

SECURE CHATTING MENGGUNAKAN ALGORITMA AES DAN BLOCKCHAIN BERBASIS MOBILE

Diajukan Untuk Menyusun Skripsi

di Jurusan Teknik Informatika Fakultas Ilmu Komputer UNSRI



Oleh :

Arya Pradata

NIM : 09021281823029

**Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2022**

LEMBAR PENGESAHAN SKRIPSI

SECURE CHATTING MENGGUNAKAN ALGORITMA AES DAN BLOCKCHAIN BERBASIS *MOBILE*

Oleh:

Arya Pradata

NIM : 09021281823029

Palembang, 19 Juli 2022

Pembimbing I



Al Farissi, M.Cs.

NIP. 198512152014041001

Pembimbing II




Kanda Januar Miraswan, M.T.

NIP. 199001092019031012

Mengetahui,

Ketua Jurusan Teknik Informatika,



Alvi Syahrini Utami, M.Kom.

NIP. 197812222006042003

TANDA LULUS UJIAN KOMPREHENSIF SKRIPSI

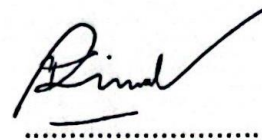
Pada hari **Kamis** tanggal **7 Juli 2022** telah dilaksanakan ujian komprehensif skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Arya Pradata
N I M : 09021281823029
Judul : *Secure Chatting* Menggunakan Algoritma AES dan Blockchain Berbasis *Mobile*

dan dinyatakan **LULUS**.

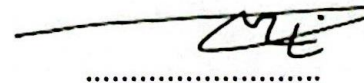
1. Ketua

Mastura Diana Marieska, M.T.
NIP. 198603212018032001



2. Penguji I

Osvari Arsalan, M.T.
NIP. 198806282018031001



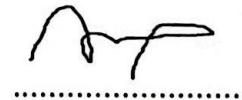
3. Penguji II

Muhammad Qurhanul Rizqie, M.T., Ph.D.
NIDN. 0203128701



4. Pembimbing I

Al Farissi, M.Cs.
NIP. 198512152014041001



5. Pembimbing II

Kanda Januar Miraswan, M.T.
NIP. 199001092019031012



Mengetahui,
Ketua Jurusan Teknik Informatika,



Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Arya Pradata
NIM : 09021281823029
Program Studi : Teknik Informatika Bilingual
Judul Skripsi : *Secure Chatting Menggunakan Algoritma AES dan Blockchain Berbasis Mobile*

Hasil pengecekan Software *iThenticate/Turnitin* : 14%

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, 11 Juli 2022



Arya Pradata
NIM. 09021281823029

MOTTO DAN PERSEMBAHAN

- Learn from what you got

Kupersembahkan karya tulis ini kepada :

- Keluargaku
- Teman-teman seperjuangan
- Fakultas Ilmu Komputer

Universitas Sriwijaya

SECURE CHAT USING MOBILE-BASED AES ALGORITHM AND BLOCKCHAIN

By:

**Arya Pradata
09021281823029**

ABSTRACT

This study proposes securing messages using the AES algorithm and blockchain to secure text messages in chatting application. AES algorithm is a symmetric algorithm with advantages in the speed of the encryption and decryption process being faster than the asymmetric algorithm and blockchain as data security in the message sending process with a security system that can only append data and cannot be changed. Therefore, speed and security can be achieved using AES and blockchain to secure text messages from cybercrime. The analytical method used to obtain the study results is the avalanche effect method and processing time measurement. Based on the results of the study, the results obtained from the processing time of the message sending process using blockchain and AES algorithm with an average of overall processing time is 33.59 ms. The Avalanche Effect value obtained from the AES algorithm is 50% for character lengths up to 16 characters, and avalanche Effect value is below 50% for character lengths of more than 16 characters. Based on the test's results, with AES algorithm that can secure the text message and blockchain that able to help store the message data, this methods combination has succeeded in securing text messages in messaging applications.

Keywords: AES, Avalanche Effect, Blockchain, Chatting, Cryptography

SECURE CHATTING MENGGUNAKAN ALGORITMA AES DAN BLOCKCHAIN BERBASIS MOBILE

Oleh:

**Arya Pradata
09021281823029**

ABSTRAK

Penelitian ini mengusulkan pengamanan pesan dengan menggunakan kombinasi dari algoritma AES dan *Blockchain* untuk mengamankan pesan teks pada aplikasi *chatting*. Algoritma AES sebagai algoritma simetri memiliki kelebihan pada kecepatan proses enkripsi dan dekripsi lebih cepat dibandingkan dengan algoritma asimetri dan *Blockchain* sebagai pengamanan data pada proses pengiriman pesan dengan sistem keamanan yang bersifat hanya dapat menambahkan data dan tidak bisa diubah. Oleh karena itu, kecepatan dan keamanan dapat dicapai dengan menggunakan AES dan *blockchain* untuk mengamankan pesan teks dari kejahatan *cybercrime*. Metode analisa yang digunakan untuk mendapatkan hasil penelitian yaitu menggunakan metode perhitungan *Avalanche Effect* dan pengukuran *Processing Time*. Berdasarkan hasil penelitian, didapatkan hasil dari waktu komputasi proses pengiriman pesan dengan menggunakan *Blockchain* dan algoritma AES dengan rata-rata waktu proses keseluruhan yaitu 33.59 ms. Hasil nilai *Avalanche Effect* yang didapatkan dari algoritma AES yaitu sebesar 50% untuk panjang karakter sampai dengan 16 karakter dan nilai *Avalanche Effect* dibawah 50% untuk panjang karakter lebih dari 16 karakter. Berdasarkan hasil pengujian yang telah dilakukan, kombinasi algoritma AES yang dapat mengamankan pesan teks dan *Blockchain* yang dapat membantu menyimpan data pesan berhasil mengamankan pesan teks pada aplikasi pengiriman pesan.

Kata Kunci: AES, *Avalanche Effect*, *Blockchain*, *Chatting*, Kriptografi.

KATA PENGANTAR

Puji dan syukur kehadiran Allah SWT yang telah senantiasa melimpahkan rahmat dan hidayah-Nya, tak lupa shalawat serta salam senantiasa tercurahkan kepada junjungan Nabi 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 sehat fisik maupun akal pikiran, sehingga penulis dapat menyelesaikan Skripsi yang berjudul “*Secure Chatting Menggunakan Algoritma AES dan Blockchain Berbasis Mobile*” dengan tepat waktu.

Penulis mengucapkan terima kasih yang tak terhingga 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. Ayah Ir. Didiek Eko Riyanto, Ibu Dyah Sri Rahayu, S.Si., Kakak Yudha Aditya Nugroho, S.T., dan Adik Aurellia Nasywa Safitri, beserta seluruh keluarga besar yang selalu memberikan dukungan, doa dan semangat untuk penulis.
3. Bapak Prof. Dr. Ir. H. Anis Saggaff, MSCE. selaku Rektor Universitas Sriwijaya.
4. Bapak Jaidan Jauhari, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.

5. Ibu Alvi Syahrini Utami, M.Kom. selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Bapak Al Farissi, M.Cs. selaku Pembimbing Skripsi Pertama Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Bapak Kanda Januar Miraswan, M.T. selaku Pembimbing Skripsi Kedua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Sahabat-sahabat seperjuangan Achmad Mirza Apriansyah, Cindy Wijaya, Dhiya Calista, Jasmine Aussie, Ihtiar Alfath Radenpangestu, Zora Cahya Ardiya Prameswari dan sahabat-sahabat lain yang tidak dapat disebutkan satu-persatu yang selalu memberikan semangat, dukungan dan bantuan terhadap penulis.
9. Teman-teman mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya.

Penulis menyadari bahwa hasil dari tugas akhir ini yang jauh dari kata sempurna. Untuk itu, penulis mengharapkan kritik dan saran yang dapat membangun untuk kemajuan pada penelitian selanjutnya. Akhir kata, apabila terdapat banyak kesalahan pada Skripsi ini, penulis mohon maaf sebesar-besarnya.

Palembang, 19 Juli 2022



Arya Pradata

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
HALAMAN PENGESAHAN.....	ii
HALAMAN TANDA LULUS	iii
HALAMAN PERNYATAAN.....	iv
HALAMAN MOTTO DAN PERSEMBAHAN	v
ABSTRACT.....	vi
ABSTRAK	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR TABEL	xiv
DAFTAR GAMBAR.....	xvi
BAB I PENDAHULUAN.....	I-1
1.1 Pendahuluan	I-1
1.2 Latar Belakang	I-1
1.3 Rumusan Masalah	I-3
1.4 Tujuan Penelitian.....	I-3
1.5 Manfaat Penelitian.....	I-4
1.6 Batasan Masalah.....	I-4
1.7 Sistematika Penulisan.....	I-5

1.8	Kesimpulan.....	I-6
BAB II KAJIAN LITERATUR		II-1
2.1	Pendahuluan	II-1
2.2	Landasan Teori	II-1
2.2.1	Kriptografi.....	II-1
2.2.2	Aplikasi Chatting	II-3
2.2.3	<i>Blockchain</i>	II-3
2.2.4	<i>Advanced Encryption Standard (AES)</i>	II-6
2.2.5.	Android	II-9
2.2.6.	Avalanche Effect.....	II-10
2.3	Penelitian Terdahulu.....	II-12
2.3.1	Implementasi Algoritma Advanced Encryption Standard pada Aplikasi Chatting berbasis Android (Randi et al., 2020).....	II-12
2.3.2	Pengembangan Aplikasi Pesan Instan Terenkripsi Menggunakan Algoritma Kriptografi AES (Advanced Encryption Standard) (Ilham & Widyassari, 2021)	II-12
2.3.3	<i>Secure Messaging Platform Using Blockchain Technology</i> (Das, 2020) II-13	
2.4	Kesimpulan.....	II-13
BAB III METODOLOGI PENELITIAN		III-1
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-2
3.3	Tahapan Penelitian	III-2
3.3.1	Kerangka Kerja	III-2
3.3.2	Kriteria Pengujian	III-6
3.3.3	Format Data Pengujian.....	III-10
3.3.4	Lingkungan dalam Pelaksanaan Penelitian.....	III-11
3.3.5	Pengujian Penelitian.....	III-11
3.3.6	Analisis Hasil Pengujian dan Membuat Kesimpulan Penelitian.....	III-12
3.4	Metode Pengembangan Perangkat Lunak	III-12
3.5	Manajemen Proyek Penelitian.....	III-15
BAB IV PENGEMBANGAN PERANGKAT LUNAK		IV-1
4.1.	Pendahuluan	IV-1
4.2.	<i>Rational Unified Process</i>	IV-1
4.2.1	Fase Insepsi	IV-1
4.2.2	Fase Elaborasi	IV-19
4.2.3	Fase Konstruksi.....	IV-26
4.2.4	Fase Transisi	IV-31
4.3.	Kesimpulan.....	IV-41
BAB V HASIL DAN ANALISIS PENELITIAN.....		V-1

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 <i>Avalanche Effect</i>	V-2
5.2.3	Hasil Pengujian <i>Processing Time</i>	V-4
5.3	Analisis Hasil Penelitian	V-7
5.4	Kesimpulan.....	V-10
BAB VI KESIMPULAN DAN SARAN.....		VI-1
6.1	Kesimpulan.....	VI-1
6.2	Saran	VI-2
DAFTAR PUSTAKA		xviii

DAFTAR TABEL

	Halaman
Tabel II-1. Tabel Urutan Data Algoritma AES	II-6
Tabel III-1. Pengujian <i>Avalanche Effect</i>	III-10
Tabel III-2. Pengujian <i>Processing Time</i>	III-10
Tabel III-3. Tabel Work Breakdown Structure (WBS) pada Penelitian	III-15
Tabel IV-1. Kebutuhan Fungsional.....	IV-3
Tabel IV-2. Kebutuhan Non-Fungsional.....	IV-3
Tabel IV-3. Definisi Aktor <i>Use Case</i>	IV-5
Tabel IV-4. Definisi <i>Use Case</i>	IV-6
Tabel IV-5. Skenario <i>Use Case</i> Mengirim Pesan Teks.....	IV-7
Tabel IV- 6. Skenario <i>Use Case</i> Menerima Pesan Teks	IV-9
Tabel IV- 7. Skenario <i>Use Case</i> Mengukur Tingkat Keamanan Metode	IV-10
Tabel IV- 8. Skenario <i>Use Case</i> Menghitung <i>Processing Time</i>	IV-12
Tabel IV-9. Implementasi Kelas	IV-28
Tabel IV-10. Rencana pengujian <i>Use Case</i> Mengirim pesan teks yang diamankan dengan algoritma AES dan Blockchain	IV-32
Tabel IV-11. Rencana pengujian <i>Use Case</i> Menerima pesan teks yang diamankan dengan algoritma AES dan Blockchain	IV-32

Tabel IV-12. Rencana Pengujian <i>Use Case</i> Mengukur tingkat keamanan metode algoritma AES.....	IV-33
Tabel IV-13. Rencana pengujian <i>Use Case</i> Menghitung processing time metode pengamanan pesan dengan algoritma AES dan Blockchain.....	IV-34
Tabel IV-14. Pengujian <i>Use Case</i> Mengirim pesan teks yang diamankan dengan algoritma AES dan Blockchain.....	IV-35
Tabel IV-15. Pengujian <i>Use Case</i> Menerima pesan teks yang diamankan dengan algoritma AES dan Blockchain.....	IV-36
Tabel IV-16. Pengujian <i>Use Case</i> Mengukur tingkat keamanan metode algoritma AES	IV-38
Tabel IV-17. Pengujian <i>Use Case</i> Menghitung <i>processing time</i> metode pengamanan pesan dengan algoritma AES dan Blockchain	IV-39
Tabel V-1. Pengujian <i>Avalanche Effect</i>	V-2
Tabel V-2. Pengujian <i>Processing Time</i>	V-4

DAFTAR GAMBAR

	Halaman
Gambar II-1. Skema Enkripsi dan Dekripsi Kriptografi Kunci Simetri	II-3
Gambar II-2. Skema Enkripsi dan Dekripsi Kriptografi Kunci Asimetri	II-3
Gambar II-3. Representasi <i>Blockchain</i> (Das, 2020).....	II-4
Gambar II-4. Representasi Blok-Blok (Nakamoto, 2008)	II-5
Gambar II-5. Proses <i>Input Bytes, State Array, Output Bytes</i> (Prameshwari & Sastra, 2018)	II-7
Gambar II-6. Ilustrasi Proses Enkripsi Aes.....	II-8
Gambar II-7. Ilustrasi Proses Dekripsi AES	II-9
Gambar III-1. Kerangka Kerja Penelitian	III-3
Gambar III-2. Proses Implementasi Metode AES dan Blockchain	III-6
Gambar III-3. Skema Pengujian <i>Avalanche Effect</i>	III-8
Gambar III-4. Skema Pengujian <i>Processing Time</i>	III-9
Gambar III-5. Tahap Menentukan Ruang Lingkup Penelitian	III-19
Gambar III-6. Tahap Menentukan Dasar Landasan Teori Pada Penelitian	III-19
Gambar III-7. Tahap Insepsi	III-20
Gambar III-8. Tahap Elaborasi	III-20
Gambar III-9. Tahap Konstruksi	III-21
Gambar III-10. Tahap Transisi.....	III-21

Gambar III-11. Tahap Melakukan Pengujian Penelitian.....	III-22
Gambar III-12. Melakukan Analisa Hasil Pengujian dan Sintesis Kesimpulan	III-22
Gambar IV-1. Diagram <i>Use Case</i>	IV-5
Gambar IV-2. Diagram <i>Activity</i> Mengirim Pesan Teks	IV-15
Gambar IV-3. Diagram <i>Activity</i> Menerima Pesan Teks.....	IV-16
Gambar IV 4. Diagram <i>Activity</i> Mengukur Tingkat Keamanan Metode	IV-17
Gambar IV-5. Diagram <i>Activity</i> Menghitung <i>Processing Time</i>	IV-18
Gambar IV-6. Perancangan Antarmuka Halaman <i>Chat Room</i>	IV-20
Gambar IV-7. Perancangan Antarmuka Halaman <i>Processing Time</i>	IV-21
Gambar IV-8. Perancangan Antarmuka Halaman <i>Avalanche Effect</i>	IV-22
Gambar IV-9. Diagram <i>Sequence</i> Mengirim Pesan Teks	IV-23
Gambar IV-10. Diagram <i>Sequence</i> Menerima Pesan Teks.....	IV-24
Gambar IV-11. Diagram <i>Sequence</i> Mengukur Tingkat Keamanan Metode.....	IV-25
Gambar IV-12. Diagram <i>Sequence</i> Menghitung <i>Processing Time</i>	IV-26
Gambar IV-13. Diagram Kelas	IV-27
Gambar IV-14. Antarmuka Halaman <i>Chat Room</i>	IV-29
Gambar IV-15. Antarmuka Halaman <i>Avalanche Effect</i>	IV-30
Gambar IV-16. Antarmuka Halaman <i>Processing Time</i>	IV-30
Gambar V-1. Grafik Pengujian <i>Avalanche Effect</i>	V-7
Gambar V-2. Grafik Pengujian Waktu Enkripsi	V-9
Gambar V-3. Grafik Pengujian Waktu Dekripsi.....	V-9
Gambar V-4. Grafik Pengujian Waktu <i>Mining</i>	V-10

BAB I

PENDAHULUAN

1.1 Pendahuluan

Bab bagian pendahuluan akan dibahas mengenai latar belakang dari topik “*Secure Chatting Menggunakan Algoritma AES dan Blockchain Berbasis Mobile*”. Selain itu juga akan membahas mengenai rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, sistematika penulisan serta gambaran secara umum keseluruhan kegiatan yang dilaksanakan pada penelitian

1.2 Latar Belakang

Perkembangan teknologi informasi yang terus meningkat mengakibatkan meningkat juga kebutuhan manusia. Untuk mempermudah kinerja manusia sehari-hari, komunikasi sangat penting agar tingkat produktivitas masyarakat tidak menurun, sehingga kinerja masyarakat tetap terjaga. *Chat Messenger* merupakan suatu sarana komunikasi pesan yang banyak digunakan oleh pengguna *mobile smartphone*, namun pesan yang dikirim belum tentu aman dari penyadap atau dari kejahatan *cybercrime*. Untuk mengatasi hal tersebut penggunaan kriptografi sangat penting agar mencegah *hacker* menyadap pesan yang dikirimkan. Kriptografi merupakan suatu ilmu untuk menjaga keamanan pesan sederhana (*plaintext*) dengan cara mengenkripsi pesan menjadi bentuk yang sulit dibaca (*ciphertext*). Ketika dekripsi, sebuah *ciphertext*

diubah menjadi *plaintext*. Enkripsi dan dekripsi ini digunakan untuk menjaga pesan dari pihak yang tidak berhak melihat isi pesan (Randi dkk., 2020).

Kriptografi memiliki beberapa metode, salah satunya yaitu algoritma *Advanced Encryption Standard* (AES). AES merupakan algoritma *block cipher* yang menggunakan kunci saat melakukan enkripsi dan dekripsi. Algoritma AES memiliki ukuran blok yang bervariasi, yaitu 128-bit, 192-bit, dan 256-bit. Perbedaan dari ketiga versi AES tersebut memengaruhi jumlah *key* dan putarannya (Prameshwari & Sastra, 2018).

Penelitian ini menggunakan teknologi *Blockchain* sebagai pengamanan data pada proses pengiriman pesan. Teknologi *Blockchain* sangat populer, terutama di bidang *Cryptocurrency*. Dengan sistem keamanan yang bersifat *append only*, hanya dapat menambahkan data dan tidak bisa diubah. Sehingga sistem *Blockchain* sulit ditembus *hacker*. Dari kelebihan itulah, sistem *Blockchain* dikembangkan pada aplikasi *Chat Messenger* dan diamankan lagi dengan enkripsi AES. *Blockchain* adalah sebuah buku besar (*ledger*) yang memiliki sifat desentralisasi dan tidak terpusat. Dengan kata sederhana, istilah *Blockchain* itu sendiri merupakan rantai blok (*chain of blocks*). Sebuah blok memiliki struktur data yang berisi data dan beberapa atribut. Blok-blok dapat dihubungkan untuk membentuk rantai blok (Das, 2020). Berdasarkan pertimbangan diatas, maka akan dilakukan penelitian mengenai *Secure Chatting Menggunakan Algoritma AES dan Blockchain Berbasis Mobile* karena sifat *Blockchain* yang tidak dapat mengubah data didalamnya. Selain itu, algoritma AES

juga merupakan algoritma simetri yang memiliki kelebihan pada proses enkripsi dan dekripsi lebih cepat dibandingkan dengan algoritma asimetri (Basri, 2016).

1.3 Rumusan Masalah

Berdasarkan latar belakang yang sudah dipaparkan diatas, permasalahan yang dapat dirumuskan pada penelitian ini adalah:

1. Bagaimana cara menjaga kerahasiaan dan keamanan pesan dengan mengimplementasikan algoritma AES dan *Blockchain* pada aplikasi *chat messenger* berbasis *Mobile*?
2. Seberapa besar tingkat keamanan metode algoritma kriptografi AES dan *Blockchain*?
3. Bagaimana hasil pengukuran waktu komputasi pada proses pengamanan pesan menggunakan metode algoritma kriptografi AES dan *Blockchain*?

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah :

1. Mengimplementasikan pengamanan pesan dengan menggunakan algoritma kriptografi AES dan *Blockchain* pada aplikasi *chat messenger* berbasis *Mobile* dalam mengamankan pesan teks.
2. Mengukur tingkat keamanan pada pesan yang diamankan menggunakan algoritma kriptografi AES dengan *Avalanche Effect*.

3. Mengukur kecepatan waktu komputasi proses pengamanan pesan menggunakan algoritma AES dan *Blockchain* berdasarkan *processing time*.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah :

1. Menghasilkan suatu perangkat lunak yang memiliki tingkat keamanan yang tinggi dengan mengimplementasikan algoritma kriptografi AES dan *Blockchain*.
2. Dapat dijadikan sebagai acuan untuk penelitian selanjutnya pada bidang kriptografi.

1.6 Batasan Masalah

Batasan masalah penelitian ini adalah :

1. Ukuran blok yang digunakan pada algoritma *Advanced Encryption Standard* yaitu 128-bit serta ukuran kunci yang diimplementasikan adalah 16 karakter dengan hasil keluaran berupa base64.
2. Perangkat lunak hanya memiliki 1 halaman *Chat Room*.
3. Mekanisme *Blockchain* yang digunakan adalah mekanisme *Proof of Work* serta tidak menggunakan jaringan *Peer to Peer*.
4. Pengamanan yang diterapkan pada pesan hanya berupa teks.

1.7 Sistematika Penulisan

Dalam penulisan laporan ini, penulis membuat suatu sistematika penulisan yang terdiri dari beberapa Bab berikut :

BAB I. PENDAHULUAN

Pada Bab ini membahas mengenai latar belakang, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah dan sistematika penulisan.

BAB II. KAJIAN LITERATUR

Pada Bab ini akan membahas mengenai dasar-dasar teori yang digunakan pada penelitian.

BAB III. METODOLOGI PENELITIAN

Pada Bab ini akan membahas mengenai tahap-tahap yang akan dijalankan pada penelitian tugas akhir. Setiap perencanaan dari tahapan penelitian diuraikan secara detil dengan acuan kerangka kerja dan perancangan manajemen proyek penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Pada Bab ini akan membahas mengenai tahapan analisis, perancangan, implementasi, dan pengujian dalam pengembangan perangkat lunak pada sistem keamanan pesan menggunakan metode algoritma AES dan Blockchain berbasis *mobile*.

BAB V. HASIL DAN ANALISIS PENELITIAN

Pada Bab ini akan membahas hasil pengujian pada perangkat lunak yang dibangun. Hasil analisis dapat digunakan sebagai basis dari kesimpulan yang diambil pada penelitian ini.

BAB VI. KESIMPULAN DAN SARAN

Pada Bab ini akan membahas kesimpulan dari uraian-uraian pada Bab sebelumnya dan juga berisi saran yang diharapkan dapat berguna pada penelitian ini.

1.8 Kesimpulan

Pada Bab ini ditemukan bahwa permasalahan yang harus diselesaikan dalam penelitian ini yaitu bagaimana cara menjaga kerahasiaan dan keamanan pesan dengan mengimplementasikan algoritma AES dan *Blockchain* pada aplikasi *chat messenger* berbasis Mobile.

DAFTAR PUSTAKA

- Alfajar, F., & Akbar, M. (2021). Implementasi Keamanan Chat Realtime Menggunakan Aes-Cbc Dan Base64. *Journal of Information System and Artificial Intelligence*, 1(2), 2-4.
- Ali, A. H., & Sagheer, A. M. (2017). Design of Secure Chatting Application with End to End Encryption for Android Platform. *Iraqi Journal for Computers and Informatics (IJCI)*, 43(1), 23-25. doi:http://dx.doi.org/10.25195/2017/4315
- Argani, A., & Taraka, W. (2020). Pemanfaatan Teknologi Blockchain Untuk Mengoptimalkan Keamanan Sertifikat Pada Perguruan Tinggi. *ADI Bisnis Digital Interdisiplin Jurnal*, 1(1), 12-15.
- Astuti, N. I., Arfani, I., & Aribowo, E. (2019). Analysis of the security level of modified CBC algorithm cryptography using avalanche effect. *IOP Conference Series: Materials Science and Engineering*, 5-6.
- Basri. (2016). Kriptografi Simetris dan Asimetris dalam Perspektif Keamanan Data dan Kompleksitas Komputasi. *Scientific Journal of Computer Science, Faculty of Computer Science, Al Asyariah Mandar University*, 2(2), 18-20.
- Das, S. K. (2020). Secure Messaging Platform Using Blockchain Technology. *International Journal of Research in Engineering and Science (IJRES)*, 8(12), 27.
- Harahap, A. K., Oktari, N. S., Kartini, A., Agung, A. A., & K, R. B. (2020). Perbandingan ROI Metode Konsensus Proof of Work, Proof of Stake, dan Proof of Service (Masternode). *Jurnal Teknologi Informasi dan Manajemen*, 2(2), 2-5.
- Ilham, L. I., & Widyassari, A. P. (2021). Pengembangan Aplikasi Pesan Instan Terenkripsi Menggunakan Algoritma Kriptografi AES (Advanced Encryption Standard). *Jurnal Teknik Elektro Smart*, 1(1), 1-4.
- Kurnia Hu, S. D., Palit, H. N., & Handojo, A. (2019). Implementasi Blockchain: Studi Kasus e-Voting. *Jurnal Infra*, 7(1), 184-185.
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin*, 1-8.
- Prameshwari, A., & Sastra, N. P. (2018). Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen. *EKSPLORA INFORMATIKA*, 8(1), 52-54.

- Putri, A. E., Kartikadewi, A., & Rosyid, L. A. (2020). Implementasi Kriptografi Dengan Algoritma Advanced Encryption Standard (AES) 128 Bit Dan Steganografi Menggunakan Metode End Of File (EOF) Berbasis Java Desktop Pada Dinas Pendidikan Kabupaten Tangerang. *Applied Information Systems and Management*, 3(2), 70-77.
- Randi, A., Lazuardy, K., Chandra, S., & Dharma, A. (2020). Implementasi Algoritma Advanced Encryption Standard pada Aplikasi Chatting berbasis Android. *JIKOMSI Jurnal Ilmu Komputer dan Sistem Informasi*, 3(1), 2-4.
- Takale, A. P., Vaidya, C. V., & Kolekar, S. S. (2018). Decentralized Chat Application using Blockchain Technology. *International Journal for Research in Engineering Application & Management (IJREAM)*, 92-93.
- Verma, R., & Sharma, A. K. (2020). Cryptography: Avalanche effect of AES and RSA. *International Journal of Scientific and Research Publications*, 10(4), 119-122.
- Yusfrizal. (2019). Rancang Bangun Aplikasi Kriptografi pada Teks Menggunakan Metode Reverse Chiper dan Rsa Berbasis Android. *Jurnal Teknik Informatika Kaputama*, 3(2), 30-33.