ELKOMIKA | ISSN (p): 2338-8323 | ISSN (e): 2459-9638 | Vol. 7 | No. 1 | Halaman 85 - 96
DOI : http://dx.doi.org/10.26760/elkomika.v7i1.85 Januari 2019

Implementasi Pengamanan Transmisi Sinyal EKG (Elektrokardiogram) secara Daring dengan Metode Anonimasi

BRAMASTA AGNANDA SETIAWAN, SONY SOLEHUDIN, IRA PUSPASARI, JUSAK JUSAK

Program Studi S1 Sistem Komputer, Institut Bisnis dan Informatika Stikom Surabaya
Email: jusak@stikom.edu

Received 11 September 2018 **|** *Revised* 3 Oktober 2018 **|** *Accepted* 7 Januari 2019

ABSTRAK

Data World Health Organization (WHO) pada tahun 2014 menunjukkan bahwa di Indonesia sebanyak 37% dari seluruh penyebab kematian adalah penyakit yang berhubungan dengan jantung. Kehadiran teknologi dan pemanfaatan Internet of Things (IoT) diharapkan dapat membantu mengurangi resiko kematian akibat penyakit jantung tersebut. Pada penelitian ini, pengukuran dan pengamatan sinyal jantung melalui tele-auskultasi sinyal elektrokardiogram (EKG) dilakukan. Untuk mengamankan sinyal EKG dalam proses transmisi melalui jaringan Internet digunakan metode anonimasi sinyal berbasis algoritma Jusak-Seedahmed. Hasil pengujian menunjukkkan bahwa algoritma Jusak-Seedahmed dapat melakukan proses anonimasi dan proses rekonstruksi sinyal dengan baik. Pengujian korelasi silang antara sinyal hasil rekonstruksi dan sinyal EKG asli sebelum anonimasi menghasilkan korelasi sebesar 1 pada lag=0. Sinyal EKG hasil rekonstruksi ditampilkan dalam aplikasi mobile untuk memudahkan analisis oleh dokter.

***Kata kunci**: elektrokardiogram, keamanan, anonimasi, IoT, FFT*

ABSTRACT

Based on the latest data released by the World Health Organization in 2014, deaths caused by cardiovascular disease in 2012 have reached 37% of the total number of non-communicable diseases deaths in Indonesia. Therefore, it is expected that the applications of the Internet of Things (IoT) might be used to reduce the risk of death due to the heart related problems. In this research, a tele-auscultation technique for measuring and monitoring electrocardiogram (ECG) signal was built. To secure transmission of the ECG signal over the Internet, we implemented a recently proposed Jusak-Seedahmed algorithm. Our examinations showed that the algorithm performed the anonymization and reconstruction processes well. Cross-correlation analysis showed that correlation between the reconstructed and the original ECG signal at lag=0 was 1. Furthermore, a mobile-based application had been built to display the reconstructed ECG signal for further analysis.

***Keywords**: electrocardiogram, security, anonimization, IoT, FFT*

1. PENDAHULUAN

Perkembangan teknologi *Internet* dan aplikasinya dalam beberapa tahun terakhir telah mengarah kepada pengembangan dan pemanfaatan teknologi *Internet of Things (*IoT). IoT merupakan kumpulan sensor atau peranti berukuran kecil yang terhubung pada sebuah perangkat transmisi yang mampu mengirimkan atau menerima data melalui jaringan komunikasi *Internet* **(Atzori, Iera, & Morabito, 2012)**. Dalam teknologi komunikasi yang akan datang, perangkat dan jaringan IoT ini diperkirakan akan mendominasi jaringan komunikasi seluler generasi kelima (5G) yang dapat mengakomodasi jaringan peranti IoT berukuran kecil dengan menggunakan konsep *heterogeneous network* **(Andrews, et al., 2014)**. Aplikasi IoT melingkupi hampir seluruh aspek di sekitar kehidupan manusia, misalnya aplikasi rumah pintar (*smart house*), kota pintar (*smart city*), berbagai macam proses pengendalian dalam industri, dan kesehatan **(Islam, Kwak, Kabir, Hossain, & Kwak, 2015)**.

Salah satu aplikasi penting dari IoT adalah aplikasi kesehatan elektronik (*e-health*), misalnya aplikasi IoT yang dimanfaatkan untuk pengukuran dan pengamatan berbagai jenis penyakit mulai dari penyakit diabetes sampai penyakit jantung **(Jusak, Pratikno, & Putra, 2016)**. Dengan fitur koneksi jaringan *Internet* yang dimiliki, peranti IoT memungkinkan pengiriman data jarak jauh lintas kota bahkan dunia dengan menggunakan protokol yang umumnya digunakan untuk aplikasi-aplikasi berbasis *Internet*. Sehingga dengan adanya aplikasi kesehatan elektronik semacam ini, diharapkan daerah-daerah terpencil yang tidak tersentuh oleh kehadiran dokter tetap dapat mendapatkan pelayanan yang baik untuk melakukan deteksi awal penyakit kronis maupun pengawasan (*monitoring*) kesehatan seseorang dengan menggunakan teknik tele-auskultasi **(Jusak & Puspasari, 2015)**. Alasan penggunaan IoT untuk kesehatan elektronik didukung oleh data terbaru yang dikeluarkan oleh *World Health Organization* (WHO) yang menunjukkan bahwa sampai tahun 2012, diestimasi bahwa di Indonesia terdapat sebanyak 37% dari seluruh penyebab kematian adalah karena penyakit yang berhubungan dengan jantung (*cardiovascular disease*) berasal dari semua umur **(WHO, 2014)**. Kehadiran aplikasi IoT dalam bidang kesehatan diharapkan dapat turut membantu menurunkan resiko kematian akibat penyakit yang berhubungan dengan jantung tersebut. Hal ini dapat dilakukan apabila deteksi terhadap gangguan jantung dapat dilakukan sedini mungkin.

Metode pengukuran dan pengamatan terhadap kesehatan jantung dapat dilakukan dengan cara melakukan perekaman dan analisis sinyal elektrokardiogram (EKG) **(Hadiyoso, Julian, Rizal, & Aulia, 2015)**. Dalam laporan penelitian tersebut, pengamatan sinyal jantung EKG dapat dilakukan secara daring karena data sinyal jantung tersimpan dalam sebuah basis data dan dapat diakses oleh komputer lain dalam jaringan yang sama. Selain itu, sinyal EKG untuk setiap orang bersifat unik karena berisi informasi kesehatan yang sangat penting bagi seorang pasien. Bahkan sinyal EKG dapat digunakan sebagai identitas biometrik untuk membedakan informasi spesifik yang dimiliki orang tertentu **(Pinto, Cardoso, & Laurenco, 2018).** Karena itu transmisi sinyal EKG yang berasal dari sebuah sumber, misalnya dari sensor EKG menuju ke sebuah penyedia penyimpanan atau penyedia layanan kesehatan yang melalui jaringan publik, menyebabkan sinyal EKG ini menjadi rentan terhadap serangan dari luar **(Yang, Zhou, Lei, Zheng, & Xiang, 2016)**. Oleh karena itu, aplikasi kesehatan elektronik berbasis *Internet* yang mengabaikan perlindungan informasi kesehatan merupakan ancaman bagi privasi seseorang. Namun sayang sekali bahwa sampai saat ini belum ada aplikasi kesehatan elektronik yang diterapkan untuk melindungi transmisi sinyal EKG tersebut.

Beberapa laporan penelitian telah mengusulkan model atau algoritma untuk pengamanan transmisi sinyal EKG. Salah satu model menggunakan kombinasi 3 (tiga) proses secara berurutan, yaitu pengkodean, kompresi dan enkripsi yang diterapkan dalam proses pengiriman sinyal EKG **(Sufi & Khalil, 2008)**. Dalam laporan penelitian tersebut dijelaskan bahwa proses pengamanan sinyal EKG dapat diterapkan pada perangkat genggam. Model lain yang diusulkan dalam pengamanan sinyal EKG adalah dengan menggunakan proses anonimasi sinyal EKG **(Mahmmoud, 2016)**. Dalam paper ini, proses anonimasi dilakukan dengan bantuan *wavelet-packet*, yaitu dengan melakukan modifikasi terhadap *sub-band* frekuensi rendah setelah proses dekomposisi sinyal EKG oleh algoritma *wavelet-packet*. Akan tetapi, kehebatan algoritma *wavelet-packet* harus dibayar dengan tingginya waktu proses anonimasi dan rekonstruksi sinyal EKG. Karena itu proses anonimasi sinyal EKG selanjutnya diperbaiki untuk menghasilkan waktu proses lebih pendek dengan tingkat kompleksitas algoritma lebih rendah **(Jusak, J., & Mahmoud, 2018)**.

Pada penelitian ini, metode anonimasi sinyal berbasis algoritma *Jusak-Seedahmed* digunakan dan diimplementasikan untuk menguraikan sinyal EKG pada domain frekuensi, yaitu dengan cara memisahkan komponen sinyal EKG frekuensi rendah dan selanjutnya melakukan rekonstruksi komponen sinyal EKG frekuensi tinggi untuk proses anonimasi. Komponen sinyal EKG frekuensi rendah yang telah dipisahkan selanjutnya disimpan sebagai kunci rahasia dan dikirimkan secara daring ke lokasi penyimpan elektronik tertentu, misalnya pada penyimpan elektronik yang ada di rumah sakit. Pada saat yang sama, sinyal EKG hasil anonimasi dikirimkan secara daring ke lokasi penyimpan elektronik publik yang berbeda, misalnya pada penyimpan eletronik *cloud server*. Pemisahan lokasi penyimpan antara kunci rahasia dan sinyal EKG hasil anonimasi ini dimaksudkan untuk meningkatkan keamanan sinyal EKG dari jangkauan para peretas. Di sisi penerima, personil yang secara resmi memiliki hak akses ke kunci rahasia dan mengetahui letak sinyal EKG hasil anonimasi dapat melakukan rekonstruksi sinyal EKG untuk mendapatkan sinyal EKG asli.

Kontribusi utama pada penelitian ini antara lain: (i) melakukan pengamanan sinyal EKG yang dikirimkan secara daring melalui jaringan *Internet* untuk melindungi sinyal EKG dari jangkauan para peretas dengan menggunakan algoritma *Jusak-Seedahmed*, (ii) melakukan implementasi pengamanan sinyal EKG dengan algoritma *Jusak-Seedahmed* pada kondisi nyata sehingga hasil akhir rekonstruksi sinyal EKG dapat dijangkau oleh seorang dokter melalui peranti genggam dengan tingkat korelasi tinggi.

Laporan hasil penelitian ini secara keseluruhan terbagi atas beberapa bagian. Bagian pertama merupakan pendahuluan yang berisi latar belakang penelitian dan kontribusi penelitian. Bagian kedua menjelaskan metode penelitian yang digunakan. Bagian ketiga mengulas hasil penelitian beserta analisisnya. Bagian terakhir merupakan kesimpulan dari penelitian.

2. METODOLOGI PENELITIAN

Bagian ini menjelaskan metodologi penelitian yang dilakukan meliputi arsitektur sistem secara keseluruhan serta model perancangan sistem anonimasi sinyal ECG dan rekonstruksinya.

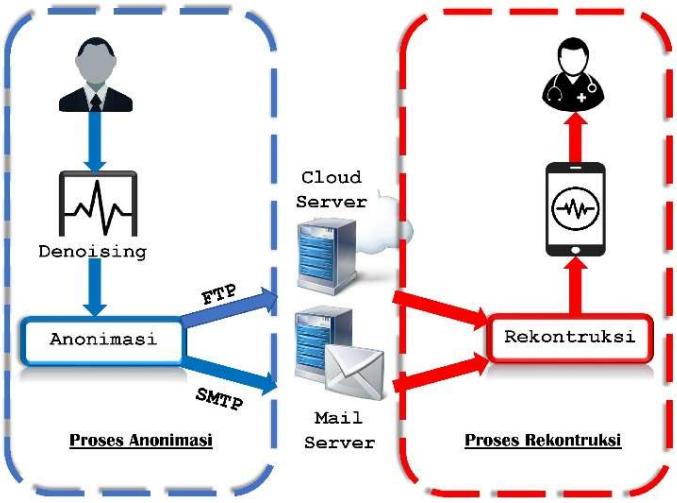
2.1 Model Perancangan

Arsitektur sistem pengamanan transmisi sinyal EKG secara daring ditunjukkan dalam Gambar 1. Seperti terlihat dalam Gambar 1, secara umum terdapat 2 (dua) proses besar, yaitu proses anonimasi dan proses rekonstruksi. Proses anonimasi melakukan fungsi pengambilan data sinyal EKG dengan menggunakan sensor EKG jepit tiga kabel, pembersihan sinyal dari berbagai macam gangguan (*noise*), anonimasi sinyal, pengiriman kunci rahasia yang sudah terenkripsi

menggunakan protokol *Internet Simple Mail Transfer Protocol* (SMTP) dan pengiriman sinyal EKG hasil anonimasi ke *cloud server* menggunakan *File Transfer Protocol* (FTP).

Untuk mendapatkan sinyal EKG asli, sisi penerima melakukan proses rekonstruksi sinyal EKG yang meliputi proses pengambilan kunci rahasia dan sinyal EKG hasil anonimasi, menggabungkan kunci rahasia yang telah didekripsi dan sinyal EKG hasil anonimasi, melakukan rekonstruksi sinyal EKG, dan terakhir memberikan tampilan hasil rekonstruksi sinyal EKG kepada penerima melalui peranti genggam.

Seperti terlihat dalam Gambar 1, sinyal EKG hasil anonimasi tersimpan di dalam sebuah *cloud server* publik yang dapat diakses oleh pengguna tertentu yang memiliki hak untuk melakukan akses ke dalam *cloud server*. Apabila dalam kondisi tertentu seorang peretas berhasil mengambil sinyal EKG pada *cloud server* tersebut, maka peretas tidak akan mendapatkan sinyal EKG yang asli. Untuk dapat mendapatkan kembali sinyal ECG asli, seorang pengguna harus memperoleh kunci rahasia dan selanjutnya melakukan proses rekonstruksi terhadap sinyal ECG hasil anonimasi tersebut.



Gambar 1. Arsitektur Pengamanan Sinyal EKG dengan Metode *Jusak-Sedahmed*

2.2 Proses Anonimasi Sinyal EKG

Dalam seluruh laporan penelitian ini, sinyal EKG disimbolkan sebagai $X(n)$, adalah urutan sinyal dalam domain waktu yang secara matematika dinyatakan dalam bentuk:

$$X(n): n = 0 \cdots N - 1, \tag{1}$$

Parameter n adalah penanda waktu dan N adalah panjang urutan sinyal EKG yang dicuplik dari sensor EKG.

Apabila pada sinyal $X(n)$ dikenakan transformasi ke domain frekuensi, misalnya menggunakan metode *Fast Fourier Transform* (FFT), maka sinyal $X(n)$ akan menjadi sinyal $S(k)$ dalam domain frekuensi yang secara matematika dinyatakan dalam bentuk :

$$S(k): k = 0 \cdots N - 1, \tag{2}$$

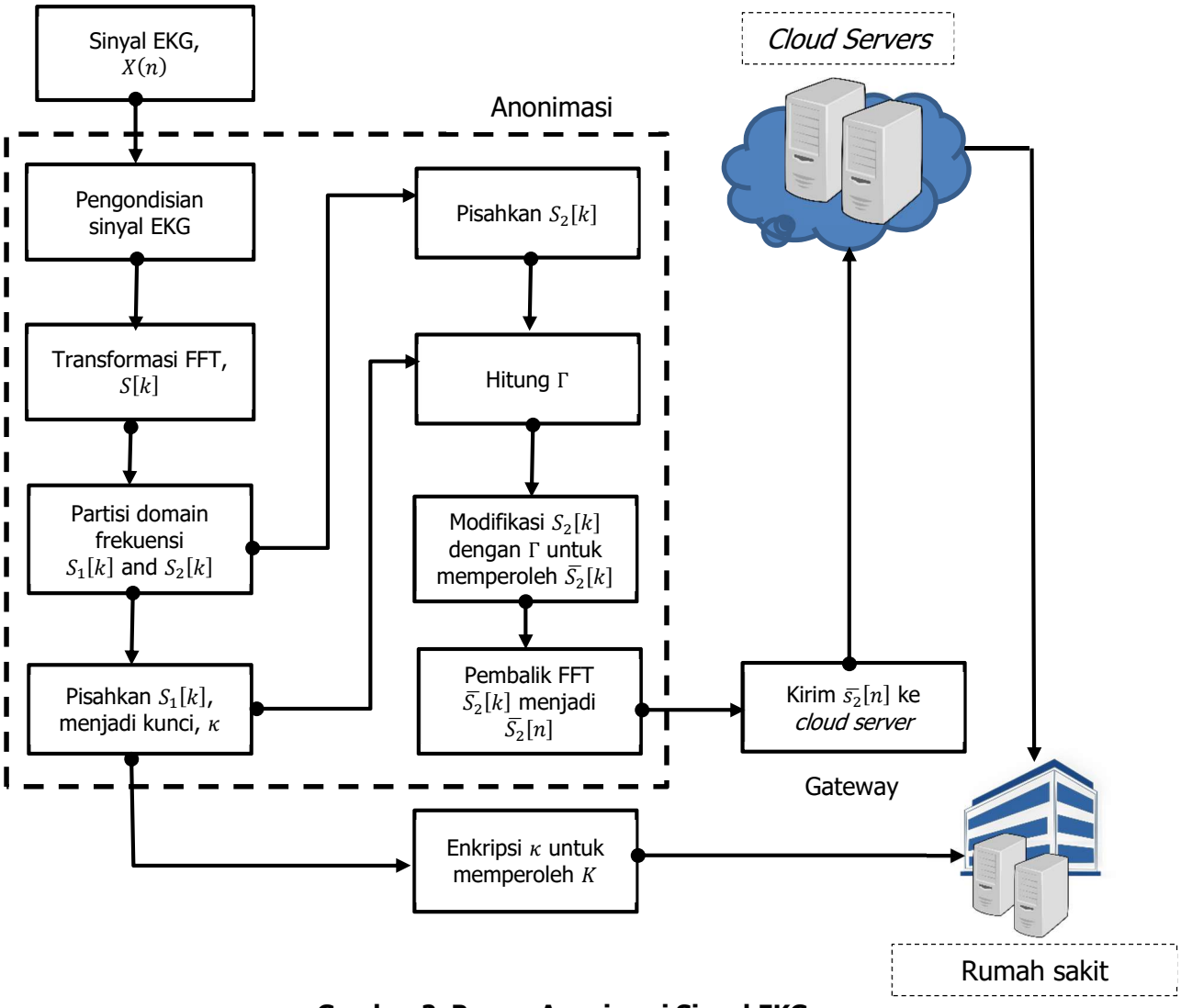
yang mana k dalam Persamaan (2) adalah penanda frekuensi.

Seperti terlihat dalam Gambar 2, proses anonimasi diawali dengan mencuplik sinyal EKG dari seorang pasien dengan menggunakan sensor EKG. Selanjutnya pada hasil cuplikan sinyal yang telah didapat tersebut dilakukan proses pengondisian sinyal yaitu pembersihan sinyal dari gangguan (*noise*). Langkah berikutnya adalah melakukan transformasi sinyal EKG dari domain waktu menjadi domain frekuensi dengan menggunakan metode FFT.

Sesuai dengan rumusan dalam algoritma *Jusak-Seedahmed* **(Jusak, J., & Mahmoud, 2018)**, sinyal EKG dalam domain waktu dipisahkan menjadi 2 (dua) bagian, yaitu komponen frekuensi rendah dan komponen frekuensi tinggi seperti ditunjukkan dalam Persamaan (3).

$$S(k) \equiv \left\{ \underbrace{S_1[0 \dots P]}_{\substack{komponen \\ frekuensi \\ renda}}, \underbrace{S_2[(P+1) \dots Q]}_{\substack{komponen \\ frekuens \\ tinggi}} \right\}, \tag{3}$$

Parameter P adalah panjang komponen sinyal frekuensi rendah dan Q adalah panjang komponen sinyal frekuensi tinggi.



Gambar 2. Proses Anonimasi Sinyal EKG

Pada langkah selanjutnya, komponen sinyal frekuensi rendah, $S_1(k)$ dipisahkan dan digunakan sebagai kunci rahasia yang disimbolkan sebagai κ. Kemudian dilakukan proses enkripsi pada kunci rahasia ini bersama-sama dengan parameter Γ sehingga menjadi K dan dikirimkan ke tempat penyimpanan elektronik yang ada di rumah sakit melalui protocol *Simple Mail Transfer Protocol* (SMTP).

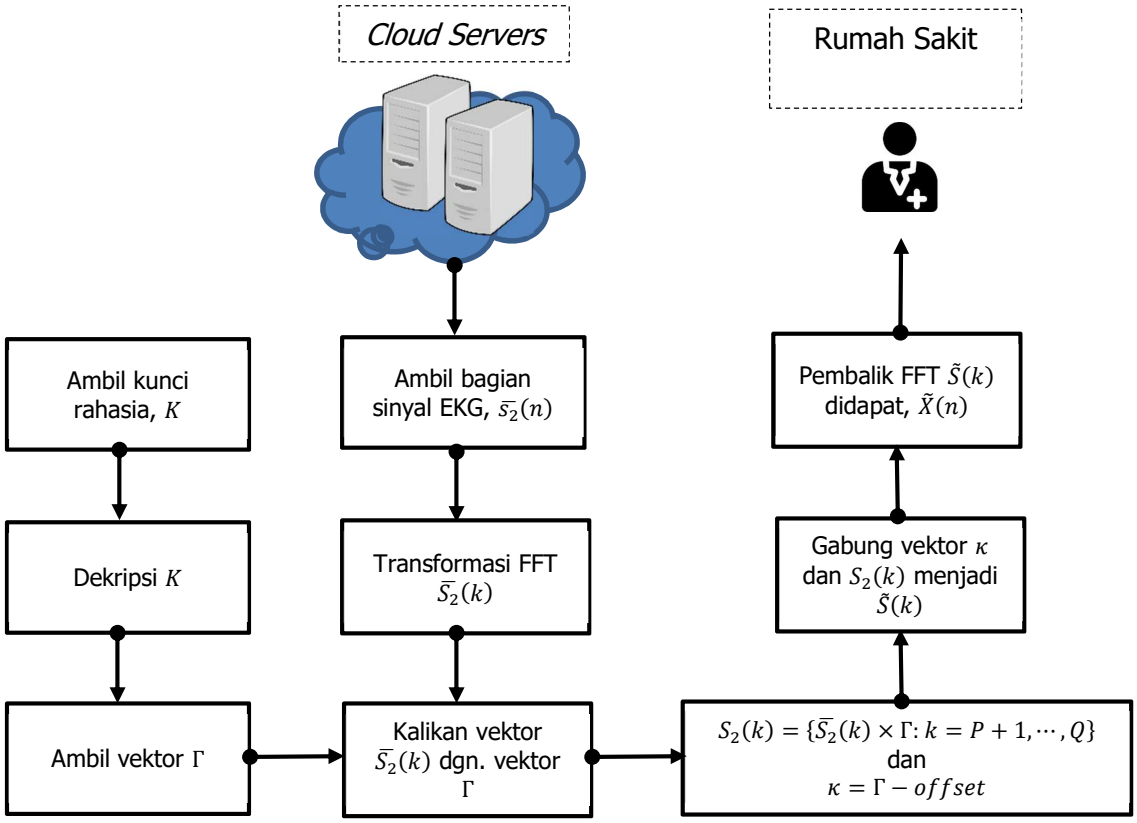
Pada komponen sinyal frekuensi tinggi, $S_2(k)$, dilakukan proses modifikasi sedemikian rupa sehingga komponen sinyal frekuensi tinggi tersebut berubah menjadi bentuk lain seperti ditunjukkan dalam Persamaan (4).

$$\overline{S_2}(k) = \left\{\frac{S_2(k)}{\Gamma} : k = P+1, \ldots, Q\right\} \quad (4)$$

Pada Persamaan (4), vektor Γ didefinisikan sebagai $\Gamma = \kappa + offset$, dengan $offset = |min(\kappa)| + \eta$. Parameter η adalah nilai konstan untuk mencegah pembagian dengan nol, sementara | | adalah operasi bilangan absolut.

Langkah terakhir pada proses anonimasi sinyal EKG adalah mentranformasi kembali sinyal dari domain frekuensi menjadi domain waktu dengan menggunakan metode pembalik FFT (*invers* FFT). Hasil pembalikan sinyal dalam domain waktu disimbolkan sebagai $\overline{s_2}(n)$. Berikutnya hasil pembalikan bagian dari sinyal EKG dalam domain waktu ini dikirimkan ke *cloud server* dengan menggunakan protokol *File Transfer Protocol* (FTP) untuk disimpan.

2.3 Proses Rekonstruksi Sinyal EKG



Gambar 3. Proses Rekonstruksi Sinyal EKG

Proses rekonstruksi dimulai dengan mengambil kunci rahasia terenkripsi, K, dari penyimpan eletronik yang ada di rumah sakit dan bagian sinyal ECG $\bar{s_2}(n)$ yang tersimpan pada *cloud server*. Setelah kedua jenis sinyal tersebut didapatkan selanjutnya dilakukan proses rekonstruksi dengan langkah-langkah seperti ditunjukkan dalam Gambar 3. Dekripsi terhadap kunci, K, menghasilkan dua buah vektor yaitu vektor kunci rahasia, κ, dan vektor Γ.

Langkah selanjutnya dalam proses rekonstruksi adalah melakukan transformasi bagian sinyal EKG, $\bar{s_2}(n)$, yang telah diambil dari *cloud server*, dari domain waktu ke domain frekuensi dengan menggunakan FFT. Setelah itu, langkah penting dalam proses rekonstruksi adalah mengalikan komponen sinyal frekuensi tinggi dengan vektor Γ untuk mendapatkan komponen sinyal frekuensi tinggi seperti saat sebelum dimodifikasi seperti terlihat dalam Persamaan (5).

$$S_2(k) = \{\bar{S_2}(k) \times \Gamma : k = P+1, \cdots, Q\} \quad (5)$$

Proses rekonstruksi diakhiri dengan menggabungkan kembali komponen sinyal frekuensi tinggi, $S_2(k)$, dengan kunci rahasia, κ, yang tidak lain adalah komponen sinyal frekuensi rendah, $S_1(k)$. Hasil penggabungan kedua sinyal, $\tilde{S}(k)$, diikuti dengan proses inversi FFT dari domain frekuensi menjadi domain waktu. Sehingga didapatkan sinyal EKG, $\tilde{X}(k)$, yang merupakan sinyal EKG yang akan dipresentasikan kepada dokter. Untuk membuktikan kesamaan sinyal EKG hasil rekonstruksi dengan sinyal EKG asli, pada bagian akhir pengujian akan dilakukan pengujian secara korelasi.

3. HASIL PENGUJIAN DAN DISKUSI

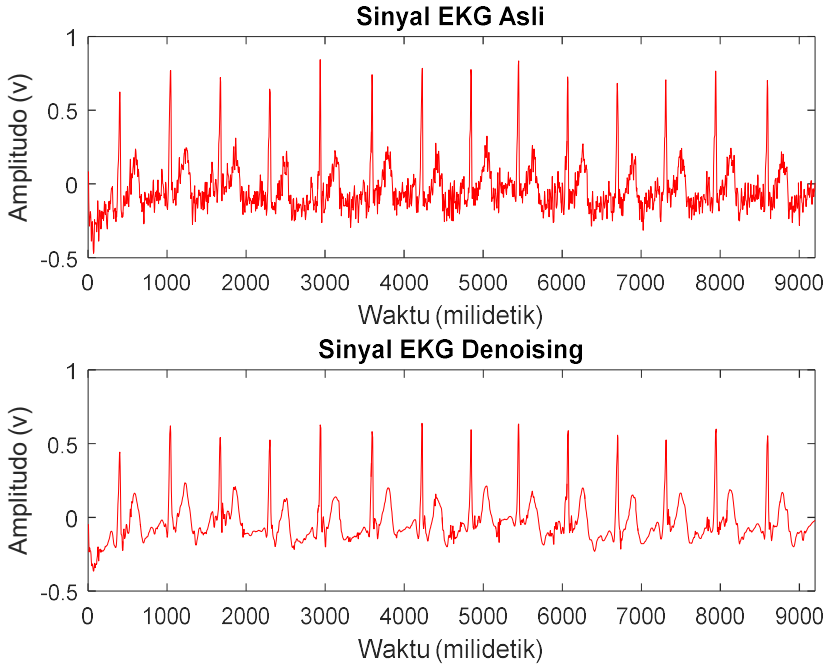
Pengambilan data sinyal EKG dilakukan dengan menggunakan sensor EKG 3 (tiga) kabel yang terhubung pada sebuah perangkat pengendali mikro (*microcontroller*) Arduino Uno yang telah diprogram dan dieksekusi melalui Arduino IDE. Dalam uji coba sinyal EKG diambil dari 2 (dua) orang yang berbeda. Pengambilan data pada masing-masing orang dilakukan sebanyak 3 (tiga) dengan waktu cuplik yang berbeda, yaitu 4 md (milidetik), 2 md, dan 1 md yang mana masing-masing waktu cuplik tersebut secara berurutan berasosiasi dengan frekuensi cuplik 250Hz, 500Hz, dan 1000Hz seperti ditunjukkan dalam Tabel 1.

Tabel 1. Data Pengujian Sinyal EKG

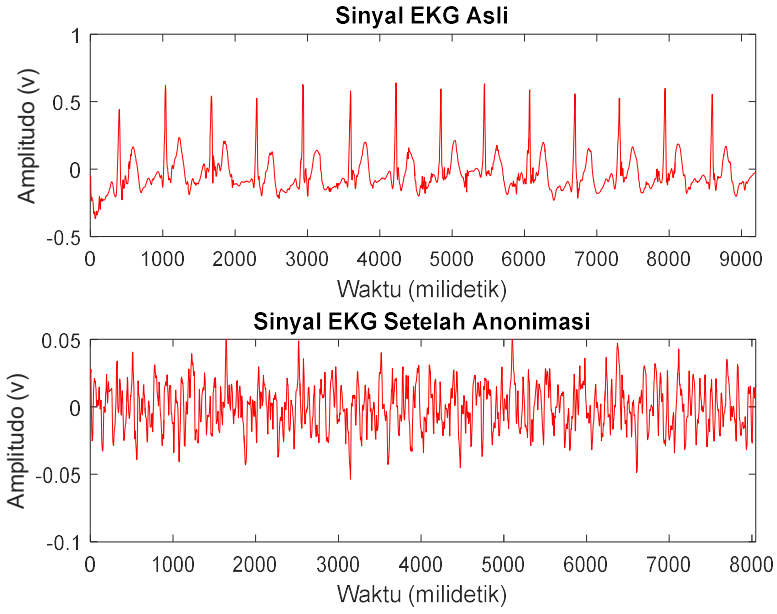
ID	Data Uji	Waktu Cuplik	Frek. Cuplik
bs10089601	1	4 md	250 Hz
ss25029501	2	4 md	250 Hz
bs10089602	3	2 md	500 Hz
ss25029502	4	2 md	500 Hz
bs10089603	5	1 md	1000 Hz
ss25029503	6	1 md	1000 Hz

Gambar 4 menunjukkan sinyal EKG asli hasil pengambilan data sinyal EKG untuk data uji 1 (bs10089601). Sinyal EKG pada data uji 1 diambil dalam rentang waktu kurang lebih 9 menit. Seperti terlihat dalam gambar, hasil pengambilan sinyal EKG dikotori oleh banyak gangguan.

Gangguan dapat berasal dari sensor EKG yang digunakan dan juga dapat berasal dari kabel penghubung peranti elektronik dari sensor EKG menuju ke perangkat pengendali mikro yang digunakan. Pada Gambar 4 juga ditunjukkan sinyal EKG *denoising* hasil dari proses pembersihan sinyal dari gangguan dengan menggunakan metode *wavelet* yang memanfaatkan *mother wavelet* daubechies 5 (db5).



Gambar 4. Sinyal EKG Data Uji 1 (bs10089601) dan Hasil Proses Pembersihan



Gambar 5. Hasil Anonimasi Sinyal EKG Data Uji 1 (bs10089601)

Hasil dari proses anonimasi sinyal EKG data uji 1 ditunjukkan dalam Gambar 5 yaitu sinyal EKG asli dan sinyal EKG setelah anonimasi. Dalam proses anonimasi tersebut digunakan panjang kunci rahasia 128 karakter. Seperti terlihat dalam gambar, sinyal EKG hasil anonimasi berbeda sama sekali dengan sinyal EKG asli. Sinyal hasil anonimasi ini dikirimkan secara daring melalui jaringan *Internet* dan disimpan di dalam peranti penyimpan elektronik yang terdapat pada sebuah *cloud server*. Apabila karena kelalaian pada administrasi *cloud server* sehingga seorang peretas dengan cara tertentu berhasil mengambil sinyal EKG tersebut, maka data sinyal EKG hasil anonimasi tersebut tidak berarti apa-apa bagi peretas. Sinyal EKG setelah anonimasi pada Gambar 5 juga menunjukkan bahwa panjang sinyal EKG hasil anonimasi berkurang sekitar 1000 md, hal ini disebabkan karena sebagian dari komponen sinyal EKG pada frekuensi rendah telah diambil sebagai kunci rahasia dan disimpan pada peranti penyimpan elektronik yang berbeda.

Tabel 2 menunjukkan pengujian waktu proses anonimasi sinyal ECG untuk berbagai data uji dengan panjang kunci rahasia yang berbeda, yaitu berturut-turut 128 karakter dan 256 karakter. Tujuan dari pengujian ini adalah untuk mengetahui pengaruh perubahan panjang kunci rahasia yang digunakan terhadap waktu pemrosesan anonimasi sinyal EKG dalam milidetik (md).

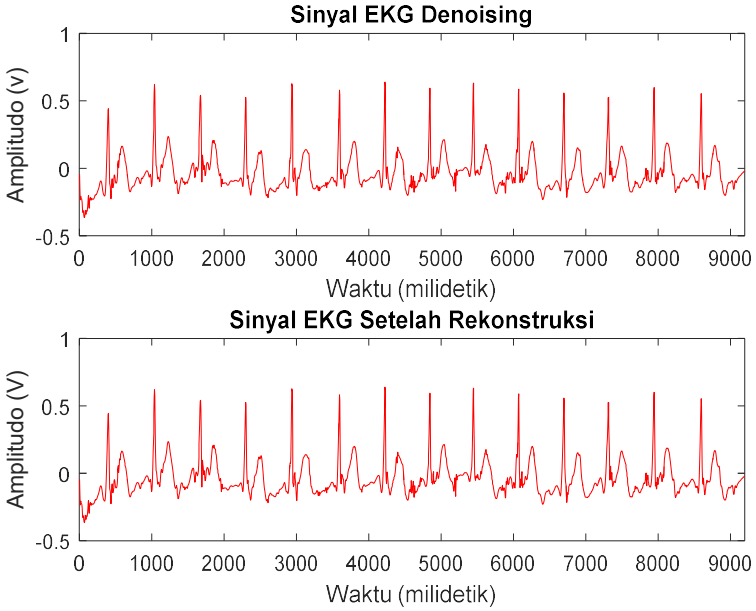
Tabel 2. Waktu Proses Anonimasi Dalam Milidetik (md) Sebagai Fungsi Perubahan Panjang Kunci Rahasia

Key	Data Uji 1	Data Uji 2	Data Uji 3	Data Uji 4	Data Uji 5	Data Uji 6
128	5,4 md	5,4 md	5,9 md	5,9 md	6,7 md	6,7 md
256	5,4 md	5,4 md	5,9 md	5,9 md	6,7 md	6,7 md

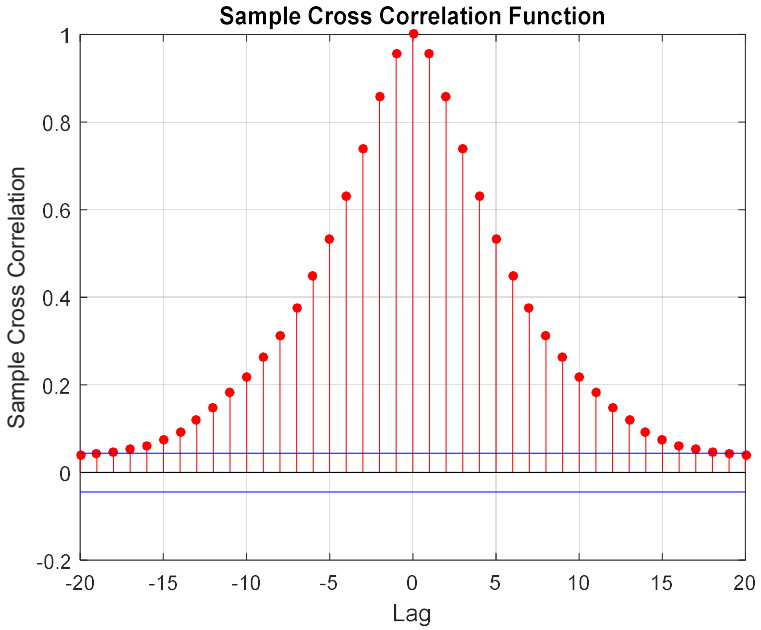
Seperti terlihat dalam Tabel 2, perubahan panjang kunci rahasia tidak mempengaruhi kecepatan pemrosesan anonimasi sinyal EKG. Kecepatan proses anonimasi sinyal EKG hanya dipengaruhi oleh panjang data uji. Sebagai contoh data uji 5 dan data uji 6 memiliki waktu pemrosesan paling lama karena kedua data tersebut diambil dengan frekuensi cuplik 1000 Hz yang berarti bahwa dalam 1 detik terdapat 1000 titik data sinyal EKG. Sedangkan pada data uji 1 dan data uji 2 yang diambil dengan frekuensi cuplik 250 Hz, maka pada data sinyal EKG tersebut dalam 1 detik hanya terdapat 250 titik data sinyal EKG.

Seperti dijelaskan sebelumnya sinyal EKG setelah anonimasi merupakan sinyal EKG yang tidak memiliki arti baik bagi seorang dokter maupun peretas yang berhasil mengambil data sinyal EKG tersebut. Karena itu untuk dapat melihat sinyal EKG asli yang tersimpan untuk pasien tertentu, peranti elektronik seorang dokter harus dilengkapi dengan aplikasi rekonstruksi sinyal EKG hasil anonimasi.

Setelah dilakukan proses rekonstruksi sinyal EKG sebagaimana dijelaskan dalam sub-bab 2.3, hasil rekonstruksi sinyal EKG data uji 1 ditunjukkan dalam Gambar 6. Gambar 6 membandingkan antara sinyal EKG asli dan sinyal EKG hasil dari proses rekonstruksi. Secara kasat mata terlihat bahwa kedua sinyal EKG memiliki kemiripan. Untuk membuktikan kemiripan antara sinyal EKG asli dan sinyal EKG hasil rekonstruksi, maka hasil korelasi silang (*cross correlation*) antara kedua sinyal EKG ditunjukkan dalam Gambar 7.



Gambar 6. Hasil Rekonstruksi Sinyal EKG Data Uji 1 (bs10089601)

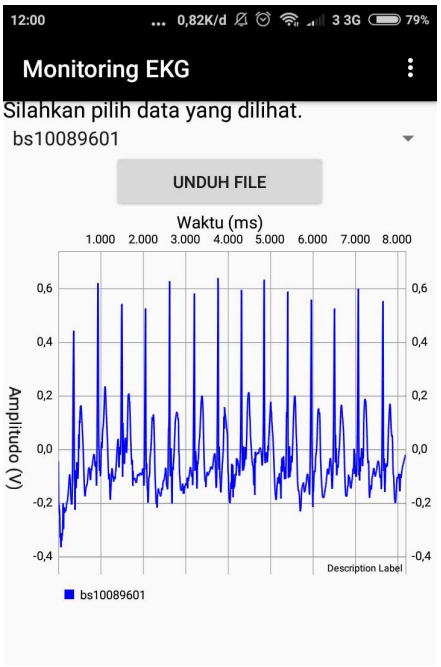


Gambar 7. Korelasi Silang Sinyal EKG Data Uji 1 (bs10089601) dan Sinyal EKG Hasil Rekonstruksi

Terlihat dalam Gambar 7 bahwa korelasi silang untuk sinyal EKG data uji 1 pada *lag*=0 antara sinyal EKG hasil rekonstruksi dengan sinyal EKG asli (sebelum proses anonimasi) memiliki nilai sebesar 1. Hal yang sama juga berlaku untuk semua data uji sinyal EKG. Hal ini berarti bahwa sinyal EKG hasil rekonstruksi sama persis dengan sinyal EKG sebelum proses anonimasi. Dengan kata lain, proses rekonstruksi sinyal EKG telah dapat dilakukan dengan sempurna untuk mendapatkan kembali sinyal EKG sebelum proses anonimasi. Proses rekonstruksi yang menghasilkan tingkat korelasi tinggi semacam ini penting bagi analisis sinyal EKG berikutnya oleh dokter. Karena itu dalam proses rekonstruksi tidak diinginkan adanya kehilangan data

sinyal EKG sama sekali. Seperti terlihat dalam pengujian, algoritma *Jusak-Seedahmed* dapat mengembalikan struktur sinyal EKG sesuai dengan sinyal EKG sebelum proses anonimasi.

Gambar 8 menunjukkan bentuk grafik sinyal EKG data uji 1 yang ditampilkan melalui aplikasi pengamatan sinyal EKG yang merupakan aplikasi *mobile* berbasis Android. Tampilan sinyal EKG data uji 1 dalam gambar merupakan hasil rekonstruksi sinyal EKG yang tersimpan pada *cloud server.* Secara umum dapat dilihat bahwa tampilan sinyal EKG dalam Gambar 8 sama dengan tampilan sinyal EKG dalam Gambar 6 sinyal EKG setelah rekontruksi, keduanya merupakan sinyal EKG hasil proses rekonstruksi.



Gambar 8. Tampilan Aplikasi *Mobile* Berbasis Android Untuk Hasil Rekonstruksi Sinyal EKG Data Uji 1 (bs10089601)

4. KESIMPULAN

Pada penelitian ini telah dibangun sebuah sistem pengamanan transmisi sinyal EKG secara daring melalui jaringan *Internet*. Metode anonimasi yang digunakan adalah metode *Jusak-Seedahmed*. Berdasarkan hasil pengujian didapatkan bahwa algoritma *Jusak-Seedahmed* dapat digunakan untuk melakukan anonimasi sinyal EKG dan juga proses rekonstruksi sinyal EKG. Dalam penelitian ini telah digunakan 3 (tiga) macam sinyal EKG dengan frekuensi berbeda-beda, yaitu 250 Hz, 500 Hz, 1000 Hz pada 2 (dua) orang yang berbeda. Pengujian secara korelasi silang antara sinyal hasil rekonstruksi dan sinyal EKG asli sebelum anonimasi menghasilkan korelasi sebesar 1 pada *lag*=0 untuk semua data uji sinyal EKG. Selain itu pengujian terhadap variasi panjang kunci rahasia menunjukkan bahwa perubahan panjang kunci rahasia (dalam penelitian ini digunakan panjang kunci 128 karakter dan 256 karakter) tidak mempengaruhi waktu pemrosesan anonimasi. Waktu pemrosesan anonimasi hanya dipengaruhi oleh panjang data sinyal EKG akibat adanya perbedaan jumlah pada pengambilan data dengan frekuensi cuplik yang berbeda. Untuk memudahkan dokter melakukan proses pengamatan terhadap sinyal EKG, aplikasi *mobile* berbasis Android telah dibangun untuk dapat menampilkan sinyal EKG hasil rekonstruksi.

UCAPAN TERIMA KASIH

Ucapan terimakasih kami sampaikan kepada bagian Penelitian dan Pengabdian kepada Masyarakat, Institut Bisnis dan Informatika Stikom Surabaya yang telah membantu dalam hal pendanaan penulisan laporan penelitian ini.

DAFTAR RUJUKAN

Andrews, J., Buzzi, S., Choi, W., Hanly, S., Lozano, A., Soong, A., & Zhang, J. (2014). What will 5G be? *IEEE Journal on Selected Areas in Communications, 32*(6), 1065-1082.

Atzori, L., Iera, A., & Morabito, G. (2012). Internet of Things: a survey. *Computer Networks, 54*(15), 2787-2805.

Hadiyoso, S., Julian, M., Rizal, A., & Aulia, S. (2015). Pengembangan Perangkat EKG 12 Lead dan Aplikasi Client-Server untuk Distribusi Data. *Jurnal ELKOMIKA, 3*(2), 91-105.

Islam, S., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*, 678-708.

Jusak, J., & Mahmoud, S. (2018). A Novel and Low Processing Time ECG Security Method Suitable for Sensor Node Platforms. *International Journal of Communication Networks and Information Security, 10*(1), 213-222.

Jusak, J., & Puspasari, I. (2015). Wireless Tele-auscultation for Phonocardiograph Signal Recording Through the Zigbee Networks. *IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob)*, (hal. 95-100). Bandung, Indonesia.

Jusak, J., Pratikno, H., & Putra, V. H. (2016). Internet of Medical Things for Cardiac Monitoring: Paving the Way to 5G Mobile Networks. *IEEE Int. Conference on Communication, Networks and Satellite (COMNETSAT 2016)*, (hal. 75-79). Surabaya, Indonesia.

Mahmmoud, S. (2016). A Generelized Wavelet Packet-Based Anonimisation Approach for ECG Security Application. *Security and Communication Networks, 9*(18), 6137-6147.

Pinto, J. R., Cardoso, J. S., & Laurenco, A. (2018). Evolution, Current Challenges, and Future Possibilities in ECG Biometrics. *IEEE Access*(6), 34746-34776.

Sufi, F., & Khalil, I. (2008). Enforcing Secured ECG Transmission for Realtime Monitoring: a Joint Encoding, Compression, and Encryption Mechanism. *Security and Communication Networks, 1*(5), 389-405.

WHO. (2014). Non-communicable Disease Country Profiles 2014. *Switzerland: WHO Document Production Services*.

Yang, Z., Zhou, Q., Lei, L., Zheng, K., & Xiang, W. (2016). An IoT-Cloud Based. *Journal of Medical Systems Wearable ECG Monitoring Systems for Smart Healthcare, 40*, 286.