Prosiding
ANNUAL RESEARCH SEMINAR 2016
6 Desember 2016, Vol 2 No. 1

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

Perancangan Pengamanan Sistem Informasi *Electronic Medical Record* (Emr) Dengan Metode Sha-512 Studi Kasus Pada Klinik Jb Palembang

Pacu Putra
Jurusan Sistem Informasi
Fakultas Ilmu Komputer, Universitas Sriwijaya
Palembang, Indonesia
pacuputra@ilkom.unsi.ac.id

Reza Winiarni
Jurusan Sistem Informasi
Fakultas Ilmu Komputer, Universitas Sriwijaya
Palembang, Indonesia
rezawiwin94@gmail.com

***Abstrak*— Electronic medical record can help document storage of medical record to be more integrated and protected from damage or loss of data. However, using electronic storage cannot ensure that the medical record documents that have been saved still legal or illegal document. To prevent the occurrence data manipulation and loss of data, linking scheme using hash function SHA-512 will be applied. By using linking scheme each document will be interconnected and contained a hash value from the previous document. The system will detect quickly if there are manipulation and loss of data.**

Intisari— Perkembangan rekam medis elektronik sangat membantu dalam hal penyimpanan dokumen rekam medis pasien agar tetap terintegrasi dan terlindung dari kerusakan ataupun kehilangan data. Namun, dengan penyimpanan secara elektronik saja tidak dapat memastikan bahwa dokumen rekam medis yang telah disimpan masih berupa dokumen legal atau sudah illegal. Untuk mencegah terjadinya manipulasi data dan kehilangan data maka akan diterapkan *linking scheme* dengan menggunakan *hash function* SHA-512. Dengan menggunakan linking scheme setiap dokumen akan saling terhubung dan mengandung nilai hash dari dokumen sebelumnya. Sehingga sistem akan mendeteksi dengan cepat apabila terjadi manipulasi dan kehilangan data.

Kata Kunci— *Electronic Medical Record, Linking Scheme, SHA-512, Hash Function, Waterfall.*

I. PENDAHULUAN

Saat ini penyimpanan data secara elektronik sudah banyak digunakan. Data-data yang berupa pesan, gambar ataupun dokumen disimpan secara elektronik dengan harapan agar terhindar dari kerusakan dan kehilangan data. Namun untuk keaslian data sangat jarang diperhatikan. Keaslian suatu data atau informasi menjadi hal yang sangat penting untuk diperhatikan karena apabila suatu data atau informasi sudah tidak asli maka akan berakibat fatal. Seperti halnya dokumen hasil rekam medis pasien apabila telah terjadi perubahan pada hasil pemeriksaan pasien maka akan menimbulkan bahaya atas keselamatan jiwa pasien. Rekam medis pasien bersifat rahasia sehingga hanya bisa dilihat dan diakses oleh pasien yang bersangkutan dan tenaga kesehatan yang berkepentingan.

Rekam medis merupakan bukti tertulis tentang proses pelayanan yang diberikan oleh dokter dan tenaga medis kesehatan lainnya kepada pasien. Bukti tertulis pelayaanan dilakukan setelah pemeriksaan, tindakan dan pengobatan. Dengan adanyan rekam medis maka pasien memiliki bukti yang sah yang dapat dipertanggung jawabkan. Menurut Permenkes No.749/menkes/Per/1989 pasal 10 ayat 1 bahwa rekam medis milik sarana pelayanan kesehatan, ayat 2 bahwa isi rekam medis merupakan milik pasien. Maka pihak instansi kesehataan berkewajiban untuk menjaga kerahasiaan isi dokumen rekam medis dan memeliharanya.

Pentingnya pengelolaan dan penyimpanan rekam medis juga menjadi perhatian bagi klinik, salah satunya Klinik JB. Dimana rekam medis yang ada pada Klinik JB sekarang masih disimpan dalam bentuk dokumen kertas yang masih rentan akan terjadinya kehilangan, kerusakan dan penyalahgunaan pada dokumen rekam medis. Perkembangan dan kemajuan rekam medis merupakan ujung tombak yang dapat membawa nama baik Klinik JB. Maka Klinik JB memerlukan rekam medis yang aman dan dapat menjaga kerahasiaan data-data pasiennya agar tidak ada penyalahgunaan terhadap data rekam medis pasien.

Prosiding
ANNUAL RESEARCH SEMINAR 2016
6 Desember 2016, Vol 2 No. 1

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

Oleh karena itu perlu adanya teknik atau metode untuk menjaga dan mendeteksi apabila terjadi manipulasi atau perubahan pada data yang telah disimpan. Penulis mencoba untuk menerapkan *linking scheme* dengan menggunakan *hash function* SHA-512 pada rekam medis elektronik di Klinik JB Palembang. Yang diharapkan dapat mencegah terjadinya kehilangan dan perubahan atau manipulasi data.

II. STUDI PUSTAKA

2.1. Electronic Medical Record

Pada prinsipnya rekam medis elektronik tidak berbeda jauh dengan sistem rekam medis biasa atau manual yang berfungsi untuk menyimpan data, seperti data sosial, catatan anamnesa, pemeriksaan fisik, pemeriksaan penunjang, diagnosa, tindakan, terapi, rencana tindakan lanjut. Rekam medis elektronik memanfaatkan perangkat teknologi informasi untuk pengumpulan, penyimpanan, pengelolaan serta pengaksesan rekam medis pasien yang tersimpan dalam suatu basis data. Rekam medis elektronik juga dapat membantu tenaga medis memonitor, mendokumentasikan, dan mengelola pelayanan yang telah diberikan kepada pasien.

2.2. SHA-512

SHA adalah fungsi hash satu arah yang didesain oleh National Security Agency (NSA) dan dipublikasi oleh National Institute of Standards and Technology (NIST) sebagai Federal Information Processing Standard (FIPS) pada tahun 1993 dan disebut sebagai SHA-0, dua tahun kemudian dipublikasikan SHA 1 generasi selanjutnya yang merupakan perbaikan dari algoritma SHA-0. Pada tahun 2002 dipublikasikan empat variasi lainnya, yaitu SHA-224, SHA-256, SHA-384, dan SHA-512, keempatnya disebut sebagai SHA-2.

Fungsi hash SHA-512 merupakan fungsi yang menghasilkan message digest ukuran 512 bit dan panjang blok 1024 bit. Terdapat 80 putaran dalam fungsi ini. Untuk melakukan padding bit dilakukan dengan cara yang sama dengan SHA-1, namun ukuran blok menjadi 1024 bit, bukan 512 bit.

Berikut adalah fungsi yang digunakan pada setiap putaran adalah:

1. Penjadwalan pesan

$$W_t = \begin{cases} M_t^{(i)} & , 0 \le t \le 15 \\ \sigma 1^{\{512\}}(W_{t-2}) + W_{t-7} + \sigma 1^{\{512\}}(W_{t-15}) + W_{t-16}, & 16 \le t \le 79 \end{cases}$$

2. Inisialisasi

$a = H_0^{(i-1)}$ $b = H_1^{(i-1)}$ $c = H_2^{(i-1)}$ $d = H_3^{(i-1)}$ $e = H_4^{(i-1)}$ $f = H_5^{(i-1)}$ $g = H_6^{(i-1)}$ $h = H_7^{(i-1)}$

3. Fungsi untuk setiap putaran

$T_1 = h + \sum_1^{\{512\}}(e) + Ch(e,f,g) + K_t^{\{512\}} + W_t$

$T_2 = \sum_0^{\{512\}}(a) + Maj(a,b,c)$

$h = g$

$g = f$

$f = e$

$e = d + T_1$

$d = c$

$c = b$

$b = a$

$a = T_1 + T_2$

$Ch(x,yz) = (x^y) \oplus (\neg x^z)$

$Maj(x,yz) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$

$\sum_0^{\{512\}}(x) = ROTR^{28}(x) \oplus ROTR^{34}(x) \oplus ROTR^{39}(x)$

$\sum_1^{\{512\}}(x) = ROTR^{14}(x) \oplus ROTR^{18}(x) \oplus ROTR^{41}(x)$

$\sigma 0^{\{512\}} = ROTR^{1}(x) \oplus ROTR^{18}(x) \oplus SHR^{7}(x)$

4. $\sigma 1^{\{512\}} = ROTR^{19}(x) \oplus ROTR^{61}(x) \oplus SHR^{6}(x)$

$$\begin{aligned} H_0^{(i)} &= a + H_0^{(i-1)} \\ H_1^{(i)} &= b + H_1^{(i-1)} \\ H_2^{(i)} &= c + H_2^{(i-1)} \\ H_3^{(i)} &= d + H_3^{(i-1)} \\ H_4^{(i)} &= e + H_4^{(i-1)} \\ H_5^{(i)} &= f + H_5^{(i-1)} \\ H_6^{(i)} &= g + H_6^{(i-1)} \\ H_7^{(i)} &= h + H_7^{(i-1)} \end{aligned}$$

5. Nilai hasil akhir

$$H_0^{(N)} \| H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)}$$

Keluaran akhir dari algoritma SHA adalah hasil penyambungan bit-bit di A, B, C, D, E, F, G dan H.

2.3. Linking Scheme

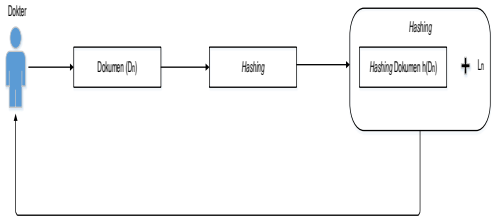
Linking scheme dirancang dengan tujuan untuk mendekteksi adanya dokumen yang tidak sah atau illegal

Prosiding
ANNUAL RESEARCH SEMINAR 2016
6 Desember 2016, Vol 2 No. 1

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

dokumen. *Linking scheme* juga menghubungkan antara satu dokumen dengan dokumen yang lainnya yang akan membentuk rangkaian dokumen. Hal tersebut dilakukan agar dapat mengetahui jika adanya perubahan dari setiap dokumen.

SHA-512 dan *Liking scheme* ini akan digunakan pada rekam medis pasien Klinik JB Palembang. Dalam penyimpanan rekam medis hanya Dokter dan petugas pelayanan kesehatan yang memiliki izin dan tanggung jawab di Klinik JB yang dapat mengakses rekam medis pasien. Rekam medis pasien yang akan digunakan dalam penelitian ini adalah rekam medis pasien umum rawat jalan. Berikut adalah linking scheme yang akan digunakan dalam perancangan sistem.



Gambar 1 *Linking Scheme*

Dari gambar 1 dapat dijelaskan bahwa dokumen yang dikirim oleh dokter akan dilakukan hashing dengan menggunakan SHA-512. Hasil dari hashing berupa rekam medis pasien, ID dari dokter, waktu, dan nomor urut dari dokumen tersebut. Berikut penjelasan dari langkah-langkah pada gambar 1:

- Dokumen (D) yang dikirim oleh dokter akan di-hashing menggunakan SHA-512. Dokter mengirimkan nilai hashing dengan menyertakan IDnya.

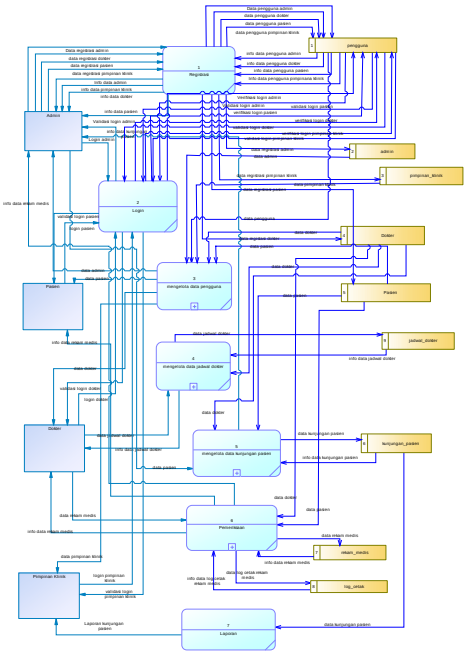
h = H (Dn, Ln)
Ln = (Dn-1, H(Ln-1))

Yang mana :
h = hasil hashing untuk dokumen yang dikirim,
H = Fungsi Hashing SHA-512,
Dn = dokumen (rekam medis pasien),
Ln = link untuk menghubungkan antar dokumen hasil pemeriksaan dari masing-masing pasien.

III. HASIL PERANCANGAN

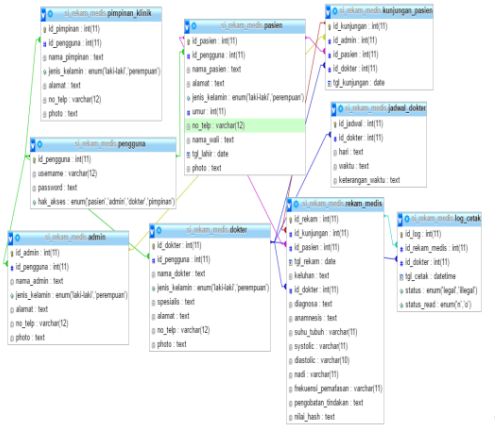
Pada bagian ini akan menjelaskan mengenai rancangan sistem mulai dari *data flow diagram* dan skema *database.*

3.1. Data flow Diagram



Gambar 2 *Data Flow Diagram*

3.2. Skema Database



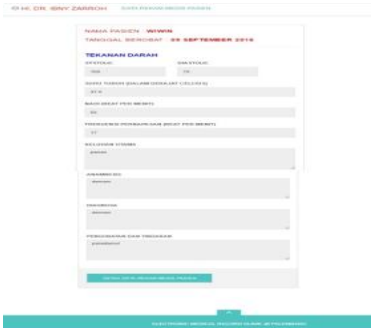
Gambar 3 Skema *Database*

IV. HASIL DAN PEMBAHASAN

Pada bagian ini akan diuraikan mengenai *interface* yang akan digunakan oleh *user*.

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

4.1.1. Halaman Detail Rekam Medis



Gambar 4 Detail Rekam Medis Pasien

Halaman ini menampilkan rekam medis pasien secara detail berdasarkan hasil pemeriksaan yang lakukan oleh dokter. Terdapat nama pasien dan tanggal pemeriksaan serta data-data pemeriksaan lainnya. Tersedia tombol cetak rekam medis pada halaman ini.

4.1.2. Dokumen Rekam Medis yang Dicetak

Gambar 5 Dokumen Rekam Medis Pasien Legal (Kanan), Dokumen Rekam Medis Pasien Illegal (Kiri)

Dokumen diatas merupakan hasil cetak dari rekam medis pasien. pada saat pencetakan rekam medis maka sistem akan memeriksa apakah dokumen rekam medis yang ingin dicetak masih legal atau sudah illegal. Pemeriksaan ini dilakukan menggunakan *linking scheme* dengan SHA-512. Sehingga saat dokumen telah selesai dicetak akan muncul status dari dokumen rekam medis tersebut.

V. KESIMPULAN

Beberapa hal yang dapat disimpulkan dari Perancangan Pengamanan Sistem Informasi Electronic Medical Record dengan Metode SHA-512 pada Klinik JB Palembang sebagai berikut :

1. Dengan adanya sistem electronic medical record ini dapat membantu pihak klinik untuk mengelolah data-data dokter, pasien, pimpinan dan admin agar lebih terorganisir dan terstruktur.
2. Pengembangan sistem informasi electronic medical record ini dapat membantu pihak klinik dalam penyimpanan dokumen-dokumen rekam medis pasien agar lebih terstruktur dan terhindar dari resiko manipulasi, kerusakan, kehilangan dan penyalahgunaan dokumen rekam medis pasien.
3. Sistem informasi electronic medical record ini dikombinasi dengan metode SHA-512 yang digunakan untuk menjaga keaslian dari dokumen rekam medis pasien sehingga apabila terjadi perubahan pada isi data rekam medis dari seorang pasien maka dokumen rekam medis yang tersimpan menjadi dokumen yang illegal karena isi dokumen sudah mengalami perubahan walaupun satu huruf dan perubahan pada satu dokumen akan mempengaruhi legalitas untuk dokumen selanjutnya.

REFERENSI

[1] J. Sembiring, "Analisis Algoritma SHA-512 dan Watermarking Dengan Metode Least Significant Bit Pada Data Citra," *Seminar Nasional Sistem Informasi Indonesia*, pp. 397-400, 2013.

[2] P. P. Suarli, "Enhancing Time-Stamping Technique By Implementing Media Access Control Address," Universiti Teknologi Malaysia, Johor Bahru, Malaysia, 2013.

[3] W. Handiwidjojo, "Rekam Medis Elektronik," *Jurnal EKSIS Vol 02 No 01*, pp. 36-41, 2009.

[4] W. Setiawan, "Analisis dan Perbandingan Algoritma Whirlpool dan SHA-512 sebagai Fungsi Hash," Bandung, 2010.

[5] M. Mulya, "Penggunaan Algoritma SHA-512 untuk Menjamin Integritas dan Keotentikan Pesan pada Intranet," *Konferensi Nasional Sistem Informasi dan Informatika*, pp. 107-111, 2009.

[6] E. H. A. S. Moh. Muttaqin, "Perancangan Aplikasi Electronic Medical Record (EMR) Pada Instalasi Rawat Inap Berbasis Web".