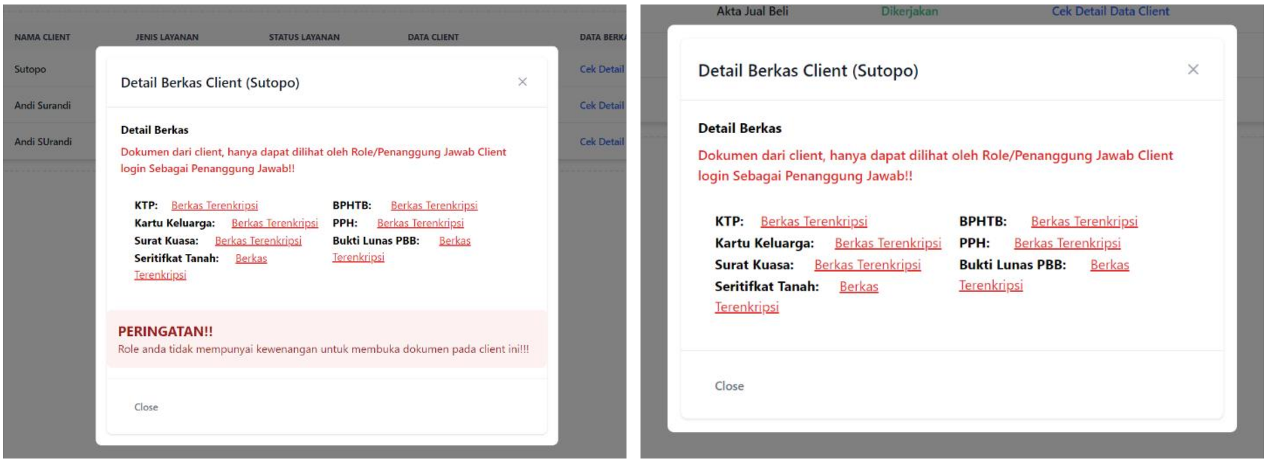
Close

PERHATIAN!!

Silahkan tunggu beberapa saat sampaui file selesai di DESKRIPSI dan file akan langsung terbuka!!

Fig. 7 Successful Download Access Rights

Then the following is the display of users who do not have access rights to the document, the text will turn red and a warning appears that the user does not have access to open the document.



Detail Berkas Client (Sutopo)

Detail Berkas

Dokumen dari client, hanya dapat dilihat oleh Role/Penanggung Jawab Client login Sebagai Penanggung Jawab!!

KTP: Berkas Terenkripsi
Kartu Keluarga: Berkas Terenkripsi
Surat Kuasa: Berkas Terenkripsi
Seritifkat Tanah: Berkas Terenkripsi
BPHTB: Berkas Terenkripsi
PPH: Berkas Terenkripsi
Bukti Lunas PBB: Berkas Terenkripsi

PERINGATAN!!
Role anda tidak mempunyai kewenangan untuk membuka dokumen pada client ini!!!

Fig. 8 Download Failed Access Rights Error

IV. CONCLUSION

The Android-based notary application has achieved a commendable level of document security through the successful implementation of the Advanced Encryption Standard (AES-256) cryptographic method. This robust encryption and decryption process, applicable to a variety of document formats including doc, docx, xls, xlsx, pdf, and txt, ensures that the original files remain unreadable and incomprehensible to unauthorized parties. The choice of the AES-256 cryptographic method underscores the commitment to a high level of security, providing a strong defense against potential misuse and unauthorized access. The decryption process, although swift, taking just one second to complete the operation, remains a crucial aspect of the application's functionality. This ensures efficiency while upholding the integrity of the notary process. By effectively addressing document security concerns, the application serves as a protective barrier, safeguarding sensitive information from falling into the wrong hands. This security measure contributes significantly to building trust between the client and the notary. The assurance of confidentiality and privacy is paramount in transactions involving legal documents, and the AES-256 encryption method plays a pivotal role in fulfilling this need. Beyond security considerations, the notary application aspires to enhance the overall user experience and strengthen the relationship between users and notaries. It is envisioned that the continued development of this system will result in improved interactions, making public services more efficient and accessible to the public. This technological advancement aligns with the broader goal of facilitating seamless, secure, and trustworthy notarial services in the digital age.

REFERENCES

[1] Aceto, G., Persico, V., & Pescapé, A. (2018). The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges. *Journal of Network and Computer Applications*, *107*, 125–154. https://doi.org/10.1016/J.JNCA.2018.02.008

[2] Adekotujo, A., Odumabo, A., Adedokun, A., & Aiyeniko, O. (2020). A Comparative Study of Operating Systems: Case of Windows, UNIX, Linux, Mac, Android and iOS. *International Journal of Computer Applications*, *176*(39), 16–23. https://doi.org/10.5120/ijca2020920494

[3] Adi Putra, R., Yupianti, & Prasetyo, E. R. (2023). Android-Based Text Message Encryption and Decryption Application Using the Advanced Encryption Standard Algorithm Aplikasi Enkripsi Dan Dekripsi Pesan Teks Berbasis Android Menggunakan Algoritma Advanced Encryption Standard. *Jurnal Media Computer Science*, *2*(1), 57–62.

[4] Afifah, K. (2017). Tanggung Jawab dan Perlindungan Hukum bagi Notaris secara Perdata Terhadap Akta yang Dibuatnya. *Jurnal Lex Privatum*, *2*(1), 147–161.

[5] Azhari, M., Perwitosari, J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains Dan Komputer*, *2*(1), 2809–476. https://doi.org/10.47709/jpsk.v2i1.1390

[6] Bancin, H., Panjaitan, M. A., Putri, S., Nasution, A. B., Informasi, S., Sains, F., & Teknologi, D. (2023). Implementation of Cryptography with the Caesar Cipher Method to Secure Data Files in Java NetBeans Implementasi Kriptografi dengan Metode Caesar Cipher untuk Mengamankan Data File di Java NetBeans. *Jurnal Sistem Telekomunikasi Elektronika Sistem Kontrol Power Sistem & Komputer*, *3*(1). https://doi.org/10.32503/jtecs.v3i1.3210

DOI: 10.17148/IJARCCE.2023.121109

[7] Cellina, M., Cè, M., Marziali, S., Irmici, G., Gibelli, D., Oliva, G., & Carrafiello, G. (2022). Computed tomography in traumatic orbital emergencies: a pictorial essay—imaging findings, tips, and report flowchart. *Insights into Imaging*, *13*(1). https://doi.org/10.1186/s13244-021-01142-y

[8] Dhansukhbhai Patel, D., & Desai, S. (2023). Securing textual information with an image in the image using a visual cryptography AES algorithm. *International Journal of Enhanced Research in Management & Computer Applications*, *12*, 2319–7471. https://www.researchgate.net/publication/372496894

[9] Hassan, R., & Abbas Majeed, A. (2023). Fingerprint Data Security System Using Aes Algorithm on Radio Frequency Identification (RFID) Based Population System. *International Journal of Informatics Technology (INJIT)*, *1*(1). https://jurnal.amrillah.net/index.php/injit

[10] Hidayat, A. (2022, March 8). *67% Penduduk Indonesia Punya Handphone pada 2022, Ini Sebarannya*. Badan Pusat Statistik.

[11] Juridical, M., Heriadi, M., Komang Luki Nanda, Mk. I., Agung Putra Arjawa, A., & Wayan Bandem, I. (2023). Juridical Analysis of The Issuance of Deeds of Sale and Purchase of Land in Jembrana District at The Office of The Notary/PPATI Komang Divo Mahayakti Heriadi, S.H., M.Kn. *Nusantara Hasana Journal*, *3*(6), Page.

[12] Kamarudin, S., & Mohammad, M. I. (2011). File Security based on Pretty Good Privacy (PGP) Concept. *Computer and Information Science*, *4*(4). https://doi.org/10.5539/cis.v4n4p10

[13] Kusuma Wardhini, N. (2022). Pembuatan Akta Jual Beli Yang Tidak Dibacakan Oleh Pejabat Pembuat Akta Tanah Di Hadapan Para Pihak Dalam Putusan Mahkamah Agung Nomor 627/PK/Pdt/2018. *Indonesian Notary*, *4*(2). https://scholarhub.ui.ac.id/notary/vol4/iss2/9

[14] Mulud Muchamad, R., & Pambudi, A. (2023). Implementasi Algoritma Advanced Encryption Standard (AES) Untuk Mengenkripsi Datastore Pada Aplikasi Berbasis Android. *Jurnal MNEMONIC*, *6*(1). https://issuetracker.google.com/issues/167697691

[15] Nurrahmi, T. F., Setyaningsih, E., & Herawati, N. (2020). Keamanan file dokumen menggunakan algoritme Advanced Encryption Standard pada aplikasi berbasis Android. *Jurnal Open Access Yayasan Lentera Dua Indonesia*, *1*(1). https://doi.org/https://doi.org/10.36802/jnanaloka.2020.v1-no1-11-23

[16] O'Reilly-Shah, V., & MacKey, S. (2016). Survalytics: An open-source cloud-integrated experience sampling, survey, and analytics and metadata collection module for android operating system apps. *JMIR MHealth and UHealth*, *4*(2). https://doi.org/10.2196/mhealth.5397

[17] Ramadhani, W. (2017). Penegakan Hukum Dalam Menanggulangi Pungutan Liar Terhadap Pelayanan Publik. *Jurnal Hukum Samudra Keadilan*, *12*(2). http://majalahkartini.co.id/berita/peristiwa/saber-pungli-program-pemerintah-sapu-bersih-pungli/

[18] Selvapriya, E. S., & Suganthi, L. (2023). Design and implementation of low power Advanced Encryption Standard cryptocore utilizing dynamic pipelined asynchronous model. *Integration*, *93*, 102057. https://doi.org/10.1016/J.VLSI.2023.102057

[19] Sharma, A. (2018). Development of android application services at Arokia and its architecture. *National Journal of Multidisciplinary Research and Development Www.Nationaljournals.Com*, *3*, 1072–1075. www.nationaljournals.com

[20] Smid, M. E. (2021). Development of the advanced encryption standard. *Journal of Research of the National Institute of Standards and Technology*, *126*. https://doi.org/10.6028/JRES.126.024

[21] Szymkowiak, A., Melović, B., Dabić, M., Jeganathan, K., & Kundi, G. S. (2021). Information technology and Gen Z: The role of teachers, the internet, and technology in the education of young people. *Technology in Society*, *65*, 101565. https://doi.org/10.1016/J.TECHSOC.2021.101565

[22] Widodo, B. E., & Purnomo, A. S. (2020). Implementasi Advanced Encryption Standard Pada Enkripsi dan Dekripsi Dokumen Rahasia Ditintelkam Polda DIY. *Jurnal Teknik Informatika (Jutif)*, *1*(2), 69–77. https://doi.org/10.20884/1.jutif.2020.1.2.21

[23] Zhang, P., Dou, W., & Liu, H. (2023). Hierarchical data structures for flowchart. *Scientific Reports*, *13*(1). https://doi.org/10.1038/s41598-023-31968-z