IMPLEMENTASI ALGORITMA KRIPTOGRAFI PADA SISTEM *BIOMETRIC PAYMENT*

IMPLEMENTATION OF CRYPTOGRAPHY ALGORITHM FOR BIOMETRIC PAYMENT

Ahmad Amran[1], Surya Michrandi Nasution, S.T., M.T.[2], Fairuz Azmi, S.T., M.T.[3]

[2,3]Fakultas Elektro dan Telekomunikasi Institut Teknologi Telkom, Bandung
[1]ammrann@gmail.com [2]michrandi@telkomuniversity.ac.id
[3]azme27@gmail.com

ABSTRAK

Perkembangan teknologi yang saat ini berkembang semakin pesat membantu memudahkan masyarakat luas dari segi pengiriman dan penyimpanan data. Dibalik manfaat tersebut ada bahaya yang mengancam yang tidak disadari oleh kebanyakan user (pengguna teknologi) pemula, yaitu penyadapan dan perubahan data. Perlu adanya suatu solusi yang dapat menyikapi dalam menjaga keamanan tersebut, kriptografi merupakan salah satu jawabannya.

Dalam penelitian ini, di implementasikan algoritma kriptografi simetris untuk mengamankan sistem pembayaran biometrik berbasis otentikasi sidik jari. Konsentrasi penelitian ini terletak pada pengimplementasian algoritma kriptografi Camellia dalam perancangan sistem pembayaran biometrik yang berperan dalam meningkatkan keamanan komunikasi data.

Hasil pengujian pada sistem ini menunjukkan bahwa Algoritma dapat diimplementasikan pada Biometric Payment. Rata-rata waktu proses enkripsi membutuhkan waktu 0.00994 detik lebih lama dibandingkan waktu proses dekripsi dan lama waktu yang dibutuhkan dalam tiap proses enkripsi dan dekripsi dipengaruhi panjang kunci yang dipakai. Nilai Avalanche Effect diperoleh dari rata-rata kedua skenario pengujian sebesar 55.5855%.
Kata Kunci: Algoritma, Kriptografi, Simetris, Camellia, Biometric Payment.

ABSTRACT

The development of technology that is currently growing more rapidly helps facilitate the wider community in terms of delivery and storage of data. Behind these benefits there is a danger that is not realized by most users (the technology) novice, which intercepts and changes the data. The solution that can respond in maintaining security is needed, cryptography is one of the answers.

In this research, implemented a symmetric cryptographic algorithm to secure payment system based on fingerprint authentication. The concentration of this research lies in the implementation symmetric cryptographic algorithms in the design of biometric payment systems that play a role in maintaining the security of data communications.

The test results on this system shows that the algorithm can be implemented on Biometric Payment. Time encryption process takes 0.00994 seconds longer than the time the decryption process and the times needed are affected by the key size that is used to do the encryption and decryption. The average of Avalanche Effect obtained from the two scenarios is 55.5855%.
Keywords: Algorithm, Cryptography, Symmetric, Camellia, Biometric Payment.

1. Pendahuluan

Teknologi dan informasi saat ini telah memberikan dampak yang signifikan di dalam berbagai bidang. Termasuk salah satunya yaitu dalam hal pertukaran data, dimana kemampuan untuk mengakses suatu data dapat dilakukan dengan cepat dan akurat menjadi sangat esensial bagi sebuah organisasi maupun individu. Seiring dengan perkembangan tersebut, memungkinkan pengiriman data menjadi relatif lebih cepat dan murah. Dilain pihak, pengiriman data jarak jauh melalui jaringan internet, gelombang radio maupun media lain yang digunakan masyarakat luas sangat memungkinkan bagi pihak lain untuk menyadap dan mengubah data yang dikirim. Oleh sebab itu, proses enkripsi diperlukan untuk mengamankan data (informasi) yang dikirim dalam upaya mengatasi kejahatan yang bisa berupa pencurian data maupun manipulasi data oleh penjahat, maka akan diimplementasikan sebuah sistem keamanan yang bisa menjaga keamanan pengiriman data dari *client-server*, sehingga proses pembayaran akan bisa dilakukan dengan aman [5].

Terdapat banyak algoritma kriptografi, masing-masing algoritma memiliki karakter dan spesifikasi yang berbeda. Salah satu jenis algoritma kriptografi adalah blok *cipher* yang menggunakan kunci simetris, contoh: AES, DES, *Camellia*, Threefish, dan TDEA.

Dari algoritma kriptografi yang ada, dipilih algoritma kriptografi *Camellia*. *Camellia* dipilih karena sudah diakui oleh ISO (*International Organization for Standardization*) dan terpilih bersama tiga algoritma lain dari 42 algoritma yang diajukan pada proyek NESSIE yang diprakarsai oleh *Information Society Technologies* (IST) dari European Union (EU) [3]. Algoritma ini akan di uji implementasinya pada sistem *biometric payment* yang dibangun menggunakan bahasa pemrograman Java. Parameter performansi yang diukur dan dibandingkan meliputi waktu proses dan *avalanche effect.*

2. Landasan Teori

2.1 *Biometric payment* [1]

Biometrik adalah ilmu dan teknologi pengukuran dan statistik yang menganalisis data biologis. Dalam teknologi informasi, biometrik biasanya mengacu kepada teknologi untuk mengukur dan menganalisis karakteristik tubuh manusia seperti sidik jari, retina mata dan iris, pola suara, pola wajah, dan pengukuran tangan, terutama untuk tujuan otentikasi. Solusi pembayaran melalui biometrik sidik jari terdiri dalam sistem *self-installing* USB yang memungkinkan untuk membaca sidik jari pelanggan, yang sebelumnya telah terdaftar dalam sistem, untuk melakukan pembayaran tanpa uang atau kartu kredit. Keuntungan pembayaran biometrik meliputi: peningkatan keamanan bagi pengguna; transaksi cepat; pengguna tidak perlu membawa uang tunai, cek atau kartu kredit; dan biaya yang lebih rendah per transaksi bagi pedagang, dibandingkan dengan biaya *debit* atau *charge card standard*.

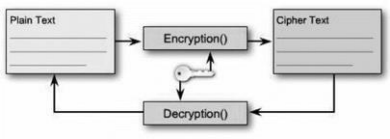
Otentikasi dengan verifikasi biometrik menjadi semakin umum dalam sistem keamanan perusahaan dan masyarakat, elektronik konsumen dan aplikasi titik penjualan (POS). Selain keamanan, kekuatan pendorong di belakang verifikasi biometrik adalah memberikan kenyamanan. Perangkat biometrik, seperti *scanner* jari, terdiri dari pembaca atau *scanning* perangkat dan *database* yang menyimpan data biometrik untuk perbandingan. Untuk mengkonversi *input* biometrik, aplikasi perangkat lunak yang digunakan untuk mengidentifikasi titik-titik tertentu dari data *match point*. Untuk mencegah pencurian identitas, data biometrik dienkripsi menggunakan algoritma kriptografi ketika diambil. Selain itu, titik biometrik perangkat penjualan *database* dapat digunakan bersama oleh beberapa toko atau oleh asosiasi bisnis, sehingga mudah mendapatkan loyalitas pelanggan karena dapat menggunakan solusi pembayaran sidik jari ini di salah satu toko-toko yang terkait. Sistem pembayaran biometrik memberikan fasilitas, keamanan, kecepatan dan kenyamanan untuk pembayaran di toko-toko, restoran, dll. Sistem pembayaran biometrik menguntungkan semua sektor yang terlibat, baik pelanggan ataupun pengusaha. Ini memberikan kenyamanan lebih, sehingga menghilangkan *margin of error* dalam perpindahan uang ketika pelanggan membayar tunai di meja kasir. Hal ini juga lebih aman, sehingga staf tidak perlu menggunakan uang dan juga sistem menghilangkan penggantian identitas karena kartu pencurian.

2.2 Kriptografi

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga data atau pesan agar tetap aman saat dikirimkan dari pengirim ke penerima tanpa mengalami gangguan. Aspek keamanan kriptografi[2].

2.2.1 Kriptografi Kunci Simetris[6]

Suatu algoritma kriptografi termasuk dalam kategori algoritma kunci simetris jika pada proses enkripsi dan dekripsi menggunakan kunci yang sama. Sebelum melakukan pengiriman pesan, pengirim dan penerima harus memilih suatu suatu kunci tertentu yang sama untuk dipakai bersama, dan kunci ini haruslah rahasia bagi pihak yang tidak berkepentingan sehingga algoritma ini disebut juga algoritma kunci rahasia (*secret-key algorithm*).



Gambar 2.1: proses enkripsi kriptografi simetris

2.2.2 *Block Cipher*[7]

Algoritma kriptografi beroperasi pada plainteks atau *ciphertext* dalam bentuk blok bit, biasanya berukuran 64 bit atau lebih. Dengan *block cipher*, *plaintext* yang sama akan selalu mengenkripsi blok dengan hasil *ciphertext* yang sama dengan kunci yang sama.

2.3 Algoritma *Camellia*

Algoritma *Camellia* merupakan jenis algoritma *block cipher* simetris yang dikembangkan di Jepang oleh perusahaan NTT dan Mitsubishi pada tahun 2000 dan sudah diakui untuk digunakan oleh ISO/IEC, proyek NESSIE yang diprakarsai European Union, dan proyek Japanese CRYPTREC. Algoritma ini bekerja pada ukuran blok 128 bit dan panjang kunci 128, 192, dan 256 bit.
Berikut adalah simbol-simbol yang digunakan dalam proses enkripsi dan enkripsi algoritma *Camellia* :

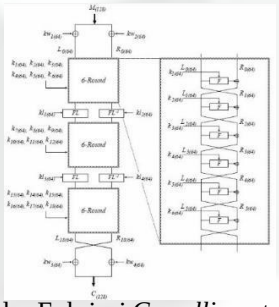
$\oplus$	bitwise exclusive-OR operation.
$\|\|$	concatenation of the two operands.
$\lll_n$	left circular rotation of the operand by n bits.
$\cap$	bitwise AND operation.
$\cup$	bitwise OR operation.
$\overline{x}$	bitwise complement of x.

Gambar 2.2 simbol-simbol operasi Algoritma *Camellia*[4]

Dalam prosesnya, algoritma *Camellia* memiliki beberapa fungsi untuk menjalankan proses enkripsi dan dekripsi[4].

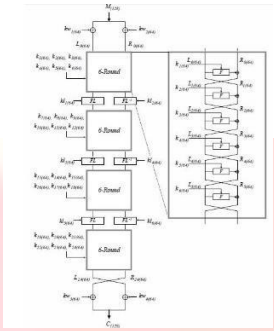
2.3.1 Proses Enkripsi *Camellia*

- **Kunci 128-bit**



Gambar 2.3 Prosedur Enkripsi *Camellia* untuk Kunci 128 bit [4]

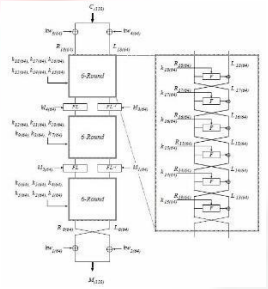
- **Kunci 192-bit dan 256-bit**



Gambar 2.4 Prosedur Enkripsi *Camellia* untuk Kunci 192/256 bit[4]

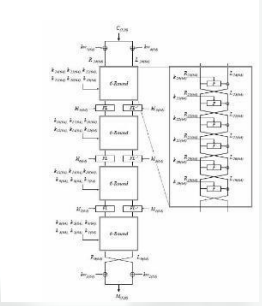
2.3.2 Proses Dekripsi *Camellia*

- **Kunci 128-bit**



Gambar 2.5 Prosedur Dekripsi *Camellia* untuk Kunci 128 bit[4]

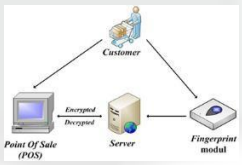
- **Kunci 192-bit dan 256-bit**



Gambar 2.6 Prosedur Dekripsi *Camellia* untuk Kunci 192/256 bit[4]

3. Perancangan Sistem

3.1 Gambaran Umum Sistem

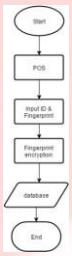


Gambar 3.1 Perancangan Umum Sistem

Gambaran umum sistem pada gambar di atas mengiilustrasikan bahwa akan dirancang *Point Of Sales* (POS) yang terkoneksi dengan *server* yang terintegrasi dengan *fingerprint* modul dan akan menyimpan data *customer* ke *database*. POS dalam perancangan ini sebagai suatu sistem aplikasi yang berfungsi untuk melakukan pendaftaran *Customer*, *top-up*, dan transaksi penjualan.

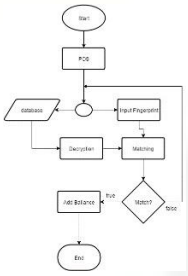
Pada penelitian ini, sistem yang dirancang adalah aplikasi algoritma kriptografi yang berfungsi untuk merahasiakan pertukaran pesan/data yang dikirim antar *client-server*, agar tidak dapat dibaca oleh orang yang tidak berhak. Aplikasi ini menggunakan algoritma kriptografi *Camellia* dan dilakukan uji performansi dalam implementasinya pada sistem *biometric payment.*

3.1.1 Diagram Alir Perancangan Umum Sistem



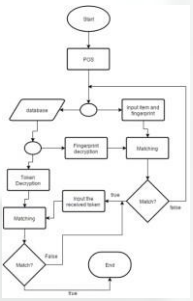
Gambar 3.2 Diagram Alir Proses *Enrollment*

Pada diagram alir diatas dapat dilihat proses *enrollment* pada perancangan umum sistem. Saat pelanggan meng*input*kan sidik jari, sidik jari di enkripsi lalu disimpan di *database*.



Gambar 3.3 Diagram Alir Proses *Top-up*

Pada diagram alir diatas dapat dilihat proses *top-up* pada perancangan umum sistem. Saat pelanggan meng*input*kan sidik jari untuk verifikasi, sistem POS memanggil data sidik jari dalam *database* untuk dicocokkan yang sebelumnya melalui proses dekripsi terlebih dahulu.



Gambar 3.4 Diagram Alir Proses Transaksi Penjualan Perancangan Umum Sistem

3.2 Deskripsi Sistem Kriptografi

Tugas utama yang dilakukan oleh sistem pada penelitian ini adalah melakukan enkripsi dan dekripsi data pada sistem *biometric payment*. Data terpilih yang disimpan ke *database* akan melalui proses enkripsi dan melalui proses dekripsi saat dipanggil oleh sistem aplikasi POS untuk digunakan. Data yang dipilih untuk diterapkan proses kriptografi pada sistem *biometric payment* ada dua, yaitu: sidik jari pelanggan, dan token yang digunakan untuk setiap transaksi.

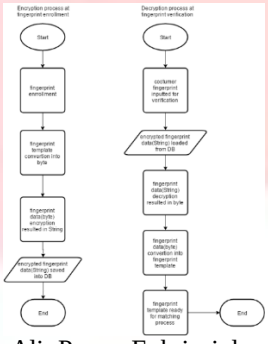
3.3 Analisa Kebutuhan Sistem

Sistem yang dibangun dalam penelitian ini akan diimplementasikan pada aplikasi POS sistem *biometric payment* untuk mengetahui apakah algoritma layak untuk diterapkan dengan melakukan analisa

performansi pada algoritma *Camellia* yang melakukan proses enkripsi dan dekripsi menggunakan ukuran kunci 128, 192, dan 256 bit.

3.4 Sistem Algoritma Kriptografi

3.4.1 Diagram Alir Proses Enkripsi dan Dekripsi



Gambar 3.5 Diagram Alir Proses Enkripsi dan Dekripsi *Fingerprint*

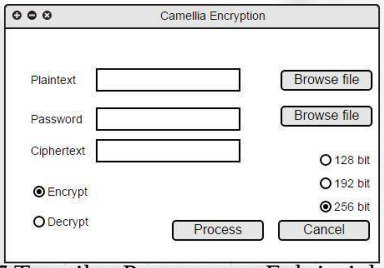
Pada diagram alir diatas dapat dilihat proses enkripsi dan dekripsi suatu *fingerprint*. Pada proses enkripsi, data *template fingerprint* yang dimasukkan pelanggan saat *enrollment* akan dikonversi menjadi data *byte* agar bisa dilakukan proses enkripsi, data *fingerprint* yang sudah di enkripsi berupa String kemudian disimpan di dalam *database.* Saat pelanggan menginputkan sidik jari untuk diverifikasi pada proses *top-up* ataupun transaksi, proses dekripsi dilakukan pada data *fingerprint* yang tersimpan dalam *database* yang kemudia menghasilkan data *fingerprint* dalam bentuk *byte*, lalu data *fingerprint(byte)* dikonversi kembali menjadi data *template fingerprint* untuk dicocokkan dengan *template fingerprint* yang diinputkan pelanggan, apabila *fingerprint* cocok maka pelanggan terverifikasi.

3.4.2 *Avalanche effect*

Avalanche effect merupakan suatu output *ciphertext* yang diinginkan dari algoritma enkripsi, dihitung dengan rumus :

$$Avalanche\ Effect = \frac{Jumlah\ bit\ yang\ berubah\ (chipertext)}{Jumlah\ bit\ (chipertext)}$$

3.5 Perancangan Antarmuka



Gambar 3.7 Tampilan Perancangan Enkripsi dan Dekripsi

3.6 Skenario Pengujian

3.6.1 Pengujian Waktu Enkripsi dan Dekripsi

Skenario pengujian waktu proses enkripsi dan dekripsi terhadap data *fingerprint* pada algoritma *Camellia* dengan kunci 128, 192 dan 256 bit.

3.6.2 Pengujian Keamanan Sistem

Pengujian *Avalanche effect* dilakukan dengan dua skenario :

1) memproses *data fingerprint* yang berbeda dan menggunakan sebuah kunci yang sama.

2) memproses sebuah *data fingerprint* dan menggunakan kunci yang berbeda.

3.6.3 Nilai *Big-o Notation*

Pencarian nilai *Big-o Notation* dilakukan dengan melakukan analisis dari algoritma *Camellia* dilihat dari ukuran masukan terhadap algoritma dan waktu yang dibutuhkan dibandingkan dengan ukuran masukan.

3.6.4 Perbandingan Hasil Pengujian

Membandingkan hasil dari proses percobaan dan kemudian membuat analisa berdasarkan data-data yang telah didapatkan dari percobaan.

4. Perancangan Sistem

4.1 Implementasi Sistem

Pada bab ini akan dilakukan implementasi terhadap sistem yang telah dibuat dan dilakukan pengujian untuk menganalisis hasil dari sistem yang dibuat.

4.2 Implementasi Perangkat

Kebutuhan yang diperlukan untuk menunjang penelitian ini terdiri dari kebutuhan perangkat lunak dan perangkat keras. Berikut ini adalah perangkat-perangkat yang digunakan dalam penelitian ini, berupa perangkat keras (*hardware*), perangkat lunak (*software*).

4.2.1 Kebutuhan Perangkat Lunak

Spesifikasi perangkat lunak yang digunakan dalam penelitian ini adalah sebagai berikut :

a) sistem operasi Windows 7

b) *java Development Kit 1.8.0 (JDK 1.8.0)*

c) *java Runtime Environment 1.8.0 (JRE 1.8.0)*

d) XAMPP v3.1.0

4.2.2 Kebutuhan Perangkat Keras

Spesifikasi perangkat keras yang digunakan dalam penelitian ini adalah sebagai berikut:

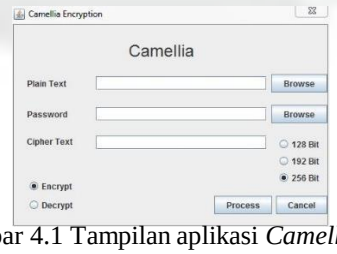
a) *processor* Intel Core 2 Duo

b) RAM 4 GByte

c) *harddisk* 1TByte

4.3 Implementasi Antarmuka

Implementasi antarmuka merupakan tampilan dari *system biometric payment* yang berupa aplikasi POS. Berikut merupakan tampilan antarmuka POS yang telah dibuat dimana proses enkripsi dan dekripsi diimplementasikan :



Gambar 4.1 Tampilan aplikasi *Camellia* terpisah

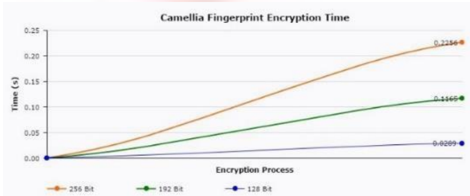
4.4 Pengujian Performansi

4.4.1 Pengujian Waktu Enkripsi *Fingerprint*

Pengujian dilakukan dengan menghitung waktu rata-rata yang dibutuhkan algoritma *Camellia* untuk mengenkrip beberapa data *fingerprint*. Plaintext atau isi dari template *fingerprint* yang akan diuji proses enkripsi dan dekripsi dapat dilihat pada table berikut :

Tabel 4.1 Contoh Plaintext *Fingerprint*

ID_1.*Fingerprint*1.txt	珣한œ췬엶顥鋫剱□ض鱶笛 ىう. .
ID_1.*Fingerprint*2.txt	珣흜϶꺳ق□繘 |嘣垄 □꾗蔟. .

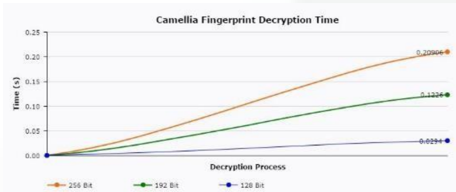


Gambar 4.2 Perbandingan Waktu Rata-rata Enkripsi *Fingerprint*

Berdasarkan tabel hasil pengujian waktu enkripsi algoritma *Camellia* pada *data fingerprint* diatas, semakin panjang kunci yang dipakai, maka semakin banyak waktu yang dibutuhkan algoritma *Camellia* untuk melakukan proses enkripsi.

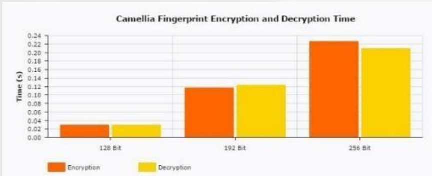
4.4.2 Pengujian Waktu Dekripsi *Fingerprint*

Pengujian waktu dekripsi dilakukan dengan menghitung waktu rata rata yang dibutuhkan algoritma *Camellia* untuk mendekripsi sebuah data *fingerprint*.



Gambar 4.3 Perbandingan Waktu Rata-rata Dekripsi *Fingerprint*

Berdasarkan tabel hasil pengujian waktu dekripsi algoritma *Camellia* pada data *fingerprint* diatas, jika ukuran kunci yang dipakai semakin panjang, maka semakin banyak waktu yang dibutuhkan algoritma *Camellia* untuk melakukan proses dekripsi.

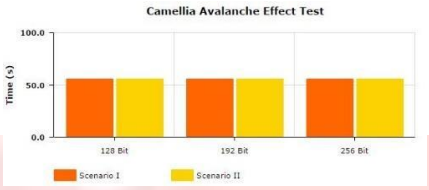


Gambar 4.4 Perbandingan Waktu Rata-rata Enkripsi dan Dekripsi *Fingerprint*

Pada diagram balok diatas dapat dilihat perbandingan waktu enkipsi dan dekripsi data *fingerprint*, terlihat bahwa rata-rata proses enkripsi membutuhkan waktu yang lebih lama daripada waktu dekripsi dan semakin panjang *key* yang digunakan maka semakin lama waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi.

4.4.3 Pengujian Keamanan Sistem

Pengujian keamanan sistem dengan mengambil sebuah *parameter* kamanan yaitu *Avalanche effect*.



Gambar 4.7 *Avalanche effect* Algoritma *Camellia*

Nilai AE rata-rata yang diperoleh dari kedua skenario sebesar 55.5928% pada *Camellia* 256 bit, 55.7154% pada *Camellia* 192 bit, dan 55.4485% pada *Camellia* 128 bit.

4.4.4 Nilai *Big-o Notation*

Big-o Notation merupakan pengujian yang digunakan untuk mengetahui seberapa kompleksitas suatu algoritma. Untuk algoritma *Camellia*, nilai kompleksitas yang dimiliki adalah O(N) karena *Camellia* merupakan algoritma yang bekerja dengan panjang *block* yang tetap yaitu 128 bit yang berarti memiliki nilai kompleksitas O(1). Dengan notasi N yang mendefinisikan banyak *block* yang harus dikerjakan untuk melakukan proses enkripsi atau dekripsi suatu *file*, jika *Camellia* harus melakukan proses sebanyak N *block* maka nilai *Big-o Notation* nya adalah O(N). Untuk proses *key scheduling* pada *Camellia* memiliki nilai O(1) karena untuk masing-masing *key* berukuran 128 bit, 192 bit ataupun 256 bit, memiliki waktu proses yang sama baik dari masukan aplikasi maupun melalui proses padding dan *key* stretching sehingga membuat berapapun ukuran *key* yang dimasukkan maka waktu prosesnya sama.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Kesimpulan yang dapat diambil dari penelitian ini adalah :

1) berdasarkan hasil pengujuan yang telah dilakukan, semakin panjang *key* yang digunakan maka semakin lama waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi dan rata-rata proses enkripsi *fingerprint* membutuhkan waktu yang lebih lama daripada proses waktu dekripsi dengan selisih rata-rata waktu semua bit sebesar 0.00994 detik.

2) dari hasil kedua skenario pengujian *avalanche effect*, disimpulkan bahwa algoritma *Camellia* dapat dikatakan tangguh dengan nilai AE rata-rata yang diperoleh dari kedua skenario sebesar 55.5928% pada *Camellia* 256 bit, 55.7154% pada *Camellia* 192 bit, dan 55.4485% pada *Camellia* 128 bit.

3) berdasarkan implementasi dan pengujian yang telah dilakukan dapat dilihat bahwa algoritma memiliki waktu rata-rata enkripsi dan dekripsi sebesar 0.209 detik dengan nilai *avalanche effect* diatas 50%. Dari pengujian tersebut dapat diambil kesimpulan bahwa algoritma kriptografi *Camellia* bisa diterapkan dalam sistem *biometric payment.*

5.2 Saran

Saran untuk penelitian selanjutnya adalah :

1) untuk pengembangan selanjutnya agar adanya proses modifikasi atau riset lebih lanjut untuk mendapatkan performansi algoritma *Camellia* yang lebih optimal agar dapat menghasilkan nilai *avalanche effect* yang lebih baik.

2) pengujian dan pengimplementasian pada *data biometric* jenis lainnya, seperti *face, iris,* atau *vein recognition.*

DAFTAR PUSTAKA

[1] Aranuma, F.O. and Ogunniye, G.B. 2012. “Enchanced Biometric Authentication System for Efficient and Reliable e-Payment System in Nigeria,” International Journal of Applied Information Systems (IJAIS), Vol.4.

[2] Ariyus, Dony, *Kriptografi: Keamanan Data Dan Komunikasi*, Graha Ilmu, September 2005.

[3] *Denning D., Irvine J., and Devlin M. 2005. "*A High Throughput Fpga *Camellia* Implementation," IEEE, no., pp.137-140 vol.1.

[4] Ichikawa, Aoki. Matsui, Kanda. Nakajima, Moriai. Tokita. (2000). Specification of *Camellia* – A 128– bit Block Cipher. NTT and Mitsubishi Electric Corporation. Japan.

[5] Khan, M. Hussain, S. and Imran, M. 2013 "Performance Evaluation of Symmetric Cryptography Algorithms: A Survey," Information Technology & Electrical Engineering (ITEE), Vol.2.

[6] Munir, R, 2006, *Kriptografi*, Bandung: Informatika Bandung.

[7] V. Rijmen J. Daemen, "Rijndael: The advanced encryption standard," Dr. Dobb˝s Journal, pp. 137-139, March 2001.