Sistem Kriptografi di Komputasi Awan Untuk Kebutuhan Data Medis

Maya Hilda Lestari Louk
Universitas Surabaya
mayalouk@staff.ubaya.ac.id

Abstrak – Komputasi awan adalah sebuah metode komputasi yang sedang berkembang saat ini untuk berbagi data dan pemrosesan data baik secara terbuka/umum atau pribadi. Komputasi awan adalah jawaban atas lingkungan komputasi yang lebih efektif dan efisien. Hal itu akan mengurangi biaya komputasi dan tenaga ahli komputasi. Komputasi awan dapat digunakan tidak hanya untuk tujuan bisnis tetapi juga untuk tujuan medis/kesehatan yang akan digunakan oleh pasien, spesialis, apoteker, perawat, dokter, dan pegawai administrasi rumah sakit. Sebagai implikasi pada sisi yang lain, keamanan adalah isu penting di dalam Komputasi awan. Perlindungan privasi data dan kontrol penerimaan data adalah tantangan keamanan di dalam Komputasi awan. Penulisan ini secara singkat membuat sketsa penggunaan sistem Kriptografi untuk kebutuhan data medis menggunakan Komputasi awan, khususnya fungsi enkripsi ulang (re-enkripsi fungsional) "*tag*" dan "tanda" untuk melakukan akses data. Penulisan ini memberi solusi alternatif untuk keamanan data pada Komputasi awan berdasarkan layanan enkripsi dan dekripsi dengan re-enkripsi fungsional untuk kebutuhan data medis dan data pelayanan kesehatan. Data dapat diakses dari mana saja dan oleh siapa saja yang memiliki hak akses untuk mengakses data sesuai dengan kebijakan akses tersebut. Penulisan ini diusulkan dan terdiri dari pembahasan terhadap ide dari penggunaan Komputasi awan dan keamanan data pada data medis dan data pleayanan kesehatan.

Kata Kunci: Data Medis, Komputasi Awan, Kriptografi, Re-enkripsi Fungsional, Tag dan Tanda.

I. PENDAHULUAN

Komputasi awan adalah sebuah paradigma komputasi yang mendapat perhatian luas dari sisi akademisi dan industrialis. Dengan menggabungkan satu set kelembagaan yang telah ada dan teknologi baru dari penelitian yang telah ada seperti *Service-Oriented Architecture* (SOA) dan virtualisasi komputasi awan yang dianggap sebagai paradigma komputasi dimana sumber data yang disimpan di dunia virtual internet. Pada komputasi awan, pengguna diberikan cara baru untuk berbagi sumber data dan jasa yang disediakan oleh berbagai tempat. Saham sumber daya komputasi awan sejak didistribusikan melalui jaringan, lingkungan di tempat terbuka. Dengan demikian masalah keamanan data adalah hal penting untuk diperhatikan. Penelitian ini untuk mengembangkan program aplikasi yang akan aman untuk dijalankan secara aman, efektif, dan efesien.

Data medis milik pasien adalah muatan informasi sensitif yang nantinya akan disampaikan kepada pihak yang memiliki hak untuk menganalisis dan memproses data. Konsep ini tidak hanya mencakup pasien kota besar yang memiliki fasilitas rumah sakit *modern* namun juga menjangkau hingga pasien kota kecil yang memiliki fasilitas rumah sakit terbatas. Dengan desain sistem ini, pegawai administrasi rumah sakit atau perawat akan dapat menolong pasien untuk mencatat data yang perlu perlukan melalui komputasi awan. Selanjutnya, dokter spesialis akan dapat untuk mengakses data di dalam komputasi awan dimanapun dia berada. Dokter akan dapat membaca, memproses, memodifikasi, dan mengirim analisisnya melalui komputasi awan sehingga pegawai administrasi rumah sakit akan dapat menjalankan instruksi yang telah diberikan oleh dokter.

Desain konsep ini akan berkaitan dengan sistem keamanan yang mencakup keseluruhan ide. Sistem keamanan merupakan prioritas utama oleh karena data pasien yang bersifat pribadi dan sensitif.

Berikut ini merupakan beberapa tantangan dalam keamanan data komputasi awan:

1. Bagaimana cara penyedia layanan komputasi awan melindungi data medis saya dari serangan siber?
2. Bagaimana cara penyedia layanan komputasi awan mengatur data medis sehingga bisa diakses hanya oleh pengguna yang memiliki hak akses?
3. Bagaimana jika penyedia layanan komputasi awan tidak bisa menyimpan data medis saya?
4. Bagaimana cara penyedia layanan komputasi awan melindungi data medis ketika sedang diakses oleh pengguna berhak?

II. METODOLOGI PENELITIAN

Menyimpan data di dalam komputasi awan bukanlah konsep yang baru. Ide ini telah diterapkan oleh para peneliti Microsoft bernama Josh Benaloh, Melissa Chase, Eric Horvitz, dan Kristin Lauter [1]. Biarpun begitu, memproses dan mengakses data medis menggunakan komputasi awan bisa jadi adalah pengalaman baru bagi beberapa peneliti. Re-

enkripsi Fungsional yang diadaptasi dari Chandran Nishanth, Chase Melissa, dan Vaikuntanathan Vinod yang mengakalkulasi dengan *tag name* untuk mengakses data serta solusi arbiter simpel yang diadaptasi dari Seny Kamara dan Mariana Raykova [1][2][3]. Proyek terkait dengan data medis yang disimpan dalam komputasi awan juga telah banyak dikembangkan oleh peneliti Microsoft. Semua riset sebelumnya juga telah berkontribusi untuk pengembangan teori dan konsep keamanan medis komputasi awan. Pertanyaan yang paling penting untuk dijawab adalah: bagaimana cara untuk mengimplementasikan konsep ini menjadi kenyataan? Hanya saja pertanyaan ini bukanlah tema utama dari paper ini.

III. DATA MEDIS PASIEN

Data pasien atau data rumah sakit sebagian besar masih tersimpan sebagai data analog. Berikut ini beberapa keunggulan untuk memindahkan data analog menjadi data digital:

1. Tidak memerlukan tempat penyimpanan fisik.
2. Pencurian data lebih jarang terjadi.
3. Tidak perlu menyewa penjaga keamanan data.
4. Tidak ada kekuatiran akan kerusakan dokumen yang disebabkan oleh bencana alam atau kebakaran.

Data digital akan menurunkan pengeluaran biaya untuk mencetak semua data medis pasien, dan tentu saja konsep ini akan menolong mengurangi pemanasan global yang disebabkan oleh penggunaan kertas yang berlebihan. Rumah sakit harus menyediakan ruang khusus untuk komputasi awan dan sistem digitasi harus dibangun agar dapat membaca, memproses, dan mengakses data dengan benar dan akurat. Komputasi data medis pasien yang akan dicakup adalah:

1. Otentikasi data medis
   Otentikasi sudah harus dimulai sejak proses *login* [4]. Semua pengguna akan memasukkan data di sistem *login*. Tiap pengguna akan memverifikasi atau diverifikasi oleh pengguna lain (sebagai contoh, pegawai rumah sakit) dengan menggunakan *password*. Kelemahan metode ini adalah *password* dapat saja dicuri, tidak sengaja ketahuan orang lain yang tidak berkaitan atau kelupaan. Berdasarkan alasan ini, aktivitas digital yang berkaitan dengan internet akan membutuhkan proses otentifikasi yang lebih ketat. Penggunakan sertifikat digital yang diterbitkan dan dilegalisir oleh *Certificate Authority* (CA) dianggap sebagai metode standar untuk melakukan otentifikasi di Internet.
2. Keakuratan data medis
   Data medis haruslah akurat karena bersifat sensitif yang membutuhkan akurasi, hal ini dikarenakan:
   - Keutuhan data menggambarkan seberapa jauh isi data yang tercakup dapat tersimpan dengan baik.
   - Keakuratan menggambarkan seberapa miripkah data yang tercatat dengan informasi lapangan.
   - Konsistensi mencakup konsistensi data jika data dimasukkan dari beberapa pengguna dari tempat yang berbeda. Tidak adanya konsistensi dapat menyebabkan data menjadi tidak akurat.
3. Keamanan data medis
   Keamanan data medis merupakan isu utama, hal ini disebabkan jika terjadi kebocoran data pasien dan rumah sakit untuk disalahgunakan, baik disebarkan melalui internet atau ditunjukkan kepada pihak lain yang tidak berkepentingan, akan membuat pasien dan para pelaku rumah sakit terancam karena pada dasarnya data rumah sakit dan data pasien merupakan data yang bersifat personal dan sensitif.
4. Keamanan dalam pengiriman data (pengunduhan/pengunggahan)
   Pada saat melakukan aktivitas pengunduhan dan atau pengunggahan data ke sebuah pusat *server* komputasi awan sangat rawan terhadap serangan *Man in the Middle Attack* (MITM) [5]. Penyedia layanan komputasi awan telah melengkapi layanan keamanan transfer data, seperti: *Secure Socket Layer* (SSL) dan AES-256 enkripsi, seperti yang disediakan oleh Dropbox.
5. Tidak ada data yang hilang
   Pada waktu penyimpanan data, pengunduhan data, atau pengunggahan data, tidak boleh ada kemungkinan atau kejadian kehilangan data, baik sepenuhnya maupun sebagian. Data pasien dan data rumah sakit tidak hanya data personal yang sangat sensitif tetapi juga butuh akurasi data karena membutuhkan akurasi analisis data.
6. Akses kontrol pengguna
   Sistem ini didesain untuk dapat digunakan oleh *multiuser* atau banyak pengguna dengan berbagai kepentingan yang berbeda-beda dan masing-masing pengguna memiliki hak akses yang berbeda-beda [6]. Satu hal yang menjadi perhatian adalah penyedia layanan komputasi awan tidak boleh memiliki hak akses terhadap data ini, baik secara sistem maupun tenaga kerja ahli penyedia layanan komputasi awan.

Selain beberapa hal di atas, Penyedia layanan komputasi awan harus dapat menyediakan proses data yang akurat sehingga pengguna, terutama dokter yang memiliki otorisasi data tersebut dapat memberikan respon yang cepat dan akurat terhadap setiap perubahan data pasien yang akan berdampak pada pemberian perwatan yang tepat dan akurat terhadap pasien.

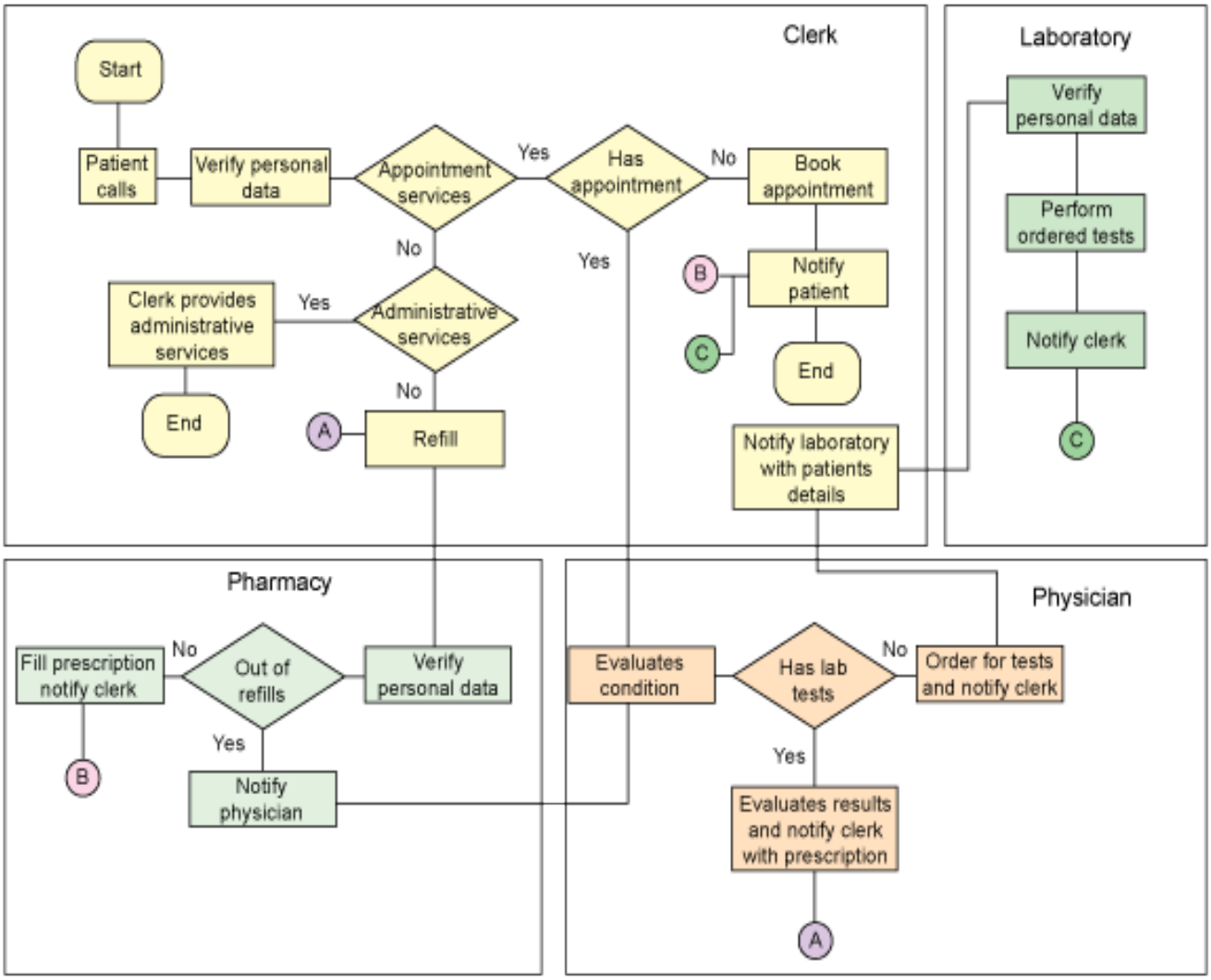
Desain sistem ini juga dapat berguna bagi rumah sakit/klinik yang berada pada daerah terpencil agar terhubung dengan dokter spesialis yang berada di kota besar. Pegawai adminstrasi/perawat/tenaga farmasi dapat memasukkan data pasien dalam sistem, dan dapat terbaca secara *real time* oleh dokter spesialis di kota besar. Dokter spesialis dapat memberikan perawatan yang tepat terhadap analisis data pasien, dalam hal ini pasien tersebut tidak perlu ke kota besar untuk mendapatkan analisis dokter spesialis (tergantung kasus tertentu). Selain itu seluruh data pasien tersimpan dengan baik dalam bentuk digital pada komputasi awan.

Gambar 1 adalah sistem tradisional untuk alur bisnis pengaturan data medis antara pasien, dokter spesialis, pegawai administrasi rumah sakit, dan laboran. Gambar 1

merupakan milik Sreevidya Krishna, seorang analis dan telah dipublikasikan oleh IBM dengan judul "*Taking Medical Records into the Digital Age Solving Traditional System Challenges with OpenEMR*" [7]. Dari sini, sistem tradisonal akan diubah atau bergerak ke arah sistem komputasi awan.

Salah satu perhatian mengenai penggunaaan data elektronik/data digital pada data medis adalah dibutuhkan tenaga ahli medis yang harus dapat beradaptasi terhadap perpindahan data analog ke data digital. Salah satunya adalah pengetikan data digital dengan baik dan akurat secara cepat dan efektif. Seringkali dokter harus memasukkan sendiri data digital ketika sedang melakukan pemeriksaan pasien. Ada kemungkinan bahwa dokter bisa saja menjadi bingung oleh teknologi yang rumit sehingga menjadi tidak terlalu berkonsentrasi kepada kesehatan pasien.

Tidak adanya sistem utama untuk data medis digital di beberapa rumah sakit menyebabkan adanya perbedaan program digital di beberapa rumah sakit. Perbedaan ini dapat menghalangi sinkronisasi data bagi seluruh tim medis. Berikut ini merupakan tabel perbandingan keunggulan dan kekurangan dari penyimpanan dan pemrosesan data medis pada komputasi awan yang tercatat dalam tabel 1.



Gambar 1. Diagram Aktivitas Untuk Sistem Tradisional.

Tabel 1. Keunggulan dan Kekurangan Data Medis Dalam Komputasi Awan.

Sisi Positif	Sisi Negatif
Biaya rendah untuk lisensi	Fitur menjadi terbatas
Tidak memerlukan piranti keras atau lunak	Ada jeda waktu yang menyebabkan sistem menjadi kurang responsif
Adanya kemungkinan kemudahan transisi ke program lain	Data pasien dapat terdistorsi jika tercampur dengan data pasien lain
Dapat menekan biaya perseorangan atau kelompok	Sangat tergantung dengan *vendor* untuk urusan *backup* dan keamanan
Bantuan manual yang lebih baik	Lebih mahal dalam jangka panjang
Mudah untuk membuat *hot-site* dalam rangka bencana alam	*Vendor* mengontrol data
Vendor memiliki prosedur keamanan yang ketat	Semua proses menjadi terhenti jika tidak ada internet
Vendor lebih dapat memenuhi persyaratan HIAA	Agak terbatas di tempat terpencil
Vendor yang banyak dapat lebih efektif	Data dapat menjadi hilang jika *vendor* bangkrut
Tepat untuk tenaga medis yang jarang di kantor	Adanya kesulitan jika harus mengirim foto gambar yang berukuran besar
	Koneksi internet bergantung terhadap kecepatan internet masing-masing

IV. RE-ENKRIPSI FUNGSIONAL UNTUK DATA MEDIS

Information Security Management System (ISMS) didefinisikan dalam ISO27000 sebagai "sistem yang menjadi model untuk membangun, mengimplementasikan, mengoperasikan, monitor, evaluasi, pemeliharaan dan meningkatkan keamanan aset informasi" [8]. Definisi ini menunjukkan bahwa penyedia layanan komputasi awan harus dapat membangun sistem yang dapat dikembangkan secara progresif dari waktu ke waktu. [2]

Re-enkripsi fungsional merupakan ekspresi umum dalam re-enkripsi. Mengubah teks *cipher* dengan "label" T dan PKa menjadi teks *cipher* dengan PK yang dideterminasi oleh F(T). Re-enkripsi fungsional diukur dengan menggunakan fungsi F:D=[n] (sebagai contoh, F memiliki domain D dan hasil output n) dipilih dalam kelas fungsi, kunci pk input publik, dan publik kunci output n. Fungsionalitas ini menerima teks *cipher* dengan m sebagai *message* dan id sebagai *identity* dalam kunci input publik pk. Dekripsi teks *cipher* menggunakan kunci rahasia sk untuk mengakses m dan id, lalu melakukan re-enkripsi m di bawah "*appropriate*" kunci *output* cpkF(id). Melalui proses ini, kita dapat mengasumsikan bahwa re-enkripsi fungsional merupakan deretan delegasi akses [2].

Desain keamanan dibawah keamanan re-enkripsi fumgsional adalah milik pasien (W). Perawat akan melakukan cek medis dan mengunggah data yang telah terenkripsi ke dalam tempat penyimpanan utama. [2][9].

Kasus 1: Ada dua pengguna, yakni pasien (W) dan dokter spesialis (P)

Pasien W memiliki PKa = ga dan SKA = a. Dokter memiliki PKB = gb dan SKB = b; Data dikirimkan ke dalam awan X = Enc (ga, M), di mana M merupakan data kosongan; Data diunduh dari awan Y = Enc (gb, M) di mana M merupakan data kosong. Data didekripsi di bawah PKB dan SKB. Re-enkripsi fungsional dari kunci ga ke kunci gb dapat dilakukan dengan kunci gb/a [2].

Kasus 2: Beberapa pengguna akan mengakses satu data pasien (W) dengan tujuan dan data yang berbeda. Beberapa data tidak ditujukan untuk pengguna yang memang tidak berhak.

Pasien W memiliki PKA = gai dan SKA = ai, ai di mana "i" adalah label nama untuk pengguna khusus yang memang diperbolehkan mengakses data. Asumsikan formula F (0) = F'(0) dan F (1) = F' (1), dan seterusnya. Lalu dokter spesialis P memiliki PK0 dan gb0 dan SK0 = b0, Perawat O memiliki PK1 = gb1 dan SK1 = b1, Apoteker T memiliki PK2 = GB2 dan SK2 = b2, Dokter Riset U memiliki PK3 = gb3 dan SK3 = b3, dan seterusnya. Data dikirimkan ke awan X = Enc (gai, M), di mana M merupakan data kosongan. Enkripsi data M dengan label i dan dengan kunci ga. Data diunduh dari awan Y = Enc (gb0(i), M), di mana M merupakan data kosongan, dan data didekripsi di bawah PKi = Ski [2].

Keunggulan dari Re-enkripsi Fungsional [2]:

1. Penggantian kunci: mengganti polis akses dengan sistem layanan komputasi awan yang terpercaya sangatlah krusial. Pasien hanya perlu untuk memberikan kunci re-enkripsi fungsional baru ke dalam layanan komputasi awan.
2. Data yang tercampur antara penerima dan layanan komputasi awan: Skema keamanan dapat ditelusuri jika terjadi kesalahan penerimaan data.

3. Penerima *offline*: penerima data tidak perlu untuk terlibat dalam fase pembentukan sistem. Nantinya mereka akan dapat menggunakan kunci milik mereka sendiri.

Skema input enkripsi adalah sebagai berikut [2]:

1. I-Gen (1^{λ},1^{d}): Ambil vektor acak a^1, …… ,a^d from Zq^d yang independen secara linear. Kita juga membuat crs, yaitu *common reference string* (disingkat CRS) untuk sistem NIZK. *Output* pk = (crs, g, g^{a1}, …… ,g^{ad}), dan sk = (a^1,….,a^d). Kunci publik pk dapat diisi dengan d kunci publik pk_i = (g,g^{ai}) dari skema yang lebih sederhana.
2. I-Enc(pk, I, ε, [d], m): untuk mengenkskripsi $m \varepsilon M$, dengan "identitas" i ε [d], pilih eksponen acak r dan r' dari Zq, dan komputasikan:
   - C = g^{rai} ; D = g^{r}m
   - C' = $g^{r'ai}$; D' = $g^{r'}$
   - π, bukti bahwa *value* terbentuk dengan baik, sebagai contoh, kode berkorespondensi dengan salah satu vektor g^{ai} yang ada dalam kunci publik.

   Output teks *cipher* (E, E', π) di mana E = (C, D) and E' = (C', D'). Selanjutnya, kita melihat bahwa E terlihat seperti sebuah enkripsi pesan m di bawah pk_i, sementara itu E' terlihat seperti enkripsi 1_G di bawah pk_i. E' biasa digunakan dalam re-enkripsi fungsional sebagai input pengacakan ulang, dan tidak dibutuhkan jika skema enkripsi digunakan secara tersendiri tanpa program re-enkripsi fungsional.
3. I-Dec (sk, (E, E')): jika ada komponen teks *cipher* E' 1_G atau jika pembuktian π tidak terverifikasi, output τ. Abaikan E' dan π, dan *parsing* E sebagai (C,D). Cek juga $i \varepsilon$ [d] dan $m \varepsilon M$, $D \cdot (C^{1/ai})^{-1} = (m, \ldots, m)$. Jika iya, output (*i*,*m*). [2]

Skema output enkripsi [2]:

1. O-Gen (1^{λ}): Pilih â Zq. set pk" = $h^{â}$ dan sk" = â.
2. O-Enc(pk", *m*): untuk enkripsi pesan $m \varepsilon M$ Ċ G,
   - Pilih angka acak r - Zq.
   - Komputasi $\hat{Y} = (h^{â})^r$ dan $\hat{W} = h^r$.
   - *Output* teks *cipher* sebagai [$\hat{S}$,$\hat{G}$] : = [e(g, $\hat{Y}$), e(g, $\hat{W}$) · e(*m*, *h*)]
3. O-Dec(sk" = â, ($\hat{S}$,$\hat{G}$)): algoritma dekripsi adalah sebagai berikut:
   - Komputasi $\hat{O} = \hat{G} \cdot \hat{S}^{-1/â}$
   - Untuk tiap $m \varepsilon M$, tes jika $e(m,h) = \hat{O}$. Jika iya, output *m* dan hentikan. (perhatikan jika *e(m,h)* telah terkomputasi sebelumnya dalam $m \varepsilon M$, maka langkah ini dapat diimplementasikan dalam tabel.) [2]

V. PENGEMBANGAN SISTEM

Beberapa hal yang perlu menjadi pertimbangan dan pengembangan ke depan berdasarkan pada:

- Dapatkah kebijakan akses diberikan untuk skala kecil dari kebijakan akses?
- Kebijakan akses arbiter: mungkinkah kebijakan akses arbiter dapat dibuat dan diakses?
- Ukuran huruf *cipher*: dapatkan kita menggunakan ukuran teks *cipher* yang lebih kecil?

Semua pertanyaan ini harus dipertimbangkan agar dapat meningkatkan kinerja dari sistem ini dalam mengamankan data. Proyek ke depannya adalah untuk mengimplementasikan sistem dan menggunakan komputasi arbiter *multi-party* secara aman ke dalam komputasi awan. Ada juga pertimbangan utnuk menambahkan kemungkinan fungsi arbiter. Eksekusi kode arbiter adalah sebuah kemampuan untuk mengeksekusi tugas komputasi. Lebih lanjut lagi, bagaimana setiap proses dapat dijalankan dalam layanan komputasi awan tanpa terjadi kebocoran data.

VI. KESIMPULAN

Desain sistem ini menyajikan keamanan data yang ditransmisi untuk kepentingan medis. Pendekatan formula re-enkripsi fungsional akan membantu *multiuser* untuk dapat menggunakan dan mempercayai rangkaian layanan komputasi awan, proses enkripsi dan dekripsi di bawah label yang dikumpulkan sebagai satu data. Metode ini akan membantu pengguna untuk mengakses dan mengontrol data medis

REFERENSI

[1] Seny, K. & Mariana, R. *Secure Outsourced Computation in a Multi-tenant Cloud*. Microsoft Research.

[2] Nishanth, C., Melissa, C. & Vinod, V. *Functional Re-encryption and Collusion-Resistant Obfuscation*. Microsoft Research.

[3] Chase, M. *Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records*. Joint work with Josh Benaloh, Kristin Lauter, and Eric Horvitz.

[4] Liu, W. (2012). *Research on Cloud Computing Security Problem and Strategy*. IEEE.

[5] Kulkarni, G., Gambhir, J., Patil, T. & Dongare, A. (2012). *A Security Aspects in Cloud Computing*. IEEE.

[6] Ramgovind, S., Eloff, & Smith, M.M. (2010). The Management of Security in Cloud Computing. *Information Security for South Asia (ISSA)*. pp. 1-7.

[7] Krishna, S. (2010). *Taking Medical Records into the Digital Age*. IBM DeveloperWorks.

[8] International Organization for Standardization (ISO). (2009). *ISO/IEC 27000 – Information Technology – Security Techniques – Information Security Management System – Overview and Vocabulary*. ISO/IEC 27000:2005(E). Diakses dari http://webstore. iec.ch/preview/info_isoiec27000%7Bed2.0%7Den.pdf pada Juni 2017.

[9] Josh, B., Melissa, C., Eric, H., Kristin, L. (2009). *Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records*. CCSW'09. USA.