IOP Conference Series:
Materials Science and
Engineering

PURPOSE-LED
PUBLISHING™

PAPER • **OPEN ACCESS**

Designing and Building Secure Electronic Medical Record Application by Applying AES-256 and RSA Digital Signature

To cite this article: Galih Wening Werdi Mukti and Hermawan Setiawan 2020 *IOP Conf. Ser.: Mater. Sci. Eng.* **852** 012148

View the article online for updates and enhancements.

You may also like

- An automatic grading system for electronic medical records with neural network
  Yi Liu
- Blockchain-powered healthcare system – a systematic literature review
  Monica Rexy F and Priya G
- Chronic inflammation in a radium dial painter cohort: elevated neutrophil to lymphocyte ratio and radiation-induced hearing loss
  R E Goans, L T Dauer, C J Iddins et al.

This content was downloaded from IP address 125.234.95.152 on 15/12/2025 at 18:02

Designing and Building Secure Electronic Medical Record Application by Applying AES-256 and RSA Digital Signature

Galih Wening Werdi Mukti, Hermawan Setiawan
National Crypto Institute
galih.wening@student.stsn-nci.ac.id, hermawan.setiawan@stsn-nci.ac.id

Abstract. Medical records consist of health data that must be kept confidential and is regulated in Indonesian law. Until now the implementation of electronic medical records in Indonesia has not been clearly regulated in a law, while Regulation of the Minister of Health of the Republic of Indonesia state that medical records must be made in writing, complete, and clearly or electronically. In view of this, another approach than the regulation is needed to be able to meet the confidentiality of the data in the regulation, in electronic form. In this study, an electronic medical record application was designed and built that can meet the requirements of the legislation. The application encrypts patient's health data stored on medical records using the AES-256 algorithm for data confidentiality. The use of AES-256 has been standardized based on the Federal Information Processing Standards Publication 197 and RSA Digital Signature digital signature because it has been standardized based on Federal Information Processing Standards Publication 186-4 and NIST Special Publication 800-89. The proposed application have been made have passed security testing using 6 testcase based on the reference paper.

1. Introduction

Medical records and health data must be kept confidential and regulated in Indonesian legislation, namely law number 29 of 2004 concerning medical practices in article 47 and 48, Government Regulation number 46 of 2014 concerning health information systems article 23 and Minister of Health Regulation Number 269 of 2008 concerning medical record article 10. In the world there are also standards, namely HIPAA which is used in America and Europe, which also regulates the confidentiality of patient data [1]. Although the confidentiality of medical records has been regulated in laws and regulations, until now the implementation of electronic medical records in Indonesia has not been clearly regulated in a statutory regulation, while based on the Minister of Health Regulation Number 269 of 2008 article 2 states that medical records must be made in writing, complete and clear or electronically, and further regulated by separate regulations.

In the current digital era, there are many cases of theft of health data in hospitals. One of the most common cases in the world is ransomware. The US Department of Justice in 2016 estimates an average of 4000 ransomware attacks per day. The health industry is the most frequent target compared to other industries, namely 88% of all ransomware detected in 2012-2016. Factors that cause an increase in ransomware attacks in the health industry are the value of patients' medical record data that can be sold up to 50 times on the black market compared to the value of credit card data, the transition of the health industry to electronics, and the lack of technological security used. One way to prevent losses caused by ransomware is to encrypt important data [2]. Data encryption causes data to be unreadable, unusable, and cannot be understood by unauthorized people. So that the application of encryption to health data in medical records causes data not to be read and used by attackers of ransomware

In 2017 in Indonesia, two central hospitals in Jakarta that were victims of ransomware i.e. Dharmais Hospital and Harapan Kita Hospital [3]. Dharmais Hospital is a class B hospital, while Harapan Kita Hospital is a class A hospital. Basically, there are four classes of public hospitals in Indonesia, namely general hospitals class A, B, C, and D which are differentiated based on facilities and service capabilities possessed. The survey results of the Directorate General of Health Services of the Ministry of Health of the Republic of Indonesia [4] indicate that class C general hospitals are the most visited hospitals by the community, which is 51.5%. The threat of ransomware that has attacked hospitals class A and B in Indonesia has the potential to also be able to attack C-class or D-class hospitals that have infrastructure

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

facilities under class A and B hospitals. Class C hospitals are hospitals in each district/city which is a direct reference from a puskesmas or class D hospital, so that class C general hospitals have a high operational level compared to general hospitals class A and B but the infrastructure and service capabilities possessed by class C hospitals are still under class A hospitals and B based on the order of classification in [5].

In this study, an electronic medical record application will be designed and built by applying encryption of patient health data stored in medical records using the AES-256 algorithm because based on literature studies [6] it can be seen that the Advanced Encryption Standard (AES) is the most efficient and become standard by Federal Information Processing Standards Publication 197 [7]. The application is made using data from SIMRS Khanza which is an open source SIMRS that has been used by more than 30 hospitals in Indonesia. Based on the Republic of Indonesia Minister of Health Regulation number 46 of 2017 also states that e-health digital signature services need to be made to support electronic data security. Digital signatures are used to authenticate doctors who make medical records. Digital signatures are implemented using RSA Digital Signature because they have been standardized based on Federal Information Processing Standards Publication 186-4 and NIST Special Publication 800-89. The application created is a web-based application that will be built using the PHP programming language because web applications are easier to update than desktop-based applications so that they can more easily adjust to changes in dynamic BPJS policies.

2. Method and materials

The methodology used for developing this system uses the Software Development Life Cycle (SDLC) methodology, Waterfall Development. Waterfall development consist of planning, analysis, design, implementation. The planning phase generates a system request and feasibility analysis, namely the reason for the project, project requirements, project benefits and special issues from the project obtained from the results of observations and interviews. At the planning stage a project work schedule is also produced.

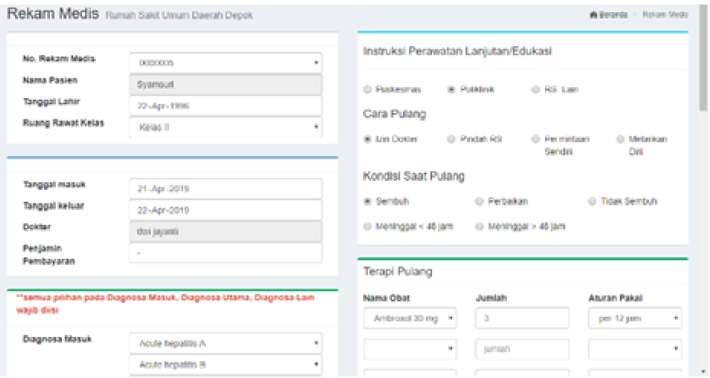
The analysis phase consists of three stages, namely understanding the system that is running. The result is obtaining the flow of the medical record making process to become a medical resume file. the medical resume that becomes the earliest sheet is given to the casemix officer for a scan and sent to BPJS for claim submission. The next step carried out in the analysis is to identify system updates that produce the flow of the medical record-making process to become a medical resume file when using the application and the next step is to define the requirements for the new system by analyzing previous results and conducting interviews. The final result of the analysis phase is the system requirements. System requirements are divided into two, namely functional and non-functional needs.

In design phase the application will be designed using the Unified Modeling Language (UML). Making UML diagrams using the Microsoft Visual Paradigm application. The results at this stage are use case diagrams, activity diagrams, sequence diagrams and class diagrams that are used at the implementation stage to make coding easier. In implementation phase, the application coding is started based on the results of the design. Making applications using the PHP programming language with CodeIgniter framework and MySQL database. After the coding process is complete, then the next application will be tested to determine the suitability of the results with the design.

3. Implementation

3.1. Create medical record file

Creating a medical resume begins with the doctor filling out the medical record form as shown in Figure 1. The form contains patient health data. The data used in the medical record form is taken from the SIMRS Khanza database. Most medical record forms consist of a dropdown menu that makes it easy for doctors to choose without having to type one by one. At the end of the medical record form, the doctor uploads the private key and the certificate that is used to process the digital signature.



Rekam Medis Rumah Sakit Umum Daerah Depok

No. Rekam Medis	0000005
Nama Pasien	Syamsul
Tanggal Lahir	22-Apr-1996
Ruang Rawat Kelas	Kelas II

Tanggal masuk	21-Apr-2019
Tanggal keluar	22-Apr-2019
Dokter	dwi jayanti
Penjamin Pembayaran	-

**semua pilihan pada Diagnosa Masuk, Diagnosa Utama, Diagnosa Lain wajib diisi

Diagnosa Masuk: Acute hepatitis A
Acute hepatitis B

Instruksi Perawatan Lanjutan/Edukasi

○ Puskesmas ● Poliklinik ○ RS Lain

Cara Pulang

● Izin Dokter ○ Pindah RS ○ Permintaan Sendiri ○ Melarikan Diri

Kondisi Saat Pulang

● Sembuh ○ Perbaikan ○ Tidak Sembuh
○ Meninggal < 48 jam ○ Meninggal > 48 jam

Terapi Pulang

Nama Obat	Jumlah	Aturan Pakai
Ambroxol 30 mg	3	per 12 jam
	jumlah	

Figure 1. Medical record page

If all data has been filled in, then at the end of the form there is a submit button to save all data entered into the database. If the data that is filled in is not complete then there is a notification so that the user fills in all the data in full. Before the data is stored, the system will encrypt patient health data based on [8] so that patient health data is stored in the database in an encrypted state. The system will display a notification of medical record data successfully saved if the data has been stored in the database. The notification page consists of two buttons, namely to create a medical pdf resume file and to send medical resume results to a medical record officer. If the button to make a medical pdf resume file is selected, the system will retrieve data from the database and decrypt the data that was encrypted beforehand. Then the system will display the data needed in the medical resume file and also display the ICD9 code and ICD10 code based on diagnosis and treatment names that have been filled by doctors on the medical record form.

3.2. Encryption and decryption

The encryption process is done automatically by the system that is after the user selects the submit button. Encrypted data include diagnosis, main diagnosis, other diagnoses, allergies, physical and supporting examinations, and treatment and patient identity, namely the name of the patient based on article 3 of [8]. The key used for encryption is a static key that is declared in the config file in Codeigniter. The decryption process occurs when the user selects a button to create a medical pdf resume file, the system will retrieve data from the database and decrypt previously encrypted data. The decrypted data is then displayed on a medical pdf resume file with a digital signature and a QR-code used to verify the doctor's identity and the integrity of the medical resume.

3.3. Digital signature

The process of digital signatures occurs when the user selects a button to create a medical pdf resume file. The library used for digital signatures is TCPDF, the private key that was previously uploaded by the doctor is used to verify certificates that have also been uploaded. If the private key matches the uploaded certificate, the system will create a digital signature based on the data on the uploaded certificate.

3.4. Medical resume verification

Medical resume verification can be done by medical record officers by selecting the medical record menu on the home page of the medical record officer. Doctor's signature verification can be done by opening files on the pdf reader application, in the implementation of this study using the Adobe Reader DC application.

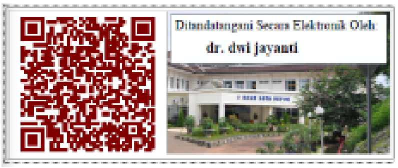
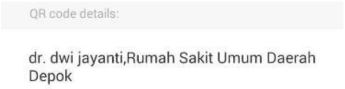


Figure 2. Digital signature in medical resume file

Verification of the identity on the medical resume maker can also be done by scanning the QR-code in the medical resume file as shown in Figure 2. Verification using QR-code can also be done if the medical resume file is printed.



QR code details:

dr. dwi jayanti,Rumah Sakit Umum Daerah Depok

Figure 3. QR-code scan result

Scanning QR-code can be done using the QR-code reader application in general, if the QR-code has been scanned it will display the name of the doctor who made the medical resume shown in figure 3.

4. Testing

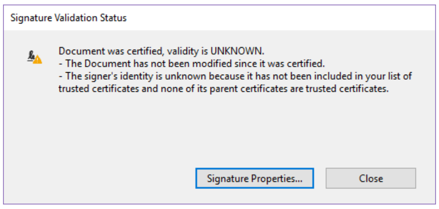
The application has passed unit testing, integration testing by testing each interface function, system testing by testing the performance of application based on the test results, the three actors had an average response time of admin 1.15 seconds, a doctor 1.58 seconds, and a medical record officer 1.92 seconds. From the test results it can be concluded that the application has a time that is still acceptable to the user which is about 1 second and under 10 seconds**.** Below is an explanation of security testing in the application :

1. Digital signature

   The use of digital signatures in medical records provides guarantees:

   a. Authentication: to authenticate the doctor who signs the medical resume is really a legitimate doctor. This is indicated by the doctor's identity contained in the QR-code and certificate used by the doctor for digital signatures.

   b. Data integrity: to ensure the integrity of the medical resume data so that it cannot be modified and can be known if data changes occur. This is indicated by the notification that the document is still intact and there is no modification if a medical resume with a digital signature is opened in the pdf reader application. The notification is in figure 4. In figure 4 shows that the document was certified and has not been modified since it was certified.

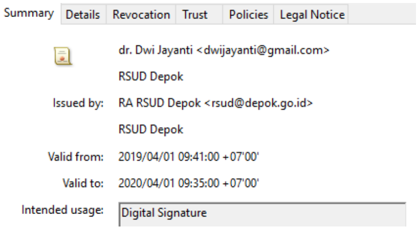


Signature Validation Status

Document was certified, validity is UNKNOWN.
- The Document has not been modified since it was certified.
- The signer's identity is unknown because it has not been included in your list of trusted certificates and none of its parent certificates are trusted certificates.

Figure 4. Digital signature

   c. Non repudiation: to deal with non-repudiation by doctors who sign and made medical resumes because digital signatures can only be done by uploading private keys and certificates, and both files are only owned by doctors. The private key and certificate contain the doctor's identity which has two files, so if there is a medical resume with a doctor's digital signature, it cannot be denied that the medical resume was made by that doctor, because only doctors who have a private key and certificate can carry out a digital signature. the identity of the doctor can be seen in the certificate details shown in figure 4. Figure 5 shows the identity of the doctor who own the certificate that constist of doctor's name, email, and the validity of certificate.



dr. Dwi Jayanti <dwijayanti@gmail.com>
RSUD Depok

Issued by: RA RSUD Depok <rsud@depok.go.id>
RSUD Depok

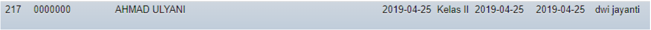
Valid from: 2019/04/01 09:41:00 +07'00'

Valid to: 2020/04/01 09:35:00 +07'00'

Intended usage: Digital Signature

Figure 5. Identity in digital signature of doctor

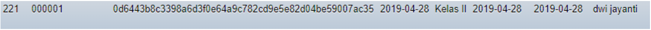
2. Encryption
   Encryption in this research is used to maintain the confidentiality of patient data in medical records to overcome data leakage of ransomeware. Figure 6 is a display of the contents of the database if encryption has not been implemented, so health data such as patient names can be read in the database. Whereas if encryption is applied to medical records, patient data cannot be known by unauthorized persons, it shown by figure 7.



```
217   0000000          AHMAD ULYANI                                   2019-04-25  Kelas II  2019-04-25   2019-04-25   dwi jayanti
```

Figure 6. Patient data on a database that has not been encrypted

   Figure 7 is the display of the contents of the database after encryption is implemented, so health data such as the patient's name cannot be read.

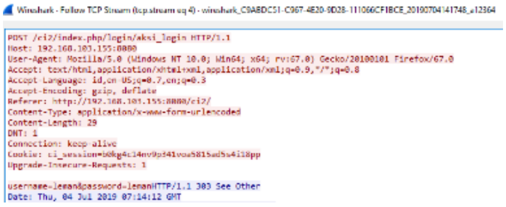


```
221   000001           0d6443b8c3398a6d3f0e64a9c782cd9e5e82d04be59007ac35  2019-04-28  Kelas II  2019-04-28   2019-04-28   dwi jayanti
```

Figure 7. Encrypted patient data

3. Test case
   The results of security testing with a test case based on [9] show that the application built is in accordance with the 6 test cases. The result of the test case 1 is that the system displays a login page, this happens because a session checking process occurs, namely the user level before it can enter the page of each account. The results of the test case 2, namely the system displays a login page, this happens because there is a session checking process, namely the user level. In the tests carried out, the admin has level 1, when the admin accesses the URL that can only be accessed by users who have level 3, the system will display a login page because the admin does not have access rights to enter the URL that goes to the page of the medical record officer. The result of the test case 3 is tests carried out are on the medical record form, for the type of input field in the form of a restricted textbox can only enter numbers. If the user enters a type of input other than a number, the textbox will not accept the input. The result of the testcase 4 is that the system displays the "Directory access is forbidden" page

   Test case 5 is about SSL in application. The application of SSL in the application built is to generate a self-signed certificate using Apache and install it on XAMPP. The tests carried out are by capturing packets sent during data transmission when the user logs in. Scanning is done twice namely when the application has not used the HTTP protocol whose results are shown in figure 8, the second scanning is when the application has applied the HTTPS protocol whose results are shown in figure 9. Testing was done using the Wireshark application. Figure 8 shows packages that are read when users log in to an application before implementing HTTPS. Packages that are read on the HTTP protocol can see the username and password used when logging in which is marked with a yellow box in figure 8. Figure 9 shows packages that are read when a user logs in to an application after implementing HTTPS. In package number 4 which shows that when the application is accessed it has implemented the TLS v1.2 protocol so that the data packets transmitted are encrypted as in Figure 9.

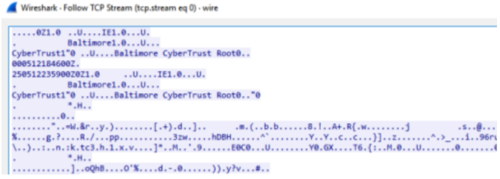


Wireshark · Follow TCP Stream (tcp.stream eq 4) · wireshark_C9ABDC51-C967-4E20-9D28-111066CF1BCE_20190704141748_a12364

```
POST /ci2/index.php/login/aksi_login HTTP/1.1
Host: 192.168.103.155:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: id,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.103.155:8080/ci2/
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
DNT: 1
Connection: keep-alive
Cookie: ci_session=b0kg4c14nv9p341voa5815ad5s4i18pp
Upgrade-Insecure-Requests: 1

username=leman&password=lemanHTTP/1.1 303 See Other
Date: Thu, 04 Jul 2019 07:14:12 GMT
```

Figure 8. Scanning result HTTP

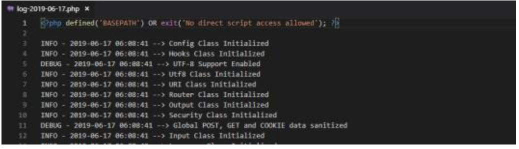


Wireshark · Follow TCP Stream (tcp.stream eq 0) · wire

```
.....0Z1.0  ..U....IE1.0...U.
.           Baltimore1.0...U...
CyberTrust1"0 ..U....Baltimore CyberTrust Root0..
000512184600Z.
250512235900Z0Z1.0     ..U....IE1.0...U.
.           Baltimore1.0...U...
CyberTrust1"0 ..U....Baltimore CyberTrust Root0.."0
.           *.H..
..........0..
........"..=W.&r..y.)........[.+).d..]..      .m.(..b.b......8.!..A+.R{.w........j          .s..@...
%......g.?....R./...pp...........3zw.....hDBH......^`........Y..Y..c..c...}]..z.......^.>_...i..96r
\..)..:..n.:k.tc3.h.1.x.v....]*..M..'.9......E0C0...U........Y0.GX....T6.{:..M.0...U.......0.......
.           *.H..
...........]..oQhB....O'%....d.-.0......)).y?v...#..
```

Figure 9. Scanning result HTTPS

a. Test case 6
The application is built using the CodeIgniter framework, to display all transactions and errors in the application that is built is by configuring the config file on framework Codeigniter that is by activating the threshold logging error. The display of the log file contents is shown in figure 10.



```
log-2019-06-17.php ×
<?php defined('BASEPATH') OR exit('No direct script access allowed'); ?>

INFO - 2019-06-17 06:08:41 --> Config Class Initialized
INFO - 2019-06-17 06:08:41 --> Hooks Class Initialized
DEBUG - 2019-06-17 06:08:41 --> UTF-8 Support Enabled
INFO - 2019-06-17 06:08:41 --> Utf8 Class Initialized
INFO - 2019-06-17 06:08:41 --> URI Class Initialized
INFO - 2019-06-17 06:08:41 --> Router Class Initialized
INFO - 2019-06-17 06:08:41 --> Output Class Initialized
INFO - 2019-06-17 06:08:41 --> Security Class Initialized
DEBUG - 2019-06-17 06:08:41 --> Global POST, GET and COOKIE data sanitized
INFO - 2019-06-17 06:08:41 --> Input Class Initialized
```

Figure 10. Log file

5. Conclusion

The proposed electronic medical record application can be an alternative electronic medical record application with encryption to maintain the confidentiality of patient health data using the AES-256 algorithm and RSA Digital Signature that can be applied in class C hospitals. The application has been validated on one Class C hospital, Depok Hospital. The electronic medical record application that has been built still has many shortcomings that can be corrected. Based on the scanning results, it shows that the applications that are built still have vulnerabilities, it is better if the vulnerability is overcome to improve application security. This application is better if it is integrated with SIMR applied in hospitals that can be integrated with other systems such as finance and pharmacy.

6. References

[1] W. P. Forum, Patient’s Guide to HIPAA How to Use the Law to Guard your Health Privacy. 2019.

[2] J. Justin Pope, “RANSOMWARE : Minimizing the Risk,” vol. 13, no. 11, pp. 37–40, 2016.

[3] Reuters, “Two major Indonesian hospitals attacked in ‘ransomware’ storm,” 2017. [Online]. Available: https://www.reuters.com/article/us-cyber-attack-indonesia/two-major-indonesian-hospitals-attacked-in-ransomware-storm-idUSKBN1890AX. [Accessed: 25-Apr-2019].

[4] K. K. R. I. Direktorat Jenderal Pelayanan Kesehatan, “Grafik Rumah Sakit Berdasarkan Kelas,” 2017. [Online]. Available: ttp://sirs.yankes.kemkes.go.id/rsonline/report/. [Accessed: 22-Nov-2018].

[5] E. Barker, D. Johnson, and M. Smid, “Recommendations for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography,” 2007.

[6] G. Singh, “A Study of Encryption Algorithms (RSA , DES , 3DES and AES) for Information Security,” vol. 67, no. 19, pp. 33–38, 2013.

[7] National Institute of Standards and Technology (NIST), “NIST FIPS 197 : Announcing the ADVANCED ENCRYPTION STANDARD (AES),” 2001.

[8] Kementerian Kesehatan Republik Indonesia, “PERATURAN MENTERI KESEHATAN REPUBLIK INDONESIA NOMOR 36 TAHUN 2012 TENTANG RAHASIA KEDOKTERAN,” no. 915, 2012.

[9] S. Kundu, “Web Testing : Tool , Challenges and Methods,” vol. 9, no. 2, pp. 481–486, 2012.