TINJAUAN DAN APLIKASI MEKANISME PENGAMANAN PADA STANDAR HEALTH LEVEL 7

Nugroho Budi Wicaksono

Dosen Program Studi D3 Instrumentasi Medis, Politeknik Mekatronika Sanata Dharma
Alamat korespondensi: Kampus Paingan Maguwoharjo Depok Sleman Yogyakarta 55282.
Email: *nugroho@pmsd.ac.id*

ABSTRACT

Health Level 7 (HL7) is not an application or a software, it is like a dictionary or an encyclopedia which contains a set of syntaxes that is used for a programmer and analyst. This set of rules is used to facilitate information exchange between two or more systems. In healthcare community, HL7 has been applied for home monitoring system and wireless body area network. Chameleon software is implemented in home monitoring system. Chameleon uses Advanced Encryption Standard (AES) as an encryption algorithm.

In recent development of information and communication technology around e-health, medical records, and security. Those topics will have an impacts for the future in healthcare services scenarios. Some of this scenarios is focused on Wireless Body Area Network (WBAN), this technology is supported by the advancement of low-power wireless technology, low-power microcontroller system, plug and play device buses, handheld computer and also an electronics medical records. The implementation HL7 in WBAN system also using a chameleon to facilitate the data transfer security.

Keywords: *health level 7, information security, home monitoring system, wireless body area network*

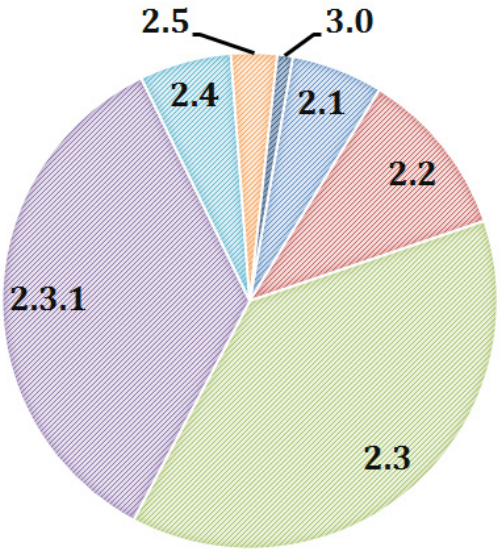
1. PENDAHULUAN

Health Level 7 (HL7) dapat dianalogikan seperti semboyan Indonesia, *Bhinneka Tunggal Ika*. Walaupun Indonesia memiliki beragam suku bangsa, bahasa, dan budaya, tetapi pada hakikatnya adalah satu. Salah satu contohnya adalah bahasa, tanpa adanya bahasa Indonesia, orang dari suku Jawa akan sulit berkomunikasi dengan orang dari suku Dayak, atau dari suku lainnya. Komunikasi dapat terjadi jika menggunakan Bahasa Indonesia sebagai bahasa persatuan.

Secara umum, HL7 merupakan standar yang digunakan untuk aplikasi klinis dalam menyampaikan sebuah pesan. Sebagian orang memiliki pandangan bahwa Sistem Informasi Rumah Sakit (*Health Information System*/HIS), Sistem Informasi Radiologi *(Radiology Information System*/RIS), Sistem Informasi Laboratorium (*Laboratory Information System*/LIS), dan Rekam Medis Elektronik (*Electronic Medical Record*/EMR) dapat berkomunikasi dan bertukar data secara langsung mengenai data-data pasien. Premis ini dapat dianggap benar jika kelima sistem tersebut menggunakan vendor perangkat lunak yang sama, dan vendor tersebut memang merancang sistemnya dapat saling terintegrasi, serta hanya dilakukan di satu Rumah Sakit. Jika data pasien harus dikirimkan antar-Rumah Sakit, maka premis tersebut dapat dianggap salah karena setiap Rumah Sakit memiliki kebutuhan dan manajemen yang berbeda.

HL7 merupakan organisasi pengembang standar (*Standard Developing Organization*) yang terakreditasi oleh *American National Standard Institute* (ANSI) (Shaver, 2007). Angka 7 pada HL7 melambangkan layer ke-7 dari 7 layer model komunikasi ISO, yaitu layer aplikasi. Layer aplikasi digunakan untuk menyediakan layanan yang terhubung dengan perangkat lunak. Komite HL7 telah merumuskan standar sejumlah format pesan yang berhubungan dengan standar klinis. Format pesan ini dapat dianggap sebagai representasi ideal untuk informasi klinis. Standar ini kemudian yang digunakan sebagai *framework* pertukaran data. HL7 bukan merupakan aplikasi perangkat lunak, tetapi merupakan 'buku aturan' yang berisi kumpulan *syntax* yang digunakan *programmer* dan analis agar sistem yang dibuat dapat melakukan pertukaran informasi dengan mudah.

HL7 dibentuk pada tahun 1987 yang berkolaborasi dengan komunitas internasional yang ahli pada bidang kesehatan dan beberapa ahli dalam bidang informasi. Sampai saat ini sudah ada beberapa standar spesifik yang juga masih terus dikembangkan: HL7 versi 2.X dan HL7 versi 3.0. Pada tahun 2010, perbandingan implementasi HL7 versi 2.X dengan HL7 versi 3.0 ditunjukkan pada Gambar 1. Sejumlah lembaga kesehatan di Eropa, Kanada, dan German juga telah berinisiatif untuk mengimplimentasikan HL7 versi 3.0.



Gambar 1. Perbandingan Penggunaan Standar HL7 Versi 2.X dengan HL7 Versi 3.0 (Carepoint, 2010)

2. DASAR TEORI

2.1 Keamanan Informasi dan Privasi pada HL7

Perkembangan pada jaringan komunikasi dipengaruhi oleh penggunaan internet dan penggunaan perangkat lunak (Blobel, 1999). Dengan adanya perkembangan tersebut, implikasi yang harus disadari adalah adanya risiko keamanan yang harus diperhatikan dalam penggunaan komunikasi berbasis TCP/IP. Fasilitas internet dapat digunakan dengan aman jika tindakan pencegahan telah dilakukan. Kerahasian atas suatu data dapat dikatakan aman jika telah dilakukan suatu tindakan pengaman. Misalnya: dalam penggunaan email, verifikasi data *username* dan *password* dikirimkan dalam bentuk *plain text* pada jaringan publik. Jika data tersebut disadap oleh penyerang, penyerang akan mendapatkan data tersebut. Risiko keamanan ini dapat dicegah dengan menggunakan kriptografi. Dari contoh tersebut, enkripsi dan menambahkan *digital signature* pada pesan HL7 sangat penting dilakukan sebagai antisipasi dalam skenario penyerangan. Dua metode tersebut dapat dikombinasikan dengan menambahkan *firewall.*

2.2. Ancaman dan Layanan Keamanan

Model ancaman pada pesan HL7 terdiri dari setidaknya dua pelaku yang memiliki kewenangan dalam melakukan transmisi (mengirim dan menerima) pesan dengan menggunakan protokol komunikasi dan infrastruktur tertentu. Ancaman ini terjadi jika penyerang melakukan interaksi yang menyebabkan kerentanan sistem. Ancaman, risiko, dan kerentanan sistem dapat dihindari jika persyaratan keamanan telah dilakukan. Beberapa model ancaman dan layanan keamanan ditunjukkan pada Tabel 1.

Tabel 1: Ancaman dan Layanan Keamanan (Blobel, 1999)

Ancaman	Layanan Keamanan
Penyamaran (penggunaan layanan secara illegal)	Identifikasi dan Autentifikasi
Manipulasi data	Integritas
Pengungkapan data (*disclosure of data*)	Kerahasian (*Confidentiality*)

2.3. Layanan Keamanan dan Mekanisme Pengamanan

Layanan keamanan didefinisikan sebagai jembatan antara persyaratan keamanan dan tujuan yang tercantum pada kebijakan keamanan, sedangkan manajemen dan mekanisme pengamanan digunakan untuk memenuhi persyaratan keamanan tersebut. Layanan keamanan dapat diimplementasikan dengan satu atau beberapa macam mekanisme pengamanan (perbandingan antara layanan pengamanan dengan mekanisme pengamanan adalah 1:n) (Blobel, 1999). Jumlah metode pengamanan yang dibutuhkan tergantung pada tingkat keamanan yang dibutuhkan dan spesifikasi aplikasi sistem yang digunakan. Untuk sistem informasi kesehatan, layanan keamanan dapat diklasifikasikan menjadi 2 bagian: layanan internal dan eksternal. Layanan keamanan internal merupakan fungsi keamanan yang dilakukan dengan mengkomunikasikan dan menggabungkan sistem informasi agar tersedianya keamanan komunikasi. Sedangkan, layanan keamanan eksternal merupakan fungsi keamanan yang disediakan oleh pihak ketiga (*Trusted Third Parties*), contohnya: *key management*, layanan registrasi, *naming services*, *certification services, directory services, secure time services, authorisation, access control,* integritas dan kerahasiaan data, pertanggungjawaban data dan prosedur, dan audit. Layanan keamanan eksternal tidak dibahas pada subbab ini. Tabel 2 merupakan contoh layanan keamanan internal yang ditawarkan oleh HL7 dalam menyediakan komunikasi yang aman. HL7 hanya menentukan *syntax* dan struktur dari suatu pesan, sehingga infrastruktur teknis (seperti: jaringan) tidak dibahas pada subbab ini.

Implementasi mekanisme pengamanan dengan spesifikasi dan algoritma tertentu tergantung pada *state of the art*, perkembangan teknologi, dan adanya penyerang. Implementasi ini merupakan sebuah prosedur yang dinamis. Terlebih lagi, dengan adanya internet mengakibatkan munculnya kemungkinan terjadinya penyerangan semakin meningkat. Dengan demikian, kebutuhan untuk mengimplementasikan mekanisme pengamanan harus dilakukan secara tepat, misalnya dengan menerapkan algoritma kriptografi pada perangkat lunak. Selain itu, perlu dibedakan antara tingkat layanan keamanan dan realisasinya seperti yang ditunjukkan pada Tabel 3.

Tabel 2: Layanan Keamanan dan Mekanisme Pengamanan

Layanan Keamanan	Mekanisme Pengamanan	
	Asimetris	Simetris
Identifikasi dan autentifikasi	*Digital Signature*, *Time Variant Parameters* (TVP)	Enkripsi, *cryptographic check value* (*Message Authentication Code*/MAC), TVP
Autentifikasi data asli	*Digital Signature, cryptographic check value*, DN (*Distinguished Name*)	Enkripsi, *cryptographic check value* (MAC), DN
Integritas	*Digital Signature, cryptographic check value*	Enkripsi, *cryptographic check value* (MAC)
Kerahasiaan (*Confidentiality*)		Enkripsi
Accountability	Audit Keamanan (dengan menggunakan laporan, *log files*, *receipts*, *time stamps* dan DN)	

Tabel 3: Realisasi pada Beberapa Tingkat Layanan Keamanan

Tingkat Layanan Keamanan	Realisasi
Aplikasi	SFTP, PEM, PGP, SHTTP, ...
Layanan	Identifikasi dan autentifikasi, integritas, ...
Mekanisme	*Digital Signature*, Enkripsi, *Check Values*, ...
Prosedur	*Security proxy* atau *security toolkits with libraries*
Cryptographic Syntax	PKCS#7, S/MIME, PGP/MIME, CMS, ...
Algoritma	DES, RSA, IDEA, MD5, RIPEMD, SHA-1, ...
Metode Teknis	Tokens (*Smart Card, Key disk*), *Software-based* PSE, ...
Perangkat Lunak dan Keras	*Directory server, Certificate server, CRL server, ...*

3. IMPLEMENTASI HL7

Berikut ini dipaparkan 2 contoh implementasi HL7 yang terkait dengan bidang Teknik Biomedika, terutama bidang *e-Health*. Dua contoh implementasi ini dikembangkan oleh Kansas State University (KSU) (Lebak, 2004) dan Kansas State University yang bekerja sama dengan University of Alabama (UA) (Warren, 2005).

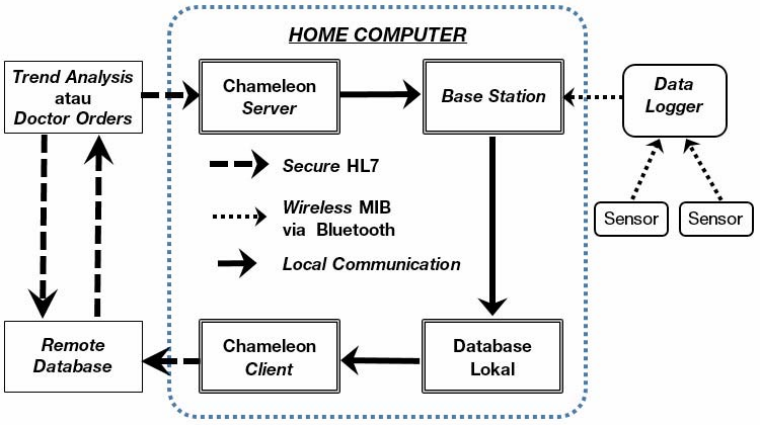
3.1 Implementasi HL7 pada *Home Monitoring System*

Dengan adanya perkembangan alat diagnostik yang dapat digunakan di rumah, sejumlah besar data pasien dapat langsung diperoleh dari rumah pasien. Di negara maju, alat diagnostik ini biasanya terhubung langsung dengan Rumah Sakit. Sistem pemantauan kesehatan pasien semacam ini disebut sebagai *home monitoring system*. Dalam memantau data pasien yang ada di rumah, dokter membutuhkan akses komunikasi yang aman dan akses dengan standar tertentu agar diagnosis bagi pasien dapat ditegakkan. Pertukaran data dari rumah pasien ke rumah sakit atau dari Rumah Sakit satu ke Rumah Sakit lain dapat direalisasikan dengan adanya standar HL7. Penelitian yang dilakukan Lebak dan Yao (Lebak, 2004) ini bertujuan untuk mengemukakan sebuah metode yang aman dalam mengimplementasikan HL7 sebagai sarana komunikasi antara rumah pasien dengan database yang ada di Rumah Sakit.

Blok diagram dari metode yang digunakan oleh Lebak dan Yao ditunjukkan pada Gambar 2. Blok diagram tersebut menunjukkan komunikasi antara *remote database* dengan komputer yang ada di rumah pasien. Data pertama-tama dikumpulkan oleh sensor yang terletak pada tubuh pasien atau sensor yang berada di dekat pasien. Data ini kemudian diunggah secara nirkabel ke sebuah *data logger* yang ada di tubuh pasien. Standar transmisi yang digunakan adalah Bluetooth. Interaksi antarsensor dikontrol dengan menggunakan standar *Medical Information Bus* (MIB/IEEE 1073). Data yang terkumpul di *data logger* kemudian dikirimkan ke *base station* dalam jangka waktu tertentu. Data dari *data logger* tersebut diterima oleh program LabVIEW yang ada di *base station.* Hasil pembacaan data pasien disimpan LabVIEW pada *database* lokal.

HL7 digunakan untuk mengirimkan data dari database lokal ke *remote database.* Perangkat lunak dari Interfaceware: Chameleon digunakan untuk mengatur layanan pesan HL7. Jika data pasien sampai pada database Rumah Sakit, dokter dan perawat dapat mengambil data tersebut dengan menggunakan koneksi yang sama. Setelah mengamati data pasien, dokter kemudian dapat mengambil tindakan dengan mengirimkan pesan ke rumah pasien. Dengan mengirimkan format pesan HL7 ini, dokter tidak hanya bisa memantau kesehatan pasien dari jarak jauh, tetapi juga bisa mengubah parameter *monitoring* seperti frekuensi sampling dan memodifikasi dosis obat pasien. Sistem *monitoring* ini akan mengubah pandangan tentang *home monitoring*, dari pemantauan pasif menjadi pemantauan aktif. Hal ini akan memberikan terobosan perawatan yang lebih efektif bagi pasien.

Setelah mengamati data pasien, dokter kemudian dapat mengirimkan perintah dalam pesan HL7 ke sistem pemantauan rumah. Dengan cara ini, dokter tidak hanya bisa memantau kesehatan rumah dari jarak jauh, tetapi juga mengubah parameter pemantauan seperti frekuensi sampling atau memodifikasi dosis obat. Sistem ini akan berubah dari monitor pasif ke monitor aktif dengan fleksibilitas yang



Gambar 2. Blok Diagram HIS untuk *Home Monitoring*

lebih besar dan akan memberikan perawatan yang lebih efektif.

3.1.1 HL7 Communication Tool: Chameleon

Para pengembang perangkat lunak yang telah berusaha mengimplementasikan HL7 mengetahui bahwa adanya kesulitan yang sangat besar dalam mengembangkan perangkat lunak yang sesuai dengan keinginan pelanggan. Apalagi integrasi sistem HL7 dalam skala besar, yang menghubungkan beberapa Rumah Sakit, laboratorium, klinik, dan/atau apotek, harus dapat menjamin keamanan data dan privasi pasien. Hal ini diperparah dengan adanya beberapa versi HL7 (versi 2.X - versi 3.0).

Permasalahan ini justru menjadi semakin besar jika diimplementasikan pada *home monitoring system*. Dengan segala kompleksitas *syntax* pesan HL7, tidak dimungkinkan standar HL7 diimplementasikan pada *home monitoring system*. Untuk pengembangan skala besar, Rumah Sakit memiliki tim yang didedikasikan untuk mengimplementasikan HL7 pada sistem yang ada. Tetapi untuk skala kecil/rumahan, tidak ada tim yang mengurusi hal semacam itu. Oleh karena itu, sistem HL7 untuk skala kecil, dibutuhkan sebuah sistem yang murah dan handal, dan Chameleon menawarkan solusi tersebut. Chameleon merupakan aplikasi berbasis HL7 yang cukup fleksibel dan tidak begitu rumit. Para pengembang perangkat lunak dapat menggunakan Chameleon dengan menggunakan Java, C++, Visual Basic, dan beberapa bahasa lainnya. Untuk menjamin keamanan data, Chameleon meyediakan fitur enkripsi sebelum data dikirimkan.

3.1.2 Enkripsi pada Chameleon

Algoritma enkripsi yang digunakan pada Chameleon (sekarang: Iguana - iNTERFACEWARE) adalah algoritma *Advanced Encryption Standard* (AES) (Texas Instruments, 2004). Algoritma ini juga dikenal sebagai algoritma *Rinjdael* yang dinamakan sesuai dengan nama penemunya: Dr. Vincent Rijmen dan Dr. Joan Daemen. *Rijndael* termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan *cipher block*. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu.

Rijndael mendukung panjang kunci 128 bit sampai 256 bit dengan step 32 bit. Panjang kunci dan ukuran blok dapat dipilih secara independen. Setiap blok dienkripsi dalam sejumlah putaran tertentu. Karena AES menetapkan panjang kunci adalah 128, 192, dan 256, maka dikenal AES-128, AES-192, dan AES-256. Perbandingan panjang kunci, panjang blok dan jumlah putaran pada algoritma enkripsi AES ditunjukkan pada Tabel 4.

Tabel 4: Perbandingan AES 128, 192, dan AES 256

	Panjang Kunci	Ukuran Blok	Jumlah Putaran
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Algoritma ini masih memungkinkan untuk diretas, tetapi dengan tingkat kemungkinkan waktu peretasan > $5x10^{18}$ tahun. Kemungkinan ini dapat tercapai jika sebuah komputer dapat 10^6 kemungkinan kunci setiap 1 milidetik.

3.1.3 Hasil Implementasi HL7 pada Home Monitoring System

Implementasi yang dilakukan oleh Lebak dan Yao membutuhkan pengembangan yang lebih lanjut pada bagian *database*. Subsistem sensor dari prototipe sistem *home monitoring system* ini sudah dapat berhasil mengambil data sinyal fisiologis pasien. Pengembangan lain yang dibutuhkan adalah pengujian pesan HL7 dan penambahan fitur pemantauan aktif pesan pada jalur komunikasi MIB dan HL7. Untuk mekanisme pengamanan pesan HL7 masih dibutuhkan penelitian yang lebih lanjut agar aplikasi yang dibuat dapat diimplementasikan secara klinis. Mekanisme pengamanan hanya mengandalkan enkripsi dari Chameleon.

3.2 Implementasi HL7 pada Wireless Body Area Network

Topik yang berkembang seputar penerapan teknologi pada bidang kesehatan beberapa di antaranya adalah *telemedicine*, diagnosis secara prediktif, dan rekam medik secara elektronik. Topik-

topik tersebut merupakan bagian dari skenario mekanisme perawatan yang digunakan di masa depan. Salah satu fokus yang disampaikan Steve Warren *et al.* pada (Warren, 2005) adalah menggabungkan *telemonitoring* dengan *Wireless Body Area Network* (WBAN). Sistem ini didukung dengan adanya perkembangan teknologi nirkabel berdaya rendah, peralatan berbasis *plug-and-play*, kit mikrokontroler berdaya rendah, *handheld computer*, EMR dan internet. Dengan adanya beberapa dukungan ini, maka model perawatan yang lebih berorientasi pada pasien dapat direalisasikan.

3.2.1 WBAN: Fungsi, Interoperabilitas, dan Keamanan

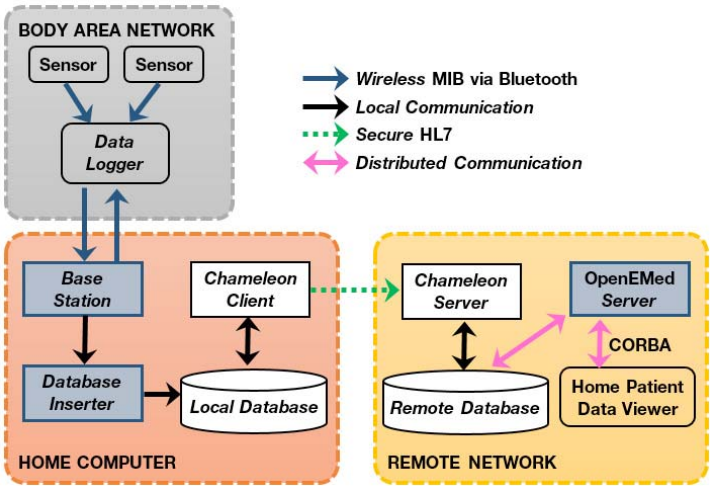
Penerapan WBAN sendiri dihadapkan pada beberapa tantangan. Karakteristik sensor yang digunakan harus spesifik, seperti: daya yang dibutuhkan dan memori penyimpanan yang disediakan, kemampuan penanganan data secara *real-time*, dan membutuhkan *personal server*. *Personal server* ini juga harus memenuhi kriteria untuk dalam menyimpan data sensor dalam satuan jam dan memeiliki kemampuan mengunggah data secara nirkabel ke Rumah Sakit dengan menggunakan internet. Saat data sudah ada di Rumah Sakit, dokter dapat melihat parameter fisiologis pasien, dan menentukan algoritma penanganan kesehatan pasien.

WBAN juga harus memenuhi persyaratan dapat dirakit dan dikonfigurasikan oleh pasien itu sendiri. Skenario rekonfigurasi ulang oleh pasien yang dibutuhkan adalah kemudahan dalam perakitan dan pembongkaran (dalam kondisi mandi, sensor harus dilepaskan), pelepasan sensor (penggantian baterai), penambahan sensor (penambahan sensor *pulse oximeter* untuk memantau kadar oksigen saat tidur), dan memodifikasi mode-operasi sensor (misal: sensor diperintahkan untuk mengirimkan data asli/*raw data*, tidak data yang sudah diolah).

Sistem WBAN termasuk dalam sistem yang terdistribusi secara geografis, tantangan selanjutnya yang dihadapi adalah integritas data, dan sistem keamanan. Pengamanan data pasien dan privasi pasien membutuhkan integritas layanan yang dapat:

1) memverifikasi identitas pasien (autentifikasi),
2) melindungi kerahasiaan pasien,
3) menjamin adanya komunikasi yang aman antar-sensor,
4) menjaga integritas data akuisisi sensor dari awal sensor digunakan sampai pada *remote database*, dan
5) melindungi data yang sudah tersimpan atau data yang akan dikirimkan.

dengan memperhatikan tantangan yang disebutkan sebelumnya, dibutuhkan mekanisme pengamanan dengan mengirimkan data yang telah terenkripsi. Salah satu keuntungan dalam sistem WBAN adalah komunikasi yang digunakan hanya pada jarak yang pendek. Diagram blok dari sistem WBAN yang digunakan ditunjukkan pada Gambar 3. Pada subsistem *Body Area Network*, komunikasi nirkabel via Bluetooth terintegrasi dengan sistem enkripsi pada level perangkat keras yang terletak pada *data logger*. Pengumpulan data pada *base station* menggunakan program LabVIEW, agar data pasien dapat dikirimkan dengan format pesan HL7 ditambahkan program berbasis Java sebagai *database inserter*. Transmisi dari subsistem *home computer* ke *remote network* menggunakan aplikasi yang sudah mendukung format pesan HL7: Chameleon.



Gambar 3. Interaksi Sistem/*Database* Via HL7

3.2.2 Hasil Implementasi HL7 pada WBAN

Implementasi HL7 pada WBAN yang dikembangkan oleh KSU dan UA menunjukkan bahwa sistem yang dikembangkan sudah layak diterapkan pada HL7 dengan infrastruktur WBAN. Sampai pada tahun 2005, HL7 belum banyak diimplementasikan untuk sistem WBAN. Sistem yang dikembangkan juga sudah mengimplementasikan enkripsi pada level perangkat keras (ChipCon CC2420 128-bit *encryption key*) dan juga enkripsi oleh Chameleon. Implementasi sub-sistem perangkat keras yang dilakukan oleh KSU dan UA menggunakan modul ZigBee, modul pengondisi sinyal, dan platform perangkat lunak TinyOS. Untuk lebih memperketat pengamanan pada implementasi HL pada WBAN, dapat ditambahkan fitur autentifikasi pasien. Beberapa contoh alat yang dapat digunakan untuk autentifikasi pasien: *scanner* sidik jari sudah tersedia pada *handheld computer*, *smart card*, bar code, RFID tag, dan kartu magnetik.

3.2.3 ChipCon CC2420

ChipCon CC2420 merupakan chip *transceiver* 2,4 GHz yang diproduksi oleh Texas Instruments (Gambar 4). Chip ini didesain untuk aplikasi nirkabel berdaya rendah dengan penguatan sebesar 9 dB dan *data rate* sekitar 250 kbps. CC2420 juga menyediakan fitur berupa: *packet handling, data buffering, burst transmissions, data encryption, data authentication, clear channel assessment, link quality indication* dan *packet timing information* (Karlof, 2004). Jika menggunakan fitur-fitur tersebut, maka beban yang dibutuhkan oleh *host controller* juga semakin berkurang.

Gambar 4. Chip ChipCon CC2420
dari Texas Instruments (Karlof, 2004)

CC2420 menggunakan standar IEEE 802.15.4 MAC *security operations*. Standar ini meliputi enksripsi/dekripsi dengan moder counter mode (CTR), autentifikasi CBC-MAC dan enkripsi - autentifikasi CCM. Semua mode pengamanan menggunakan enkripsi AES 128 bit. CC2420 juga menyediakan enkripsi AES 128 bit secara *stand-alone* yang mengenkripsi 128 bit *plaintext* menjadi 128 bit *chipertext.*

CC2420 digunakan oleh University of Alabama untuk diimplementasikan pada HL7 WBAN karena sistem operasi yang digunakan oleh UA adalah TinyOS, dan CC2420 merupakan salah satu perangkat keras *transceiver* yang didukung oleh TinyOS (TinyOS, 2013).

3.2.4 TinyOS dan TinySec

TinyOS merupakan sistem operasi open-source yang didesain khusus untuk jaringan sensor nirkabel. TinyOS memiliki arsitektur berbasis komponen yang mendukung adanya inovasi dan implementasi jaringan sensor nirkabel dengan meminimalisasi ukuran kode yang dibutuhkan sebagaimana karakteristik jaringan sensor yang memiliki sedikit memori. Komponen librari TinyOS terdiri dari protokol jaringan, layanan distribusi sensor, driver sensor, dan software pengamatan data sensor yang dapat digunakan untuk melakukan monitoring jaringan sensor. Tidak seperti sistem operasi seperti pada umumnya, tinyOS merupakan sebuah perangkat lunak dalam bentuk kerangka kerja yang digunakan untuk sistem yang saling terikat (*embedded system*) dan untuk mengatur komponen untuk membangun aplikasi jaringan sensor nirkabel. TinyOS didesain untuk tidak memiliki file-system, hanya mendukung alokasi memori statik, mengimplementasikan pemodelan fungsi sederhana, serta menyediakan perangkat dan abstraksi jaringan yang minimal.

TinyOS versi 1.X memiliki fitur yang disebut TinySec, sebuah mekanisme enkripsi pada layer jaringan (*link-layer*). TinySec memiliki 2 mode operasi: *autenticated encryption* (TinySec-AE) dan *authentication only* (TinySec-Auth). Algoritma enkripsi yang digunakan adalah algoritma Skipjack dengan mode operasi CBC (*cipher block chaining*). Proses autentifikasi disediakan oleh mode CBC tersebut dengan menambahkan 4-byte *tag* pada pesan yang digunakan.

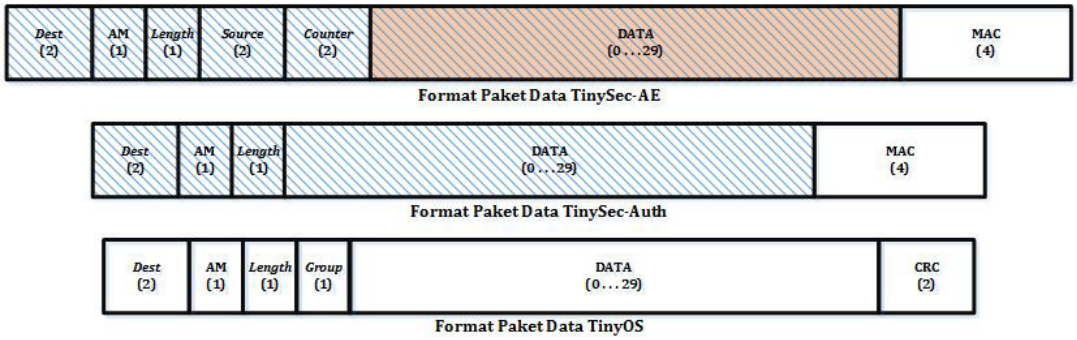
Format paket data yang digunakan pada TinySec diturunkan dari format paket data yang digunakan pada TinyOS (Karlof, 2004). Perbedaan format paket datanya ditunjukkan pada Gambar 5. *Field* yang sama terdapat pada *field* alamat tujuan (*destination address*), tipe pesan aktif (*active message (AM) type*), dan panjang (*length*). AM *type* memiliki kesamaan dengan penomoran pada TCP/IP dan digunakan untuk mengekstrak dan interpretasi pesan pada penerima/ *receiver.* Dalam menangani kesalahan pada transmisi,

TinyOS menggunakan 16-bit *cycle redundancy check (CRC)* pada paket datanya. Bagian *receiver* pesan menghitung ulang CRC pada saat penerimaan data dan mencocokkannya dengan data yang telah diterima. Jika CRCnya sama, maka paket datanya akan diterima, dan akan ditolak jika CRCnya berbeda. Bagaimanapun juga, CRC tidak menyediakan pengamanan data terhadap modifikasi, dan pemalsuan data. Untuk itu, TinySec mengganti CRC dengan MAC. Dengan menggunakan MAC, MAC juga akan melindungi alamat tujuan (*destination address*), tipe pesan aktif (*active message (AM) type*), panjang (*length*), alamat asal (*source address*) dan penghitung (*counter*), serta data (walaupun terenkripsi atau tidak). Pada format paket data TinyOS terdapat *field group* untuk menghindari adanya interferensi antar-sensor. Karena TinySec menggunakan MAC, maka TinySec tidak membutuhkan field *group*.

yang tepat untuk jaringan tergantung pada beberapa faktor seperti model ancaman, kemudahan penggunaan, dan persyaratan jaringan dan keamanan aplikasi. Dalam desain kriptografi, aturan praktis yang digunakan adalah menggunakan kunci yang berbeda untuk aplikasi yang berbeda. Bila merujuk kunci yang digunakan pada TinySec, maka yang digunakan adalah kunci Skipjack: satu kunci untuk mengenkripsi data dan kunci lain untuk komputasi MAC.

4. KESIMPULAN

Penggunaan standar HL7 akan mempengaruhi layanan kesehatan yang lebih efisien, dinamis, dan akan mengurangi risiko terjadinya kesalahan. Dengan melihat 2 contoh implementasi di atas, skenario penanganan kondisi pasien adalah sebagai berikut:



Gambar 5. Format Paket Data TinySec dan TinyOS. Ukuran Byte setiap Field Ditunjukkan di Bawah Label. *Field* yang Diarsir Menunjukkan bahwa *Field* tersebut Terlindungi dengan Adanya MAC. Pada TinySec-AE, *Field* Datanya Terenkripsi.

Mekanisme penguncian menentukan bagaimana kunci kriptografisnya terdistribusi dan dibagikan pada jaringan. Protokol TinySec tidak terbatas pada mekanisme penguncian tertentu, apapun mekanismenya dapat digunakan untuk TinySec. Rangkuman beberapa mekanisme yang digunakan ditunjukkan pada Tabel 5. Mekanisme penguncian

pasien menelepon Rumah Sakit mengabarkan keluhan penyakitnya, data sinyal fisiologis pasien dikirimkan secara nirkabel dan langsung dari rumah pasien ke Rumah Sakit, selanjutnya dokter meminta pemeriksaan laboratorium, dan hasil pemeriksaan laboratorium dapat dikeluarkan secara langsung, dan seluruh skenario penanganan ini terekam pada EMR pasien.

Tabel 5: Rangkuman Mekanisme Penguncian pada Pengamanan Lapisan *Link* (*Link-layer*) [11]

Mekanisme Penguncian	Keuntungan	Kekurangan
Single network-wide key	Sederhana, mudah disebarkan, mendukung *passive participation* dan *local broadcast*	Tidak terlalu tangguh untuk pada jaringan *node*
Per-link keys between neighboring nodes	*node* tidak mudah terserang	Membutuhkan protokol pendistribusian kunci, tidak mendukung *passive participation* dan *local broadcast*
Group keys	*node* tidak mudah terserang, mendukung *passive participation* dan *local broadcast*	Membutuhkan protokol pendistribusian kunci, *tradeoff* antara ketangguhan dan fungsionalitas.

Tentu saja, pengimplementasian HL7 tidak serta merta membuat kemajuan teknologi seperti skenario di atas, tetapi dengan menggunakan dan mengimplementasikan standar pesan HL7 akan mempermudah terrealisasinya sistem penanganan kesehatan yang ideal untuk pasien. HL7 pada saatnya akan menjadi sebuah komponen utama dalam sebuah evolusi dalam pelayanan kesehatan.

DAFTAR PUSTAKA

B. Blobel and K. Engel. 1999. "Health Level Seven Security Services Framework; Part 2: Fundamentals of HL7 Security (Final Draft)". HL7 Secure Transactions Special Interest Group, Tech. Rep.

Carepoint. 2010. "The hl7 Evolution: Comparing hl7 Version 2 to Version 3, Including a History of Version 2". Carepoint Health, Tech. Rep.

C. Karlof, N. Sastry, and D. Wagner. 2004. "Tinysec: a link layer security architecture for wireless sensor networks," in *Proceedings of the 2nd international conference on Embedded networked sensor systems*, ser. SenSys '04. New York, NY, USA: ACM, 2004, pp. 162175. [Online]. Available: *http://doi.acm.org/10.1145/1031495.1031515*.

D. Shaver. 2007. "HL7 101: A beginner's guide", *For The Record*. Januari.

J. W. Lebak, J. Yao, and S. Warren. 2004. "Hl7-compliant healthcare information system for home monitoring," in *Proceedings of the 26th Annual International Conference of the IEEE EMBS*, San Francisco, CA, USA. Pp. 33383341. September.

R. Munir. 2013. "Advanced encryption standard (aes) bahan kuliah if3058 kriptografi," Mei. [Online]. Available: *http://informatika.stei.itb.ac.id/ rinaldi.munir/Kriptogra/*.

S. Warren, J. Lebak, J. Yao, J. Creekmore, A. Milenkovic, and E. Jovanov. 2005. "Interoperability and security in wireless body area network infrastructures, in *Proceedings of the 27th IEEE EMBS Annual International Conference*, Shanghai, China. Pp. 38373840. September.

TexasInstruments. 2004. *Chipcon AS SmartRF® CC2420 Preliminary Datasheet*. June.

TinyOS. 2013. *TinyOS Documentation Wiki*. [Online]. Available: *http://tinyos.stanford.edu*.