Implementasi Algoritme 3DES pada Sistem *Sharing Electronic Health Record* (EHR) Berbasis *Cloud*

Haryadi Amran Darwito[1], Mike Yuliana[2], Reni Soelistijorini[3]

***Abstract*— Electronic Health Record (EHR) or medical history has been widely adopted to enable healthcare providers such as hospitals, insurance companies, and patients, to create, organize, and access EHR information from anywhere and at any time. From a health standpoint, to improve the quality of patient care, an EHR storage center is needed to ensure the EHR's novelty at all times. This underlies the need for an efficient, safe, and inexpensive mechanism for sharing EHR among health care providers. Cloud Computing has become a promising paradigm and gains more attention from academia and industry. This paradigm shifts the location of the computer infrastructure to third parties. Cloud computing not only increases the efficiency of storage and exchange of medical data but also allows accessing medical data from anywhere and anytime. In this paper, a mechanism of cloud-based sharing system equipped with the 3DES algorithm to secure health history data and the use of the smart card as a medium for controlling patient information access is proposed. The results of the tests indicate that the built system has fulfilled the security requirements such as privacy, authentication, confidentiality and integrity.**

***Intisari*— *Electronic Health Record* (EHR), atau dikenal dengan riwayat kesehatan, telah diadopsi secara luas untuk memungkinkan penyedia layanan kesehatan seperti puskesmas, rumah sakit, perusahaan asuransi, dan pasien menciptakan, mengatur, dan mengakses informasi EHR dari mana saja dan kapan saja. Dari sudut pandang kesehatan, untuk meningkatkan kualitas perawatan pasien, diperlukan sebuah pusat penyimpanan EHR yang dapat memastikan kebaruan EHR setiap waktu. Hal inilah yang mendasari diperlukannya mekanisme yang efisien, aman, dan murah untuk berbagi EHR antara penyedia layanan kesehatan. *Cloud Computing* telah menjadi paradigma yang menjanjikan serta mendapat perhatian yang lebih dari akademisi dan industri. Paradigma ini menggeser lokasi dari infrastruktur komputer ke pihak ketiga. *Cloud computing* tidak hanya meningkatkan efisiensi dari penyimpanan serta pertukaran data medis, tetapi juga memungkinkan pengaksesan data medis dari mana saja dan kapan saja. Pada makalah ini diusulkan sebuah mekanisme sistem *sharing* berbasis *cloud* yang dilengkapi dengan algoritme 3DES untuk mengamankan data riwayat kesehatan serta penggunaan *smart card* sebagai media pengontrolan akses informasi pasien. Hasil pengujian yang dilakukan menunjukkan bahwa sistem yang dibuat telah memenuhi persyaratan keamanan seperti privasi, autentikasi, kerahasiaan, dan keutuhan.**

***Kata Kunci*— EHR, *Cloud Computing*, *sharing*, 3DES, *smart card*.**

[1,2,3] *Staf Pengajar, Politeknik Elektronika Negeri Surabaya, Raya ITS Keputih Sukolilo Surabaya 60111 (tlp: 031-5947280; fax: 031-5946111; e-mail: amran@pens.ac.id, mieke@pens.ac.id, reni@pens.ac.id)*

I. PENDAHULUAN

Di era lingkungan kesehatan modern, EHR, atau dikenal dengan riwayat kesehatan, telah diadopsi secara luas untuk memungkinkan penyedia layanan kesehatan seperti puskesmas, rumah sakit, perusahaan asuransi, dan pasien untuk menciptakan, mengatur, dan mengakses informasi EHR dari mana saja dan kapan saja. Dari sudut pandang kesehatan, untuk meningkatkan kualitas perawatan pasien diperlukan sebuah pusat penyimpanan EHR yang dapat memastikan kebaruan EHR setiap waktu [1]. Hal inilah yang mendasari diperlukannya mekanisme yang efisien, aman, dan murah untuk berbagi EHR antara penyedia layanan kesehatan. Dalam situasi darurat, pertukaran EHR secara cepat dapat menyelamatkan nyawa pasien. Namun, kondisi yang ada saat ini menunjukkan bahwa penyedia layanan kesehatan menyimpan EHR sendiri-sendiri. Hal ini berdampak pada sulitnya mekanisme integrasi dan pertukaran EHR antar penyedia layanan kesehatan [2].

Cloud Computing telah menjadi paradigma yang menjanjikan serta mendapat perhatian yang lebih dari akademisi dan industri. Paradigma ini menggeser lokasi dari infrastruktur komputer ke pihak ketiga. *Cloud computing* tidak hanya meningkatkan efisiensi penyimpanan serta pertukaran data medis, tetapi juga memungkinkan pengaksesan data medis dari mana saja dan kapan saja. Perlu dicatat bahwa pengelolaan layanan kesehatan dengan *cloud computing* akan membuat perubahan revolusioner dalam pengaksesan layanan kesehatan [3].

Aplikasi dan layanan EHR di *cloud* sangat menguntungkan penyedia layanan kesehatan dan pasien. Namun, adopsi tersebut juga dapat memberikan tantangan keamanan yang berkaitan dengan manajemen identitas pasien, pengontrolan pengaksesan, integrasi kebijakan, manajemen kepatuhan, dan lain lain. Jika tantangan tersebut tidak dapat diselesaikan dengan baik, maka akan menghalangi kesuksesan layanan kesehatan di *cloud*. Dengan melihat tantangan-tantangan tersebut, makalah ini fokus pada permasalahan keamanan pertukaran EHR antar penyedia layanan kesehatan dalam sistem *cloud*, karena mekanisme pertukaran adalah mekanisme yang kompleks dan melibatkan banyak entitas. Selain itu, adanya potensi terungkapnya EHR pasien menunjukkan perlunya mekanisme privasi dan keamanan yang terintegrasi dengan sistem layanan kesehatan [4].

Secara khusus, pertukaran (*sharing*) EHR terdiri atas informasi kesehatan yang sensitif seperti informasi alergi, riwayat kesehatan, tes hasil laboratorium, dan lain lain. Pengontrolan akses informasi harus mampu menjamin bahwa hak akses ke informasi yang sensitif hanya mampu dilakukan oleh entitas yang memiliki hak/*privilege* yang telah disetujui

pasien. Misalnya ada sebuah kondisi ketika pasien tidak bersedia untuk *sharing* informasi tentang penyakit tertentu ke seorang dokter kecuali jika diperlukan untuk perawatan khusus. Karenanya, mekanisme keamanan yang sistematis dan fleksible dibutuhkan untuk *sharing* EHR sesuai dengan persyaratan pengontrolan akses informasi [5], [6].

Pada makalah ini diusulkan sebuah mekanisme sistem *sharing* berbasis *cloud* yang dilengkapi dengan algoritme 3DES untuk mengamankan data riwayat kesehatan serta penggunaan *smart card* sebagai media pengontrolan akses informasi pasien. Algoritme 3DES adalah suatu algoritme pengembangan dari algoritme *Data Encryption Standard* (DES). Perbedaan DES dengan 3DES terletak pada panjangnya kunci yang digunakan. Pada DES digunakan satu kunci yang panjangnya 56 bit, sedangkan 3DES menggunakan tiga kunci yang panjangnya 168 bit (masing-masing panjangnya 56 bit). Karena tingkat kerahasiaan algoritme 3DES terletak pada panjangnya kunci yang digunakan, maka penggunaan algoritme 3DES dianggap lebih aman dibandingkan dengan algoritme DES.

Sisa bagian dari makalah ini diatur sebagai berikut. Bagian II membahas tentang algoritme 3DES. Bagian III mendiskusikan tentang desain sistem yang berisi tentang berbagai persyaratan keamanan dan pengontrolan akses informasi. Bagian IV berisi hasil dan pembahasan, sedangkan kesimpulan dari makalah ada pada Bagian V.

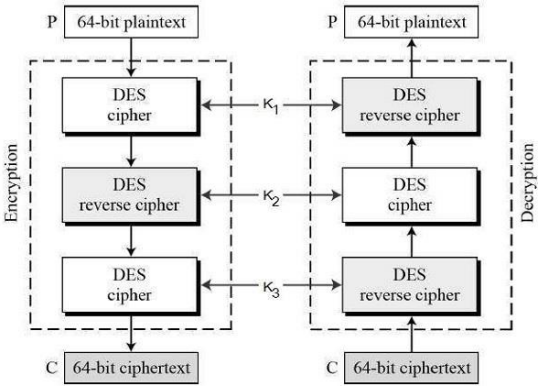
II. *TRIPLE DATA ENCRYPTION STANDARD* (3DES)

Kecepatan pencarian kunci DES setelah 1990 menyebabkan ketidaknyamanan di antara pengguna DES. Namun, pengguna tidak ingin mengganti DES karena dibutuhkannya sejumlah besar waktu dan biaya untuk mengubah algoritme enkripsi yang telah diadopsi secara luas dan tertanam dalam arsitektur keamanan yang besar. Pendekatan pragmatis tidak mengabaikan DES seluruhnya, tetapi hanya mengubah cara menggunakan DES. Hal inilah yang menyebabkan adanya modifikasi DES yang dikenal dengan *Triple DES* (kadang-kadang dikenal dengan 3DES). Terdapat dua varian 3DES yang dikenal dengan *3-key Triple DES* (3TDES) dan *2-key Triple DES* (2TDES) [7], [8].

Sebelum menggunakan 3DES, pertama-tama pengguna membangkitkan dan mendistribusikan kunci *K* yang terdiri atas tiga kunci *K1, K2*, dan *K3*.

Proses enkripsi dan dekripsi, seperti yang ditunjukkan oleh Gbr. 1, adalah sebagai berikut:

1. Melakukan enkripsi blok pesan (*plain text)* menggunakan DES tunggal dengan kunci *K1*.
2. Melakukan dekripsi terhadap hasil yang diperoleh dari langkah 1 menggunakan kunci *K2*.
3. Melakukan enkripsi terhadap keluaran dari langkah 2.
4. Keuaran dari langkah 3 adalah *cipher text*.
5. Dekripsi dari *ciphertext* adalah proses kebalikannya. Pengguna melakukan dekripsi dengan menggunakan *K3*, melakukan enkripsi dengan *K2*, dan akhirnya melakukan dekripsi dengan *K*1.



Gbr. 1 Proses enkripsi dan dekripsi 3DES.

Mengacu pada desain 3DES sebagai proses enkripsi dan dekripsi, maka sangat dimungkinkan untuk menggunakan implementasi perangkat keras untuk DES tunggal dengan menggunakan nilai *K1, K2, K3* yang sama. Varian kedua dari 3DES yaitu 2TDES memiliki proses yang sama dengan 3DES. Perbedaannya hanya adanya penggantian *K3* dengan *K1*. Dengan kata lain, pengguna melakukan enkripsi blok pesan dengan menggunakan *K1*, melakukan dekripsi dengan *K2*, dan melakukan enkripsi dengan *K1* lagi. 2TDES memiliki kunci dengan panjang 112 bit, sehingga bisa dikatakan bahwa 3DES lebih aman dari DES tunggal, tetapi memiliki proses enkripsi yang lebih lama.

III. DESAIN SISTEM

Pada makalah ini didesain keamanan sistem *sharing* serta pengontrolan akses informasi untuk menjamin privasi riwayat kesehatan pasien. Desain sistem seperti ini dibutuhkan untuk meningkatkan layanan sistem kesehatan, khususnya untuk meningkatkan tingkat kepercayaan pengguna.

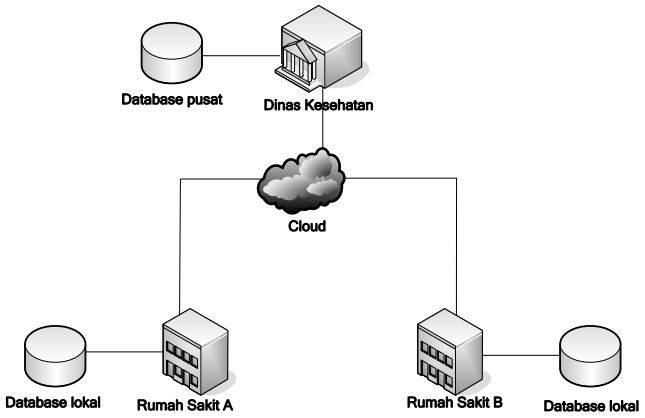
A. Entitas dan Definisi

Entitas yang terlibat dalam sistem *sharing* meliputi pasien, rumah sakit perujuk, rumah sakit yang dirujuk, Dinas Kesehatan, basis data local, dan basis data pusat, seperti yang ditunjukkan pada Gbr. 2. Pasien adalah orang yang akan diamankan riwayat kesehatannya. Pada prosedur sistem *sharing*, rumah sakit yang melakukan *sharing* disebut sebagai rumah sakit perujuk, sedangkan rumah sakit yang menerima data *sharing* disebut sebagai rumah sakit yang dirujuk. Pada makalah ini, Rumah Sakit A disebut sebagai rumah sakit perujuk, sedangkan Rumah Sakit B disebut sebagai rumah sakit yang dirujuk. Basis data lokal diletakkan di masing-masing rumah sakit dan digunakan untuk menyimpan EHR pasien. Basis data pusat diletakkan di Dinas Kesehatan dan digunakan untuk menyimpan EHR pasien yang akan dirujuk.

B. Persyaratan Keamanan

Sistem *sharing* yang dibuat harus memenuhi persyaratan kemanan yang meliputi hal-hal sebagai berikut.

1) Privasi: Sistem *sharing* akan terpenuhi privasinya jika EHR dan identitas pribadi pasien hanya bisa diakses oleh dokter yang berwenang dengan alasan yang sah.



Gbr. 2 Entitas dan definisi.

2) Autentikasi: Auntentikasi ditunjukkan dengan adanya pengaturan bahwa semua entitas yang terlibat di sistem harus melakukan autentikasi atau verifikasi satu sama lain dengan menggunakan *smart card*.

3) Kerahasiaan (Confidentiality): Kerahasiaan dibutuhkan untuk memastikan bahwa EHR dan riwayat kesehatan pasien yang akan dirujuk tidak dapat dipelajari oleh penyerang (*attacker)*.

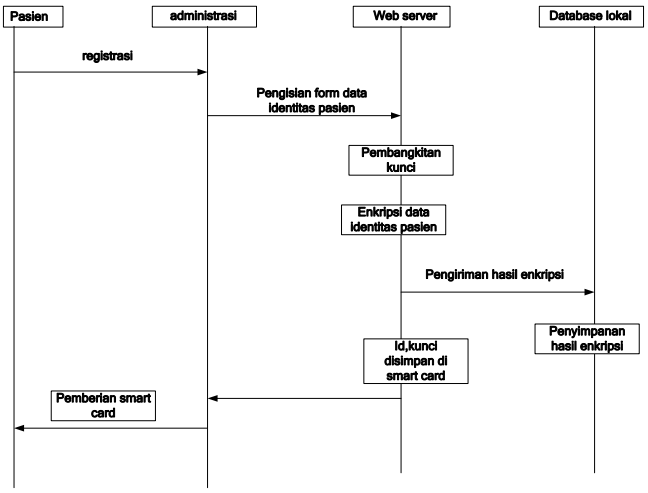
4) Keutuhan (*Integrity)*: Sistem yang dibuat harus dapat memastikan bahwa riwayat kesehatan yang disimpan tidak dapat diubah kecuali oleh dokter yang berwenang dengan persetujuan pasien.

C. Desain Sistem Sharing

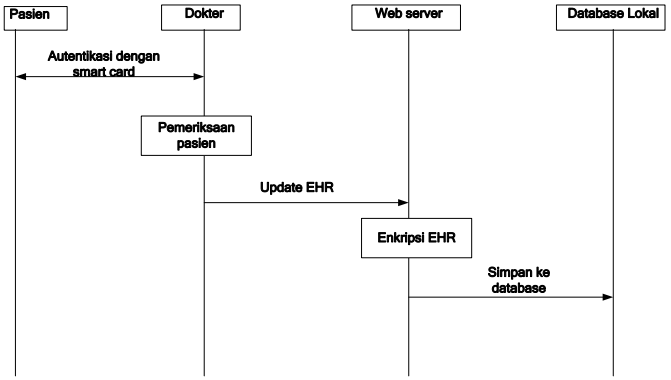
Secara garis besar, terdapat tiga protokol yang dibuat untuk memenuhi persyaratan keamanan sistem *sharing* serta pengontrolan akses informasi untuk menjamin privasi riwayat kesehatan pasien. Protokol tersebut meliputi protokol registrasi dokter dan pasien, protokol konsultasi, serta protokol *sharing* data riwayat kesehatan pasien.

1) Protokol Registrasi Dokter dan Pasien: Untuk memastikan terpenuhinya persyaratan keamanan, yaitu autentikasi, maka pasien dan dokter harus melakukan registrasi untuk mendapatkan *smart card*. Kartu kartu ini digunakan untuk melakukan verifikasi keabsahan pengguna saat proses konsultasi dan rujukan. Gbr. 3 menunjukkan proses registrasi pasien. Prosedur ini dilakukan jika pasien belum terdaftar sebagai anggota rumah sakit tersebut. Data yang tersimpan di *smart card* pasien adalah ID pasien dan kunci yang akan digunakan untuk melakukan autentikasi dan enkripsi/dekripsi identitas pribadi pasien, sedangkan data yang tersimpan di *smart card* dokter adalah ID dokter dan kunci yang digunakan untuk melakukan autentikasi dan enkripsi/dekripsi EHR.

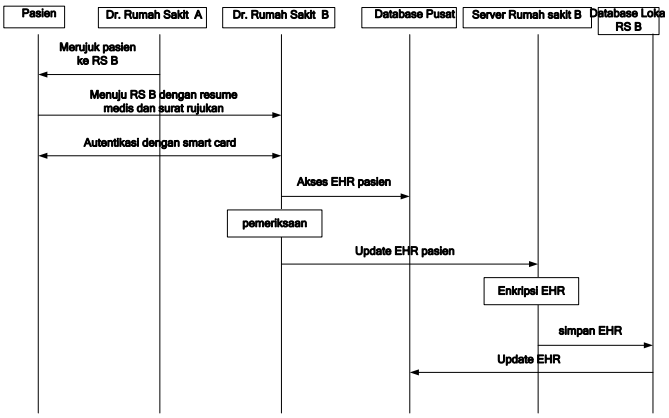
2) Protokol Konsultasi: Pemeriksaan dilakukan di klinik yang ditunjuk atau dipilih oleh pasien. Sebelum melakukan pemeriksaan dan konsultasi, seperti yang terlihat pada Gbr. 4, dokter dan pasien harus melakukan autentikasi terlebih dahulu dengan menggunakan *smart card*. Dokter memasukkan hasil pemeriksaan ke EHR pasien dengan terlebih dahulu dienkripsi menggunakan 3DES. Enkripsi dilakukan menggunakan kunci yang tersimpan di *smart card* dokter.



Gbr. 3 Proses registrasi pasien.



Gbr. 4 Proses konsultasi.



Gbr. 5 Protokol *sharing* data.

3) Protokol Sharing Data Riwayat Kesehatan Pasien: Pada mekanisme *sharing*, terdapat dua mekanisme yang dilakukan, yang mekanisme tersebut meliputi *sharing* internal (dalam lingkup rumah sakit tersebut) dan *sharing* eksternal (menuju rumah sakit lain dengan fasilitas yang lebih lengkap). Gbr. 5 menunjukkan mekanisme *sharing* eksternal yang dilakukan antara Rumah Sakit A ke Rumah Sakit B. Pada kasus rujukan,

Rumah Sakit A membekali pasien dengan *resume* medis dan surat rujukan. Sebelum dilakukan pemeriksaan, dokter di Rumah Sakit B mengakses EHR pasien yang tersimpan di basis data pusat untuk mendapatkan tambahan informasi riwayat kesehatan pasien. Setelah pasien selesai ditangani, dokter melakukan *update* EHR yang tersimpan di basis data lokal Rumah Sakit B dan basis data pusat.

IV. HASIL DAN PEMBAHASAN

Pada bagian ini dibahas tentang implementasi dan analisis sistem yang meliputi pengujian dan analisis data menggunakan algoritme 3DES sebagai sistem pengaman data dan *smart card* berbasis RFID sebagai media autentikasi.

A. *Implementasi Sistem*

RFID *reader* dan *writer* yang digunakan memiliki antarmuka USB. Perangkat ini terbuat dari mikrokontroler Arduino Uno R3 dan perangkat pendukung RFID *shield*, dengan spesifikasi seperti ditampilkan pada Tabel I dan Tabel II. *Tag* RFID yang digunakan adalah *Tag* RFID pasif Mifare 4 KB, seperti yang ditunjukkan pada Gbr. 6. Pengujian mekanisme sistem *sharing* dilakukan pada PC dengan spesifikasi seperti disajikan pada Tabel III.

TABEL I
SPESIFIKASI RFID ARDUINO UNO R3

Parameter	Spesifikasi
Interface	USB *Interface*
VDD Operating	DC5 V
Microcontroler	ATmega328
Clock Speed	16 MHz
SRAM	2KB (ATmega328)
EEPROM	1KB (ATmega328)
Weight	25 gram

TABEL II
SPESIFIKASI RFID SHIELD MFRC522

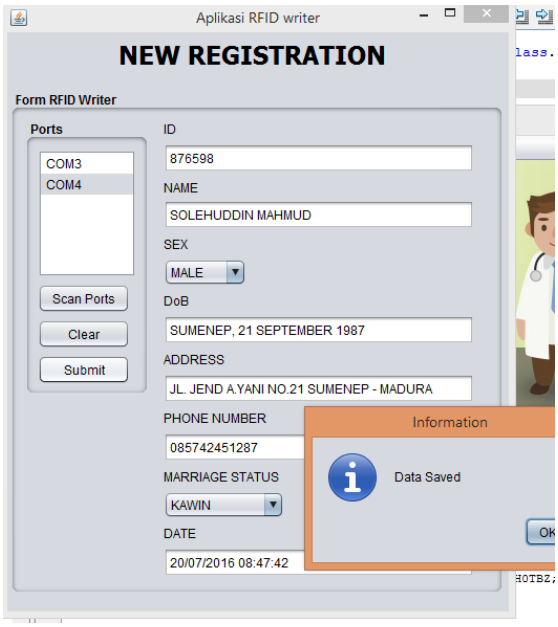
Parameter	Spesifikasi
VDD Operating	DC 2,5 – 3,3 V
Operating Frequency	125kHz
Weight	10 gram
Support Card	MF1xxS20, MF1xxS70 *and* MF1xxS50

Registrasi pasien diperuntukkan bagi pasien baru yang belum mendapatkan atau memiliki *smart card*. ID pasien akan otomatis terisi berurutan dengan ID yang terakhir terdaftar pada rumah sakit bersangkutan. Apabila data berhasil disimpan ke dalam basis data, akan muncul *pop up message* dengan teks "*Data Saved*" dan pada *smart card* akan tersimpan ID pasien serta kunci untuk enkripsi/dekripsi identitas pribadi pasien. Identitas pribadi pasien, meliputi nama, jenis kelamin, tempat/tanggal lahir, alamat, nomor telepon, serta status perkawinan, seperti terlihat pada Gbr. 7. Semua identitas pribadi akan dienkripsi dengan kunci pasien kecuali nama dan jenis kelamin. Hal ini bertujuan untuk menjaga privasi pasien, sehingga identitas pribadi hanya bisa diakses oleh dokter yang berwenang setelah dilakukan autentikasi. Autentikasi yang dilakukan oleh dokter bertujuan untuk membuka EHR pasien, seperti yang terlihat pada Gbr. 8.

TABEL IIII
SPESIFIKASI PC

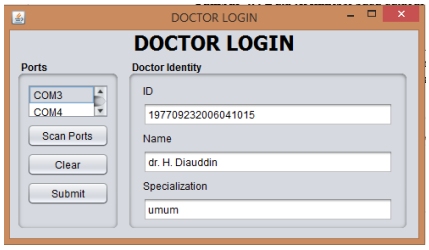
Parameter	Spesifikasi
Sistem Operasi	Microsoft Windows 7 Professional 64-Bit (Build 7601)
Processor	Intel® Core™ i5-3210M / i3-3110M
Memory	4 GB DDR3 1600MHz
HDD (Hard disk drive)	500 GB Serial ATA 7200 RPM
Graphics Adapter	Intel® HD Integrated Graphics 4000
Networking	802.11 a/b/g/n/ac
Interface	4 x USB 3.0, 2 x USB 2.0, 1 x HDMI, 1 x mini DisplayPort, 1 x RJ45 LAN, 1 x COM Port(Serial Port)

Gbr. 6 *Tag* RFID Mifare 4 KB.

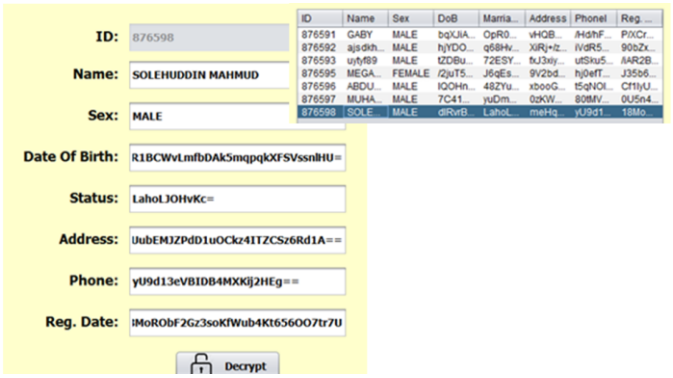


Gbr. 7 Halaman registrasi pasien.

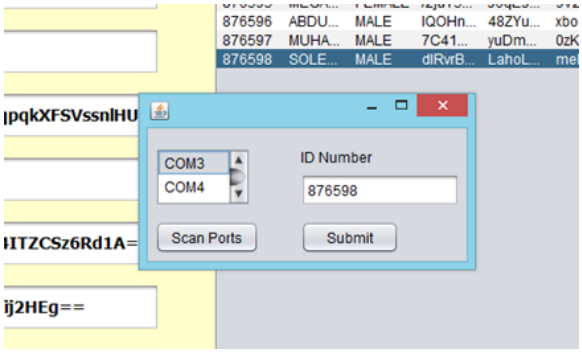
Setelah dilakukan autentikasi, baik oleh pasien maupun dokter, akan ditampilkan data pasien yang telah terdaftar pada rumah sakit tersebut, seperti ditunjukkan pada Gbr. 9. Data yang ditampilkan masih dalam bentuk terenkripsi, dan untuk menampilkan data yang sebenarnya, diperlukan autentikasi dari pasien terkait, klik pada tombol *decrypt* setelah sebelumnya memilih data pasien yang ingin dilihat, dan akan muncul *pop up* autentikasi, seperti yang ditunjukkan pada Gbr. 10. Setelah dilakukan autentikasi dengan *smart card* pasien, maka identitas pribadi pasien yang telah terdekripsi akan ditampilkan seperti pada Gbr. 11.



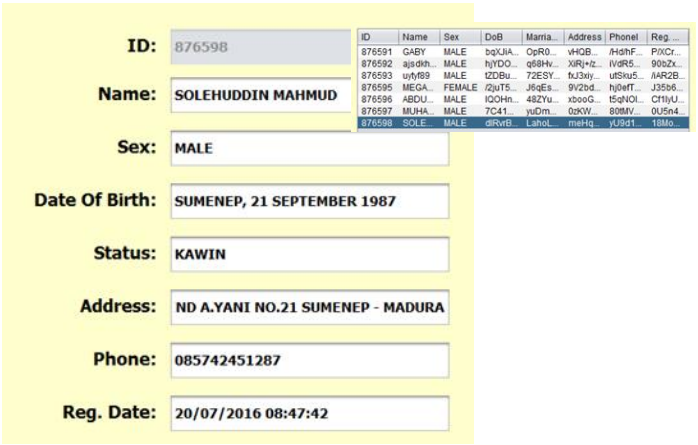
Gbr. 8 Halaman autentikasi dokter.



Gbr. 9 Daftar pasien.

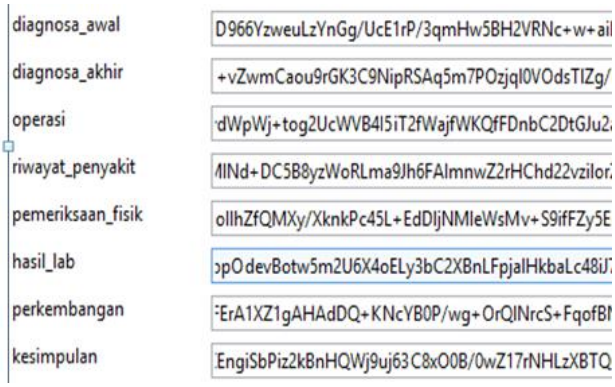


Gbr. 10 *Pop up* autentikasi.

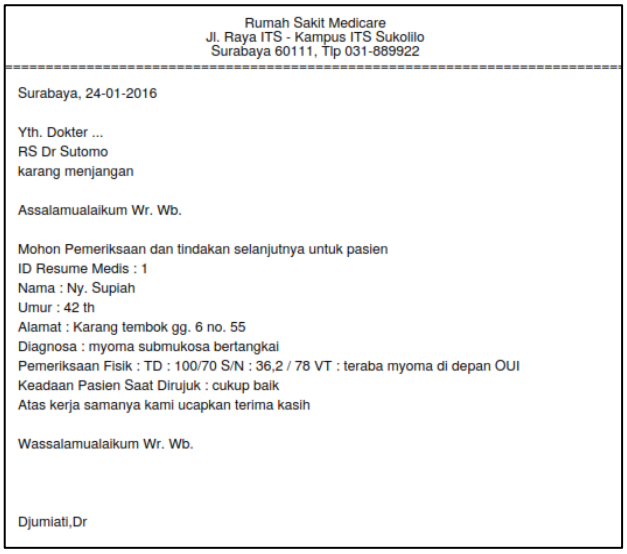


Gbr. 11 Data hasil dekripsi.

Gbr. 12 menunjukkan data EHR pasien yang masih terenkripsi dan hanya bisa dibuka menggunakan *smart card* dokter yang berwenang. Contoh surat rujukan ditunjukkan pada Gbr. 13. Surat ini dibawa oleh pasien saat terjadi kasus rujukan.



Gbr. 12 Data EHR pasien yang masih terenkripsi.



Rumah Sakit Medicare
Jl. Raya ITS - Kampus ITS Sukolilo
Surabaya 60111, Tlp 031-889922

Surabaya, 24-01-2016

Yth. Dokter ...
RS Dr Sutomo
karang menjangan

Assalamualaikum Wr. Wb.

Mohon Pemeriksaan dan tindakan selanjutnya untuk pasien
ID Resume Medis : 1
Nama : Ny. Supiah
Umur : 42 th
Alamat : Karang tembok gg. 6 no. 55
Diagnosa : myoma submukosa bertangkai
Pemeriksaan Fisik : TD : 100/70 S/N : 36,2 / 78 VT : teraba myoma di depan OUI
Keadaan Pasien Saat Dirujuk : cukup baik
Atas kerja samanya kami ucapkan terima kasih

Wassalamualaikum Wr. Wb.

Djumiati,Dr

Gbr. 13 Surat rujukan.

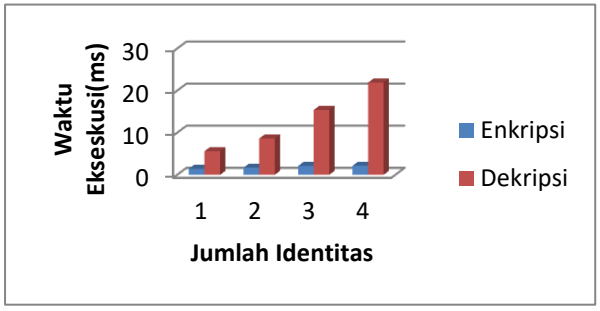
B. *Hasil Pengujian dan Analisis*

Beberapa pengujian yang dilakukan pada sistem *sharing* yang telah dibuat meliputi pengujian *avalanche effect*, serta waktu enkripsi dan dekripsi dari algoritme 3DES.

1) Pengujian Avalanche Effect: Salah satu karakteristik untuk menentukan baik atau tidaknya suatu algoritme kriptografi adalah dengan melihat *avalanche effect*-nya. Perubahan yang kecil pada *plain text* maupun kunci akan menyebabkan perubahan yang signifikan terhadap *ciphertext* yang dihasilkan. Suatu *avalanche effect* dikatakan baik jika perubahan bit yang dihasilkan berkisar antara 45% - 60% [7]. Hal ini dikarenakan perubahan tersebut berarti membuat perbedaan yang cukup sulit untuk *cryptanalist* melakukan serangan. Pada pengujian *avalanche* seperti yang ditampilkan pada Tabel IV, kunci yang ditetapkan adalah "12345678ABCDEFGH" dengan *plaintext* sebagai perbandingan berupa string "0000000000000000". Nilai *avalanche effect* diperoleh dengan mengubah data *cipher* ke dalam bentuk angka biner, dan dari dua *cipher* yang dibandingkan dihitung jumlah angka yang berbeda lalu dibandingkan dengan total jumlah bit *cipher*. Dari hasil percobaan sebanyak sepuluh kali, dengan perubahan parameter pada *plaintext*, data yang diperoleh berada pada kisaran nilai ideal dari *avalanche effect*, yaitu 51,4 %.

TABEL IV
PENGUJIAN *AVALANCHE EFFECT*

Plain Text	***Ciphertext***	***Avalanche* (%)**
0000000000000000	320D2DC83FCF3996	43,75
0000000000000001	37DB2E2B85FCABB2	
0000000000000000	320D2DC83FCF3996	59,375
0000000000000010	E76184A374848A29	
0000000000000000	320D2DC83FCF3996	53,125
0000000000000100	51E018E0E3FDEB48	
0000000000000000	320D2DC83FCF3996	39,0625
0000000000001000	62AB6D600FC1D6DB	
0000000000000000	320D2DC83FCF3996	53,125
0000000000010000	EEAA68E3FBD18067	
0000000000000000	320D2DC83FCF3996	57,8125
0000000000100000	FB90F9A6E151E01F	
0000000000000000	320D2DC83FCF3996	51,5625
0000000001000000	238A9AD391FCA5B8	
0000000000000000	320D2DC83FCF3996	46,875
0000000010000000	B04C79FFF624D96E	
0000000000000000	320D2DC83FCF3996	57,8125
0000000100000000	ECB18CD6CC0C6362	
0000000000000000	320D2DC83FCF3996	51,5625
0000001000000000	BCD8EA630EC99200	
Rata-rata		51,40625



Gbr. 14 Waktu eksekusi enkripsi dan dekripsi identitas pribadi.

2) Unjuk Kerja Sistem: Pengujian ini dilakukan sebanyak sepuluh kali untuk mengetahui kecepatan rata-rata enkripsi menggunakan algoritme 3DES. Pengujian enkripsi dilakukan pada identitas pribadi pasien. Tabel V sampai Tabel VIII menunjukkan pengujian enkripsi dan dekripsi dengan jumlah identitas pribadi yang berbeda-beda. Gbr. 14 menunjukkan bahwa semakin banyak jumlah identitas, maka waktu eksekusi enkripsi dan dekripsi juga semakin meningkat, dengan waktu eksekusi terlama diperoleh saat pengujian empat identitas, yaitu 2,16 ms untuk proses enkripsi dan 21,92 ms untuk proses dekripsi.

Pengujian waktu komputasi enkripsi/dekripsi juga dilakukan pada panjang karakter yang bervariasi, mulai satu hingga 300 karakter. Tabel IX menyajikan perbandingan waktu komputasi enkripsi/dekripsi antara metode 3DES dan HIBE. Hasil pengujian yang dilakukan menunjukkan bahwa waktu komputasi yang dibutuhkan untuk enkripsi/dekripsi data dengan metode 3DES lebih cepat jika dibandingkan dengan metode HIBE [4].

TABEL V
PENGUJIAN SATU IDENTITAS

Pengujian ke-	**Enkripsi (ms)**	**Dekripsi (ms)**
1	1,42	4,98
2	1,03	6,37
3	1,78	5,79
4	1,63	4,95
5	1,40	5,17
6	1,03	4,70
7	1,29	6,79
8	1,78	6,71
9	1,63	5,82
10	1,60	4,91
Rata-rata	1,46	5,62

TABEL VI
PENGUJIAN DUA IDENTITAS

Pengujian ke-	**Enkripsi (ms)**	**Dekripsi (ms)**
1	1,66	9,85
2	1,35	8,46
3	1,39	8,43
4	1,48	8,82
5	2,26	9,13
6	2,43	8,23
7	1,83	8,43
8	1,27	7,95
9	1,72	8,62
10	1,65	8,47
Rata-rata	1,70	8,64

TABEL VII
PENGUJIAN TIGA IDENTITAS

Pengujian ke-	**Enkripsi (ms)**	**Dekripsi (ms)**
1	2,22	17,92
2	2,15	14,78
3	1,68	16,61
4	1,93	15,43
5	1,96	14,31
6	2	14,07
7	2,08	16,87
8	1,62	15,50
9	2,86	14,16
10	2,6	14,51
Rata-rata	2,11	15,42

TABEL VIII
PENGUJIAN EMPAT IDENTITAS

Pengujian ke-	**Enkripsi (ms)**	**Dekripsi (ms)**
1	2,25	23,52
2	1,93	22,12
3	2,14	20,35
4	2,19	25,38
5	2,79	20,38
6	1,73	20,47
7	1,83	22,36
8	2,27	20,55
9	2,42	23,50
10	2,05	20,65
Rata-rata	2,16	21,92

TABEL IX
PERBANDINGAN WAKTU KOMPUTASI 3DES DAN HIBE

Panjang Pesan	Waktu Komputasi (ms)		Waktu Komputasi [4] (ms)	
	Enkripsi	Enkripsi	Enkripsi	Dekripsi
1	1,1	5,2	320	57
5	1,35	5,65	310	56
10	1,44	7,5	310	54
15	1,99	9,2	310	55
20	2,12	11,2	310	55
30	2,13	15,41	310	55
50	2,18	22,93	310	54
100	3,25	27,7	310	55
200	4,43	32,5	310	54
300	5,55	37,55	310	55

V. KESIMPULAN

Pada makalah ini diusulkan sebuah mekanisme sistem *sharing* berbasis *cloud* yang dilengkapi dengan algoritme 3DES untuk mengamankan data riwayat kesehatan serta penggunaan *smart card* sebagai media pengontrolan akses informasi pasien. Sistem yang dibuat telah memenuhi persyaratan keamanan, seperti privasi, autentikasi, kerahasiaan, dan keutuhan. Pengujian *avalanche effect* menunjukkan bahwa sistem yang dihasilkan telah memenuhi syarat keamanan karena perubahan bit yang dihasilkan berada pada kisaran nilai ideal dari *avalanche effect* yaitu 51,4%. Hasil pengujian unjuk kerja sistem menunjukkan bahwa waktu eksekusi terlama diperoleh saat pengujian empat identitas, yaitu 2,16 ms untuk proses enkripsi dan 21,92 ms untuk proses dekripsi.

UCAPAN TERIMA KASIH

Penelitian ini didanai oleh Kementrian Riset, Teknologi, dan Pendidikan Tinggi, Penelitian Produk Terapan 2017.

REFERENSI

[1] J. L. Fernandez-Aleman, I.C. Senor, P.A.O. Lozoya and A. Toval, "Security and privacy in electronic health records: A systematic literature review", *Journal of Biomedical Informatics*, pp. 541-562, 2013.

[2] J. Rodrigues, I. De La Torre, G. Fernandez and M. Lopez-Coronado, "Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems", *Journal of Medical Internet Research*, Vol 15, No 8, August 2013.

[3] M. Arfan, "Model Implementasi Centralized Authentication Service pada Sistem Software As A Service", *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI)*, Vol. 03, No. 1, Februari 2014.

[4] M. Yuliana, H.A. Darwito, A. Sudarsono, G.M. Yovie, "Privacy and security of sharing referral medical record for health care system", *Proceeding of 2nd International Conference on Science in Information Technology (ICSITech)*, pp.232-237, Balikpapan , Indonesia.

[5] M. Hassanalieragh, A. Page, T. Soyata, and G. Sharma, "Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-based Processing: Opportunities and Challenges", *Proceeding of IEEE International Conference on Services Computing*, pp.285-292, 2015.

[6] G. Nalinipriya and R. Aswin Kumar, "Extensive medical data storage with prominent symmetric algorithms on cloud - a protected framework," *IEEE Int. Conf. on Smart Structures and Systems (ICSSS)*, March 2013, pp. 171–177

[7] A. Page, O. Kocabas, T. Soyata, M. Aktas, and J.-P. Couderc, "CloudBased Privacy-Preserving Remote ECG Monitoring and Surveillance," *Annals of Noninvasive Electrocardiology (ANEC)*, 2014.

[8] Govinda, Sathiyamoorthy, and S. Agarwal, "Secure Key Exchange for Cloud Environment Using Cellular Automata with Triple-DES and Error-Detection", *International Journal of Engineering and Technology (IJET)*, ISSN : 0975-4024 Vol 5 No 2 Apr-May 2013, 1004-1009.