ISSN 2088-6225
E-ISSN 2580-2798

MODIFIKASI IDENTITY-BASED ENCRYPTION PADA KEAMANAN DAN KERAHASIAAN DATA REKAM MEDIS

Dian Neipa Purnamasari[1], Amang Sudarsono[1], Prima Kristalina[1]

[1]Politeknik Elektronika Negeri Surabaya, Kampus ITS,
Jl. Raya ITS, Keputih, Sukolilo, Kota Surabaya, Jawa Timur Indonesia

Email: dneipa12@gmail.com, amang@pens.ac.id, prima@pens.ac.id

Abstrak

Keamanan pada data rekam medis menjadi hal yang penting selain mengingat pentingnya isi dari rekam medis tersebut, keamanan pada data rekam medis telah diatur oleh kemeterian di Indonesia. Perkembangan teknologi membawa pengaruh pada penyimpanan data rekam medis, salah satunya perubahan data rekam medis dari konvensional menjadi elektronik. Namun, perkembangan teknologi ini juga memiliki dampak buruk yaitu munculnya oknum-oknum yang menjalankan kegiatan ilegal untuk mendapatkan keuntungan pribadi atau kelompok. Salah satunya adalah mencuri data rekam medis untuk memeras pasien, bahkan melakukan perubahan pada data rekam medis yang berdampak fatal pada kesehatan pasien. Pada penelitian ini diusulkan metode keamanan data rekam medis menggunakan modifikasi skema *Identity-based Encryption* (IBE) dan algoritma AES atau dapat disebut dengan mIBE-AES. Keunikan dari metode yang diusulkan adalah nilai awal yang telah ditentukan dari tiap byte pada identitas pengguna sehingga dapat menekan waktu komputasi pada proses pembangkitan kunci. Metode yang diusulkan akan dibandingkan dengan metode keamanan yang hanya menggunakan algoritma AES. Evaluasi performa yang telah dilakukan adalah pengujian kinerja dan tingkat keamanan pada penyerangan *Man in The Middle* (MITM). Didapatkan hasil bahwa metode mIBE-AES lebih unggul dengan total waktu komputasi 0,799 detik serta mampu menangani penyerangan MITM dengan skenario *sniffing* dan *chosen-plaintext.*

Kata Kunci: Keamanan, *Identity-based Encryption* (IBE), AES, Serangan *Man in The Middle* (MITM).

Abstract

The security of the medical record data is important besides remembering the importance of the contents of the medical record, the security of the medical record data has been regulated by the ministry in Indonesia. The development of technology has an effect on the storage of medical record data, one of which is a change in the storage of medical record data from conventional to electronic. However, the development of this technology also has a negative impact, namely the emergence of individuals who carry out illegal activities to gain personal or group benefits. One of them is stealing medical record data to blackmail patients, even making changes to medical record data that have a fatal impact on patient health. In this paper, the security method of medical record data was proposed using a modification of the Identity-based Encryption (IBE) scheme and the AES algorithm or it could be called mIBE-AES. The uniqueness of the proposed method is the predetermined value of each byte in the user's identity so that it can reduce computing time in the key generation process. The proposed method will be compared with security methods that only use the AES algorithm. The performance evaluation that has been done is testing the performance and level of security in the Man in The Middle (MITM) attack. It was found that the mIBE-AES method was superior with a total computing time of 0.799 seconds and was able to handle MITM attacks with sniffing and chosen-plaintext scenarios.

Keywords: Security, Identity-based Encryption (IBE), AES, Man in The Middle (MITM) Attack.

1. PENDAHULUAN

Informasi merupakan hasil pengolahan data yang memiliki arti. Menurut Keputusan Menteri [1], keamanan informasi merupakan hal penting dalam penyelenggaraan layanan. Keamanan informasi yang handal akan meningkatkan kepercayaan masyarakat terhadap penyelenggaraan sistem elektronik untuk pelayanan publik. Salah satu upaya untuk meningkatkan pelayanan publik adalah dengan adanya perubahan penyimpanan data rekam medis. Data rekam medis yang awalnya disimpan di rak berupa tumpukan-tumpukan kertas, sekarang diubah menjadi data rekam medis elektronik. Sehingga semua data rekam medis pasien tersimpan pada *cloud*.

Menurut Peraturan Menteri Kesehatan Republik Indonesia [2], informasi tentang identitas, diagnosis, riwayat penyakit dan data yang menunjang kesehatan pasien harus dijaga kerahasiaannya. Peraturan ini berlaku untuk

semua data rekam medis baik konvensional maupun elektronik. Perkembangan teknologi menggiring semua aspek untuk menggunakan internet baik sebagai media penyimpanan atau jalur komunikasi antar sistem. Kenyataannya bahwa internet juga memiliki dampak negatif yaitu dengan banyaknya informasi di internet maka muncul oknum-oknum yang dapat bertindak ilegal seperti *attacker*. *Attacker* mampu mengambil data informasi dengan berbagai teknik penyerangan. Salah satunya adalah *Man in The Middle Attack* (MITM), bentuk penyerangan ini dapat dilakukan dimana saja. Tujuan dari penyerangan ini adalah untuk melihat, mengambil atau mengubah sebuah informasi rahasia.

Telah banyak para peneliti yang membahas tentang data rekam medis dengan tujuan untuk mengamankan isi dari data tersebut. Umumnya untuk mengamankan sebuah data rekam medis digunakan teknik kriptografi baik dengan algoritma simetris [3-5], asimetris [6-11] maupun kombinasi dari keduanya [12-13]. Adapun terdapat empat aspek pada kriptografi untuk menjamin sebuah informasi terlindungi dengan aman yaitu *Confidentiality*, *Integrity*, *Authentication*, dan *Non–Repudiation*.

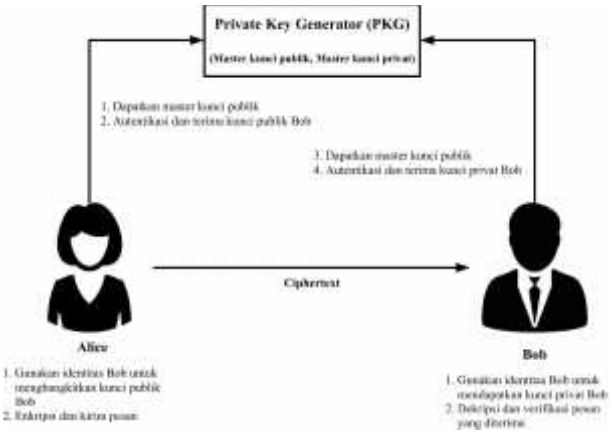
Pada paper ini membahas tentang metode keamanan untuk menjaga keamanan dan kerahasiaan data rekam medis menggunakan skema *identity-based encryption* (IBE). Skema IBE atau skema enkripsi berbasis identitas merupakan skema enkripsi yang menggunakan kunci publik berupa informasi unik dari identitas pengguna. Pengirim pesan memiliki akses untuk membangkitkan kunci publik penerima dan mengenkripsi pesan dengan mengirimkan identitas penerima ke otoritas pusat, sedangkan penerima mendapatkan kunci rahasia dengan mengirimkan identitasnya ke otoritas pusat. Skema ini telah dimodifikasi menjadi 3 tahapan yaitu Key Generator, *Encrypt* dan *Decrypt*. Tahap setup digunakan untuk membangkitkan kunci enkripsi yang akan digunakan. Sedangkan tahap *Encrypt* dan *Decrypt* digunakan untuk proses enkripsi dan dekripsi dengan menggunakan algoritma enkripsi AES sehingga metode yang diusulkan disingkat menjadi mIBE-AES. Metode keamanan yang diusulkan telah dibandingkan dengan metode keamanan yang hanya menggunakan AES. Dilakukan beberapa pengujian untuk mengukur kinerja dari metode yang diusulkan.

Paper ini disusun sebagai berikut: bagian 2 menyajikan penjelasan dari metode keamanan yang diusulkan untuk melindungi data rekam medis. Bagian 3 menyajikan hasil dan pembahasan dari uji kinerja algoritma, uji keacakan kunci dan uji keamanan dari metode yang diusulkan. Hasil kesimpulan dirangkum pada Bagian 4.

2. METODE

Bagian ini menjelaskan metode keamanan yang diusulkan untuk mengamankan data rekam medis. Metode keamanan yang diusulkan menggunakan modifikasi dari skema IBE dengan algoritma enkripsi AES atau dapat disingkat menjadi mIBE-AES.

Ide skema IBE diusulkan tahun 1984 oleh penelitian Shamir [14], yang menyajikan enkripsi berbasis identitas dan menerapkannya pada tanda tangan. Kemudian pada tahun 2001, peneliti Boneh dan Franklin [15] memecahkan permasalahan IBE dengan menggunakan kriptografi kurva eliptik berbasis *pairing*. Ilustrasi skema Boneh-Franklin ditunjukkan pada Gambar 1.



Gambar 1. Ilustrasi Skema *Identity-based Encryption*

Pada paper ini, skema IBE digunakan untuk menghilangkan penggunaan *Trusted Third Party* (TTP) karena pengguna dapat membangkitkan kunci enkripsi secara mandiri dengan menanamkan identitas. Serta untuk menghindari adanya pertukaran kunci di kanal komunikasi. Sedangkan algoritma AES digunakan karena merupakan kriptografi simetris yang hanya menggunakan satu kunci untuk proses enkripsi dan dekripsi. Ukuran block cipher pada AES adalah 128 bit dengan tiga variasi ukuran kunci yaitu 128 bit, 192 bit dan 256 bit. Kemudahan dan kesederhanaan dari AES dapat mempercepat waktu kerja sistem dalam mengamankan data rekam medis.

Skema IBE dimodifikasi dengan menghilangkan satu tahapan pada penelitian IBE sebelumnya [15]. Tahapan pada metode keamanan yang diusulkan adalah *Key Generator*, *Encrypt* dan *Decrypt*.

a. Key Generator

Tahap ini dijalankan sebelum komunikasi dilakukan dan bertindak sebagai *key server*. Sebelum melakukan pertukaran data, pengirim harus mengirimkan identitas penerima untuk mendapatkan kunci publik penerima. Kunci publik ini digunakan pada proses enkripsi. Sedangkan pada sisi penerima, penerima harus mengirimkan identitasnya untuk mendapatkan kunci rahasia yang digunakan pada proses dekripsi.

Algoritma AES pada penelitian ini menggunakan ukuran kunci 256 bit. Kunci yang digunakan untuk proses enkripsi dan dekripsi adalah sama. Terdapat empat tahap pada AES yaitu *Add Round Key*, *Sub Bytes*, *Shift Rows*, dan *Mix Columns*.

Langkah-langkah pembentukan kunci tiap pengguna adalah sebagai berikut:

1. Pengguna mengirimkan identitas penerima (ID).
2. Key generator akan membangkitkan nilai r yang merupakan bilangan acak. Pembangkitan nilai r menggunakan fungsi hash SHA1 dan *pseudorandom number generator* (PRNG) yang nilai awalnya ditentukan dari nilai *byte* pada ID.
3. Kunci dibangkitkan secara random menggunakan *key generator* dan di inisialisasi agar kunci memiliki panjang 256 bit dan memiliki nilai yang sama dengan nilai r.
4. Kunci ini merupakan kunci rahasia yang digunakan untuk proses enkripsi dan dekripsi.

b. Encrypt

Tahap ini digunakan untuk melakukan proses enkripsi pada data rekam medis. Untuk menjalankan proses enkripsi, sistem harus melewati empat tahap yaitu *Add Round Key*, *Sub Bytes*, *Shift Rows*, dan *Mix Columns* dengan jumlah putaran sebanyak 14. Langkah-langkah proses enkripsi adalah sebagai berikut:

1. Data rekam medis diubah menjadi block cipher 128 bit yang dimasukkan ke dalam state awal yaitu matriks 4x4 *byte*.
2. AddRoundKey: tahap ini disebut sebagai *initial round*. Sistem akan mengkombinasikan data rekam medis *(state)* dengan *cipher key* dengan hubungan XOR. XOR dilakukan per kolom yaitu satu kolom di state di XOR dengan satu kolom di *cipher key* dan seterusnya.
3. Selanjutnya dilakukan putaran sebanyak 13 kali yang setiap putarannya menjalankan proses berikut:
   i. SubBytes: sistem melakukan subtitusi byte dengan menukar isi matriks dengan tabel substitusi (S-box).
   ii. ShiftRows: sistem melakukan proses shift atau pergeseran ke bawah pada setiap elemen matriks yang dilakukan tiap baris.
   iii. MixColumns: sistem akan mengalikan tiap elemen dari state dengan matriks iv. Perkalian ini dilakukan untuk mengacak data di masing-masing kolom *array state*.
   iv. AddRoundKey: sistem akan melakukan XOR antara state terbaru dengan *round key* 1-13.
4. Kemudian dijalankan satu kali putaran yang disebut *final round*. *Final round* ini

hanya berisikan proses *SubBytes*, *ShiftRows*, dan *AddRoundKey*.

5. Hasil dari final *round* merupakan *ciphertext* dengan panjang 128 bit.

c. Decrypt

Tahap ini digunakan untuk melakukan proses dekripsi pada *ciphertext* rekam medis. Langkah yang digunakan untuk mendekripsi ciphertext merupakan kebalikan dari proses enkripsi yaitu sebagai berikut:

1. *Ciphertext* rekam medis dimasukkan ke dalam matriks 4x4 byte.
2. Pada putaran pertama, dilakukan proses *AddRoundKey, Inverse ShiftRows* dan *Inverse SubBytes*. Pada putaran ini kunci yang digunakan adalah *round key* 14.
3. Selanjutnya dilakukan putaran sebanyak 13 kali yang setiap putarannya menjalankan proses berikut:
   i. AddRoundKey: sistem akan melakukan XOR antara *ciphertext* dengan round key yang digunakan pada saat enkripsi.
   ii. *Inverse Mix Columns*: proses ini merupakan kebalikan dari *Mix Columns* pada enkripsi. perbedaannya adalah matriks yang digunakan adalah inverse dari matrik iv. Perkalian ini dilakukan untuk mengembalikan data di masing-masing kolom *array state*.
   iii. *Inverse ShiftRows*: sistem melakukan proses shift atau pergeseran ke atas pada setiap elemen matriks yang dilakukan tiap baris.
   iv. *Inverse SubBytes*: sistem melakukan subtitusi byte dengan menukar isi matriks dengan tabel *inverse S-box*.
4. Kemudian hasil dari akan diputar satu kali pada final round yang berisikan proses *Inverse SubBytes*, *Inverse ShiftRows*, dan *AddRoundKey*.
5. Hasil dari final *round* ini adalah data rekam medis dengan panjang data 128 bit.

3. HASIL DAN PEMBAHASAN

Metode mIBE-AES yang diusulkan telah diimplementasikan secara simulasi dengan menggunakan skenario client dan *server*. Komunikasi yang dilakukan menggunakan pemrograman *socket*, yang mana pengguna harus terhubung pada satu jaringan yang sama. Tujuan dari penelitian ini adalah menganalisa dan menguji performa dari metode yang diusulkan. Terdapat beberapa parameter untuk pengujian yaitu waktu komputasi, jumlah data yang dikirim, dan tingkat keamanan untuk mengatasi penyerangan MITM.

A. *Uji Kinerja Metode yang Diusulkan*

Pengujian kinerja ini dilakukan dengan skenario *client-server,* yang mana pengirim mengirimkan data rekam medis yang telah dienkripsi menggunakan mIBE-AES. Hasil dari proses enkripsi dan dekripsi akan merepresentasikan kebenaran dari data rekam medis yang dikirimkan. Format data rekam medis yang digunakan pada penelitian ini mengacu pada syarat isi data rekam medis yang ditunjukkan pada Tabel 1.

Pengujian ini mengamati waktu komputasi tiga tahap pada skema IBE. Metode pada penelitian ini akan dibandingkan dengan metode keamanan data rekam medis yang menggunakan algoritma AES. Hasil dari pengujian ditunjukkan pada Tabel 2.

ISSN 2088-6225
E-ISSN 2580-2798

Tabel 1. Format Data Rekam Medis

Format	Panjang Data	Keterangan
Flag	1 byte	@
Delimiter	1 byte	#
No. Identitas	10 byte	No. Identitas Kesehatan Pasien
Delimiter	1 byte	#
Nama Pasien	±30 byte	Nama Lengkap Pasien
Delimiter	1 byte	#
Waktu Pemeriksaan	±20 byte	Waktu dan Tanggal Pemeriksaan
Delimiter	1 byte	#
Data-1	7 byte	Data Tekanan Darah
Delimiter	1 byte	#
Data-2	3 byte	Data Laju Nadi
Delimiter	1 byte	#
Data-3	2 byte	Data Laju Nafas
Delimiter	1 byte	#

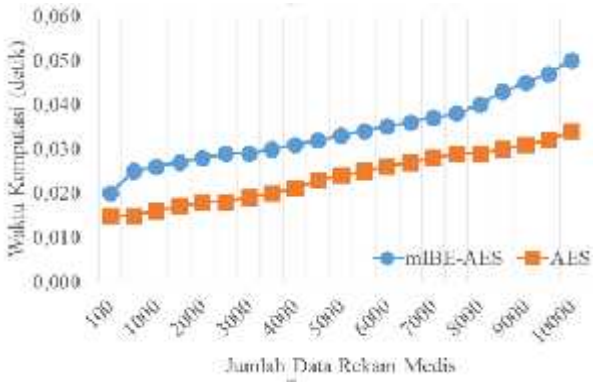
Berdasarkan Tabel 2 didapatkan bahwa untuk membangkitkan kunci, metode yang diusulkan lebih unggul 0,292 detik daripada AES. Hal ini dikarenakan nilai awal untuk membangkitkan kunci sudah ditentukan yaitu berdasarkan nilai byte pada identitas penerima, sehingga dapat menekan waktu komputasi. Sedangkan pada tahap Encrypt dan Decrypt, waktu komputasi metode yang diusulkan sedikit lebih lambat ± 0,005 detik. Total waktu komputasi pada metode yang diusulkan adalah 0,799 detik untuk menjalankan ketiga tahap. Sedangkan pada metode pembanding, total waktu komputasinya adalah 1,075 detik. Sehingga metode yang diusulkan lebih unggul untuk mengamankan data rekam medis berdasarkan waktu komputasinya.

Tabel 2. Waktu Komputasi Tiap Tahap

Tahap	mIBE-AES	AES
Key Generator	0,765	1,051
Encrypt	0,018	0,012
Decrypt	0,016	0,012

Banyaknya data rekam medis yang mengalami perubahan juga menjadi tantangan bagi para peneliti yaitu bagaimana membuat metode keamanan yang mampu mengamankan data rekam medis dengan jumlah yang banyak dan dalam waktu singkat. Pengujian kinerja ini juga menguji waktu komputasi dari ke dua metode dengan parameter jumlah data yang dikirim. Hasil dari pengujian merupakan nilai dari waktu enkripsi data rekam medis yang ditunjukkan pada Gambar 2.

Pada Gambar 2 menunjukkan perbandingan waktu komputasi pada ke dua metode. Data yang dikirimkan mulai dari 100 hingga 10.000 data dalam sekali pengiriman. Waktu yang dibutuhkan mIBE-AES adalah 0,020 detik untuk mengirimkan 100 data, sedangkan metode pembandingnya memiliki waktu komputasi 0,015 detik. Pada pengiriman 10.000 data, metode mIBE-AES memiliki waktu komputasi 0,050 detik sedangkan metode AES memiliki waktu komputasi 0,034 detik. Berdasarkan Gambar 2 dapat diketahui bahwa metode pembanding memiliki kestabilan waktu komputasi yang lebih unggul dibandingkan metode yang diusulkan.



Gambar 2. Perbandingan Waktu Komputasi Terhadap Jumlah Data Rekam Medis

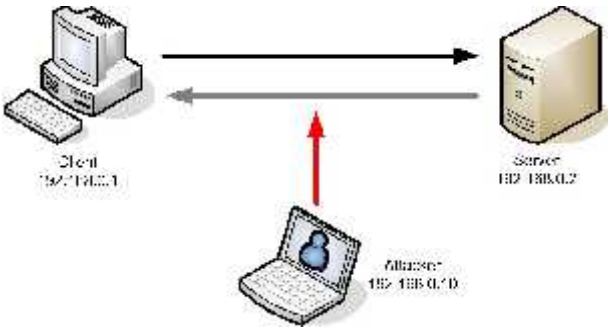
B. Uji Keamanan

Serangan MITM bertujuan untuk menyadap komunikasi data rahasia seperti sniffing. *Sniffing* merupakan bentuk penyerangan pasif karena *attacker* tidak melakukan apa-apa selain memantau pertukaran data. Penyerangan ini mudah dilakukan apabila *attacker* berada satu

jaringan dengan target. Serangan MITM dapat berbahaya apabila *attacker* melakukan penyerangan aktif dengan memotong komunikasi dan mengubah data rahasia. Pada pengujian ini dilakukan dua serangan yaitu *sniffing* dan *chosen-plaintext*.

1. *Sniffing*

Serangan *sniffing* terjadi ketika *attacker* bertindak untuk memantau data antara dua pengguna yang saling berkomunikasi yang ditunjukkan pada Gambar 3. Biasanya Attacker menggunakan aplikasi *Wireshark* untuk mengamati waktu pengiriman, protocol yang digunakan, panjang data yang dikirim, hingga isi dari data yang dikirim.



Gambar 3. Ilustrasi Skenario *Sniffing*

Pada pengujian ini, pengirim menggunakan alamat IP 192.168.0.1 dan penerima menggunakan alamat IP 192.168.0.2. Attacker harus berada dalam satu jaringan yang sama dengan target, alamat IP yang digunakan adalah 192.168.0.10.

Pengirim akan mengenkripsi data rekam medis menggunakan mIBE-AES dan mengirimkannya dalam bentuk *ciphertext*. Setelah dilakukan proses pengiriman data maka hasilnya menunjukkan bahwa *attacker* mampu memantau semua data *ciphertext* yang dikirimkan. Pada skenario ini dapat diketahui pentingnya keamanan untuk menjaga data rahasia karena *attacker* hanya mampu memantau data dalam bentuk *ciphertext* sehingga data rekam medis asli dapat terjaga kerahasiaannya.

2. *Chosen-Plaintext*

Serangan *chosen-plaintext* terjadi ketika *attacker* bertindak sebagai pengirim palsu dengan mengubah sumber alamat IP. Teknik ini dikenal dengan sebutan IP *spoofing*. Attacker tidak akan mendapatkan *feedback* apakah penyerangan ini berhasil atau tidak. Penyerangan ini bersifat acak, jika target tidak memastikan pengirim dengan baik maka dapat terkena serangan ini. Sebaliknya, serangan ini menjadi tidak efektif jika target rutin memastikan pada pengirim data setiap hendak melakukan pertukaran data.

Pada pengujian ini diasumsikan bahwa attacker tidak mengetahui identitas target dan algoritma enkripsi yang digunakan. Hasil dari pengujian adalah *attacker* dapat mengirimkan pesan menuju target, tetapi dapat diketahui oleh penerima. Hal ini dikarenakan tidak adanya identitas pada ciphertext yang dikirimkan, serta pesan yang dikirimkan tidak dapat di dekripsi. Pada skenario ini didapatkan bahwa *ciphertext* rekam medis yang dihasilkan oleh *attacker* berbeda dengan *ciphertext* yang dihasilkan pengirim asli.

4. KESIMPULAN

Metode keamanan yang diusulkan pada penelitian ini menggunakan skema IBE dengan algoritma enkripsi AES untuk mengamankan data rekam medis. Algoritma AES digunakan untuk membangkitkan kunci enkripsi dan melakukan proses enkripsi. Penelitian ini dapat digunakan untuk segala jenis data rahasia yang membutuhkan waktu komputasi yang cepat. Keunikan dari metode yang diusulkan adalah nilai awal yang telah ditentukan dari tiap byte pada identitas pengguna. Hal ini digunakan untuk menekan waktu komputasi. Selain itu skema IBE yang diusulkan juga dimodifikasi menjadi tiga tahap yaitu *Key Generator, Encrypt* dan *Decrypt.* Pada tahap *Key Generator*, metode mIBE-AES lebih unggul 0,292 detik dibandingkan metode pembandingnya. Sedangkan pada tahap

Encrypt dan *Decrypt*, metode pembanding lebih unggul ± 0,005 detik. Dari total waktu komputasi keseluruhan, metode mIBE-AES lebih unggul dengan waktu 0,799 detik. Selain waktu komputasi, metode mIBE-AES diuji berdasarkan tingkat keamanan untuk penyerangan MITM. Hasil pengujian membuktikan bahwa metode yang diusulkan mampu menangani penyerangan MITM dengan skenario *sniffing* dan *chosen-plaintext*.

UCAPAN TERIMAKASIH

Penulis mengucapkan terimakasih kepada Kementerian Riset Teknologi dan Pendidikan Tinggi – Politeknik Elektonika Negeri Surabaya atas beasiswa studi pascasarjana. Semoga penelitian yang telah dilakukan bermanfaat.

DAFTAR PUSTAKA

[1] Kemenkumham RI, "Keputusan Menteri Hukum dan Hak Asasi Manusia Republik Indonesia Nomor : M.HH-01.TI.06.02 Tahun 2017 Tentang Sistem Manajemen Keamanan Informasi Di Lingkungan Kementerian Hukum dan Hak Asasi Manusia." pp. 1–42, 2017.

[2] Kemenkes RI, "Peraturan Menteri Kesehatan Republik Indonesia Nomor 269/MENKES/PER/III/2008 Tentang Rekam Medis," Peraturan Menteri Kesehatan tentang Rekam Medis. pp. 1-7, 2008.

[3] Kumar, B. Vinoth, M. Ramaswami, dan P. Swathika. "*Data security on patient monitoring for future healthcare application*" International Journal of Computer Applications 163(6): 20-23, 2017.

[4] Adeshina, A. M., dan R. Hashim. "*Computational approach for securing radiology-diagnostic data in connected health network using high-performance gpu-accelerated aes*" Interdisciplinary Sciences: Computational Life Sciences 9(1): 140-152, 2017.

[5] A. Jammu, "*Improved AES for Data Security in E-Health*," vol. 8, no. 5, pp. 2016–2020, 2017.

[6] Guo, Cheng, et al. "*Fine-grained database field search using attribute-based encryption for e-healthcare clouds*" Journal of medical systems 40(11): 235, 2016.

[7] D. N. Purnamasari, A. Sudarsono, dan P. Kristalina, "*Secure Data Sharing Scheme using Identity-based Encryption for e-Health Record*," in 2018 International Electronics Symposium on Engineering Technology and Applications (IES-ETA), pp. 60–65, 2019.

[8] W. Susilo dan K. T. Win, "*Securing electronic health records with broadcast encryption schemes*," Int. J. Electron. Healthc., vol. 2, no. 2, pp. 175–184, 2006.

[9] S. Maheswari dan U. Gudla, "*Secure sharing of personal health records in Jelastic cloud by attribute-based encryption*," in 2017 4th International Conference on Advanced Computing and Communication Systems, ICACCS 2017, pp. 4–7, 2017.

[10] J. Sun, X. Zhu, C. Zhang, dan Y. Fang, "*HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare*," in Proceedings - International Conference on Distributed Computing Systems, 2011, pp. 373–382, 2011.

[11] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption," Futur. Gener. Comput. Syst., vol. 52, pp. 67–76, 2015.

[12] Sadikin, Mohamad Ali, dan Rini Wisnu Wardhani, "*Implementation of RSA 2048-bit and AES 256-bit with digital signature for secure electronic health record application*", 2016 International Seminar on Intelligent Technology and Its Applications (ISITIA), IEEE, pp. 387-392, 2016.

[13] A. Sudarsono, M. Yuliana, and H. A. Darwito, "*A secure data sharing using identity-based encryption scheme for e-healthcare system*," in International Conference on Science in Information Technology (ICSITech), pp. 429–434, 2018.

[14] A. Shamir, "*Identity-based Cryptosystems and Signature Schemes*," Adv. Cryptol. - CRYPT0 '84, LNCS 196, pp. 47–53, 1985.

[15] D. Boneh and M. Franklin, "*Identity-Based Encryption from the Weil Pairing*," Proc. Crypto 2001, vol. 2139, pp. 213–229, 2001.