PERANCANGAN KEAMANAN DATA PADA DATA HASIL *MONITORING* PASIEN

Antonius Hendro Noviyanto

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

ABSTRACT

Patient monitor is a device which is used to monitor the patient condition. This device records and displays the result of patient condition. The recorded data can be sent to the medical expert over the internet or radio frequency. The recorded data is still a raw data, in other words, the data can be easily read or modified by everyone. Patient data is highly confidential data, so it is necessary to process encryption-decryption of data, therefore, the patient data cannot easily be read or modified by unauthorized person. The process of data encryption is done by the RC4 algorithm, so that the data which has been stored or sent will be an encrypted one. Decryption process can be used to restore encrypted data to be the original one.

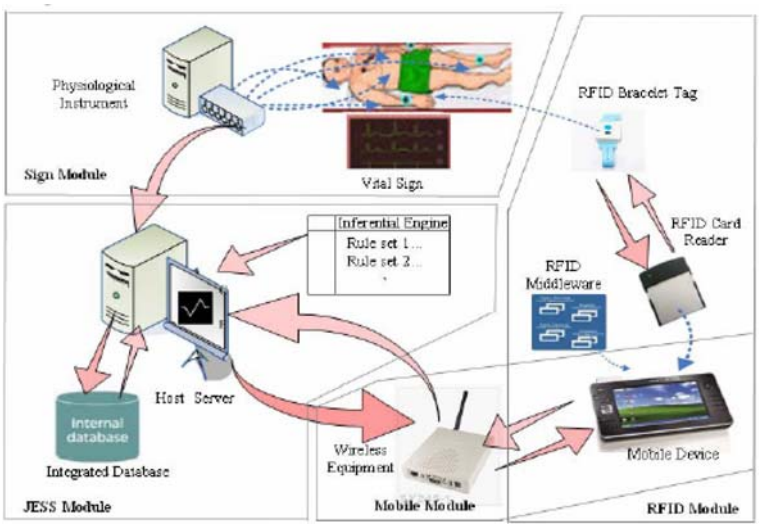
Keyword: *patient monitor, encryption, decryption, RC4.*

1. PENDAHULUAN

Seiring dengan berkembangnya jaman, berkembang pula peralatan medis yang dapat menunjang kesehatan manusia. Peralatan medis dapat dikategorikan sebagai peralatan diagnosa, peralatan *monitoring* dan peralatan terapi.

Peralatan *monitoring* atau sering disebut dengan *patient monitor* memiliki fungsi untuk memantau kondisi pasien. Data dari hasil *monitoring* biasanya disimpan dalam memori agar bisa dibuka kembali datanya untuk dilakukan diagnosa, atau langsung dikirim pada ahli kesehatan melalui jaringan internet atau frekuensi radio.

Pada gambar 1, dijelaskan bahwa data hasil *monitoring* pasien dikirimkan pada ahli kesehatan dengan cara melalui frekuensi radio. Persoalannya adalah, berdasarkan sistem distribusi data seperti pada gambar 1, "penjahat" mudah melakukan manipulasi data hasil *monitoring*. Oleh karena itu, diperlukan sistem keamanan data yang dapat menjamin kerahasiaan data *monitoring*. Tulisan ini akan membahas persoalan tersebut.



Gambar 1. Sistem Distribusi Data *Monitoring* Pasien Daftar Pustaka
(Trappey Charles V. dkk., 2009)

2. DASAR TEORI

2.1 *Patient Monitor*

Patient monitor adalah peralatan medis yang digunakan untuk melakukan *monitoring* atau memantau kondisi fisiologis pasien. Proses *monitoring* dilakukan secara *real-time*, sehingga dapat diketahui kondisi fisiologis pasien pada saat itu juga (Ahmad Fuad, 2014).

Ada tiga jenis *patient monitor* yang digunakan pada rumah sakit, seperti dijelaskan berikut ini:

a. *Patient Monitor Vital sign.*
Patient monitor ini bersifat pemeriksaan stándar, yaitu pemeriksaan ECG, respirasi, tekanan darah atau NIBP, dan kadar oksigen dalam darah atau saturasi darah atau SpO2.

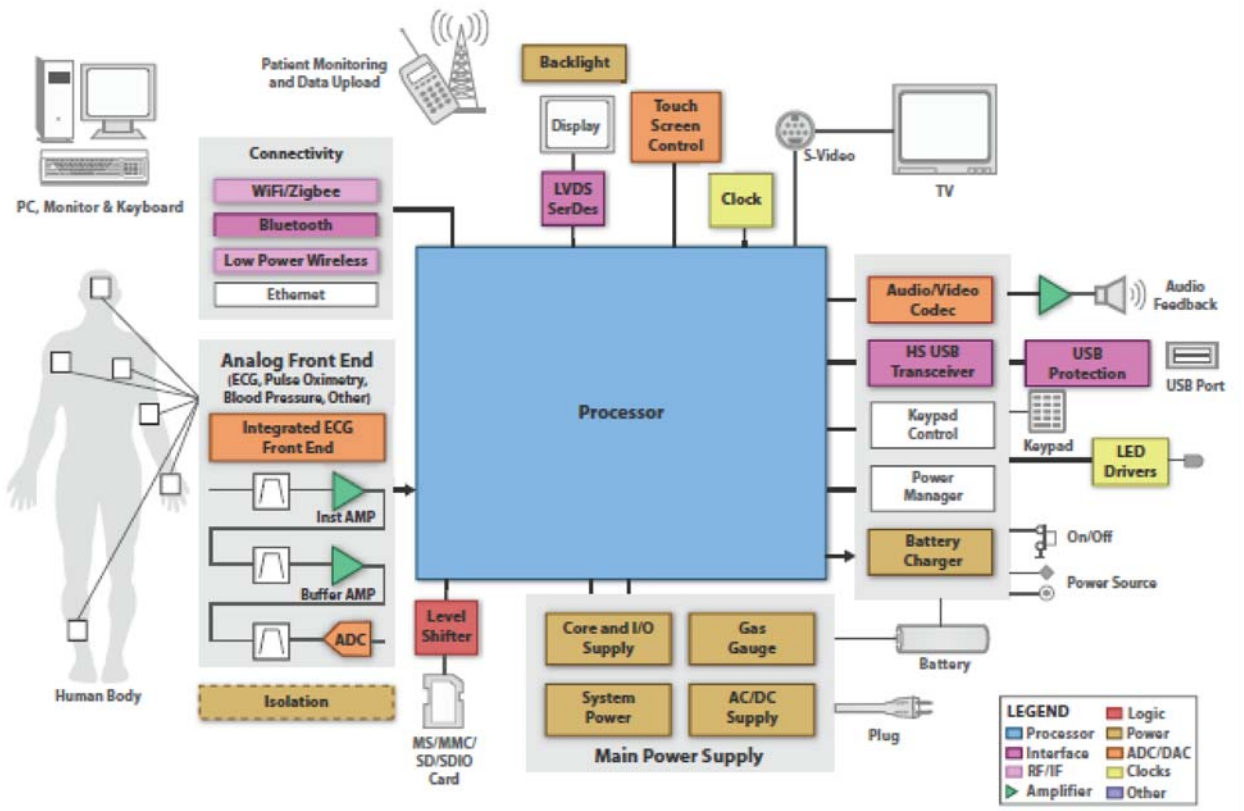
b. *Patient Monitor* 5 Parameter.
Patient monitor ini bisa melakukan pemeriksaan seperti ECG, respirasi, tekanan darah atau NIBP, kadar oksigen dalam darah atau saturasi darah atau SpO2, dan temperatur.

c. *Patient Monitor* 7 Parameter.
Patient monitor ini biasanya dipakai diruangan operasi, karena ada satu parameter tambahan yang biasa dipakai pada saat operasi, yaitu "ECG, respirasi, tekanan darah atau NIBP (*Non Invasive Blood Pressure*), kadar oksigen dalam darah atau saturasi darah atau SpO2, temperatur, dan sebagai tambahan adalah IBP (*Invasive Blood Pressure*) pengukuran tekanan darah melalui pembuluh darah langsung, EtCO2 (End Tidal CO2) yaitu pengukuran kadar karbondioksida dari sistem pernafasan pasien".

Berdasarkan gambar 2, data fisiologis pasien diambil melalui sensor, kemudian data tersebut akan dikonversi ke dalam bentuk digital yang akan diolah oleh *processor*. Hasil pengolahan data tersebut akan ditampilkan pada monitor dan juga disimpan pada memori. Agar ahli medis dapat memantau kondisi pasien secara *real-time* dan tanpa harus berada pada ruangan perawatan pasien, maka data *monitoring* tersebut juga akan dikirim pada ahli medis melalui jaringan internet atau melalui frekuensi radio.

2.2 Kriptografi

Kriptografi adalah ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirim, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga (C. Febrian Wahyu dkk., 2012). Pada dasarnya ada tiga aspek mendasar dalam sistem keamanan informasi, sebagai berikut:



Gambar 2. Diagram Blok *Patient Monitor* (Texas Instrument, 2010)

a. *Confidentiality atau Privacy.*
   Sistem keamanan mampu menjaga kerahasiaan data atau informasi.
b. *Integrity.*
   Sistem keamanan mampu menjaga integritas dari data atau informasi, sehingga tidak ada data atau informasi yang berubah.
c. *Availability.*
   Sistem keamanan harus mampu menyediakan data atau informasi setiap saat ketika dibutuhkan.

Kriptografi sering digunakan dalam proses pengamanan data karena prosesnya yang mudah. Pada dasarnya kriptografi memiliki empat variabel utama, yaitu:

a. Algoritma yaitu metode yang digunakan untuk melakukan proses *encryption* dan *decryption*.
b. Kunci yaitu kode yang digunakan untuk melakukan *encryption* dan *decryption*.
c. *Plaintext* yaitu informasi atau data yang masih bisa dibaca.
d. *Ciphertext* yaitu informasi atau data yang sudah dilakukan *encryption* sehingga tidak bisa dibaca.

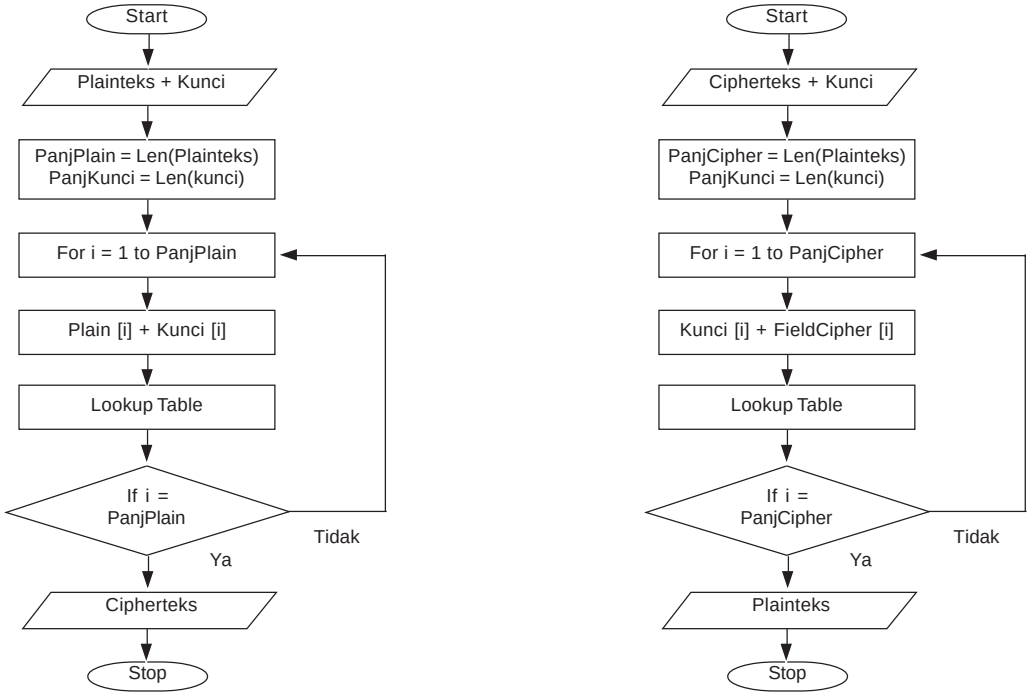
Encryption-decryption merupakan salah satu proses dasar yang dilakukan oleh kriptografi dalam melakukan pengamanan data (Haji Wachyu Hari dkk., 2012). Dimana *encryption* merupakan suatu proses untuk melakukan pengamanan data atau informasi agar data atau informasi tersebut tidak dapat dibaca. Sedangkan *decryption* merupakan suatu proses untuk mengembalikan data atau informasi yang telah menjalani proses *encryption*, sehingga data atau informasi tersebut dapat dibaca kembali.

Pada kriptografi memiliki banyak algoritma, dalam makalah ini algoritma yang akan digunakan adalah algoritma *Rivest Code 4* (RC4). Algoritma RC4 merupakan algoritma kunci simetris yang memiliki dua S-box. Dimana S-box pertama berisi permutasi bilangan 0-255, sedangkan S-box kedua berisi permutasi kunci yang diulang sampai S-box kedua terisi seluruhnya.

2.3 Flowchart Proses *Encryption* RC4 dan *Decryption* RC4

Pada gambar 3(a), dijelaskan flowchart proses melakukan *encryption* data atau informasi, dimana langkah awal dari proses *encryption* adalah menentukan jumlah data pada *plainteks* dan kunci yang digunakan pada proses *encryption*. Setelah itu, dilakukan proses pengacakan data berdasarkan *plainteks* dan kunci sehingga menghasilkan *cipherteks*.

Pada gambar 3(b), dijelaskan mengenai alur proses melakukan *decryption* data atau informasi, dimana langkah awal dari proses *decryption* adalah menentukan jumlah data pada *cipherteks* dan kunci yang digunakan pada proses *encryption*. Setelah itu, dilakukan proses pengacakan data berdasarkan *cipherteks* dan kunci sehingga menghasilkan *plainteks*.



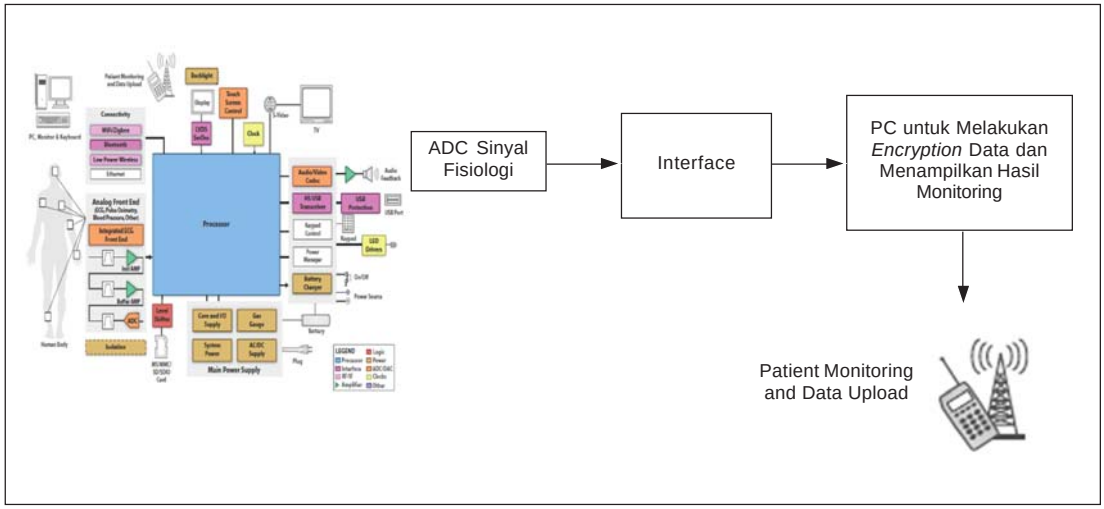
(a) Flowchart *Encryption* RC4 (b) Flowchart *Decryption* RC4

Gambar 3.Flowchart *Encryption* dan Flowchart *Decryption* RC4

3. PERANCANGAN KEAMANAN DATA PASIEN MONITOR

3.1 Diagram Blok Sistem

Sesuai dengan kebutuhan dalam melakukan pengamanan data atau informasi pada hasil *monitoring* pasien, maka perancangan keamanan data atau informasi dapat dilakukan dengan cara melakukan proses kriptografi pada hasil *monitoring* pasien. Diagram blok sistem dapat dilihat pada gambar 4 (proses pengiriman data) dan gambar 5 (proses penerimaan data).



Gambar 4. Diagram Blok Proses Pengiriman Data

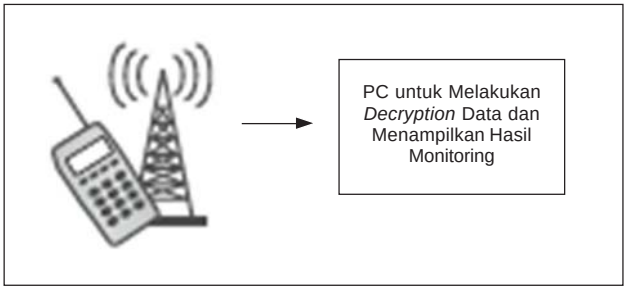
Gambar 4 menjelaskan bahwa sensor mengambil data fisiologis dari pasien yang masih berupa data analog. Data tersebut kemudian akan dikonversi kedalam bentuk digital untuk dikirim ke PC agar dapat diproses lebih lanjut. Dimana pemrosesan data tersebut bertujuan agar data dapat dimengerti oleh ahli medis. Setelah dilakukan pemrosesan maka data tersebut akan ditampilkan dalam monitor.

Pemrosesan data tidak hanya berhenti sampai pada penampilan hasil pada monitor. Pemrosesan data ini juga melakukan *encryption* data agar data tidak bisa dibaca oleh orang lain. Proses *encryption* ini bertujuan untuk mengamankan data ketika data tersebut disimpan dalam memori atau data tersebut dikirim pada ahli medis yang sedang tidak berada pada ruang pengobatan melalui jaringan internet.

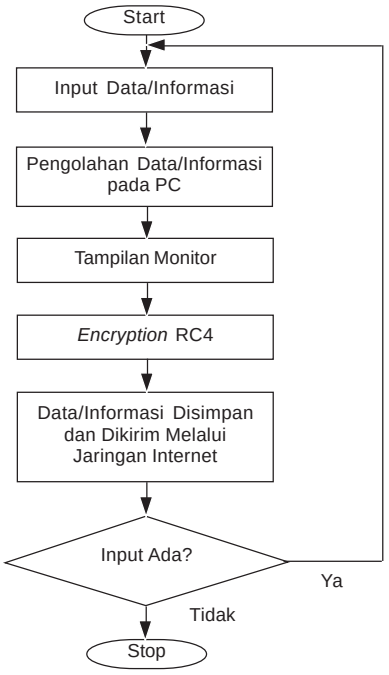
Pada Gambar 5 menjelaskan bahwa data yang telah dikirim oleh blok pengiriman data melalui jaringan internet diterima oleh PC. Data yang diterima tersebut kemudian akan dilakukan proses *decryption* agar data dapat dibaca dan ditampilkan pada PC yang digunakan oleh ahli medis untuk melakukan diagnosa.

3.2 Flowchart Proses Sistem

Pada Gambar 6, menjelaskan mengenai proses kerja dari blok pengiriman data, dimana pada blok tersebut data atau informasi fisiologis pasien diperoleh dari pembacaan sensor. Hasil dari pembacaan sensor diubah kedalam bentuk digital, yang kemudian hasil pembacaan sensor tersebut akan diproses lebih lanjut oleh PC. Setelah dilakukan pemrosesan, data tersebut akan ditampilkan pada monitor untuk mengetahui informasi fisiologis dari pasien.



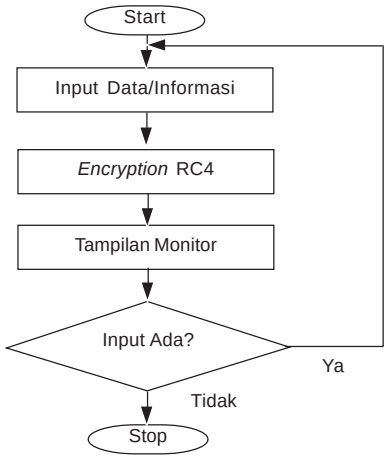
Gambar 5. Diagram Blok Proses Penerimaan Data



Gambar 6. Flowchart Proses Blok Pengiriman Data dan *Encryption* Data

Proses berikutnya adalah dilakukan proses *encryption* pada data atau informasi yang telah diproses oleh PC. Proses *encryption* disini difungsikan agar data atau informasi tidak bisa dibaca. Setelah dilakukan proses *encryption* data atau informasi tersebut kemudian akan disimpan pada memori dan juga akan dikirim pada ahli medis melalui jaringan internet.

Pada Gambar 7 menjelaskan mengenai proses pada blok penerimaan data. Data atau informasi diterima melalui jaringan internet. Data tersebut kemudian akan dilakukan proses *decryption* agar data tesebut dapat dibaca. Setelah proses *decryption*



Gambar 7. Flowchart Proses Blok Penerimaan Data dan *Decryption* Data

selesai, data tesebut akan ditampilkan pada monitor.

4. KESIMPULAN

Proses kriptografi pada data atau informasi medis dapat meningkatkan kerahasiaan dan keamanan pada data atau informasi medis yang akan disimpan atau dikirim kepada ahli medis melalui jaringan internet atau frekuensi radio. Data yang disimpan atau dikirim melalui jaringan internet dalam bentuk data yang telah terenkripsi, sehingga kerahasiaan data tersebut dapat terjamin. Agar dapat membaca data yang telah tersimpan atau dikirim tersebut perlu dilakukan proses *decryption*, sehingga data tersebut dapat kembali ke semula seperti aslinya.

DAFTAR PUSTAKA

Charles V., Trappey. dkk. 2009. "Develop Patient Monitoring and Support System Using Mobile Communication and Intelligent Reasoning". *Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics.* Hlm. 1195-1200.

Fuad, Ahmad. 2014. "*Pasien Monitor*", diakses dari: *http://dumedpower.com/tag/pasien-monitor/*. Tanggal 11 November.

Hari, Haji Wachyu. dkk. 2012. "Implementasi RC4 Stream Cipher untuk Keamanan Basis Data". *Seminar Nasional Aplikasi Teknologi Informasi 2012.*

Instrument, Texas. 2010. *"Diagnostic, Patient Monitoring and Therapy Applications Guide"*. Diakses dari: *www.ti.com/medical,* Tanggal 11 November 2014.

Wahyu, C. Febrian. dkk. 2012. "Penerapan Algoritma Gabungan RC4 dan Base64 pada Sistem Keamanan E-Commerce". *Seminar Nasional Aplikasi Teknologi Informasi 2012.*