International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.
© 2024 Scholar AI LLC.

Vol. 42 No. 2 January 2024, pp. 293-299

AES 128 Feasibility at Dr.Mintoharjo for National Defense

Ni Putu Ayu Astriyani[1], Danang Rimbawa[2], Budi Raharjo[3]

[1]Study Program: Cyber Defense Engineering
Faculty of Defense Technology, Defense University
Sentul, Indonesia

[2]Study Program: Cyber Defense Engineering
Faculty of Defense Technology, Defense University
Sentul, Indonesia

[3]Study Program: Cyber Defense Engineering
Faculty of Defense Technology, Defense University
Sentul, Indonesia

Abstract—The research project creates a standard for applying the Advanced Encryption Standard (AES) 128 to the Dr. Mintoharjo Hospital database. Beginning with a hacking incident on the Health Social Security Administering Body (BPJS) website bpjs-kesehatan.go.id, which is expected to occur around the end of May 2021 and resulted in the leak and sale of data belonging to 279 million Indonesians on Raid Forums this demonstrates a vulnerabilities in national cyber protection, the author proposes a new storage method for the information technology division that is safer than traditional storage techniques. MYSQL uses the Advanced Encryption Standard (AES) 128 technique defined here. When the Dr. Mintoharjo Hospital management information system was built in MYSQL, security levels were assessed using Advanced Encryption Standard (AES) 128 encryption technology. The experimental results of this study show enhanced safety results from an efficiency aspect. The study's conclusion shows that the storage method studied improves the security system, hence it is strongly recommended that it be adopted at Dr. Mintoharjo.

Keywords—Defense, Cyber, Security, AES, Encrypt.

I. INTRODUCTION

An agency must have seven basic principles in cyber security policy, where the organization must have a clear information security policy and communicate it to all related parties planning, where the organization must develop an information security plan that includes steps to reduce cyber security risks implementation and operations, where organizations must implement and operate cybersecurity controls to reduce cybersecurity risks; and assessment and audit, where organizations must regularly assess and audit the effectiveness of their cybersecurity controls, continuous improvement where organizations must continuously improve their information security management systems [7]. Considering the accelerated development of digital technology in society resulting in the digital transformation of health services so that medical records need to be held electronically with the principles of security and confidentiality of data and information, Minister of Health Regulation Number 269/MENKES/PER/III/2008 concerning Medical Records is no longer in accordance with scientific developments. knowledge and technology, health service needs, and community legal needs. Based on the considerations as intended in letters a and b, as well as to implement the provisions of Article 47 paragraph (3) of Law Number 29 of 2004 concerning Medical Practice and

Article 72 of Law Number 36 of 2014 concerning Health Personnel, it is necessary to stipulate a Regulation of the Minister of Health about Medical Records. So changes to medical records that are adjusted to the acceleration of technological development are adjusted in the Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 concerning Medical Records. Indonesia's defense system in cyber terrorism is still quite lax, due to a lack of public education and awareness in using the media [9]. Indonesia has taken various efforts to maintain its independence, one of which is by building a strong defense system. The development of a strong defense system is aimed at defending state sovereignty, the integrity of the Republic of Indonesia, and the safety of the entire nation from threats and disturbances to the integrity of the nation and state. To defend the country's sovereignty from threats and disturbances, Indonesia implements a universal defense system (sishanta) [8]. Reporting from the official website of the Ministry of Defense, it is explained that Indonesia's defense system is universal, involving all national resources which were prepared early by the government. Held in a total, integrated, directed and sustainable manner to uphold state sovereignty and maintain its integrity.

II. METHOD

2.1 National Defense of Critical State Object

National hospital is one of critical state object thus, the security of data held in the hospital must be considered. A systematic process was used to improve data center security by developing a complete risk assessment model. This strategy begins by defining the scope and objectives of the investigation. Following this initial phase, a detailed literature review was done to lay the groundwork for the model. The data collection method involves gathering historical event data and external threat information feeds from the data center environment.

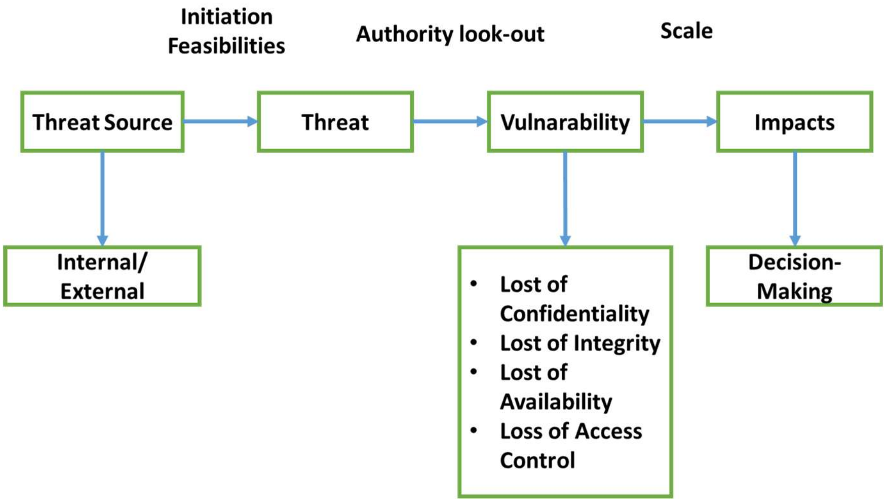


Fig 1. Hospital information system feasibility design at Dr. Mintoharjo

The nest phase entails creating a risk assessment model. This includes designing the model architecture, developing algorithms, and integrating important features such as machine learning, as well as taking into account human factor threats. The model's intelligence, accuracy, and effectiveness are extensively evaluated against real-world data. In addition, the model is tested in a simulated data center setting to determine its practical applicability. Comprehensive documentation and reporting are required for clarity.

2.2 Encryption and Decryption AES 128

Cryptographic algorithms are also called ciphers, namely the rules for enciphering and decrypting, or mathematical functions used for encryption and decryption, [3]. Some ciphers require different algorithms for enciphering and dechipering. The security of a cryptographic algorithm is often measured by the amount of work required to break the ciphertext into plaintext without knowing the key used. If the more processing required means the longer it takes, the stronger the algorithm and the safer it is to use to encode messages.

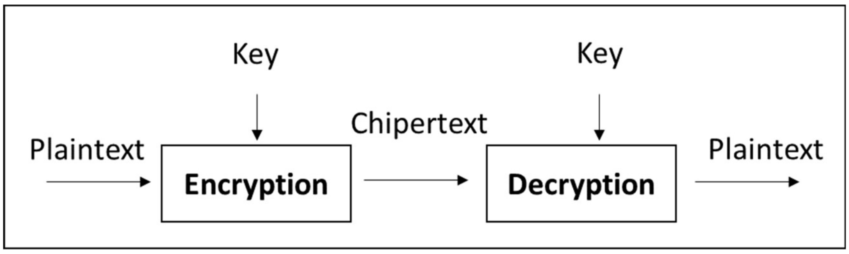


Fig. 2 Encryption and Decryption Process

Cryptographic algorithms consist of several basic functions, namely encryption, which is very important in cryptography which is the security of data sent and kept confidential, the original message is called plaintext which is changed into codes that cannot be understood and decryption, which is the opposite of encryption, is a message that has been encrypted is returned to its original form (plaintext) which is called message decryption while the key is the key used to carry out encryption and decryption, the key is divided into 2 (two) parts, namely the private key and the public key. In general, the encryption and decryption process can be shown in Figure 2. Dr. Vincent Riment and Dr. Joan Daemen won a competition organized by NIST in 2001 to develop the AES algorithm in order to improve the DES method; since then, the AES algorithm has been referred to as the Rijdel algorithm [4]. The Rijndael method was picked as the winner not because it is the safest algorithm, but because it strikes a balance between security and versatility across multiple software and hardware platforms [13].

III. IMPLEMENTATION AND DISCUSSION

In various activities, Dr. Mintoharjo plays an active role in various national and international events, such as cooperation in military and non-military matters. A hospital that has received accreditation by the Ministry of Health of the Republic of Indonesia, making Dr. Hospital. Mintohardjo always develops health activities and current developments in information technology.

3.1 Encryption for National Defense

Following an inspection and assessment of the study region. Researchers conducted an analysis related to the problems, goals and targets of the system that was running to determine the flow of the health information system owned by the Dr Mintohrdjo. The status of the Hospital information system that is now in use can be seen in figure 3.

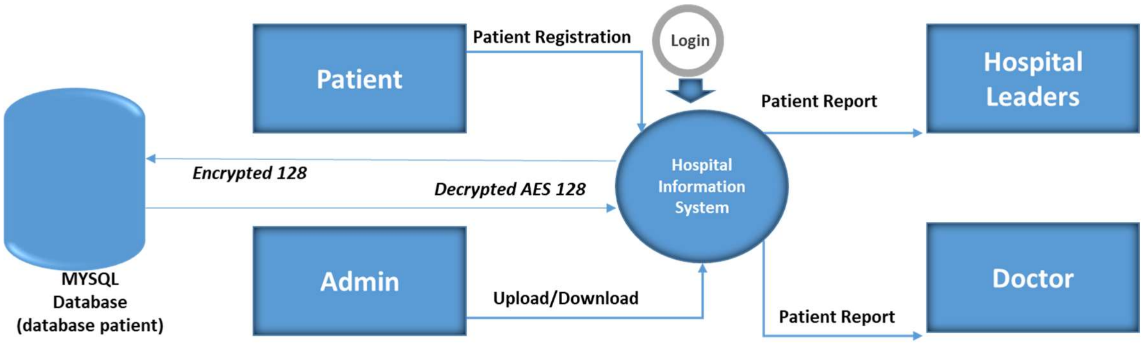


Fig. 3 Proposed Management Information System Dr. Mintoharjo with AES 128

Dr. Mintoharjo hospital management information system based on Figure 3 accommodates patient data from the military. Securing this data is very important in maintaining the country's defense from data leaks that lead to acts of terrorist threats or espionage carried out by other countries. The Hospital Management Information System proposed by this research is a Management Information System that implements AES encryption on the MYSQL database, where this security system is highly recommended in government agencies.

3.2 Aes 128 Implementation in Hospital Manajemen Information System

Based on the description of the current system analysis, a system is needed that is an alternative solution for securing databases related to patient data at the Indonesian Navy Hospital. where this application secures the database using AES encryption.

Functional requirements are the functions of the system that are visible after the system has been described, these functional requirements will later become the main features of the system. The following is an overview of the proposed system that will be implemented.

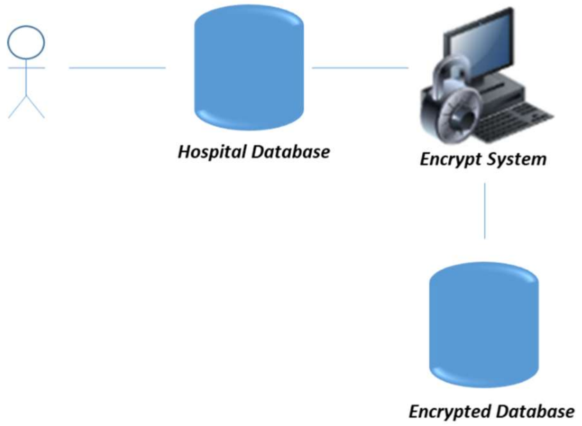


Fig 4. AES 128 encryption implementation proposed at Dr. Mintoharjo

Figure 4 explain the system will be propose. Where’s the IT staff will secure the patient-related database using the encryption system that the researcher created. Then the system will save the database in the form of an encrypted file so that it is difficult to crack.

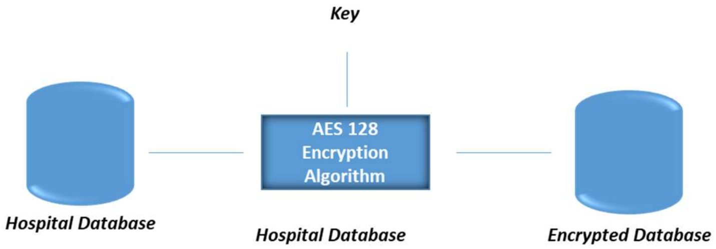


Fig. 5 Design of encryption AES 128

This encryption process begins when the IT staff wants to secure the database by uploading a file with the extension .sql through the system.

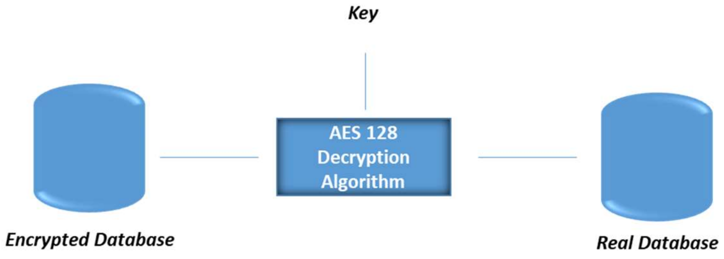
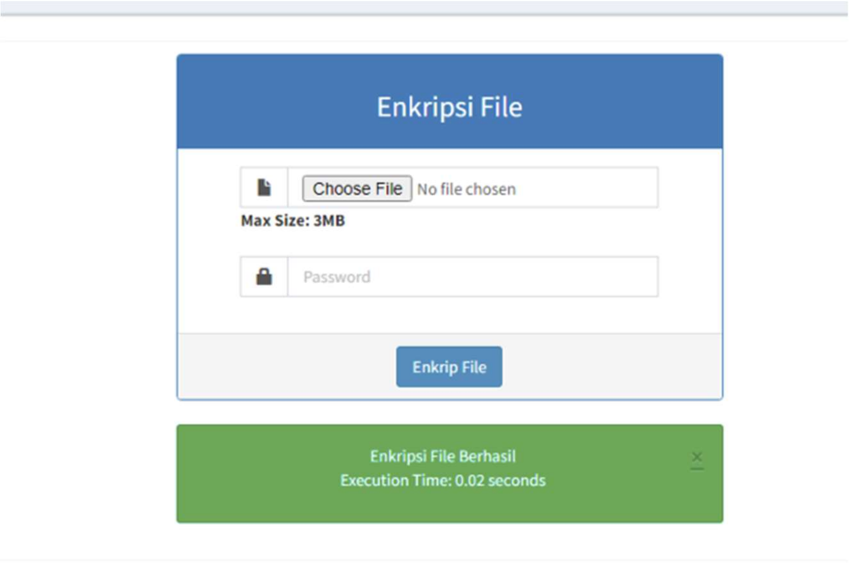


Fig. 6 Desix`gn of decryption AES 128

This decryption process is a process to restore a database that has been encrypted into an initial database file that can be read by hospital IT staff. To decrypt the database, IT staff needs to upload the encrypted database into the system that the author has created. Then the system will match the database you want to decrypt with the previously determined keywords. If successful, the system will carry out the process of decrypting the database file. The output that will be produced is a database file with the extension of sql.



Enkripsi File

Choose File No file chosen

Max Size: 3MB

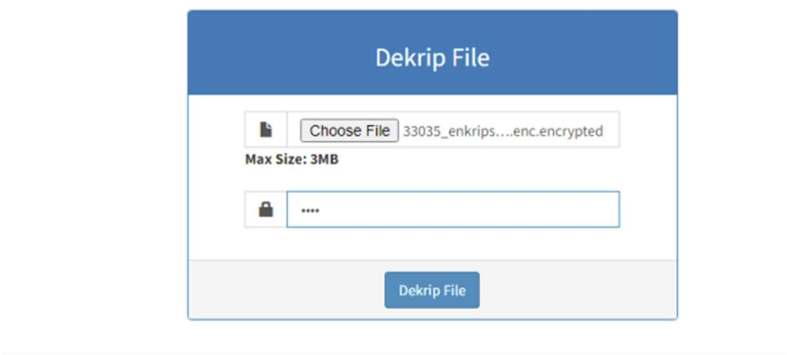
Password

Enkrip File

Enkripsi File Berhasil
Execution Time: 0.02 seconds

Fig. 7 Successful database encryption system

Figure 7 is successful encryption system form, it will provide a notification that the database file encryption has been successful and display the AES encryption computing time to encrypt the database. Next is the form for decrypting the encrypted database file. Users will be directed to select a database that has been encrypted and enter the password that was created during the encryption process.



Dekrip File

Choose File 33035_enkrips....enc.encrypted

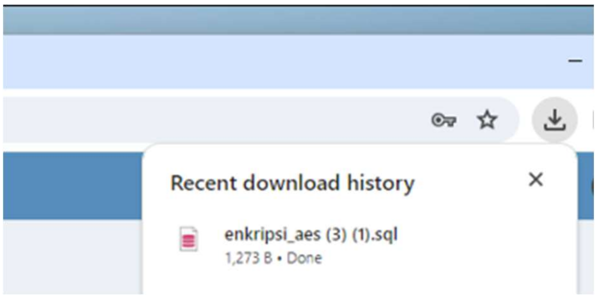
Max Size: 3MB

••••

Dekrip File

Fig. 8 Form decryption file

Next, if the fields are filled in, click the decrypt file button. If successful, the database file will return to its origin before encryption is carried out as shown in figure 8 with an output file with the extension .sql, shown in figure 9.



Recent download history

enkripsi_aes (3) (1).sql
1,273 B • Done

Fig. 9 Output file with sql. extention

IV. CONCLUSION

Based on the test scenarios that have been carried out, the following are the conclusions of this research regarding the implementation of an AES128-based encryption system that is effective in securing databases at Dr. Mintohardjo with aim of increasing national defense.

4.1 Research Development Advise

Following are suggestions regarding the development of this research:

1.1.1 *Perform other security algorithm method*

1.1.2 *Implement a level of security not only for the database.*

4.2 Recommendation to Government

This research can be utilized to help the government design safety system regulations. This rule can then serve as a mechanism for the military sector to design safe ignition systems while prioritizing user safety.

4.3 Recommendation to Defense Industri

It is hoped hat cryptography research on hospital information data security would be a type of technological breakthrough in cyber security systems established by the defense sector.

References

The template will number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use “Ref. [3]” or “reference [3]” except at the beginning of a sentence: “Reference [3] was the first ...”

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors’ names; do not use “et al.”. Papers that have not been published, even if they have been submitted for publication, should be cited as “unpublished” [4]. Papers that have been accepted for publication should be cited as “in press” [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

[1] A. Colussi and D. Algoritma, *“Perancangan Aplikasi Pencarian File Teks dengan Menggunakan,”* vol. 6, no. 1, pp. 24–29, 2019.

[2] A. F. Marisman and A. Hidayati, “Pembangungan Aplikasi Pembanding Kriptografi dengan Caesar Cipher dan Advance Ecryption Standard(AES) untuk File Teks,” J. Penelit. Komun. dan Opini Publik, vol. 19, no. 3, pp. 213–222, 2015.

[3] A. Kurniawati and M. D. Darmawan, *“Implementasi Algoritma Advanced Encryption Standard (Aes) Untuk Enkripsi Dan Dekripsi Pada Dokumen Teks.”*

[4] A. Arif and P. Mandarani*, “Rekayasa Perangkat Lunak Kriptografi Menggunakan Algoritma Advanced Encryption Standard (AES) 128 Bit Pada Sistem Keamanan Short Message Service (SMS) Berbasis Android,”* Teknoif, vol. 4, no. 1, pp. 1–10, 2016.

[5] A. R. Tulloh, Y. Permanasari, and E. Harahap, “Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen Cryptography Advanced Encryption Standard (AES) for File Document Encryption sebagai agensi departemen perdagangan AS menetapkan sebuah standard kriptografi Standard (AES),” Pros. Mat., vol. 2, no. 2460–6464, pp. 118–125, 2016.

[6] Ariyus, Doni, *Kriptografi Keamanan Data dan Komunikasi*, Yogyakarta: Graha Ilmu, 2006.

[7] Indonesia. ISO 27001, *Information security cybersecurity and privacy protection-information security management systems-requirement*,. Jakarta, 2022.

[8] Indonesia. Permenhan 82 Tahun 2014, Pedoman Pertahanan.

[9] R. Primartha, *"Penerapan Enkripsi dan Dekripsi File menggunakan Algoritma Advanced Encryption Standard (AES),"* J. Res. Comput. Sci. Appl., vol. 2, no. 1, pp. 13–18, 2013.

[10] S. Kom, *"Implementasi Algoritma Brute Force Dalam Pencarian Kebudayaan Di Indonesia Berbasis Mobile Application,"* vol. 4, pp. 31–38, 2018.

[11] S. Meitarice, M. Begum Peer Mustafa, and D. O. Andi, *"AUTOMATED TASK MANAGEMENT SYSTEM USING ANALYTICAL HIERARCHY*

PROCESS," J. Tek. Inform., vol. 13, no. 2, 200AD.

[12] S. H. Putra, E. Santoso, and L. Muflikhah, *"Implementasi Algoritma Kriptografi Advanced Encryption Standard (AES) Pada Komprsi Data Teks,"* 2012.

[13] M. S. Dharmawan, Eka Adhitya , Erni Yudaningtyas*, "Perlindungan Web pada Login Sistem Menggunakan Algoritma Rijndael,"* Eeccis, vol. 7, no. 1, pp. 77–84, 2013.