SATIN – Sains dan Teknologi Informasi
Journal Homepage : http://jurnal.sar.ac.id/index.php/satin

Implementasi Metode AES pada Aplikasi Chat Menggunakan *Flutter*

Khusaeri Andesa [1], Afnand Fachzevi [2], Torkis Nasution [3], Herwin [4]
[1]STMIK Amik Riau, khusaeri@sar.ac.id, Jl.Cemara, Pekanbaru, Indonesia
[2]STMIK Amik Riau, zzeviafnand@gmail.com, Jl. Purwodadi Indah, Pekanbaru, Indonesia
[3]STMIK Amik Riau, torkisnasution@sar.ac.id, Jl.Purwodadi KM 10, Pekanbaru, Indonesia
[4]STMIK Amik Riau, herwin@sar.ac.id, Jl.Purwodadi KM 10 , Pekanbaru, Indonesia

Informasi Makalah

Submit : Desember 4, 2023
Revisi : Desember 20, 2023
Diterima : Desember 21, 2323

Kata Kunci :

Asynchronous
Aplikasi *Chatting*
Firebase
Flutter
Dart

Abstrak

Perkembangan komunikasi dari percakapan lisan hingga era digital telah mengubah cara manusia berinteraksi. Era modern menghadirkan aplikasi chatting untuk komunikasi global dalam bentuk teks, panggilan, dan video call. Namun, kemajuan ini juga menghadirkan risiko privasi dan keamanan data. Pengiriman data melalui media chatting diperlukan perlindungan dari ancaman seperti spam, penyadapan, modifikasi, dan fabrikasi data. Penelitian ini bertujuan untuk merancang aplikasi chatting dengan keamanan melalui enkripsi data menggunakan *Algoritma Advanced Encryption Standard* (AES). Metode perancangan menggunakan algoritma AES-128 dengan penerapan dalam pengiriman pesan menggunakan Flutter dan Bahasa pemrograman Dart. Data hasil enkripsi disimpan di Firebase untuk menjaga keamanan. Penelitian ini dapat menyediakan komunikasi yang aman dalam era digital. Hasil dari penelitian ini berupa aplikasi chat dengan keamanan pesan menggunakan metode AES berbasis mobile.

Abstract

The development of communication from oral conversations to the digital era has transformed the way humans interact. The modern era has introduced chatting applications for global communication in the form of text, calls, and video calls. However, this progress has also brought about risks to privacy and data security. The transmission of data through chatting media requires protection against threats such as spam, eavesdropping, data modification, and data fabrication. This research aims to design a chatting application with security through data encryption using the Advanced Encryption Standard (AES) algorithm. The design method employs the AES-128 algorithm with implementation in message transmission using Flutter and the Dart programming language. Encrypted data results are stored in Firebase to ensure security. This research can provide secure communication in the digital era. The outcome of this research is a chat application with message security using the AES method based on mobile technology.

Khusaeri Andesa,
Email: khusaeri@sar.ac.id.

SATIN – Sains dan Teknologi Informasi
Vol. 9, No. 2, Desember 2023, pp. 216-226
ISSN: 2527-9114, DOI: 10.33372/stn.v9i2.1075

1. Pendahuluan

Pada perkembangan komunikasi yang dapat kita lihat adalah berupa percakapan atau penyampaian gagasan antar manusia secara lisan dan bertatap muka baik berupa pidato maupun diskusi, dengan tujuan mendidik, membangkitkan kepercayaan, dan menggerakkan perasaan orang lain.

Pada Era sekarang chatting dapat diartikan sebagai fasilitas yang dapat digunakan untuk berbincang-bincang dalam bentuk teks secara langsung dengan pengguna internet diseluruh dunia yang sedang online pada saat bersamaan yakni aplikasi *chatting* di *platfrom smartphone*. Aplikasi ini menjadi sarana alternatif untuk berkomunikasi diera modern bisa melalu teks pesan, berbagi *file*, panggilan dan *video call*.

Pada era digital saat ini pengiriman data melalui media *chatting* merupakan hal yang biasa dilakukan di web, PC maupun *smartphone*. Dimana masyarakat sudah memiliki perangkat dan akses terhadap jaringan *internet* yang cukup memadai. Dalam penyampaian informasi menggunakan media *internet* membutuhkan suatu tingkat keamanan data, agar data tidak dapat diakses oleh orang yang tidak memiliki izin sehingga kerahasiaannya dapat terjaga terutama aplikasi *chatting*.

Ada beberapa ancaman-ancaman yang dapat terjadi melalui aplikasi *chatting* yang harus diwaspadai dari serangan *hacker*, hal tersebut bisa berupa spam *text* interupsi, penyadapan, malware dan virus.

Penelitian ini bertujuan untuk merancang aplikasi chatting dengan keamanan melalui enkripsi data menggunakan Algoritma *Advanced Encryption Standard* (AES).

Algoritma Advanced Encryption Standard(AES) adalah suatu algoritma *block chipper* dan mempunyai sifat simetri yang menggunakan kunci simetri pada waktu proses enkripsi dan dekripsi. dengan enkripsi data *chating* pada *user* dapat menghindari terjadinya pencurian data pribadi dalam *chatting* antar *user* lainnya dikarenakan data *chating* yang masuk ke *database* sudah terenkripsi dimana dengan menerapkan mekanisme kriptografi akan menutup celah keamanan yang ada pada aplikasi pesan sederhana tersebut. aplikasi ini nantinya memiliki tingkat keamanan yang memuaskan bagi para *user* dengan enkripsi "*end to end*" baik *chat text* dan telepon *video call*. Dengan penerapan aplikasi dapat dihasilkan mekanisme komunikasi yang aman untuk dipakai dalam komunikasi penting agar tidak disadap pihak yang tidak bertanggung jawab (Amalia&Rosyani, 2018).

2. Metode Penelitian

2.1 *Advanced Encryption Standart (AES)*

Algoritma *Advanced Encryption Standard* (AES) adalah suatu algoritma block chipper dan mempunyai sifat simetri yang menggunakan kunci simetri pada waktu proses enkripsi dan dekripsi (Amalia & Rosyani, 2018).

Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (*National Institute of Standard and Technology*) sebagai pengganti algoritma DES (*Data Encryption Standard*) yang sudah berakhir masa penggunaannya. Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan decimal kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit.

Perbedaan dari ketiga urutan tersebut adalah decimal kunci yang mempengaruhi jumlah *Round* (perputaran) yang dapat di lihat pada tabel berikut

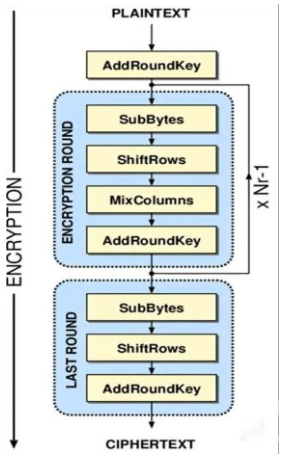
Tabel 1. Jumlah *Round* AES

	Panjang Kunci	**Panjang Blok**	**Jumlah Putaran**
AES– 128	4	4	10
AES– 129	6	4	12
AES– 254	8	4	14

SATIN – Sains dan Teknologi Informasi
Vol. 9, No. 2, Desember 2023, pp. 216-226
ISSN: 2527-9114, DOI: 10.33372/stn.v9i2.1075

A. Enkripsi AES

Proses enkripsi pada algoritma AES terdiri dari 4 jenis transformasi *byte* yaitu *SubBytes*, *ShiftRows*, *Mix Columns* dan *Add Round Key*. Padaawal proses enkripsi, input yang telah di salin ke dalam *state* akan mengalami transformasi *byte Add Round Key*. Setelah itu, *state* akan mengalami transformasi Sub *Bytes*, *Shift Rows*, *Mix Columns* dan *Add Round Key* secara berulang-ulang sebanyak Nr. Jumlah perulangan Nr tergantung pada kunci yang digunakan pada saat awal proses enkripsi. Untuk kunci 128 bit akan melakukan 10 putaran, 192 bit melakukan 12 putaran dan 256 bit melakukan 14 putaran. Proses perulangan sebanyak Nr dalam algoritma AES disebut sebagai *round function*. Round yang terakhir (*last round*) berbeda dengan sebelumnya dimana *state* tidak mengalami transformasi *Mix Columns* (RezaAhmad Kurniawan & Donny Avianto, 2019).

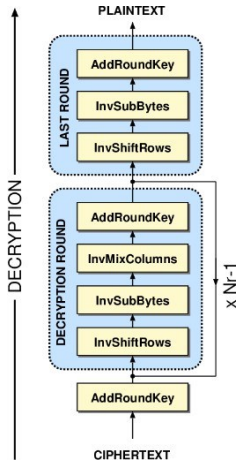


Gambar 1. Enkripsi AES

Gambar 1 merupakan proses dari keseluruhan dekripsi dengan algoritma AES.

B. Dekripsi AES

Transformasi cipher dapat dibalikkan dan di implementasikan dalam arah yang berlawanan untuk menghasilkan inverse *cipher* yang mudah dipahami pada algoritma AES. Transformasi *byte* yang digunakan untuk *inverse cipher* adalah *Inv Shift Rows, Inv Sub Bytes, Inv Mix Columns dan Add Round Key*. Proses dekripsi diawali dengan transformasi *bytes Add Round Key* yang berasal dari *cipher text*. Setelah itu, state akan mengalami transformasi *Inv Shift Rows*, *Inv Sub Bytes, Inv Mix Columns* dan Add *Round Key* secara berulang-ulang sebanyak Nr. Jumlah perulangan Nr tergantung pada kunci yang digunakan pada saat proses enkripsi. Panjang kunci pada saat proses enkripsi dan dekripsi harus sama. Proses perulangan sebanyak Nr dalam algoritma AES disebut sebagai round function. Round yang terakhir (last round) berbeda dengan sebelumnya dimana state tidak mengalami transformasi *Inv Mix Columns*.



Gambar 2. Deskripsi AES

Dari gambar diatas dekripsi AES adalah kebalikan dari enkripsi AES dan dekripsi AES di implementasikan dalam arah yang berlawanan untuk menghasilkan *inversecipher* yang mudah dipahami pada algoritma AES. Transformasi *byte* yang digunakan untuk *inver secipher* adalah *Inv Shift Rows,* Inv *Sub Bytes*, *Inv Mix Columns* dan *Add Round Key.*

2.2 *Platform Android*

Android adalah sistem operasi berbasis Linux yang dirancang untuk perangkat seluler Iayar sentuh seperti telepon pintar dan kompu tertablet. Android awalnya dikembangkan oleh Android, Inc, dengan dukungan finansial dari *Google*, yang kemudian membelinya pada tahun 2005. Sistem operasi ini dirilis secara resmi pada tahun 2007. Antarmuka pengguna Android didasarkan pada manipulasi langsung, menggunakan masukan sentuh yang serupa dengan tindakan di dunia nyata, seperti menggesek, mengetuk, mencubit, dan membalikkan cubitan untuk memanipulasi objek di layar. Android adalah sistem operasi open source, dan Google merilis kode-nya dibawah Lisensi *Apache*. Kode *open source* dan lisensi perizinan pada Android memungkinkan perangkat lunak untuk dimodifikasi secara bebas dan di distribusikan oleh para pembuat perangkat, operator nirkabel, dan pengembang aplikasi (Aryasa & Kurniawan, 2019).

2.3 *Flutter*

flutter merupakan sebuah SDK (*Software Development Kit*) yang digunakan untuk mengembangkan aplikasi mobile yang dibuat oleh *Google*. Flutter dikembangkan untuk membuat aplikasi yang mempunyai *performance* yang tinggi dan dapat dipublikasikan untuk *platform* Android dan iOS dari *codebase* tunggal. Flutter menggunakan bahasa pemrograman dart sehingga dapat dengan mudah untuk dipelajari. Bahasa pemrograman dart dianggap mudah apabila telah terbiasa dan familiar menggunakan Bahasa pemrograman Java atau *Javascript*. Selain itu, Flutter juga menyediakan kerangka *reactive- functional*, mesin render 2D, *widget* yang siap untuk digunakan, dan tools yang digunakan untuk membantu dalam melakukan pengembangan aplikasi (Sari et al, 2022).

Menurut penjelasan diatas dapat disimpulkan bahwa flutter adalah sebuah *framework* aplikasi *mobile* sumber terbuka yang diciptakan oleh *Google* menggunakan Bahasa pemograman *Dart*. Flutter digunakan dalam pengembangan
aplikasi untuk sistem operasi Android, iOS, Windows, Linux, MacOS, serta menjadi metode utama untuk membuat aplikasi. Flutter juga mendukung untuk pengembangan aplikasi berbasis web.

2.4 *Dart*

Dart merupakan bahasa pemrograman yang dibuat oleh *Google* dan didesain oleh *Lars Bak* dan *Kasper Lund*. Bahasa pemrograman Dart dapat digunakan untuk membangun aplikasi *server* atau dalam bentuk *command line interface*, web, ataupun *mobile* (*Android* dan iOS). Dart merupakan Bahasa pemrograman yang mendukung adanya pendefinisian fungsi di luar kelas atau sering disebut dengan top- level function. Dalam Dart. Kode program utama disimpan didalam fungsi main() samahalnya seperti C/C++[10]. Dart merupakan bahasa pemrograman yang bersifat *open source*. Dart merupakan bahasa pemrograman yang menggunakan konsep berorientasi objek dengan sintaks gaya C. Hal tersebut mendukung konsep pemrograman seperti antarmuka, *class*, tidak seperti bahasa pemrograman lainnya, Dart tidak mendukung *array*. Dart dapat mereplikasi struktur data seperti *array*, *generic* dan pengetikan *opsional* (Sari et al, 2022).

2.5 *Firebase Realtime Database*

Firebase Realtime Database merupakan sebuah *Cloud Hosted database* yang dapat menyimpan dan melakukan sinkronisasi data secara realtime untuk setiap client yang terhubung. Setiap kali pengguna memperbarui data, maka akan menyimpan data pada cloud dan sekaligus memberitahu kesemua client yang terhubung dan secara otomatis client menerima pembaruan dengan data terbaru (Aryasa & Kurniawan, 2019).

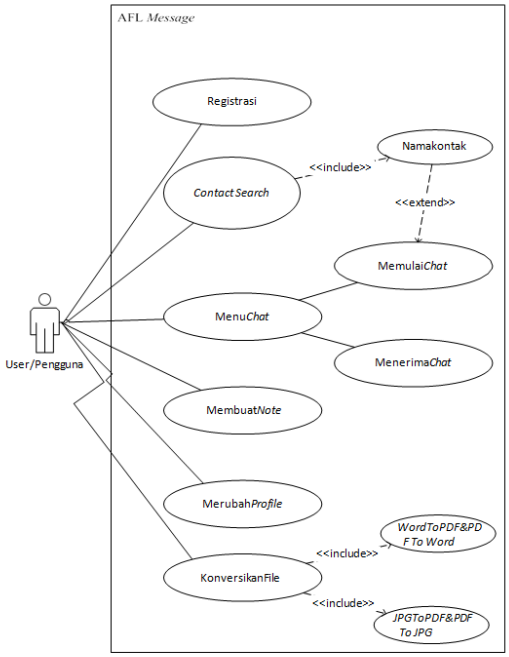
SATIN – Sains dan Teknologi Informasi
Vol. 9, No. 2, Desember 2023, pp. 216-226
ISSN: 2527-9114, DOI: 10.33372/stn.v9i2.1075

2.6 *Model Unified Modeling Language*

Model UML digunakan untuk pemodelan secara visual dalam sarana perancangan sistem berorientasi objek, atau definisi UML yaitu sebagai suatu bahasa yang sudah menjadi standar pada visualisasi, perancangan dan juga pendokumentasian sistem.

A. *Use case* Diagram

Use case diagram digunakan untuk menjelaskan manfaat sistem menurut perspektif orang yang berada diluar sistem. Sehingga kebutuhan masukan, keluaran serta interaksi aktor terhadap sistem dapat digambarkan sebelum pembuatan dari sistem itu dilakukan.



Gambar 3. *Usecase Diagram*

Untuk mendiskripsikan *use case* apa saja dan siapa saja aktor yang terlibat, maka untuk lebih jelas digunakan tabel sebagai beriktu:

Tabel 2. *Usecase Diagram*

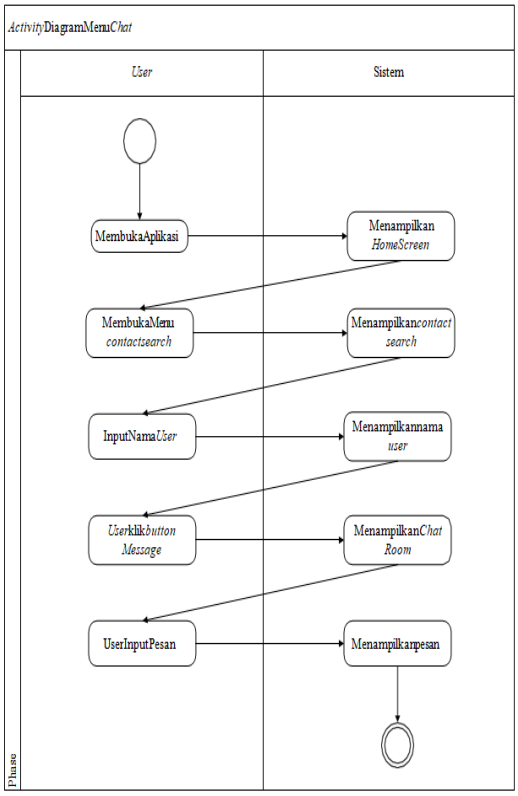
Actor	Use Case	Deskripsi
User	Registrasi	Proses dimulai dari user melakukan registrasi pada aplikasi chat dengan memasukkan nomor telepon dan mulai menggunakan aplikasi chat kemudian user akan melakukan pencarian user berdasarkan nama kontak dan user memulai aktifitas chat dengan user lain selanjutnya user membuat catatan berupa note dan mengubah format file sesuai yang di inginkan user.
	SearchUser	
	MulaiAplikasi (chat)	
	MulaiAplikasi (note)	
	MulaiAplikasi (converter)	

B. *Activity* Diagram

Activity Diagram adalah diagram yang menggambarkan aktivitas dari sebuah sistem atau worlflow aliran kerja. Yang perlu diperhatikan adalah bahwa diagram aktivitas menggambarkan aktivitas sistem bukan apa yang dilakukan aktor, jadi aktivitas yang dapat dilakukan oleh sistem.

Activity diagram ini menggambarkan kejadian yang terjadi pada saat pengguna mengakses menu chat. Adapun kejadian tersebut dapat dilihat pada gambar diagram berikut ini:

SATIN – Sains dan Teknologi Informasi
Vol. 9, No. 2, Desember 2023, pp. 216-226
ISSN: 2527-9114, DOI: 10.33372/stn.v9i2.1075

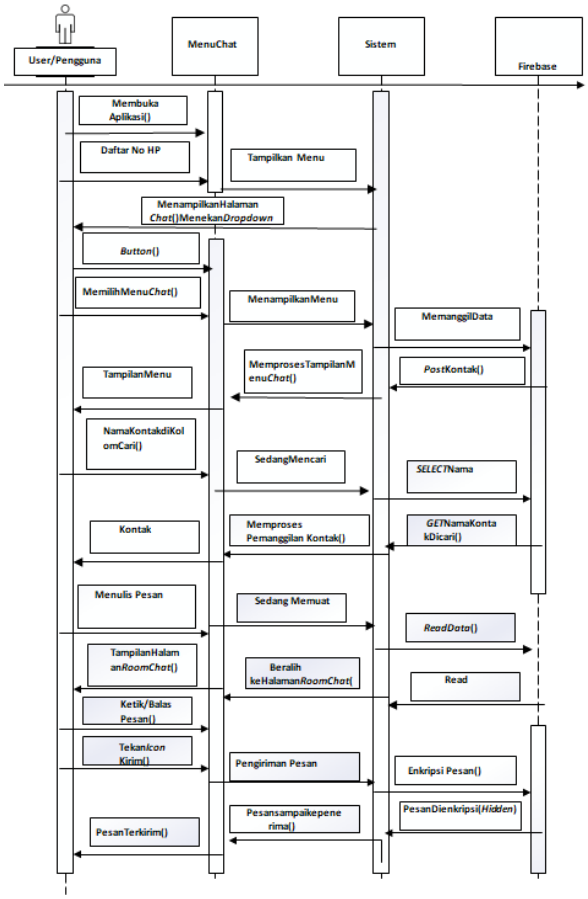


Gambar 4. *Activity Diagram* Chat

C. Sequence Diagram

Sequence diagram menggambarkan interaksi antar objek di dalam dan di sekitar sistem termasuk pengguna, *display*, dan sebagainya berupa *message* yang digambarkan terhadap waktu. *Sequence diagram* terdiri atas dimensi vertikal waktu dan dimensi *horizontal* objek-objek yang terkait. Tujuan utama dari pembuatan diagram urutan adalah untuk mengetahui urutan kejadian yang dapat menghasilkan output yang diinginkan. Selain itu, tujuan dari diagram urutan ini mirip dengan *activity diagram* loh, seperti menggambarkan alur kerja dari sebuah aktivitas, serta dapat menggambarkan aliran data dengan lebih detail, termasuk data atau perilaku yang diterima atau dikirimkan.

Pada diagram ini terdapat satu aktor sebagai user yang terlibat dengan alur skema aplikasi "*Chat*". Berdasarkan aliran perintah setiap aktor, sehingga aplikasi *message* dapat berjalan sesuai rancangan. Berikut gambaran *sequence diagram* pada aktor user dalam aplikasi Chat ini adalah :



Gambar 5. *Sequence Diagram* Chat

3. Metode Penelitian

Model proses pembangunan aplikasi untuk penelitian ini menggunakan metode *Advanced Encryption Standard*. AES algoritma kriptografi simetris yang dapat digunakan untuk mengamankan data. Algoritma ini merupakan standar enkripsi dengan kunci simetris. Contah proses enkripsi dan deskripsi sebagai berikut :

A. Proses *Algoritma Enkripsi* AES – 128

Diketahui *Plaintext*= 'afnandafnandafna'. Dengan kunci 'fachzfachzfachzf'. Panjang kunci XOR untuk mengenkripsi *plain teks*. Nilai karakter-karakter tersebut akan dikonversi kedalam *American Standard Code for Information Interchange* (ASCII) Menurut Winarno & Cahyanto, 2021 merupakan tabel karakter printable maupun *non-printable* ASCII adalah sebuah kode

SATIN – Sains dan Teknologi Informasi
Vol. 9, No. 2, Desember 2023, pp. 216-226
ISSN: 2527-9114, DOI: 10.33372/stn.v9i2.1075

standar yang digunakan dalam pertukaran informasi pada komputer. Jumlah karakter ASCII adalah sebanyak 255, dimana karakter ASCII urutan 0 sampai 127 merupakan karakter ASCII untuk manipulasi teks, karakter ASCII urutan 128 sampai 255 merupakan karakter ASCII untuk manipulasi grafik. ASCII memiliki karakter kontrol yang dibedakan menjadi 5 kelompok sesuai penggunaan berturut-turut yaitu *Logical Communication, Device Control, Information Separator, Code Extension,* dan *Physical Communication.* Karakter ASCII ini banyak di jumpai pada papan ketik computer atau instrumen-instrumen digital. kemudian di konversikan kedalam kode biner kemudian dilakukan oprasi XOR pada tiap-tiap karakter antara plainteks terhadap kuncinya, sehingga didapat hasil sebagai berikut:

Plain: a=61, f=66, n =6E,a=61, n =6E,d=64

Tabel 3. *Plain teks*

a	f	n	a		61	66	6E	61
n	d	a	f	ASCII	6E	64	61	66
n	a	n	d		6E	61	6E	64
a	f	n	a		61	66	6E	61

Key: fachzfachzfachzf

f =66, a=61, c=63, h=68, z=7A

Tabel 4. *Key*

f	a	c	h		66	61	63	68
z	f	a	c	ASCII	7A	66	61	63
h	z	f	a		68	7A	66	61
c	h	z	f		63	68	7A	66

1. Tahapan *Add Round key*
   fungsi Add Round Key juga dikenal sebagai transformasi forward add round key. 128-bit status adalah bitwise XOR-ed dengan 128 bit kunci bulat add roundkey menghasilkan satu kolom pada satu waktu. Dalam add round key konversi American Standard Code for Information Interchange (ASCII) kedalam biner.

Tabel 5. *Add RoundKey*

61	66	6E	61	66	61	63	68	07	07	00	09
6E	64	61	66	7A	66	61	63	14	02	00	05
6E	61	6E	64	68	7A	66	61	06	1B	08	05
61	66	6E	61	63	68	7A	66	02	0E	14	00

Proses

Tabel 6. *Proses Add RoundKey*

61XOR 66 =07	6EXOR 7A =14	6EXOR 68 =06	61XOR 63 =02
66XOR 61 =07	64XOR 66 =02	61XOR 7A =1B	66XOR 68 =0E
6EXOR 63 =00	61XOR 61 =00	6EXOR 66 =08	6EXOR7A= 14
61XOR 68 =09	66XOR 63 =05	64XOR 61 =05	61XOR 61 =00

2. Tahapan *SubByte*
   Fungsi *transformasi American Standard Codefor Information Interchange* (ASCII) Ke *Substitute* Box(S Box).

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Gambar 6. Tahapan *SubByte*

Tabel 7. Hasil *SubByte*

07	07	00	09	63	63	7C	7D
14	02	00	05	CA	AF	7D	AF
06	1B	08	05	A7	6E	A4	AF
02	0E	14	00	C7	5A	7C	63

SATIN – Sains dan Teknologi Informasi
Vol. 9, No. 2, Desember 2023, pp. 216-226
ISSN: 2527-9114, DOI: 10.33372/stn.v9i2.1075

3. Tahapan *ShiftRow*
   1. *Row* 1: *byte* 2 bergeser kekanan menuju byte 4 pada *byte* 4 dan 3 kekiri menuju *byte* 3 dan 2
   2. *Row* 2: *byte* 1 bergeser kekanan menuju *byte* 3, *byte* 4 menuju *byte* 3 dan seterusnya pada *byte* 3 dan 2 berbalik menuju kiri
   3. *Row* 3: *byte* 1 bergeser kekanan menuju *byte* 4, *byte* 2 menuju *byte* 4 dan seterusnya pada *byte* 4 dan 3 berbalik menuju kiri
   4. *Row* 4: *byte* 4 geser kekiri menuju *byte* 1 , *byte* 1 geser kekanan dan seterusnya pada *byte* 2 dan 3

Tabel 8. Hasil *Shift Row*

63	7C	7D	63	
AF	7D	AF	CA	=R2
A4	AF	A7	6E	
63	C7	5A	7C	

4. Tahap *Mix Culumn*

Tabel 9. Hasil *Mix Culum*

63 7C 7D 63		02 03 01 01		EF 51 1D 1E
AF 7D AF CA	x	01 02 03 01	=	DE 1A 17 16
A4 AF A7 6E		01 01 02 03	R4	9D 0E D4 58
63 C7 5A 7C		03 01 01 02		5C 6B 6A 9F

Proses:

Untukkolom pertama (63AFA4 63)
02 * 63 +03 * AF +01 *A4 +01 * 63 =3E+8E+A4 +63 =EF

01 * 63 +02 * AF +03 *A4 +01 * 63 =63 +5E+FC +63=DE

01 * 63 +01 * AF +02 *A4 +03 * 63 =63 +AF +48 +FA =9D

03* 63 +01 * AF +01 *A4 +02 * 63 =E9+AF + A4 +C6 =5C

B. Proses *Algoritma Deskripsi* AES – 128

Dekripsi adalah kebalikan dari proses enkripsi, Proses dekripsi diawali dengan transformasi bytes *Add Round Key* yang berasal dari *cipher text*. Setelah itu, state akan mengalami transformasi *Inv Shift Rows, Inv Sub Bytes*, *Inv Mix Columns* dan *Add Round Key.*

1. Tahapan *Add Round key*

Tabel 10. *Add RoundKey*

7A	F6	02	0F	66	61	63	68	14	97	61	67
D8	75	70	D4	7A	66	61	63	13	15	15	B7
7D	C3	CF	3C	68	7A	66	61	11	5D	7C	71
1F	19	4D	81	63	68	7A	61	37	E0	7C	71

Tabel 11. *Proses Add RoundKey*

7AXOR 66 =14	D8XOR7A=A2	75 7D XOR 68 = 15	1FXOR 63 =7C
	XOR 66 = 13	C3XOR7A=B9	
F6XOR61=97	70XOR 61 =11	CFXOR 66 =A1	19XOR 68 =71
	D4XOR 63 =B7	3CXOR 61 =5D	
02XOR 63 =61			4DXOR 7A =37
0FXOR 68 =67			81XOR 61 =E0

2. Tahapan *Inverse Shifting Row*

Tabel 12. *Inverse Shifting Row*

14	97	61	67	14	97	61	67
13	15	15	B7	A2	15	B7	13
11	5D	7C	71	7C	71	11	5D
37	E0	7C	71	71	37	E0	7C

3. Tahapan *Inverse SubByte*

Tabel 13. *Inverse SubByte*

B1	4A	30	23
10	72	D5	C9
E4	F6	8E	94
5A	85	8B	4A

4. Tahapan *Inverse Mix Column*

Tabel 14. *Inverse Mix Column*

B1	4A	30	23	0E	0B	0D	09	A0	24	6A	01
10	72	D5	C9	09	0E	0B	0D	6C	02	6D	02
E4	F6	8E	94	0D	09	0E	0B	1C	22	24	30
5A	85	8B	4A	0B	0D	09	0E	2A	30	3E	3D

Proses

SATIN – Sains dan Teknologi Informasi
Vol. 9, No. 2, Desember 2023, pp. 216-226
ISSN: 2527-9114, DOI: 10.33372/stn.v9i2.1075

0E* B1 + 0B * 10 + 0D * E4 +09 * 5A =9E+1B +2D +46 = A0

09* B1 +0E * 10 +0B * E4 +0D * 5A=A9 +0E +E5 +3E =6C

0D * B1 + 09 * 10 +0E* E4 +0B * 5A =BD +90 +C8 +67 =1C

0B * B1 +0D * 10 +09 * E4 +0E * 5A=AB+D0 +B8 +72 =2A

4. Hasil dan Pembahasan

Hasil dan pembahasan adalah tahapan penggunaan atau penerapan desain perancangan input output yang telah dirancang dan diimplementasi pada sistem yang telah dibuat dapat dilihat seperti pada gambar dibawah ini :

Dalam tahapan implementasi tampilan aplikasi ini diperlukan perangkat smartphone untuk mengakses aplikasi ini. Berikut hasil implementasi tampilan aplikasi "AFL Chat" yang telah dirancang.

A. *Splashscreen*

Tampilan Awal ketika pertama kali aplikasi ini di load

Gambar 6. *Splashscreen*

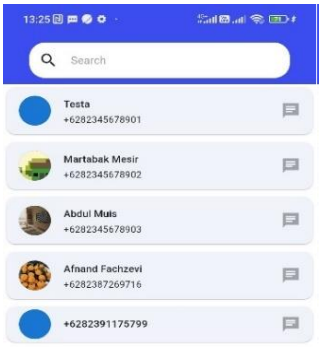
B. Home *Screen*

Tampilan Home *Screen* adalah tampilan awal pengguna yang terdiri dari beberapa manajemen menu yang dapat di gunakan oleh user.

Gambar 7. *Home Screen*

C. *Search Screen*

Tampilan ini adalah menu pencarian data pengguna aplikasi chat.

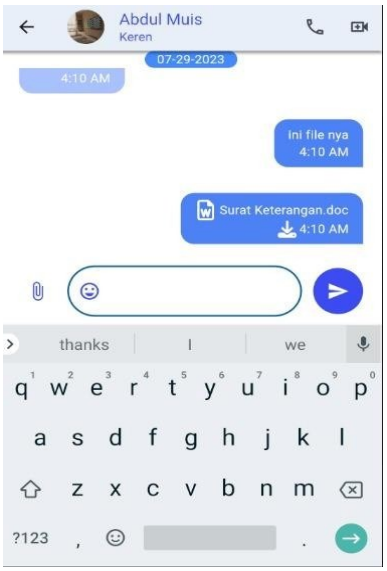


Gambar 8. *Search Screen*

D. *Chat Screen*

Tampilan ini adalah halaman *chatting* Yang bias dilakukan oleh pengguna aplikasi yang dapat saling bertukar informasi berupa text, video dan file yang sudah di convert dan di lakukan proses enkripsi dan deskripsi.

SATIN – Sains dan Teknologi Informasi
Vol. 9, No. 2, Desember 2023, pp. 216-226
ISSN: 2527-9114, DOI: 10.33372/stn.v9i2.1075



Gambar 9. *Chat Screen*

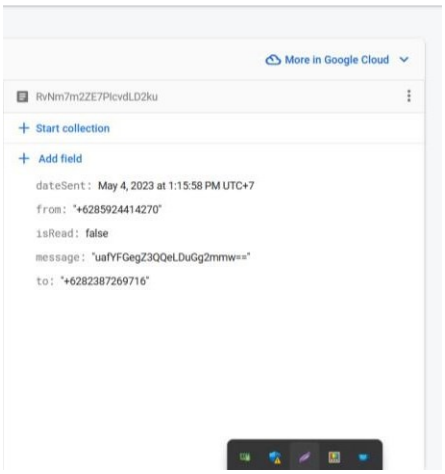
E. *Files Convert*

Tampilan hasil convert file pada aplikasi

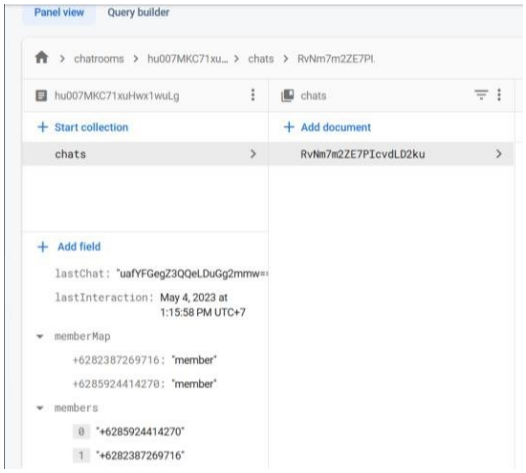
Gambar 10. *Files Convert*

F. Enkripsi & Deskripsi Chat

Rancang aplikasi chat dengan keamanan pesan menggunakan metode kriptografi Advanced Encryption Standart(AES) berbasis mobile dengan prosesen crypt dan decrypt pada pesan



Gambar 11. Enkripsi & Deskripsi Chat 1



Gambar 12. Enkripsi & Deskripsi Chat II

5. Simpulan

Berdasarkan hasil pembahasan penulis lakukan dari bab bab sebelumnya maka dapat disimpulkan bahwa aplikasi memiliki fitur yang beragam yang dapat memudahkan penggunanya seperti note yang berfungsi untuk sebuah catatan kecil dan converter untuk mengubah format file kemudian aplikasi juga memungkinkan pengguna untuk berkomunikasi secara instan dengan orang lain, baik dalam bentuk teks, suara, atau video. Hal ini memungkinkan pengguna untuk berinteraksi secara real-time, tanpa keterbatasan waktu dan jarak.

Aplikasi chat yang telah diimplementasikan dengan tingkat keamanan yang baik dan menggunakan enkripsi data

menyajikan lingkungan komunikasi yang aman dan terlindungi. Dengan menerapkan teknologi enkripsi seperti Advanced Encryption Standard (AES), aplikasi ini memastikan bahwa setiap pesan yang dikirimkan melalui platform tersebut terjaga kerahasiaannya dan tidak dapat diakses oleh pihak yang tidak berwenang.

6. Referensi

Saefudin., & . Syamsudin. (2017). Aplikasi Enkripsi Pesan Teks Dengan Metode Advanced Encryption Standard Pada Ponsel Berbasis Android. JSiI (*Jurnal Sistem Informasi*), 3, 29 - 31.

Ajhari,A.A.,&Windarto,W.(2018).ImplementasiAlgoritmaAffineCipherDan Aes-128UntukPengamananPesanDanOneTimePasswordRegistrasiAkun Pada Aplikasi Chatting Berbasis Android Di Sma Hang Tuah 1 Jakarta. Skanika, 1(1), 323–334.

Amalia, R., & Rosyani, P. (2018). Implementasi Algoritma AES dan Algoritma XOR pada Aplikasi Enkripsi dan Dekripsi Teks Berbasis Android. Faktor Exacta, 11(4), 370.https://doi.org/10.30998/faktorexacta.v11i4.2878.

Amiruddin, A., & Rohmani, M. F. (2021). Perancangan Spesifikasi Keamanan untuk Pengembangan Aplikasi Secure Chat Berdasarkan *Common Criteria For It Security Evaluation*. *Jurnal Teknologi Informasi Dan Ilmu Komputer*,8(6), 1215.https://doi.org/10.25126/jtiik.2021863637.

Aryasa,K.,&Kurniawan,Y.E.(2019).ImplementasiFirebaseRealtimeDatabase Untuk Aplikasi Pemesanan Menu Berbasis Android. *Sensitif: Seminar Nasional Sistem Informasi Dan Teknologi Informasi*, 71–78.

Azanuddin, A., Yakub, S., & Prayudha, J. (2022). Implementasi Keamanan Citra Menggunakan Algoritma AES-128 Dengan Aplikasi Client-Server. Jurasik (*Jurnal Riset Sistem Informasi Dan Teknik Informatika*), 7(1),51.https://doi.org/10.30645/jurasik.v7i1.415.

Bahari, M. F. (2022). Analisa Dan Implementasi Keamanan Pesan Chatting Menggunakan Algoritma Challenge Response. JUSSI: *Jurnal Sains Dan Teknologi Informasi*, 1(2), 49–53.

Fadhlurrahman, Z., & Ariyani, F. (2018). Aplikasi Chatting Notaris Berbasis Android Dengan Metode Kriptografi AES-128 dan Blowfish. Skanika, 1(2), 656–661.

Fitriani,I.,&Utomo,A.B.(2020).ImplementasiAlgoritmaAdvancedEncryption Standard (AES) pada Layanan SMS Desa. JISKA (Jurnal Informatika Sunan Kalijaga), 5(3), 153–163. https://doi.org/10.14421/jiska.2020.53-03.

Halim,R.C.,&Sugiarto,S.(2018).PenerapanAlgoritmaAESdalamPerancangan Aplikasi Media Sosial Berbasis Android. Jurnal ENTER, 1, 368–379.

Ridlo, I. A. (2017). Pedoman Pembuatan Flowchart. Academia.Edu, 27. academia.edu/34767055/Pedoman_Pembuatan_Flowchart.