Sistem Pengamanan Data Menggunakan Kriptografi AES dan Blockchain Berbasis Android

Dhiya Calista[*1], Al Farissi[*2], Mastura Diana Marieska[*3]
[*1,2,3]Jurusan Teknik Informatika, Universitas Sriwijaya,
Jl. Palembang – Prabumulih Km. 32 Inderalaya Ogan Ilir 30662
e-mail: **[*1]**dhiyacalista@gmail.com, [2]alfarissi.ilkom@gmail.com, [3]diana@informatika.org

Abstrak

Keamanan data atau informasi merupakan hal yang sangat penting untuk diperhatikan bagi pengguna internet sekarang, agar data atau informasi yang dimiliki tidak diserang oleh pihak yang tidak bertanggung jawab. Maka, dalam penelitian ini akan dilakukan suatu implementasi dari kombinasi kriptografi Blockchain dan AES agar dapat terhindar dari serangan aktif maupun pasif yang dilakukan oleh penyerang. Metode Blockchain dapat mendeteksi perubahan data dari penyerang secara cepat dan mudah. Namun, metode Blockchain masih dapat diserang secara pasif, maka dari itu metode AES dipadukan dengan Blockchain sebagai pelengkap yang digunakan untuk mengenkripsi data dari plaintext menjadi ciphertext agar data atau informasi yang ada dapat terhindar dari serangan aktif ataupun pasif. Dalam penelitian ini, metode pengembangan perangkat lunak yang digunakan adalah metode Rational Unified Process (RUP) dan pengujian yang dilakukan adalah pengujian ketahanan Blockchain terhadap serangan modifikasi dan pengujian Avalanche Effect pada metode AES.

Kata kunci*— Kriptografi, Blockchain, AES, RUP, Avalanche Effect*

Abstract

Data or information security is a very important thing for internet users to pay attention to now, so that the data or information owned is not attacked by irresponsible parties. So, in this research, an implementation of a combination of Blockchain and AES cryptography will be carried out in order to avoid active and passive attacks by attackers. Blockchain method can detect data changes from attackers quickly and easily. However, Blockchain method can still be attacked passively, therefore AES method is combined with Blockchain as a complement that is used to encrypt data from plaintext to ciphertext so that existing data or information can be avoided from active or passive attacks. In this research, the software development method is using Rational Unified Process (RUP) method and the tests carried out are Blockchain resistance to modification attacks testing and Avalanche Effect testing on AES method.

Keywords— *Cryptography, Blockchain, AES, RUP, Avalanche Effect*

1. PENDAHULUAN

Teknologi informasi yang telah berkembang secara pesat pada saat ini semakin memberikan kemudahan dalam melakukan aktivitas, mulai dari aktivitas sehari-hari yang ringan maupun aktivitas lainnya yang dilakukan di perkantoran, pendidikan, industri, pemerintahan, dan meluas ke seluruh aspek kehidupan. Teknologi informasi ini tentunya akan memberikan kemudahan-kemudahan dalam melakukan aktivitas, misalnya untuk memesan tiket dalam melakukan perjalanan, melakukan kegiatan belajar mengajar secara daring, pembayaran kartu kredit, pembayaran listrik, air, dan lain sebagainya hanya dapat dilakukan dengan menggunakan telepon seluler yang pada saat ini telah dimiliki hampir oleh setiap orang dengan

kuota internet yang terjangkau sehingga lebih memudahkan dalam melakukan kegiatan-kegiatan tersebut dimana saja dan kapan saja, selagi masih ada jaringan internet. Tetapi harus disadari bahwa kemudahan yang didapat pada saat ini dengan ketersediaan aplikasi dalam segala aspek tentunya tidak dapat menjamin keamanan data atau informasi pengguna yang ada di dalam jaringan internet yang besar. Maka dari itu, perlu diterapkan ilmu kriptografi yang dapat menjaga keamanan data atau informasi pengguna.

Kriptografi ilmu sekaligus seni untuk menjaga keamanan pesan (*message*). Pengertian lain kriptografi yaitu suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi [1].

Algoritma kriptografi dapat dibagi ke dalam kelompok algoritma simetris dan algoritma asimetris. Algoritma simetris merupakan algoritma kriptografi yang menggunakan kunci yang sama dalam proses enkripsi dan dekripsi [2]. *Advanced Encryption Standard* (AES) adalah algoritma kriptografi yang menjadi standar algoritma enkripsi kunci simetris pada saat ini. AES secara garis besar beroperasi pada blok 128-bit atau 16 karakter, yang berarti dapat digunakan untuk enkripsi teks [3]. Selain AES, *Blockchain* juga merupakan salah satu metode kriptografi yang dapat digunakan untuk mengamankan data atau informasi pengguna. *Blockchain* adalah kumpulan lebih dari satu blok yang membentuk rantai. Setiap blok memiliki 3 elemen yaitu data, nilai hash dari blok, dan nilai hash dari blok sebelumnya [4].

Maka dari itu, *Blockchain* merupakan metode yang tepat dalam mengamankan data pengguna dari serangan aktif agar penyerang tidak dapat mengubah data yang ada di dalam suatu blok. Namun, metode ini masih dapat diserang secara pasif yang dimana penyerang dapat menyadap data. Hal ini dikarenakan data yang ada di dalam suatu blok *Blockchain* masih belum ter-enkripsi. Maka dari itu, digunakanlah metode AES yang dapat meng-enkripsi data untuk dikombinasikan dengan metode *Blockchain* agar sistem pengamanan data pada penelitian ini dapat aman dari serangan aktif maupun pasif.

2. METODE PENELITIAN

Metode pengembangan perangkat lunak yang digunakan adalah metode pengembangan *Rational Unified Process* (RUP). Pada metode ini terdapat empat fase, yaitu fase insepsi, fase elaborasi, fase konstruksi, dan fase transisi.

2.1 Fase Insepsi

Pada fase ini dilakukan pembuatan pemodelan bisnis (*business modelling*) dan penentuan kebutuhan (*requirements*) yang juga berisi kebutuhan fungsional dan non-fungsional yang dibutuhkan oleh sistem. Selain itu, dilakukan juga tahapan analisis dan desain pada fase ini. Pada tahap analisis dilakukan analisa kebutuhan sistem dan analisa metode yang digunakan. Sementara pada tahap desain dilakukan perancangan diagram dan skenario *use case* serta perancangan diagram *activity*.

2.2 Fase Elaborasi

Pada fase ini dilakukan perancangan yang berkaitan dengan arsitektur sistem, yaitu perancangan basis data, perancangan antarmuka (*interface*), dan perancangan diagram sequence. Pada perancangan basis data dilakukan pembuatan *Entity Relationship Diagram* (ERD) sebagai rancangan dalam membuat basis data yang akan menjadi tempat penyimpanan data. Pada perancangan antarmuka dirancang sesuai dengan kebutuhan yang telah ditentukan sebelumnya.

2.3 Fase Konstruksi

Pada fase ini RUP dilakukan perancangan diagram kelas yang kemudian kelas-kelas tersebut diimplementasi menggunakan kode program ke dalam sistem bersamaan dengan ERD dan tampilan antarmuka yang telah dirancang pada fase sebelumnya. Fase konstruksi berfokus

kepada pengembangan sistem menggunakan bahasa pemrograman Kotlin dalam mengembangkan sistem berbasis Android. Pengembangan sistem dilakukan berdasarkan tahapan analisis dan perancangan yang telah dilakukan pada fase-fase sebelumnya.

2.4 Fase Transisi

Pada fase ini dilakukan perancangan pengujian berdasarkan *use case* yang telah dirancang pada fase insepsi. Selain itu, pada fase ini pula ditentukan perangkat yang akan digunakan untuk melakukan pengujian. Pengujian *Black Box* terhadap perangkat lunak dilakukan berdasarkan rancangan pengujian yang dibuat yang kemudian dicatat ke dalam tabel kasus uji. Selain pengujian *Black Box* berdasarkan *use case*, dilakukan pula pengujian ketahanan *Blockchain* terhadap serangan modifikasi dan pengujian *Avalanche Effect* pada metode AES.

3. HASIL DAN PEMBAHASAN

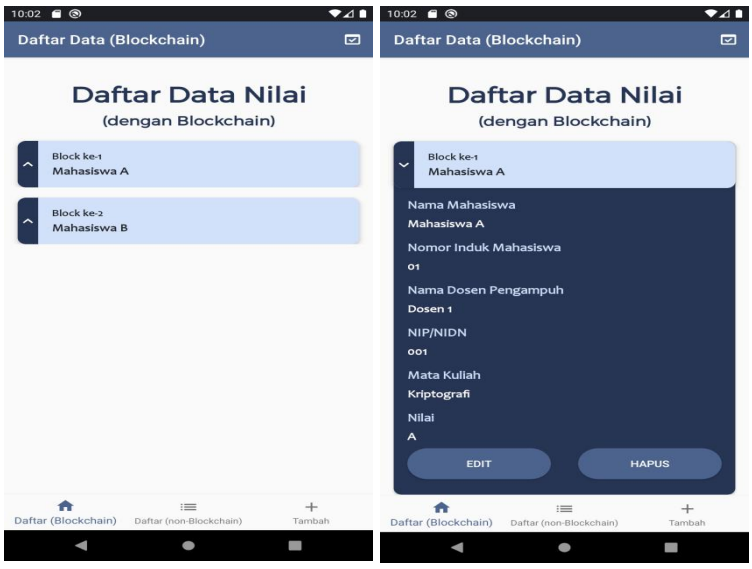
Pada bab ini akan dibahas mengenai hasil dari implementasi dan pengujian pada perangkat lunak yang telah dibangun. Hasil implementasi perangkat lunak merupakan hasil dari pengimplementasian fase-fase metode pengembangan perangkat lunak RUP yang telah diuraikan pada bab sebelumnya. Sementara, hasil pengujian perangkat lunak merupakan hasil dari pengujian kinerja metode AES dan *Blockchain*.

3.1 Hasil Implementasi Perangkat Lunak

Ada empat halaman yang di dalam perangkat lunak yang telah dibangun, yaitu halaman Daftar *Blockchain*, halaman Daftar *Non-Blockchain*, halaman Tambah, dan halaman Edit.

3.1.1 Halaman Daftar Blockchain

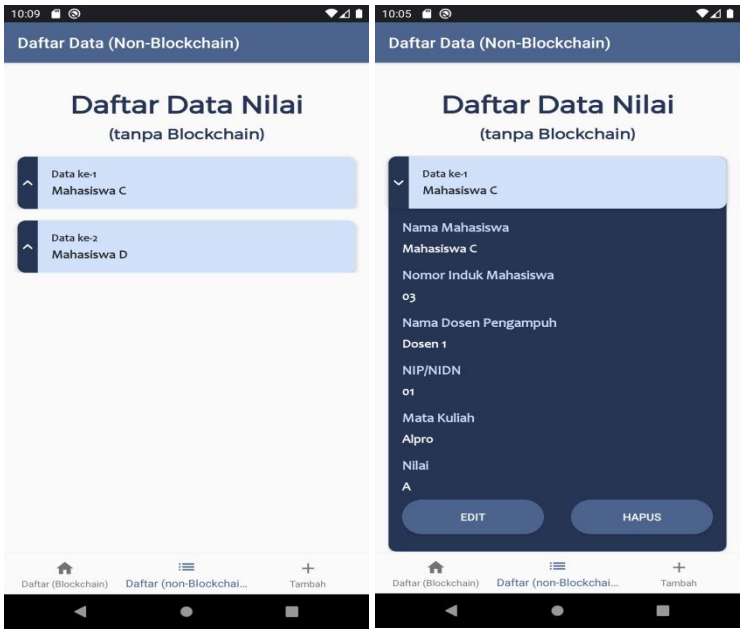
Pada halaman ini menampilkan seluruh data yang menggunakan metode pengamanan *Blockchain* dan AES. Data yang ditampilkan adalah nama mahasiswa, nomor induk mahasiswa, nama dosen, nomor induk pegawai/nomor induk dosen nasional kepemilikan dosen, mata kuliah, dan nilai mahasiswa. Pada halaman ini terdapat tombol cek validasi yang berada di *action bar* sebelah kanan atas. Tombol ini digunakan untuk memeriksa kevalidan *Blockchain*. Selain itu, terdapat pula tombol *drop down* untuk melihat detil data beserta tombol Edit dan Hapus. Tombol Edit dan Hapus digunakan untuk mengedit data *block* dan menghapus *block.* Hasil implementasi halaman ini dapat dilihat pada Gambar 1.



Gambar 1. Halaman Daftar *Blockchain*

3.1.2 Halaman Daftar Non-Blockchain

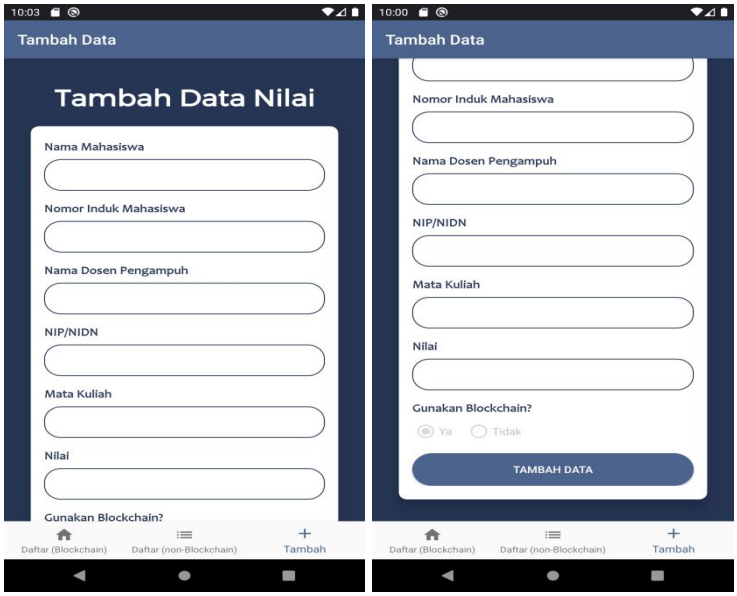
Pada halaman ini menampilkan seluruh data yang tidak menggunakan metode pengamanan *Blockchain* dan AES. Data yang ditampilkan sama dengan data pada halaman Daftar *Blockchain*. Sama seperti halaman Daftar Blockchain, terdapat pula tombol *drop down* untuk melihat detil data beserta tombol Edit dan Hapus. Tombol Edit dan Hapus digunakan untuk mengedit dan menghapus data. Hasil implementasi halaman ini dapat dilihat pada Gambar 2.



Gambar 2. Halaman Daftar *Non-Blockchain*

3.1.3 Halaman Tambah

Halaman ini digunakan untuk menginput data atau *block*. Terdapat 6 kolom data yang harus diinput dan 1 opsi untuk memilih penggunaan metode *Blockchain* dan AES, serta 1 tombol Tambah Data untuk mengirimkan data setelah mengisi seluruh data. Hasil implementasi halaman ini dapat dilihat pada Gambar 3.



Gambar 3. Halaman Tambah

3.1.4 Halaman Edit

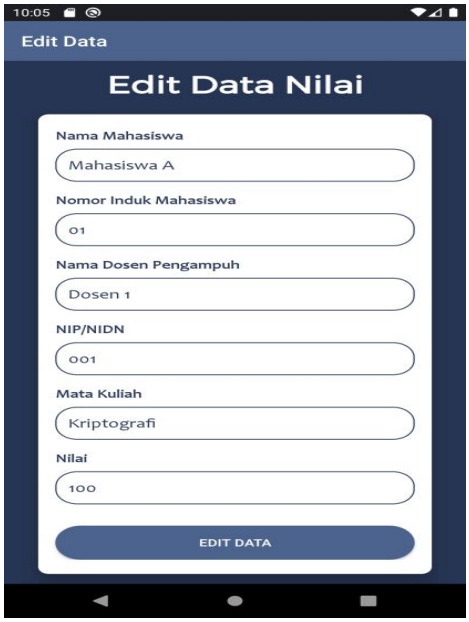
Halaman yang digunakan untuk mengedit data ataupun data *block* ini akan muncul setelah tombol Edit pada halaman Daftar *Blockchain* atau Daftar *Non-Blockchain* ditekan. Terdapat 6 kolom data yang harus diinput dan 1 tombol Edit Data untuk mengirimkan data setelah mengedit data. Hasil implementasi halaman ini dapat dilihat pada Gambar 4.

3.2 Hasil Pengujian Perangkat Lunak

Terdapat dua pengujian perangkat lunak yang dilakukan dalam penelitian ini, yaitu pengujian ketahanan *Blockchain* terhadap serangan modifikasi dan pengujian *Avalanche Effect* pada metode AES.

3.2.1 Hasil Pengujian Ketahanan Blockchain Terhadap Serangan Modifikasi

Pengujian ini dilakukan dengan melakukan pengamatan pada sejumlah masukan yang berkaitan dengan pengamanan menggunakan metode *Blockchain* dan menentukan kevalidan masukan tersebut. Terdapat total 28 kondisi yang berbeda sebagai masukan kondisi yang akan diuji pada pengujian ini. Hasil dari pengujian ini dapat dilihat pada Tabel 1.



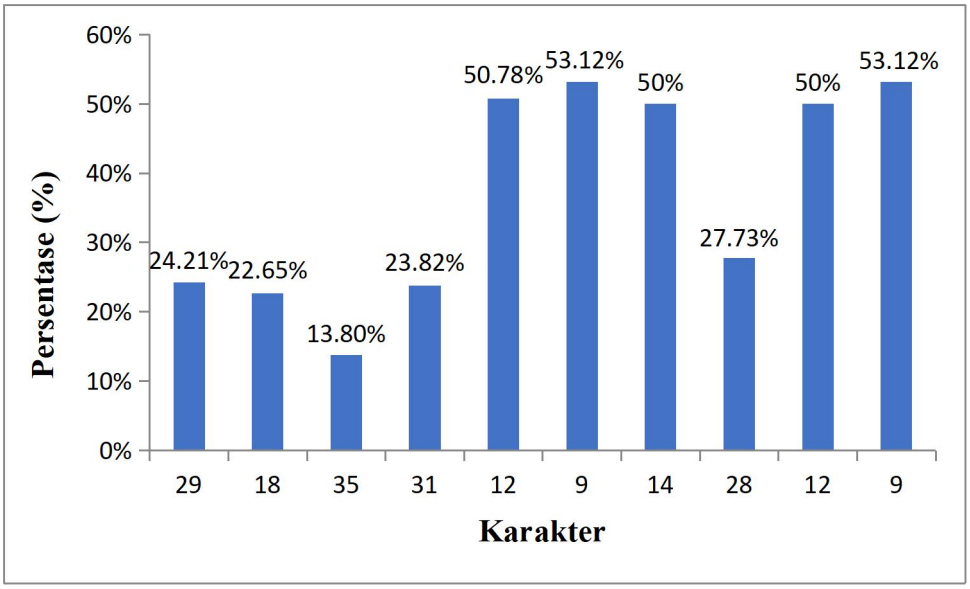
Gambar 4. Halaman Edit

Tabel 1. Pengujian Ketahanan *Blockchain* Terhadap Serangan Modifikasi

Pengujian *Blockchain*	Tidak Edit Data	Edit Data Pertama	Edit Data Tengah	Edit Data Terakhir
Tidak Hapus Data	Valid	Tidak Valid	Tidak Valid	Tidak Valid
Hapus Data Pertama	Valid	Valid	Tidak Valid	Tidak Valid
Hapus Data Tengah	Tidak Valid	Tidak Valid	Tidak Valid	Tidak Valid
Hapus Data Terakhir	Valid	Tidak Valid	Tidak Valid	Valid
Hapus Data Pertama dan Tengah	Valid	Valid	Valid	Tidak Valid
Hapus Data Pertama dan Terakhir	Valid	Valid	Tidak Valid	Valid
Hapus Data Tengah dan Terakhir	Valid	Tidak Valid	Valid	Valid

3.2.2 Hasil Pengujian Avalanche Effect pada Metode AES

Dalam pengujian ini terdapat dua buah *plaintext* yang berbeda satu bit yang dienkripsi dengan satu kunci yang sama. Pengujian ini dilakukan sebanyak 10 kali, sehingga terdapat total 20 buah *plaintext* dengan panjang karakter yang berbeda, serta 10 buah kunci. Hasil dari pengujian *Avalanche Effect* pada metode AES dapat dilihat pada Gambar 5.



Gambar 5. Grafik Pengujian *Avalanche Effect*

Hasil pengujian pada Gambar 5 menunjukkan bahwa metode kriptografi AES menghasilkan persentase sekitar 50%. Namun dapat dilihat bahwa semakin panjang suatu teks, maka hasil persentase dari *Avalanche Effect* akan semakin menurun.

4. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan pada bab sebelumnya, maka dapat diambil beberapa kesimpulan yaitu sebagai berikut.

1. Telah dilakukan pembangunan perangkat lunak yang mengombinasikan metode kriptografi AES dan *Blockchain* dalam menjaga keamanan data dari serangan aktif maupun pasif.
2. Dari hasil pengujian *Avalanche Effect* pada metode AES menunjukkan bahwa metode AES dinilai cocok untuk menjaga data dari serangan pasif dengan tingkat keamanan yang menengah ke tinggi dengan hasil persentase sekitar 50% untuk data yang memiliki panjang teks sekitar 16 karakter.
3. Hasil pengujian ketahanan metode *Blockchain* terhadap serangan modifikasi dengan masukan 28 kondisi yang berbeda menunjukkan bahwa serangan modifikasi dapat terdeteksi oleh *Blockchain* sehingga data dapat terjaga dari serangan aktif.

5. SARAN

Pada penelitian ini masih memiliki banyak kekurangan sehingga diperlukan rencana pengembangan di penelitian selanjutnya. Beberapa saran yang dapat disampaikan adalah sebagai berikut.

1. Menambahkan fitur input kunci AES kepada pengguna saat ingin menginput data untuk meningkatkan keamanan data enkripsi AES.
2. Meningkatkan keamanan kriptografi AES untuk teks yang lebih panjang.
3. Menggunakan mekanisme jaringan *peer-to-peer* dalam *Blockchain* untuk meningkatkan keamanan data *block* di dalam *Blockchain*.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada redaksi jurnal JUPITER yang telah memberi kesempatan kepada penulis sehingga artikel ini dapat diterbitkan.

DAFTAR PUSTAKA

[1] Munir, R. (2006). *Kriptografi.* Bandung: Informatika.

[2] Meko, D. A. (2018). Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data. *Jurnal Teknologi Terpadu*, 8.

[3] Tulloh, A. R., Permanasari, Y., & Harahap, E. (2016). Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen. *Jurnal Matematika UNISBA*, 7-8.

[4] Noorsanti, R. C., Yulianton, H., & Hadiono, K. (2018). BLOCKCHAIN - TEKNOLOGI MATA UANG KRIPTO (CRYPTO CURRENCY). *Prosiding SENDI_U*, 307.