Securing the electronic medical record by implementing Advanced Encryption Standard (AES) on the information system of a health service place

C Rahmad¹, A R Syulistyo¹,*, and A D W Sumari¹,²,³

¹Department of Information Technology, State Polytechnic of Malang, Jl. Soekarno-Hatta No. 9, Malang 65141, East Java, Indonesia
²Cognitive Artificial Intelligence Research Group (CAIRG), Department of Electrical Engineering, State Polytechnic of Malang, Jl. Soekarno-Hatta No. 9, Malang 65141, East Java, Indonesia
³Faculty of Defense Technology, Indonesia Defense University, IPSC, Sentul, Bogor, West Java, Indonesia

*arie.rachmad.s@polinema.ac.id

Abstract. Medical records are very crucial in health services all over the world. This is due to not only to record individual health conditions but also for getting the most appropriate medical services at a local health facility when in mobile conditions. By having a look at the medical records, the local health workers can know the medical history and give their best service in treating the patient. Conventional medical records commonly are written manually and are not flexible for the mobile environment. Therefore, the electronic medical record (EMR) has become mandatory to be implemented to cope with such problems. Another important thing that requires attention is the patient has the right to know the contents of the medical record, especially when having health services at a different hospital or other health services when at mobile conditions. Accessing the EMR from the mobile environment brings a crucial matter, namely, how to secure the contents of EMR and ensure that the access can only be given to the legitimate owner fit as well as other legitimated actors such as the related doctors and the EMR officials. Based on the arisen problem, the contribution of this research is to make the implementation of encryption algorithms that will be used on Secure Electronic Medical Record (SEMR) systems using secure and fast encryption techniques by using Advanced Encryption Standard (AES) on the information system of a health service place.

1. Introduction
The advancement of information and communication technology (ICT) along with the introduction of Industrial Revolution 4.0 technologies a couple of years ago does not always have a big impact on health services such as hospitals primarily community health services or Public Health Center or Puskesmas [1]. Providing the best services to patients, medical records are one of the keys [2]. The medical record is a compilation of facts about the health condition and illness of a patient which includes documented data about the present and past illness condition, and written medication that has been and will be carried out by a health worker [3]. This is very important when patients change public health care places so that it makes it easier for medical personnel at that place to find out about the patient’s medical history. The
facts show that medical records of the patient on several hospitals and Public Health Center are still handled conventionally [4,5]. Meaning, the records are still stored in hard-form folders and not in digital format.

On the other hand, the dynamic mobility of the community allows people to seek treatment at the hospital or Puskesmas where they are at that time. These situations make medical records a very important document and access to medical records is very crucial in health care services [3]. This mobile condition happens for everyone who travels a lot whether in-country or abroad. Conventional medical records that are stored in hard-form folders are no longer able to support this condition. Therefore, medical records that are stored in electronic form have become mandatory since they have to comply with the recent technologies and in order to enhance the health services. Since then Electronic Medical Record (EMR) became a standard for storing health services given to patients as well as recording their health conditions.

There is one important thing that has to get serious attention, namely patients have the privilege to know the contents of the medical records, especially when receiving health services from hospitals or Puskesmas. One solution to dealing with this problem is to create an information system that stores medical records electronically and has a standard so that it can be easily integrated between hospitals and Puskesmas. Accessing the EMR from the mobile environment brings a crucial matter, namely, how to secure the contents of EMR and ensure that the access can only be given to the legitimate owner of it as well as other legitimated actors such as the related doctors and the EMR officials. However, the application of EMR made medical personnel doubt, but after being passed the Law on Information and Electronic Transactions (UU ITE) Number 11 of 2008 has provided answers to such doubts [6]. The ITE Law has provided opportunities for EMR implementation. Based on the arisen problem, the contribution of this research implements an encryption algorithms that will be used on Secure Electronic Medical Record (SEMR) systems using secure and fast encryption techniques by using Advanced Encryption Standard (AES).

2. Background study

2.1. Electronic Medical Record (EMR)
EMR is a digital version of a patient’s medical record which consists of a patient’s treatment from certain care delivery organizations (CDO) such as hospital or community health service by a particular medical worker such as general doctor, specialist doctor, and dentist. It also contains the doctor’s diagnosis and drugs given to the patient as well as other related medical information. EMR is said only documented and stored at CDO such hospitals or community health services especially in remote areas that are very far from the closest hospitals in their areas. Meanwhile, Electronic Health Record (EHR) is said that the MR file can be brought by the patient and can be accessed by other CDOs that deliver health care to the patient. It is like the MR is attached to the patient wherever he/she goes. EHR is more flexible that EMR but anything that is relaxed will invite threats.

As has been known, MR is an old kind of health data recording which has been carried out for a long time in the health care world. MR is a very important private health document not only for the patient him/herself but also for the caring doctor as well as CDO that delivers health care. The introduction of information technology brought positive impacts to EH/MR where it was recorded by hand-written and put in the folders, now it can be done electronically and stored in an electronic manner. In the era of cyberspace, medical or health information becomes an important target for certain actors and it can be used to do harmful things. Another thing that has become big attention is the possibility of unauthorized actors to access EM/HRs database and make them as ransom. Therefore protecting EM/HRs for this case will be considered as very important.

2.2. System Usability Scale (SUS)
The System Usability Scale (SUS) was created by John Brooke in 1986 as a "quick and dirty" questionnaire. This questionnaire allows practitioners to quickly and easily assess the usability of a
particular product and services [7]. Originally this tool consisted of 10 questionnaire items with five response scales with a minimum score of 1 which means strongly disagree and a maximum value of 5 which means strongly agree. The three steps for calculating the SUS score are as follows [8]:

- For each of the odd numbered questions, subtract 1 from the score.
- For each of the even numbered questions, subtract their value from 5.
- Take new values which you have found, and add up the total score. Then multiply this by 2.5.

The calculation results that you have a maximum score of 100.

2.3. Advanced Encryption Standard (AES)

Medical image record should be encrypted to ensure privacy and integrity, and it was recommended to use AES [9]. AES has been introduced by NIST in 2000 which has 4 main operational blocks, such as:

- Substitute byte transformation: An S-box is used to substitute each data block byte with another block.
- Shift transformation of rows: Each row of the state matrix is given a cyclic shift to the right side according to its location.
- Mix Transformation of Columns: It is a matrix multiplication operation where each column of the state matrix is multiplied by that of the fixed matrix.
- Add Round Key Transformation: XOR operation is performed between the new state matrix and the round key one.

AES algorithm based on electronic codebook is simplest to implement however, the same block of plaintext will always generate the same block of ciphertext, this can give clues for attackers. So, in this research, we choose AES encryption based on cipher block chaining (CBC) mode which illustration can be seen in Figure 1 [10].

![Figure 1. AES cipher block chaining mode structure.](image_url)
3. Proposed method
This research consists of 3 stages, namely information system development, encryption algorithm implementation, and the last integrating encryption algorithm and information system. The encryption algorithms are used to encrypt digital images only. Three stages of this research are given in the following illustration.

![Figure 2. Research stages.](image)

3.1. Information system development
The information system was mainly developed by using PHP language. The information system has several functions, including online queuing and recording medical records. In recording medical records in the digital image section, an encryption algorithm will be integrated to encrypt digital image data.

3.2. Advanced Encryption Standard (AES) algorithm implementation
This research focuses on encrypting digital image data using the AES algorithm. The illustration on the x-rays image is as follows. The image is taken from several open sources on the internet and the size of the image used for the experiment varies.

![Figure 3. Head X-rays.](image) ![Figure 4. Chest X-rays.](image)

4. Results and discussion

4.1. Usability measurement of information system
The information system which has develop can be seen on figure 5 and 6. After the development of information system then we measure the usability of this system by using system usability scale. The usability scale which used on this paper consist of 7 questions, such as:

- The information system has no benefit for the user
- The information system provides the promised online queue feature
- The information system is difficult for users to access
- The information systems can be operated comfortably without problems
- The information systems can produce data information accurately as needed
- The information systems can solve long time problems in patient queues
- The information system user interface is good
The SUS which already designed and distributed to 3 users then we recapitulate the questionnaire. We get score 69 of the overall usability score of the system. Based on the usability score, these scores above the average however, this system should be improved to get a better score. This can be caused due to the lack of the information system flow or the information provided to the user that is not precise so that the user feels moderate about the application being developed.

4.2. Implementation Result of Advanced Encryption Standard (AES)

Encryption of digital images has been implemented using the PHP language. The steps to encrypt medical images by converting medical images into strings with the base64 function in PHP. Then the string is encrypted using the AES algorithm in Figure 1. Based on the evaluation results, the AES algorithm can perform encryption and decryption with an average speed of 1MB / sec. Encryption illustration can be seen in Figure 7. The results of the decryption can be converted back into an image with the decode_base64 function in PHP.
5. Conclusion
Medical record documentation is essential to provide good quality services for patients, accurate and timely to reduce the risk of malpractice. And to help health care providers evaluate, plan patient handling, and maintain continuity of treatment. This research succeeded in developing an information system for recording medical records that has been integrated with an encryption algorithm so that only users who have access can view medical records.

References
[1] Min J, Kim Y, Lee S, Jang T W, Kim I and Song J 2019 The fourth industrial revolution and its impact on occupational health and safety, worker's compensation and labor conditions Safety and health at work 10(4) 400-408
[2] Ajami S, Ketabi S and Torabiyan F 2015 Performance improvement indicators of the Medical Records Department and Information Technology (IT) in hospitals Pakistan Journal of Medical Sciences 31(3) 717
[3] Bali A, Bali D, Iyer N and Iyer M 2011 Management of medical records: facts and figures for surgeons Journal of maxillofacial and oral surgery 10(3) 199
[4] Tang P C, Fafchamps D and Shortliffe E H 1994 Traditional medical records as a source of clinical data in the outpatient setting In Proceedings of the Annual Symposium on Computer Application in Medical Care (p. 575) American Medical Informatics Association
[5] Vaidotas M, Yokota P K O, Negrini N M M, Leiderman D B D, Souza V P D, Santos O F P D and Wolosker N 2019 Medication errors in emergency departments: is electronic medical record an effective barrier? Einstein (São Paulo) 17(4)
[6] P. R. INDONESI 2019 "https://kominfo.go.id," [Online] Available: https://web.kominfo.go.id/sites/default/files/users/4761/UU%2019%20Tahun%202016.pdf. [Accessed 24 August 2020]
[7] Anonim 2020 "https://www.usability.gov," [Online]. Available: https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html. [Accessed 24 August 2020].
[8] Thomas N 2020 Usability Geek [Online]. Available: https://usabilitygeek.com/how-to-use-the-system-usability-scale-sus-to-evaluate-the-usability-of-your-website/. [Accessed 25 August 2020].
[9] P Patil, P. Narayankar and e. al., "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," in International Conference on Information Security & Privacy, Nagpur, India, 2015.
[10] Veness C 2020 Movable Type Scripts [Online] Available: https://www.movable-type.co.uk/scripts/aes.html. [Accessed 24 August 2020]