IMPLEMENTASI SISTEM PERLINDUNGAN DAN PRIVASI KLIEN PADA LAYANAN APOTIK BERBASIS E-ID

Isbat Uzzin Nadhori[1)], Mike Yuliana[2)], Amang Sudarsono[2)]
[1]Departemen Teknik Informatika, Politeknik Elektronika Negeri Surabaya
[2]Departemen Teknik Elektro, Politeknik Elektronika Negeri Surabaya
Jl.Raya ITS Keputih, Surabaya,60111
Telp : (031) 5947280, Fax : (031) 5946114
E-mail : isbat@pens.ac.id[1)], mieke@pens.ac.id[2)], amang@pens.ac.id[2)]

Abstrak

Proteksi akan informasi yang sifatnya personal terhadap status kesehatan merupakan salah satu isu yang berhubungan dengan privasi seseorang atau masyarakat. Pada penelitian ini, akan dibahas tentang proteksi informasi-informasi yang bersifat sangat personal, privasi dan sensitif yang berkenaan dengan status kesehatan. Kami memperkenalkan sebuah desain berupa sebuah sistem apotik dengan berbasis e-ID menggunakan anonymous credential system. Sistem yang kami perkenalkan berfokus pada penebusan obat dan berbagai macam layanan apotik, yang dibangun dengan bahasa pemrograman Java. Hasil pengujian menunjukkan bahwa sistem yang dibuat telah mampu untuk melindungi data pribadi pasien, serta dokter. Rata-rata waktu komputasi untuk berbagai macam layanan apotik kurang dari 0.009 detik, sedangkan proses anonymous credential system kurang dari 1 detik.

Kata kunci: *apotik, e-ID, privacy, anonymous credential system.*

Abstract

Protection of information personal nature on health status is one of the issues relating to privacy of a person. In this research, it will be discussed the protection of personal information that is highly personal, and sensitive to privacy with regard to health status. We introduce a design in the form of system based pharmacies with e-ID using anonymous credential system. We focused on medicine redemption and other pharmacy services, which are built with the Java programming language. The experimental results showed that the system has been able protect the patient's and physician's personal data. The average computation time for a wide range of pharmacy services is less than 0.009 second, and anonymous credential system process less than 1 second.

Keywords: *pharmacy, e-ID, privacy, anonymous credential system.*

1. PENDAHULUAN

Saat ini teknologi *e–ID* telah berkembang pesat dan banyak diaplikasikan dalam kehidupan sehari – hari. Salah satu penerapan dari *e–ID* adalah Radio-Frequency Identification (*RFID)* yang mulai banyak digunakan dalam layanan *e-health* untuk berbagai kasus, diantaranya menawarkan peningkatan efisiensi dalam pendataan pasien, pemberian obat dengan teratur dan benar, serta untuk mengetahui lokasi pasien. E-ID pada dasarnya berisi informasi tentang atribut-atribut yang dimiliki oleh klien, misalnya nama, alamat, jenis kelamin, pekerjaan, tempat dan tanggal lahir, dan sebagainya. Informasi-informasi ini dalam kasus komersial adalah sangat penting dan dapat digunakan dalam sistem autentikasi berbasis atribut dari klien sebagai ganti dari proses identifikasi.

Salah satu isu serius dalam sistem-sistem e-ID yang ada saat ini adalah informasi yang berkaitan dengan privasi klien. Kebanyakan sistem e-ID yang ada membocorkan informasi yang bersifat privasi yang dimiliki oleh klien. Dengan begitu, *service provider* dengan leluasa memperoleh, mengkoleksi dan menyimpan semua informasi yang berkaitan dengan masing-masing klien pada saat klien mengakses layanan. Di samping itu, sebagian dari informasi-informasi tersebut sifatnya sangat privasi dan sensitif bagi klien (high privacy-sensitive) yang dengan mudah dapat dibocorkan oleh *service provider* ke pihak ketiga untuk tujuan bisnis/komersial. Salah satu solusi yang dapat digunakan untuk menanggulangi kebocoran informasi-informasi penting tersebut adalah *anonymous credential system* [1-2]. Anonymous credential system mengijinkan organisasi resmi yang dipercaya (*issuing authority*) untuk mengeluarkan sertifikat elektronik ke seorang klien. Sertifikat itu adalah sebuah bukti (*proof*) keanggotaan (*membership*) dan berisi informasi atribut-atribut yang dimiliki klien. Dengan sertifikat, klien dapat

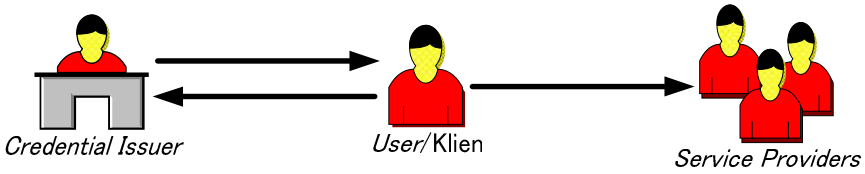
meyakinkan *verifier* atau *service provider* atas kepemilikan atribut tertentu tanpa harus memberikan informasi lainnya yang sifatnya privasi dan sensitif.

Sebagian besar literatur yang berhubungan dengan *e-health* menitikberatkan migrasi dari sistem layanan kesehatan konvensional (yaitu: pemakaian kertas) menjadi sistem layanan kesehatan berbasis TIK. Isu yang lain sebagai solusi dalam kasus ini, seperti kehandalan, kemudahan akses, ketersediaan layanan, integritas data, dan toleransi kesalahan [4][5][6]. Penelitian tentang RFID yang berhubungan dengan *e-health* juga telah dilakukan, namun masih menitikberatkan pada keberhasilan sistem yang dibuat [3]. Di lain pihak isu tentang privasi adalah sebuah solusi yang sangat tepat untuk mengatasi masalah ini. Misalnya,[2] memperkenalkan sebuah sistem *role-based access control* (RBAC) dan diaplikasikan dalam konteks layanan kesehatan. Sayangnya, [2] tidak memikirkan tentang proteksi privasi yang berdasarkan penggunaan teknik *public-key* tradisional dan pemakaian atribut, sertifikat belum mampu menyembunyikan identitas dan informasi lain yang sifatnya privasi.

Pada penelitian ini akan dibuat sebuah sistem aplikasi Electronic Health (*e-Health*) untuk menunjang pelayanan medis berbasis web, dengan studi kasus yang digunakan adalah sistem penebusan obat di Apotik. Sistem ini akan terintegrasi dengan database pada web server. Identitas elektronik pasien menggunakan *RFID,* dimana RFID tersebut berisi *signature/credential* pasien yang bersangkutan untuk mengakses daftar resep yang akan ditebus. Penggunaan *signature/credential* tersebut bertujuan untuk menyembunyikan identitas dari dokter dan pasien (*anonymous*), karena pemain yang terlibat dalam *e-health* hanya diperbolehkan untuk mengetahui informasi-informasi tertentu yang digunakan pada saat akses ke sistem dan bukan berupa informasi yang bersifat privasi seseorang (pasien, dokter, dan lain-lain). Dengan demikian, peneliti berharap akan membuka mata, memberikan wawasan, dan membuat komitmen keamanan terhadap sistem *e-health* di Indonesia sehingga *e-health* mendapat kepercayaan dari masyarakat.

2. ANONYMOUS CREDENTIAL SYSTEM

Pemain-pemain yang terlibat dalam *anonymous credential system* adalah: *issuer*, *recipient*, *prover* dan *verifier*. Pemain-pemain tersebut memiliki peran dalam menjalankan *issuing protocol*, dimana sebuah *credential* yang dibuat oleh *issuer* diberikan kepada *recipient*. Sedangkan pada *proving protocol*, pemegang *credential* menciptakan sebuah *proof* untuk meyakinkan *verifier* bahwa dirinya adalah klien yang *valid*. Seorang apoteker dapat berperan sebagai *verifier* dan menjalankan *proof protocol* dengan klien. Seorang klien memilih *master secret key (msk)* nya berdasarkan parameter-paramter *group* dari sistem. Klien menggunakan *msk* untuk mendapatkan *pseudonym* yang nantinya digunakan sebagai *session identifier* dalam proses komunikasi. Dan untuk memenuhi *anonymity*, klien menciptakan *pseudonym* baru setiap kali terjadi komunikasi, sehingga setiap *session* komunikasi tidak dapat di-*link* (*unlinkability*)[1][2][4][6].



Gambar 1. Anonymous Credential System

Gambar 1 memberikan ilustrasi tentang sistem *anonymous credential*. Sistem ini pada prinsipnya terdiri atas *user*/klien dan organisasi. Organisasi bisa bertindak sebagai *credential issuer* maupun sebagai *verifier* (misalnya *service provider*). Organisasi memiliki kemungkinan dapat berperan sebagai *issuer* dan *verifier* pada satu transaksi, misalnya ketika mengeluarkan sebuah *credential* dan pada saat memverifikasi *credential* yang lain. Pada sisi *user*/klien memiliki peran menggunakan *pseudonym* dan mendapatkan sebuah *credential* dari *issuer*, dan kemudian menunjukkan *credential* yang dimiliki ke organisasi yang lain untuk dilakukan verifikasi.

2.1 Skema *Signature* CL (Camenisch-Lysyanskaya)

Langkah-langkah dari skema *signature* Camenisch-Lysyanskaya adalah [4]:

Pembangkitan Kunci. Pada *input* l_n, pilih l_n bit modulo RSA n sehingga $n \leftarrow pq, p \leftarrow 2p' + 1, q \leftarrow 2q' + 1$ dimana p, q, p' dan q' adalah bilangan prima. Pilih secara acak, $R_0, \dots, R_{L-1}, S, Z \in QR_n$. Hasil yang didapatkan adalah kunci publik $(n, R_0, \dots, R_{L-1}, S, Z)$ dan kunci privat.

Message space. Parameter yang digunakan adalah parameter l_m. *Message space* adalah himpunan dari

$$\{(m_0, \dots, m_{L-1}) : m_i \in \pm\{0,1\}^{l_m}\} \quad (2)$$

Signing Algorithm. Pada *input* $m_0, \dots, m_{L-1}$, pilih bilangan prima e dimana $l_e > l_m + 2$, dan bilangan acak v dengan $l_v \leftarrow l_n + l_m + l_r$, dimana l_r adalah parameter keamanan. Hitung nilai A

$$A \leftarrow \left(\frac{Z}{R_0^{m_0} \ldots\ldots R_{L-1}^{m_{L-1}} S^v}\right)^{1/e} mod\ n \quad (3)$$

Signature dari pesan $(m_0, \ldots, m_{L-1})$ terdiri dari (A, e, v)

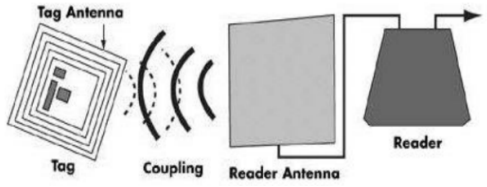
Verification Algorithm. Untuk melakukan verifikasi dari *signature* (A, e, v) dari pesan $(m_0, \ldots, m_{L-1})$, pastikan bahwa

$$Z \equiv A^e R_0^{m_0} \ldots R_{L-1}^{m_{L-1}} S^v (mod\ n) \quad (4)$$

dimana $m_i \in \pm\{0,1\}^{l_m}$, dan $2^{l_e} > e > 2^{l_e-1}$ semua terpenuhi.

3. RADIO-FREQUENCY IDENTIFICATION (RFID)

Pada sistem *RFID* umumnya, tag atau transponder ditempelkan pada suatu objek. Setiap tag dapat membawa informasi yang unik, di antaranya: serial number, model, warna, tempat perakitan, dan data lain dari objek tersebut. Gambar 2 menunjukkan, ketika tag ini melalui medan yang dihasilkan oleh pembaca *RFID* yang kompatibel, tag akan mentransmisikan informasi secara *LOS (Line of Sight)* yang ada pada tag kepada pembaca *RFID*, sehingga proses identifikasi objek dapat dilakukan.



Gambar 2. Hubungan antara tag, reader, dan antenna

RFID reader dihubungkan dengan PC melalui kabel serial DB9. Gambar 3. menunjukkan *output* data ASCII dari *RFID reader* yang dihasilkan dari pembacaan *RFID* tag menggunakan komunikasi serial.

☻041A21EE34E5
♥

02 (1byte)	10 ASCII Hex Data Characters (10bytes)	2 ASCII char's Checksum (2byte)	CR (1byte)	LF (1byte)	03 (1byte)

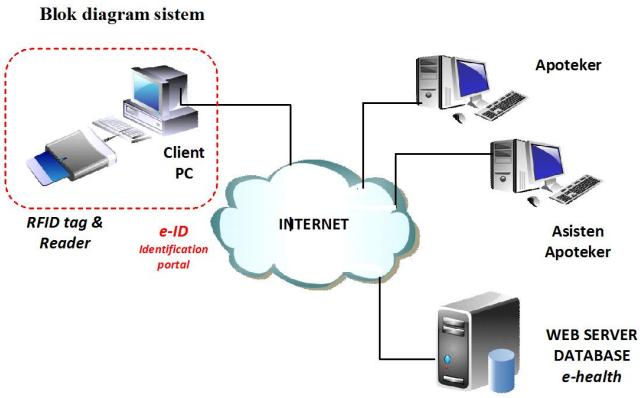
Gambar 3. Format paket data output RFID reader 16 bytes.

4. DESAIN SISTEM APOTIK

Sistem yang dibuat berusaha memaksimalkan perlindungan privasi identitas dari pasien dan dokter yang memberikan resep obat. Dikarenakan kondisi di lapangan, dimana dalam transaksi *e-health* banyak pemain yang harus dilibatkan, sehingga harus dipastikan setiap pemain yang terlibat dalam *e-health* hanya diperbolehkan mengetahui informasi-informasi tertentu yang digunakan pada saat akses ke sistem dan bukan berupa informasi yang bersifat privasi seseorang (pasien, dokter, dan lain-lain). Untuk mewujudkan tujuan seperti ini, kami mengadopsi teknik kontrol akses beserta aturan-aturannya, dan melakuakn pengeblokan terhadap akses yang sifatnya akan membocorkan data-data yang sangat privasi dan *sensitive*.

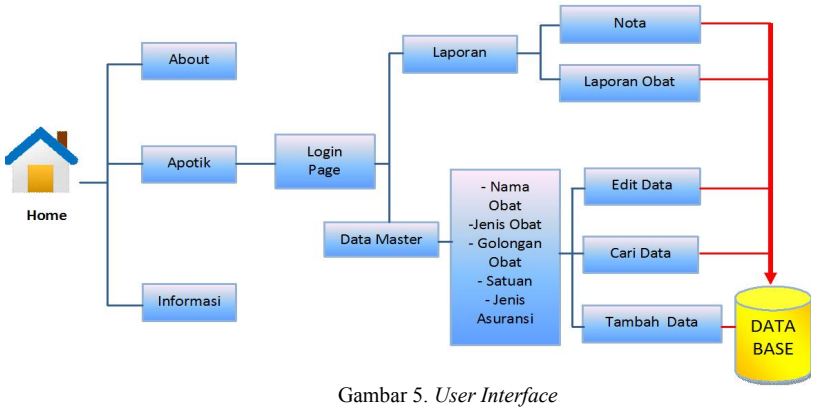
Pada Gambar 4 yang berkaitan dengan blok diagram sistem, dijelaskan bahwa pengguna dari sistem Apotik *e-health* adalah pasien dan petugas Apotik. Petugas Apotik merupakan pihak yang menjadi administrator sedangkan pasien merupakan *client*. Administrator memiliki kendali penuh untuk sistem ini, sedangkan *client* merupakan user biasa. Petugas Apotik terdiri dari staff Apoteker dan Asisten Apoteker. Asisten Apoteker bertugas untuk meracik obat, sedangkan Apoteker bertugas menerima resep dan memproses biaya yang akan dibayarkan oleh si pasien melalui aplikasi ini. Pada saat pasien menerima resep dari dokter, ia pergi ke Apotik untuk mendapatkan obat. Pasien menunjukkan kualifikasinya dengan menggunakan e-ID. Data dari e-ID pasien akan diolah oleh Apoteker untuk mengetahui daftar resep valid serta status sosialnya melalui jaringan internet yang terkoneksi ke database e-health. Kemudian Asisten Apoteker akan meracik obat yang dibutuhkan, lalu list obat yang telah diracik tersebut diserahkan kembali ke Apoteker yang akan mengkalkulasi total biaya dari pasien menurut bantuan kesehatan yang dimiliki serta pertimbangan status sosialnya. Dan terakhir obat akan diterima oleh pasien.

Pada saat penebusan obat baik apoteker maupun pasien harus menggunakan e-id untuk memverifikasi kevalidan resep, demikian juga pada saat persetujuan obat yang akan dibeli sebelum proses pembayaran. E-ID berisi data *signature/credential* yang dibangkitkan dari *hiding identity* pasien, dokter dan apoteker.



Gambar 4. Blok diagram sistem

Gambar 5 menunjukkan *user interface* dari sistem yang dibuat. Halaman web terdiri dari 3 link menu, yakni informasi, Apotik, dan *About*. Menu informasi berisi info seputar dunia kesehatan terkini, seperti informasi perkembangan teknologi dunia medis, gejala suatu penyakit, tips menjaga pola hidup sehat, dll. Link kedua adalah menu Apotik, menu ini merupakan menu utama untuk mengakses dan mengolah data yang berada pada database *e-health,* untuk *account administrator* dapat melakukan *login* dengan *username* dan *password*. Sedangkan *user* / pasien hanya dapat *login* menggunakan *RFID tag*(*Smart Card*). Dan link ketiga adalah menu *About*, menu ini berisi informasi seputar aplikasi seperti, nama aplikasi, fitur, petunjuk penggunaan serta *Frequently Asked Questions (FAQ)* untuk lebih memudahkan pengguna dalam menggunakan aplikasi ini.



Gambar 5. *User Interface*

5. IMPLEMENTASI DAN ANALISA SISTEM

Pada bagian ini, akan dilakukan implementasi dan pengujian dari desain sistem yang telah dibuat. Pengujian sistem dilakukan pada PC dengan spesifikasi pada Tabel 1, sedangkan format dari *reader* RFID yang digunakan bisa dilihat pada Tabel 2. Pada waktu proses registrasi di rumah sakit, pasien diminta untuk memasukkan data pribadi seperti nama, alamat, tempat/tanggal lahir serta beberapa data pribadi lainnya. Proses registrasi yang dilakukan, akan menghasilkan *cryptographic* data pribadi yang dikenal dengan nama *credential/signature*. Gambar 6 menunjukkan contoh *credential/signature*, dimana *signature* tersebut akan dimasukkan pada *smart card* berbasis rfid atau lebih dikenal dengan nama e-id. Hal yang sama juga dilakukan oleh apoteker untuk mendapatkan *smart card*. *Smart card* yang telah diterima oleh pasien dan apoteker akan digunakan pada proses penebusan resep.

Tabel 1. Spesifikasi dari PC

Spesifikasi	Keterangan
Software	java
O/S	Windows 8 (64 bit)
CPU	Intel Core™ i5-3317U Processor (1.70 GHz)

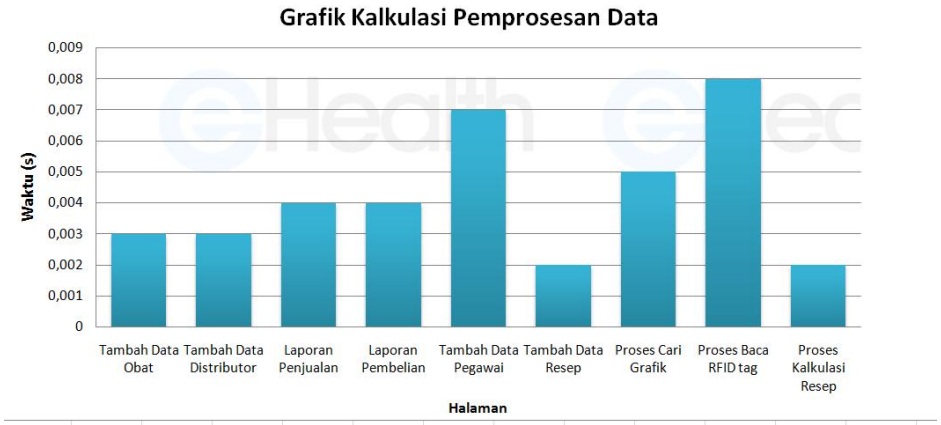
Tabel 2. Spesifikasi dari *Reader* RFID

Spesifikasi	Keterangan
Type	EM9918
Frekuensi	125 KHz
Format	EM4100,
Kartu	GK4001/4011,T5557(format EM)
Baud Rate	9600
Interface	Serial UART RS232
Supply	9-12 V DC

Gambar 6. Contoh *credential/signature*

Gambar 7. List Resep

Gambar 7 menunjukkan list resep, dimana list ini bisa dilihat jika autentikasi pasien dan apoteker dengan menggunakan e-id berhasil. Untuk mencetak nota pembayaran, harus mendapatkan persetujuan dari pasien dengan menggunakan e-id. Hal ini menunjukkan bahwa, sistem yang dibuat telah melindungi data pribadi dari pasien dan dokter karena tidak ada tampilan informasi data pribadi seperti nama dokter, nama pasien, umur pasien serta alamat pasien. Beberapa kemungkinan yang mungkin terjadi, jika data tersebut diketahui adalah terjadi kecurangan antara apoteker dan dokter serta digunakannya data pribadi pasien untuk keperluan pihak yang tidak bertanggung jawab misalnya sales produk tertentu.



Gambar 8. Grafik kalkulasi Pemrosesan Data

Gambar 8 menunjukkan grafik kalkulasi pemrosesan data, dimana terlihat bahwa proses pembacaan RFID tag membutuhkan waktu paling lama yaitu 0.008 detik, hal ini terjadi karena adanya proses transfer data dari RFID *reader* ke PC. Sedangkan Tabel 3 menunjukkan bahwa proses pembangkitan kunci membutuhkan waktu yang paling lama yaitu 4.2 detik, hal ini terjadi karena pada proses ini terjadi pembangkitan modulus RSA. Pembangkitan kunci publik membutuhkan waktu yang lebih lama, karena komponen/elemen yang dibangkitkan lebih banyak bila dibandingkan dengan kunci privat.

Tabel 3. Performansi Anonymous Credential Process

No	Proses	Waktu(s)
1	Pembangkitan kunci	4.2
	Kunci privat	2
	Kunci publik	2.2
2	Issuing credential/signature	0.2
3	Proving credential/signature	0.5

6. SIMPULAN DAN SARAN

6.1 Simpulan

Pada penelitian ini telah disajikan sistem perlindungan dan privasi klien pada layanan apotik yang berbasis e-id menggunakan *anonymous credential system.* Dari hasil pengujian terlihat bahwa waktu yang dibutuhkan untuk kalkulasi pemrosesan data membutuhkan waktu yang cepat, karena rata-rata waktu yang dibutuhkan kurang dari

1 detik. Demikian juga untuk proses *anonymous credential system*, rata-rata waktu yang dibuthkan dibawah 1 detik kecuali pada saat proses pembangkitan kunci yang membutuhkan waktu 4.2 detik

6.2 Saran

Penelitian yang telah dibuat ini, belum menambahkan sistem untuk *update credential*. Sistem ini sangat dibutuhkan karena informasi dari klien pada rentang waktu tertentu ada kemungkinan mengalami perubahan atau penambahan.

7. DAFTAR RUJUKAN

[1] B.Kellermann and I.Scholz, 2010. "Anonymous Credentials in Web Applications : A child's Play with a Prrime Core", Proceedings of IFIP AICT, pp 237-245.

[2] Y.yang, R. H. Deng, F. Bao, 2009. "Privacy-Preserving Rental services using One Show Anonymous Credential System", Security and Communication Networks, Vol 2, Issue 6. Pages 531-545.

[3] Kou-Hui Yeh, Nai-Wei Lo, Tzong-Chen Wu, and Chieh Wang, 2013. "Secure E-Health System on Passive RFID : Outpatient Clinic and Emergency Care", International Journal of Distributed Sensor Networks, Article ID 752412.

[4] R. Krummenacher, E. P. B. Simperl, L. J. B. Nixon, D. Cerizza, and E. Della Valle. 2007. "Enabling the european patient summary through triplespaces", In CBMS, pages 319–324. IEEE Computer Society.

[5] G. L. Kreps and L. Neuhauser, 2010. "New directions in eHealth communication: opportunities and challenges," Patient Education and Counseling, vol. 78, no. 3, pp. 329–336.

[6] L.Guo, C. Zhang, J.Sun, Y.Fang, 2012. "A Privacy-Preserving Attribute-Based Authentication System for eHealth Networks", Proceeding of ICDCS, pp 224-233.