SISTEM PENGAMANAN DATA MENGGUNAKAN KRIPTOGRAFI AES DAN BLOCKCHAIN BERBASIS ANDROID

Diajukan Untuk Menyusun Skripsi
di Jurusan Teknik Informatika Fakultas Ilmu Komputer UNSRI

Oleh :

Dhiya Calista
NIM : 09021381823105

Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2022

LEMBAR PENGESAHAN SKRIPSI

SISTEM PENGAMANAN DATA MENGGUNAKAN
KRIPTOGRAFI AES DAN BLOCKCHAIN
BERBASIS ANDROID

Oleh :

Dhiya Calista
NIM : 09021381823105

Palembang, 6 Januari 2022

Pembimbing I

Al Farissi, S.Kom., M.Cs.
NIP. 198512152014041001

Pembimbing II

Mastura Diana Marieska, M.T.
NIP. 198603212018032001

Mengetahui,
Ketua Jurusan Teknik Informatika,

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

TANDA LULUS UJIAN SIDANG SKRIPSI

Pada hari **Jumat** tanggal **31 Desember 2021** telah dilaksanakan ujian sidang skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Dhiya Calista
NIM : 09021381823105
Judul : Sistem Pengamanan Data Menggunakan Kriptografi AES dan Blockchain Berbasis Android

1. Pembimbing I

Al Farissi, S.Kom., M.Cs.
NIP. 198512152014041001

2. Pembimbing II

Mastura Diana Marieska, M.T.
NIP. 198603212018032001

3. Penguji I

Julian Supardi, M.T.
NIP. 197207102010121001

4. Penguji II

Muhammad Qurhanul Rizqie, M.T.
NIDN. 0203128701

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

HALAMAN PERNYATAAN

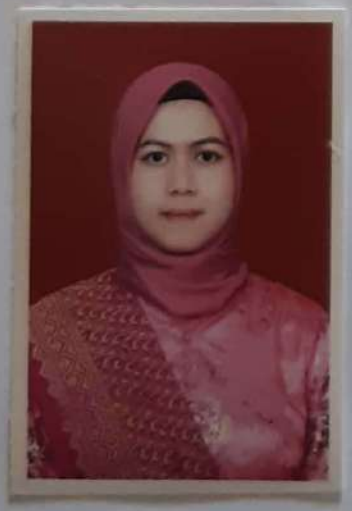
Yang bertanda tangan di bawah ini :

Nama	: Dhiya Calista
NIM	: 09021381823105
Program Studi	: Teknik Informatika Bilingual
Judul Skripsi	: Sistem Pengamanan Data Menggunakan Kriptografi AES dan Blockchain Berbasis Android

Hasil pengecekan Software *iThenticate/Turnitin* : 15%

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.



Palembang, 5 Januari 2022

Dhiya Calista
NIM. 09021381823105

MOTTO DAN PERSEMBAHAN

Motto:

- *And He is with you, wherever you are.* (Al-Hadid, 57:4)
- *Our parents are always an important part of our inner life.*
- *Be better than you were yesterday.*
- *If you want to be happy, be.*
- *You didn't come this far to only come this far.*

Kupersembahkan karya tulis ini kepada:

- Allah SWT
- Keluarga
- Teman-teman seperjuangan
- Fakultas Ilmu Komputer Universitas Sriwijaya

DATA SECURITY SYSTEM USING AES CRYPTOGRAPHY AND BLOCKCHAIN ANDROID-BASED

By:

Dhiya Calista
09021381823105

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.

SISTEM PENGAMANAN DATA MENGGUNAKAN KRIPTOGRAFI AES DAN BLOCKCHAIN BERBASIS ANDROID

Oleh:

Dhiya Calista
09021381823105

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*.

KATA PENGANTAR

Alhamdulillahirabbil'alamin. Puji dan syukur kehadirat Allah SWT atas rahmat dan hidayah-Nya, tak lupa shalawat serta salam senantiasa tercurahkan kepada junjungan Nabi Agung Muhammad SAW yang selalu kita nantikan syafa'atnya di akhirat nanti. Penulis mengucapkan syukur kepada Allah SWT atas limpahan nikmat sehat-Nya, baik itu berupa sehar fisik maupun akal pikiran, sehingga penulis dapat menyelesaikan Skripsi yang berjudul "Sistem Pengamanan Data Menggunakan Kriptografi AES dan Blockchain Berbasis Android" dengan tepat waktu.

Penulis mengucapkan terima kasih sebanyak-banyaknya kepada semua pihak yang telah mendukung, membimbing, dan membantu penulis selama proses penyelesaian Skripsi ini, diantaranya:

1. Allah SWT yang telah memberikan nikmat, rahmat dan hidayah-Nya kepada penulis dalam menyelesaikan Skripsi ini.
2. Bapak Prof. Dr. Ir. H. Anis Saggaf, MSCE. selaku Rektor Universitas Sriwijaya.
3. Bapak Jaidan Jauhari, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Ibu Alvi Syahrini Utami, M.Kom. selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Al Farissi, S.Kom., M.Cs. selaku Pembimbing Skripsi Pertama Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

6. Ibu Mastura Diana Marieska, M.T. selaku Pembimbing Skripsi Kedua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Papa H. Sumantri, S.E., M.Si., Mama Dr. Hj. Indrayani, S.T., M.T., Kakak Arsyil Sumantri Putra, A.P., dan Adik Amanda Trindra Ramdani, beserta keluarga yang selalu memberikan dukungan, doa, semangat hingga motivasi yang tiada henti kepada penulis.
8. Sahabat-sahabat seperjuangan Zora Cahya Ardiya Prameswari, Cindy Wijaya, Arya Pradata, Ihtiar Alfath Radenpangestu, M. Aqil Citrayasa, Asthilia Lelzaba, dan sahabat-sahabat lain yang tidak dapat disebutkan satu persatu yang selalu memberikan semangat, dukungan, dan motivasi, serta mendengarkan keluh kesah penulis.
9. Teman-teman mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya yang telah memberikan dukungan kepada penulis.

Penulis tentu menyadari bahwa Skripsi ini masih jauh dari kata sempurna dan masih banyak terdapat kesalahan serta kekurangan di dalamnya. Untuk itu, penulis mengharapkan kritik serta saran dari pembaca untuk Skripsi ini untuk kemajuan penelitian selanjutnya. Demikian apabila terdapat banyak kesalahan pada Skripsi ini, penulis mohon maaf yang sebesar-besarnya.

Palembang, Januari 2022

Penyusun

DAFTAR ISI

Halaman

HALAMAN JUDUL i
HALAMAN PENGESAHAN ii
HALAMAN PERSETUJUAN KOMISI PENGUJI iii
HALAMAN PERNYATAAN iv
HALAMAN MOTTO DAN PERSEMBAHAN v
ABSTRACT vi
ABSTRAKSI vii
KATA PENGANTAR viii
DAFTAR ISI x
DAFTAR TABEL xv
DAFTAR GAMBAR xvii

BAB I PENDAHULUAN

1.1 Latar Belakang I-1
1.2 Perumusan Masalah I-3
1.3 Tujuan Penelitian I-3
1.4 Manfaat Penelitian I-4
1.5 Batasan Masalah I-4
1.6 Sistematika Penulisan I-5
1.7 Kesimpulan I-6

BAB II KAJIAN LITERATUR

2.1 Pendahuluan II-1

2.2 Landasan Teori II-1
2.2.1 Sistem Pengamanan II-1
2.2.1.1 Pengertian Sistem II-1
2.2.1.2 Pengertian Pengamanan II-2
2.2.1.3 Pengertian Sistem Pengamanan II-2
2.2.2 Data II-2
2.2.3 Kriptografi II-3
2.2.3.1 Pengertian Kriptografi II-3
2.2.3.2 Tujuan Kriptografi II-4
2.2.3.3 Terminologi dalam Kriptografi II-5
2.2.3.4 Jenis-Jenis Kriptografi II-7
2.2.3.5 Serangan terhadap Kriptografi II-9
2.2.4 *Advanced Encryption Standard* (AES) II-10
2.2.5 *Blockchain* II-15
2.2.6 Android II-17
2.2.7 Android Studio II-17
2.2.8 *Application Programming Interface* (API) II-18
2.2.9 *Rational Unified Process* (RUP) II-18
2.3 Penelitian Lain yang Relevan II-20
2.4 Kesimpulan II-22

BAB III METODOLOGI PENELITIAN

3.1 Pendahuluan III-1
3.2 Pengumpulan Data III-1
3.2.1 Jenis Data III-1

3.2.2 Sumber Data III-1
3.2.3 Metode Pengumpulan Data III-1
3.3 Tahapan Penelitian III-2
3.3.1 Kerangka Kerja III-2
3.3.2 Lingkungan Pengembangan Perangkat Lunak III-5
3.3.3 Pengujian Penelitian III-5
3.3.3.1 Pengujian Ketahanan *Blockchain* Terhadap Serangan Modifikasi III-5
3.3.3.2 Pengujian *Avalanche Effect* pada Metode AES III-6
3.3.4 Analisis Hasil Pengujian dan Membuat Kesimpulan III-7
3.4 Metode Pengembangan Perangkat Lunak III-8
3.5 Manajemen Proyek Penelitian III-14

BAB IV PENGEMBANGAN PERANGKAT LUNAK

4.1 Pendahuluan IV-1
4.2 *Rational Unified Process* IV-1
4.2.1 Fase Insepsi IV-1
4.2.1.1 Pemodelan Bisnis IV-1
4.2.1.2 Kebutuhan Sistem IV-2
4.2.1.3 Analisis dan Desain IV-4
4.2.1.3.1 Analisis Kebutuhan Perangkat Lunak IV-4
4.2.1.3.2 Desain Perangkat Lunak IV-4
4.2.2 Fase Elaborasi IV-20
4.2.2.1 Pemodelan Bisnis IV-21
4.2.2.2 Perancangan Basis Data IV-21
4.2.2.3 Perancangan Antarmuka IV-22

4.2.2.4 Diagram *Sequence* IV-25
4.2.3 Fase Konstruksi IV-29
4.2.3.1 Kebutuhan Sistem IV-30
4.2.3.2 Diagram Kelas IV-30
4.2.3.3 Implementasi IV-31
4.2.3.3.1 Implementasi Kelas IV-31
4.2.3.3.2 Implementasi Antarmuka IV-32
4.2.4 Fase Transisi IV-35
4.2.4.1 Pemodelan Bisnis IV-35
4.2.4.2 Kebutuhan Sistem IV-35
4.2.4.3 Rencana Pengujian IV-36
4.2.4.4 Kasus Uji IV-40
4.3 Kesimpulan IV-46

BAB V HASIL DAN ANALISIS PENELITIAN

5.1 Pendahuluan V-1
5.2 Data Hasil Percobaan/Penelitian V-1
5.2.1 Konfigurasi Percobaan V-1
5.2.2 Hasil Pengujian Ketahanan *Blockchain* Terhadap Serangan Modifikasi V-1
5.2.2 Hasil Pengujian *Avalanche Effect* pada Metode AES V-9
5.3 Analisis Hasil Penelitian V-12
5.4 Kesimpulan V-15

BAB VI KESIMPULAN DAN SARAN

6.1 Kesimpulan VI-1

6.2 Saran VI-1

DAFTAR PUSTAKA xix

DAFTAR TABEL

Halaman

Tabel II-1. Perbedaan Versi Algoritma AES..... II-11

Tabel III-1. Penjadwalan Penelitian.....III-14

Tabel IV-1. Kebutuhan Fungsional IV-3

Tabel IV-2. Kebutuhan Non-Fungsional.....IV-3

Tabel IV-3. Definisi Aktor *Use Case* IV-5

Tabel IV-4. Definisi *Use Case* IV-6

Tabel IV-5. Skenario *Use Case* Melihat Seluruh *Block* atau Data.....IV-7

Tabel IV-6. Skenario *Use Case* Menambah *Block* atau Data.....IV-9

Tabel IV-7. Skenario *Use Case* Mengedit Data *Block* atau Data.....IV-11

Tabel IV-8. Skenario *Use Case* Menghapus *Block* atau Data IV-13

Tabel IV-9. Skenario *Use Case* Memeriksa Validasi *Blockchain*.....IV-14

Tabel IV-10. Implementasi Kelas.....IV-31

Tabel IV-11. Rencana Pengujian *Use Case* Melihat Seluruh *Block* atau Data IV-36

Tabel IV-12. Rencana Pengujian *Use Case* Menambah *Block* atau Data.....IV-36

Tabel IV-13. Rencana Pengujian *Use Case* Mengedit Data *Block* atau Data IV-37

Tabel IV-14. Rencana Pengujian *Use Case* Menghapus *Block* atau Data IV-38

Tabel IV-15. Rencana Pengujian *Use Case* Memeriksa Validasi *Blockchain* IV-38

Tabel IV-16. Pengujian *Use Case* Melihat Seluruh *Block* atau Data IV-40

Tabel IV-17. Pengujian *Use Case* Menambah *Block* atau Data.....IV-41

Tabel IV-18. Pengujian *Use Case* Mengedit Data *Block* atau Data IV-44
Tabel IV-19. Pengujian *Use Case* Menghapus *Block* atau Data IV-45
Tabel IV-20. Pengujian *Use Case* Memeriksa Validasi *Blockchain* IV-46
Tabel V-1. Hasil Pengujian *Avalanche Effect* V-9
Tabel V-2. Hasil Pengujian Ketahanan *Blockchain* Terhadap Serangan Modifikasi V-13

DAFTAR GAMBAR

Halaman

Gambar II-1. Proses Kriptografi Simetris II-8
Gambar II-2. Proses Kriptografi Asimetri II-8
Gambar II.3. Proses Enkripsi AES II-13
Gambar II.4. Proses Dekripsi AES II-14
Gambar III-1. Kerangka Kerja Penelitian III-2
Gambar III-2. Skema Pengujian Ketahanan *Blockchain* Terhadap Serangan Modifikasi III-6
Gambar III-3. Skema Pengujian *Avalanche Effect* pada Metode AES III-7
Gambar III-4. Flowchart Fase Metodologi Pengembangan Perangkat Lunak RUP III-8
Gambar III-5. *Flowchart* Fase *Inception* RUP III-9
Gambar III-6. *Flowchart* Fase *Elaboration* RUP III-10
Gambar III-7. *Flowchart* Fase *Construction* RUP III-11
Gambar III-8. *Flowchart* Implementasi Metode AES dan *Blockchain* III-12
Gambar III-9. *Flowchart* Fase *Transition* RUP III-13
Gambar IV-1. Diagram *Use Case* IV-5
Gambar IV-2. Diagram *Activity* Melihat Seluruh *Block* atau Data IV-16
Gambar IV-3. Diagram *Activity* Menambah *Block* atau Data IV-17
Gambar IV-4. Diagram *Activity* Mengedit Data *Block* atau Data IV-18
Gambar IV-5. Diagram *Activity* Menghapus *Block* atau Data IV-19
Gambar IV-6. Diagram *Activity* Memeriksa Validasi *Blockchain* IV-20
Gambar IV-7. Perancangan Basis Data IV-22

Gambar IV-8. Perancangan Antarmuka Halaman Daftar IV-23
Gambar IV-9. Perancangan Antarmuka Halaman Tambah dan Edit IV-24
Gambar IV-10. Diagram *Sequence* Melihat Seluruh *Block* atau Data.....IV-25
Gambar IV-11. Diagram *Sequence* Menambah *Block* atau Data IV-26
Gambar IV-12. Diagram *Sequence* Mengedit Data *Block* atau Data.....IV-27
Gambar IV-13. Diagram *Sequence* Menghapus *Block* atau Data.....IV-28
Gambar IV-14. Diagram *Sequence* Memeriksa Validasi Blockchain IV-29
Gambar IV-15. Diagram Kelas.....IV-30
Gambar IV-16. Antarmuka Halaman Daftar *Blockchain*.....IV-33
Gambar IV-17. Antarmuka Halaman Daftar *Non-Blockchain*.....IV-33
Gambar IV-18. Antarmuka Halaman Tambah IV-34
Gambar IV-19. Antarmuka Halaman Edit IV-34
Gambar V-1. Pengujian Ketahanan *Blockchain* Tanpa Serangan Modifikasi.....V-4
Gambar V-2. Pengujian Ketahanan *Blockchain* Terhadap Serangan Modifikasi pada Data *Block* Pertama V-5
Gambar V-3. Pengujian Ketahanan *Blockchain* Terhadap Serangan Modifikasi pada Data *Block* Tengah V-7
Gambar V-4. Pengujian Ketahanan *Blockchain* Terhadap Serangan Modifikasi pada Data *Block* Terakhir.....V-8
Gambar V-5. Grafik Pengujian *Avalanche Effect* V-15

BAB I

PENDAHULUAN

1.1 Latar Belakang

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.

Pada saat ini dalam dunia pendidikan, khususnya di perguruan tinggi telah menggunakan sistem informasi akademik untuk meningkatkan mutu pendidikan dan memberikan kemudahan kepada dosen dan tenaga kependidikan dalam melakukan pengolahan nilai, serta memberikan kemudahan bagi mahasiswa untuk mendapatkan informasi nilai. Namun fasilitas akademik ini

masih belum sepenuhnya memberikan keamanan pada nilai yang di-*input* karena masih seringkali terjadi serangan pada sistem yang mengakibatkan kerugian pada nilai mahasiswa, seperti nilai yang bocor ke pihak yang tidak berwenang terhadap nilai maupun nilai yang diubah oleh penyerang yang ingin mendapat keuntungan secara pribadi. Kedua hal ini tentu merugikan pihak kampus dan mahasiswa yang bersangkutan. Maka dari itu, perlu diterapkan ilmu kriptografi yang dapat menjaga keamanan data atau informasi pengguna.

Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan (*message*). Dalam buku-buku sebelum tahun 1980-an menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dibaca dan dimengerti lagi maknanya. Pengertian lain dari kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi (Munir, 2006).

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. (Meko, 2018). *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. (Tulloh, dkk, 2016). 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 (Noorsanti, dkk, 2018).

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.

1.2 Perumusan Masalah

Berdasarkan latar belakang dan fakta-fakta yang telah dipaparkan di atas, maka permasalahan yang dapat dirumuskan dalam penelitian ini adalah bagaimana membangun suatu sistem yang dapat menjaga keamanan data pengguna dari serangan aktif maupun pasif menggunakan metode *Advanced Encyrption Standard* (AES) dan *Blockchain*?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah:

1) Untuk mengetahui bagaimana cara membangun suatu sistem yang dapat menjaga keamanan data dari serangan aktif dan pasif?
2) Untuk mengetahui bagaimana cara menerapkan metode *Advanced Encyrption Standard* (AES) dan *Blockchain* di dalam suatu sistem pengamanan data?

1.4 Manfaat Penelitian

Beberapa manfaat dari penelitian ini adalah sebagai berikut:

1) Membantu meningkatkan keamanan data atau informasi pengguna dari serangan aktif dan pasif dengan mengkombinasikan metode *Advanced Encyrption Standard* (AES) dan *Blockchain*.
2) Memberikan informasi dan rekomendasi kepada para pengguna aplikasi dalam bidang ilmu kriptografi, terhadap pengamanan dan kerahasiaan keamanan data menggunakan kriptografi *Advanced Encryption Standard* (AES) dan *Blockchain*.
3) Bermanfaat dan dijadikan perbandingan dengan penelitian serupa, serta menjadi bahan pertimbangan untuk penelitian dan pengembangan lebih lanjut.

1.5 Batasan Masalah

Batasan-batasan yang diterapkan adalah sebagai berikut :

1) Panjang kunci AES di dalam penelitian ini dibatasi hanya bisa sampai 16 karakter atau 128 bit.
2) Teknologi *Blockchain* yang digunakan pada penelitian ini tidak sampai pengelolaan secara terdistribusi menggunakan jaringan *peer-to-peer*, melainkan dibatasi hanya sampai mekanisme *Proof-of-Work*.
3) Pengamanan yang dilakukan dalam *Blockchain* hanya berupa data teks.
4) Data yang digunakan dalam penelitian ini adalah data nilai mahasiswa Jurusan Teknik Sipil Politeknik Negeri Sriwijaya.

1.6 Sistematika Penulisan

Dalam penulisan laporan ini, penulis membuat suatu sistematika penulisan yang terdiri dari beberapa bab dimana masing-masing bab terdapat uraian-uraian sebagai berikut :

BAB I. PENDAHULUAN

Pada bab ini diuraikan mengenai latar belakang, perumusan masalah, tujuan dan manfaat penelitian, batasan masalah atau ruang lingkup serta sistematika penulisan.

BAB II. KAJIAN LITERATUR

Pada bab ini akan dibahas dasar-dasar teori yang digunakan dalam penelitian, seperti definisi-definisi sistem, sistem pengamanan, data, kriptografi, *Advanced Encryption Standard* (AES), *Blockchain* dan lain sebagainya.

BAB III. METODOLOGI PENELITIAN

Pada bab ini akan dibahas mengenai tahapan yang akan dilaksanakan pada penelitian ini. Masing-masing rencana tahapan penelitian dideskripsikan dengan rinci dengan mengacu pada suatu kerangka kerja. Di akhir bab ini berisi perancangan manajemen proyek pada pelaksanaan penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Pada bab ini akan dibahas mengenai analisis, perancangan, implementasi, serta pengujian dalam pengembangan perangkat lunak menggunakan metode pengembangan perangkat lunak *Rational Unified Process* (RUP) pada aplikasi android yang menggunakan metode pengamanan *Advanced Encryption Standard* (AES) dan *Blockchain*.

BAB V. HASIL DAN ANALISIS PENELITIAN

Pada bab ini berisi hasil pengujian berdasarkan langkah-langkah yang telah direncanakan disajikan. Analisis diberikan sebagai basis dari kesimpulan yang diambil dalam penelitian ini.

BAB VI. KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dari semua uraian-uraian pada bab-bab sebelumnya dan juga berisi saran-saran yang diharapkan berguna dalam penelitian ini.

1.7 Kesimpulan

Pada bab ini telah dijelaskan mengenai latar belakang dan permasalahan yang harus diselesaikan dalam penelitian ini, tujuan dan manfaat penelitian ini, serta batasan masalah yang ada. Pada bab ini juga diuraikan sistematika penulisan pada penelitian ini.

DAFTAR PUSTAKA

Bawono, H. R. C. (2015). "KRIPTANALISIS PADA ALGORITMA CIPHER VIGENERE". Skripsi. FAKULTAS SAINS DAN TEKNOLOGI, JURUSAN TEKNIK INFORMATIKA, UNIVERSITAS SANATA DHARMA, YOGYAKARTA.

Fachrozi, M. F., & Fahmi, H. (2021). Penerapan Metode AES-128 Untuk Pengamanan Data Absensi Finger Print Di Balai Penelitian Sungei Putih. *JIKOMSI [Jurnal Ilmu Komputer dan Sistem Informasi] Vol.3 No.3*, 1-8.

Fikri, I. A., Herumurti, D., & Rahman, R. (2016). Aplikasi Navigasi Berbasis Perangkat Bergerak dengan Menggunakan Platform Wikitude untuk Studi Kasus Lingkungan ITS. *JURNAL TEKNIK ITS Vol. 5, No. 1*, A48.

Fitriani, I., & Utomo, A. B. (2020). Implementasi Algoritma Advanced Encryption Standard (AES) pada Layanan SMS Desa. *JISKa, Vol. 5, No. 3*, 153-163.

Gumira, G., Ernawati, & Erlanshari, A. (2016). IMPLEMENTASI METODE ADVANCED ENCRYPTION STANDARD (AES) DAN MESSAGE DIGEST 5 (MD5) PADA ENKRIPSI DOKUMEN (STUDI KASUS LPSE UNIB). *Jurnal Rekursif, Vol. 4 No. 3,* 280-281.

Jogiyanto. (2005). *Analisis dan Desain Sistem Informasi.* Yogyakarta: Andi Offset.

Kristanto, A. (2007). *Perancangan Sistem Informasi Dan Aplikasinya.* Yogyakarta: Gava Media.

Kurniawan, Y. (2004). *Kriptografi Keamanan Internet dan Jaringan Komunikasi.* Bandung: Informatika.

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

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

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

Nurfaizah, Sarmin, & Novitasari, O. (2017). Implementasi Rational Unified Process Pada Sistem Informasi Simpan Pinjam Kelompok Perempuan. *CITISEE*, 126-127.

Pinata, S. G. (2017). "PERANCANGAN APLIKASI PENGENALAN MACAM-MACAM ILMU HADITS BESERTA CONTOHNYA BERBASIS ANDROID MENGGUNAKAN JAVA ECLIPSE". Skripsi. FAKULTAS TEKNIK, PROGRAM STUDI TEKNIK INFORMATIKA, UNIVERSITAS MUHAMMADIYAH PONOROGO.

Pressman, R. S. (2010). *Software Engineering : A Practitioner's Approach.* New York: McGraw-Hill.

Riswanto, H. R., Safinah, K., Muslikah, A. N., & Holle, K. F. (2020). Implementasi Teknik Kriptografi RSA Untuk Pengamanan Data Pengiriman SMS. *Jurnal Ilmiah Informatika Volume 5 No. 1*, 61-66.

Rosa, A., & Shalahuddin, M. (2013). *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek.* Bandung: Informatika.

Safaat, N. H. (2011). *Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android*. Bandung: Informatika.

Simargolang, M. Y. (2017). IMPLEMENTASI KRIPTOGRAFI RSA DENGAN PHP. *JURNAL TEKNOLOGI INFORMASI (JurTI) Volume 1, Nomor 1*, 3.

Skousen. (2007). *Pengantar Akuntansi Keuangan.* Jakarta: Salemba Empat.

Supriadi, F., & Hardian, R. (2019). PENERAPAN METODE RATIONAL UNIFIED PROCESS PADA PERANCANGAN SISTEM PENGOLAH DATA ARISANKITA. *Jurnal Infotekmesin Vol.10, No.02*, 23.

Surahman, S., & Setiawan, E. B. (2017). Aplikasi Mobile Driver Online Berbasis Android Untuk Perusahaan Rental Kendaraan . *ULTIMA InfoSys, Vol. VIII, No. 1* , 36.

Sutabri, T. (2005). *Sistem Informasi Manajemen.* Yogyakarta: Andi.

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

Williams, B. K., & Sawyer, S. C. (2007). *Using Information Technology: Pengenalan Praktis Dunia Komputer dan Komunikasi.* Yogyakarta: Andi Offset.

Zulkifli, S. (2003). *Dasar-dasar Akuntansi Perbankan Syariah.* Jakarta: Zikrul Hakim.