Pembuatan Aplikasi Chat Messenger Menggunakan *Advanced Encryption* Standard (AES) dan *Firebase Realtime Database*

Vinsensius Arka Biwara Adi[1], Ramadhian Agus Triono Sudalyo[2], Abdillah Baraja[3]
[1,2,3]Universitas Surakarta
email: [1]vinsensiusarka@gmail.com, [2]ramadhian_at@unsa.ac.id, [3]abdillahbaraja@unsa.ac.id

Abstract: *Currently the chat messenger application is used so that fellow Android users can communicate online using the internet. Chat messenger is one of the most widely used communication media for smartphone users. However, the messages sent are not necessarily safe from cybercrime crimes such as message tapping or message manipulation. The development of this chat messenger application uses Advanced Encryption Standard (AES) cryptography as a message data security system. AES cryptography is a federal information standard established by the National Institute of Standards and Technology (NIST). Messages sent will be encrypted in advance using the password to be ciphertext, so that the message cannot be read by unauthorized persons. When the message is received, the message decryption process is carried out using the same key during the encryption process where the incoming ciphertext will be converted back into plaintext or a message that can be read according to the initial message sent. If during transmission, the message sent is changed or manipulated by someone, then the incoming message cannot be read because during the decryption process, the key and ciphertext will not match each other. Through compatibility testing carried out by using several types of mobile devices with various devices using Android version 5.1 Lollipop to Android version 8.0 Oreo with the system functional test feature, valid results were obtained and based on the results of usability testing, the MyChat messenger application after testing by measuring learnability (how much easy application), efficiency (speed in operating the application), memorability (the user's ability to memorize application features when they are not using them), error (the system provides feedback interaction to the user) and satisfaction (user satisfaction after using the application) obtained 97% results with interpretation succeed*

Keywords*: Android, Chat Messenger, Advanced Encryption Standard, Firebase*

Abstrak: Saat ini aplikasi *chat messenger* digunakan agar sesama pengguna Android dapat berkomunikasi secara *online* menggunakan internet. *Chat messenger* merupakan salah satu media komunikasi yang paling banyak digunakan para pengguna *smartphone*. Namun pesan yang dikirimkan belum tentu aman dari kejahatan *cybercrime* seperti penyadapan pesan atau manipulasi pesan. Pembangunan aplikasi *chat* m*essenger* ini menggunakan kriptografi Advanced Encryption Standard (AES) sebagai sistem keamanan data pesan. Kriptografi AES merupakan standar informasi federal yang ditetapkan oleh National Institute of Standards and Technology (NIST). Pesan yang dikirim akan di enkripsi terlebih dahulu menggunakan kata kunci menjadi *chipertext*, sehingga pesan tersebut tidak dapat terbaca oleh orang yang tidak berkepentingan. Pada saat pesan sampai dipenerima dilakukan proses dekripsi pesan menggunakan kunci yang sama saat proses enkripsi dimana *chipertext* yang masuk akan diubah kembali menjadi *plaintext* atau pesan yang dapat dibaca sesuai pesan awal yang dikirimkan. Jika pada saat transmisi, pesan yang dikirimkan diubah atau dimanipulasi oleh orang, maka pesan yang masuk tidak akan dapat dibaca karena pada saat proses dekripsi, kunci dan *chipertext* tidak akan cocok satu sama lain. Melalui pengujian *compatibility* dilakukan dengan cara menggunakan beberapa macam perangkat *mobile* dengan berbagai *device* menggunakan Android versi 5.1 Lollipop hingga Android versi 8.0 Oreo dengan fitur uji fungsional system didapatkan hasil valid dan berdasarkan hasil dari pengujian *usability*, aplikasi MyChat *messenger* setelah dilakukan pengujian dengan mengukur *learnability* (seberapa mudah aplikasi), *efficiency* (kecepatan dalam pengoperasian aplikasi), *memorability* (kemampuan pengguna dapat menghafal fitur aplikasi ketika sudah tidak menggunakanya), *error* (sistem memberikan interaksi *feedback* pada *user*) dan *satisfaction* (kepuasan pengguna setelah menggunakan aplikasi) diperoleh hasil 97% dengan interpretasi berhasil.
Kata kunci*: Android, Chat Messenger, Advanced Encryption Standard, Firebase*

Pendahuluan

Pemerhati Keamanan Siber sekaligus staf *Engagement and Learning SpeciaList* di Engage Media, Yerry Niko Borang, mengingatkan, penting bagi masyarakat untuk mempelajari aplikasi percakapan yang akan digunakan. Termasuk pula, penting dalam hal menyelidiki dan menelaah aplikasi *chat* yang aman melalui keterangan hak konsumen yang biasanya dicantumkan di bagian *help* atau *website*. Pada sebuah kasus, di media sosial, para pengguna Whatsapp mengungkapkan kekhawatirannya soal keamanan data dengan adanya kebijakan baru Whatsapp. Ada pula yang memilih untuk pindah aplikasi yang dianggap lebih aman. Sebagai konsumen, masyarakat harus waspada terhadap adanya perubahan kebijakan ini. Kondisi Ini juga merupakan tugas pemerintah untuk memproteksi data dan privasi warganya. Ada pula kekhawatiran, dengan perubahan kebijakan ini akan mengarah pada pengambilan data warga negara oleh entitas negeri lain tanpa bisa dicegah. Kebijakan privasi dan aturan layanan baru dari WhatsApp ini dinilai memiliki potensi ancaman luas. Misalnya, kekhawatiran data yang dikumpulkan akan digunakan untuk kepentingan ekonomi, politik, hingga keamanan. Misalnya jika data-data ini dihubungan dengan data-data lain, dan siapa yang suka produk spesifik. Siapa yang memiliki tendensi politik tertentu. Bahkan, suatu saat bisa saja data-data tersebut digunakan untuk memprediksi siapa yang akan memilih kandidat atau partai mana di masa depan. Kasus *Cambridge Analytica* yang dengan bantuan Facebook berhasil memengaruhi pemilu Amerika khususnya dalam kenaikan Trump, adalah contoh nyata yang sangat berbahaya (Aida, 2021).

Dari kondisi dan kasus di Indonesia dan dunia, maka untuk menghadapi permasalahan *cybercrime* perlu untuk membuat suatu sistem keamanan, salah satu cara untuk meningkatkan keamanan pesan adalah dengan menggunakan kriptografi. Kriptografi merupakan ilmu yang mempelajari tentang mengamankan pesan dengan cara disandikan. Dengan penggunaan kriptografi, data atau pesan akan diamankan dengan cara dienkripsi menjadi *ciphertext* sehingga data atau pesan tidak dapat dibaca langsung. Supaya data atau pesan dapat dibaca diperlukan suatu proses dekripsi yang berfungsi untuk mengubah data *chipertext* kembali menjadi *plaintext* yang dapat dibaca.

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian *modern*, kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi *modern* saja tidak berurusan hanya dengan penyembunyian pesan, namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi (Mukhtar, 2017).

Berdasarkan Jubilee Digital (2016), c*hatting* adalah suatu *feature* atau suatu program di internet untuk berkomunikasi langsung sesama pengguna internet yang sedang *online* dan sedang sama-sama menggunakan Internet. Komunikasi ini dapat berupa teks (text *Chat*) ataupun suara *voice chat* atau definisi *chatting* adalah suatu pesan *instant* ataupun *instant messaging* di sebuah teknologi jaringan komputer yang mengijinkan pemakainya untuk mengirimkan pesan ke pengguna lain yang tersambung dalam sebuah jaringan komputer ataupun internet.

AES atau Advanced Encryption Standard merupakan standar enkripsi kunci simetri yang pada awalnya diterbitkan dengan algoritma Rijndael. Algoritma ini dikembangkan oleh dua kriptografer Belgia, Joan Daemen dan Vincent Rijmen. Advanced Encryption Standard (AES) dipublikasikan oleh NIST (National Institute of Standard and Technology) pada tahun 2001. AES merupakan blok kode simetris untuk menggantikan DES (Data Encryption Standard). Algoritma AES merupakan algoritma simetris yaitu menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu

e-ISSN: 2685-5615
p-ISSN: 2715-5315

tipe : AES-128, AES-192, dan AES-256. Masing-masing tipe menggunakan kunci internal yang berbeda yaitu round *Key* untuk setiap putaran (Prasetyo, 2006).

AES mendukung panjang kunci 128 bit sampai 256 bit. Panjang kunci dan ukuran Blok dapat dipilih secara independen dan setiap blok dienkripsi sejumlah putaran tertentu. AES mempunyai panjang kunci paling sedikit 128 bit, maka AES tahan terhadap serangan *exhaustive Key search* dengan teknologi saat ini. Dengan panjang kunci 128 bit, maka terdapat sebanyak: 2128 = 3,4 × 1038 kemungkinan kunci. Jadi Jika digunakan komputer tercepat yang dapat mencoba 1 juta kunci setiap detik, maka akan dibutuhkan waktu 5,4 × 1024 tahun untuk mencoba seluruh kemungkinan kunci. Jika digunakan komputer tercepat yang dapat mencoba 1 juta kunci setiap milidetik, maka akan dibutuhkan waktu 5,4 × 1018 tahun untuk mencoba seluruh kemungkinan kunci (Prasetyo, 2006).

Salah satu fitur yang dimiliki oleh Firebase adalah sebuah layanan basis data yang dapat disinkronkan secara *realtime* kepada permintaan klien yang terhubung. Data disimpan dalam format JSON. Saat mengembangkan aplikasi lintas *platform* seperti Android, iOS, maupun JavaScript, semua klien berbagi sebuah instance Realtime Database dan menerima *update* data terbaru yang sama dan secara otomatis (Purnomo, Purbo, dan Aziz, 2021).

Metode

Pertama Studi pustaka merupakan sumber data tertulis yang didapat dari berbagai referensi seperti buku, sumber arsip, jurnal, dan dokumen-dokumen resmi untuk mendapatkan hal yang ada kaitannya dengan pembuatan aplikasi c*hatting*. Kedua metode observasi adalah sistem pengumpulan data dengan cara melakukan pengamatan secara langsung pada beberapa contoh aplikasi *chatting online*. Ketiga menganalisis bagaimana cara yang digunakan membuat aplikasi *chat messenger* secara aman dan cepat sehingga harapan aplikasi ini dapat membantu pengguna untuk memberikan fasilitas *chat messenger* yang nyaman.

Dari data yang didapatkan, selanjutnya dilakukan analisa dan perencanaan terhadap sistem yang akan dibuat. Meliputi perancangan sistem, analisa data, dan perancangan *interface*. Kemudian Melakukan pembuatan *database* penyimpanan sistem dengan Google Firebase, pembuatan dan perancangan desain aplikasi menggunakan Android Studio dengan menggunakan bahasa pemrograman Java. Terakhir dilakukan uji aplikasi dengan perangkat keras *smartphone* menggunakan *Black Box Testing* dan *white box Testing* serta dengan pengujian kuisioner.

Hasil

Tampilan Halaman *Register*

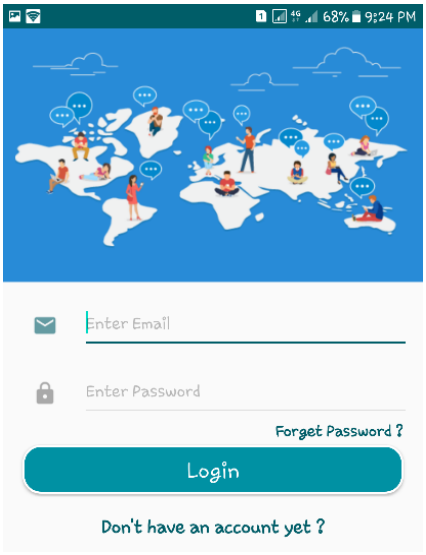
Halaman *register* seperti pada Gambar 1 merupakan halaman awal untuk masuk ke halaman *home* dan agar *user* dapat membuat akun untuk mengakses aplikasi

Gambar 1. Halaman *register*

e-ISSN: 2685-5615
p-ISSN: 2715-5315

Tampilan Halaman *Login User*

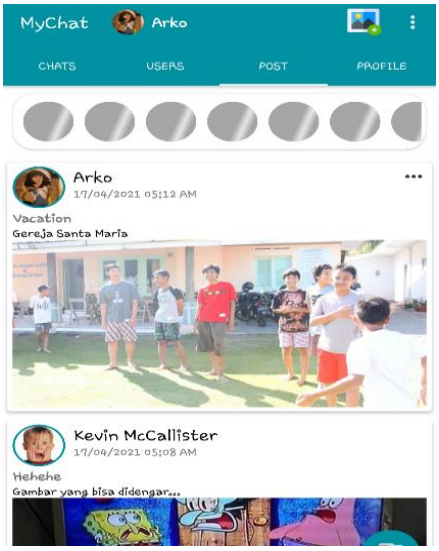
Halaman *login* seperti pada Gambar 2 merupakan halaman setelah pengguna *login* menggunakan *user account* yang sudah didaftarkan pada halaman *register*.



Gambar 2. Halaman *login*

Tampilan Halaman *Home User*

Halaman seperti pada Gambar 3 *home user* merupakan halaman yang berisi fungsi seperti *chat list*, *user list*, *post*, profil, *setting* dan *logout*.

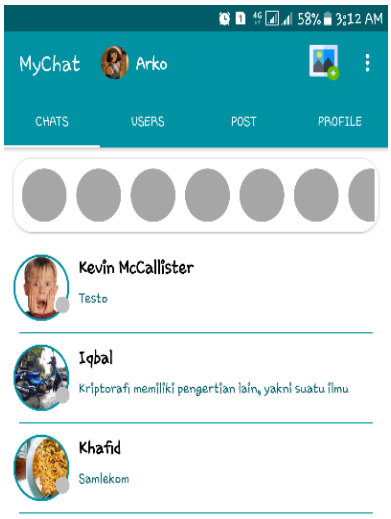


Gambar 3. Halaman *home user*

Tampilan Halaman Daftar *Chat*

Halaman c*hat* seperti pada Gambar 4 merupakan halaman untuk melihat daftar *chat* terakhir pada aplikasi dimana dapat melakukan membalas pesan terakir, dan menghapus pesan.

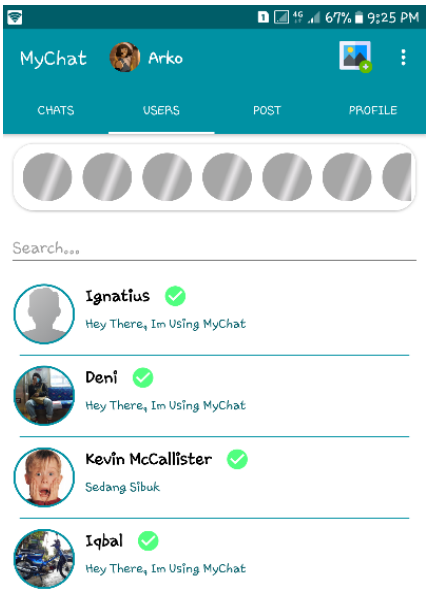
e-ISSN: 2685-5615
p-ISSN: 2715-5315



Gambar 4. Halaman daftar *chat*

Tampilan Halaman Daftar *User*

Halaman berisi daftar *user* yang terdaftar pada aplikasi my*chat* seperti pada Gambar 5.

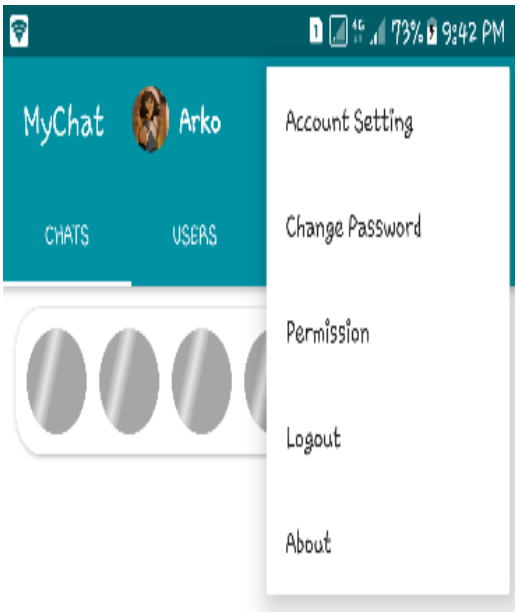


Gambar 5. Halaman daftar *user*

Tampilan Halaman Daftar *Post*

Halaman yang berisi daftar *post* dari beberapa *user* yang terdaftar di aplikasi my*chat* seperti pada Gambar 6.

e-ISSN: 2685-5615
p-ISSN: 2715-5315



Gambar 6. Halaman Daftar *Post*

Tampilan Halaman *Chat* Room

Halaman yang berisi ruang obrolan antar pengguna aplikasi my*chat* seperti pada Gambar 7.

Gambar 7. Halaman *chat room*

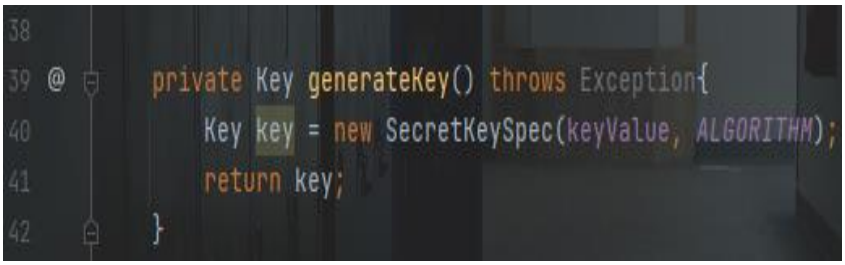
e-ISSN: 2685-5615
p-ISSN: 2715-5315

Hasil Pengembangan Sistem

Hasil dari implementasi kode program enkripsi dan dekripsi menggunakan bahasa pemrograman Java seperti pada Gambar 8.

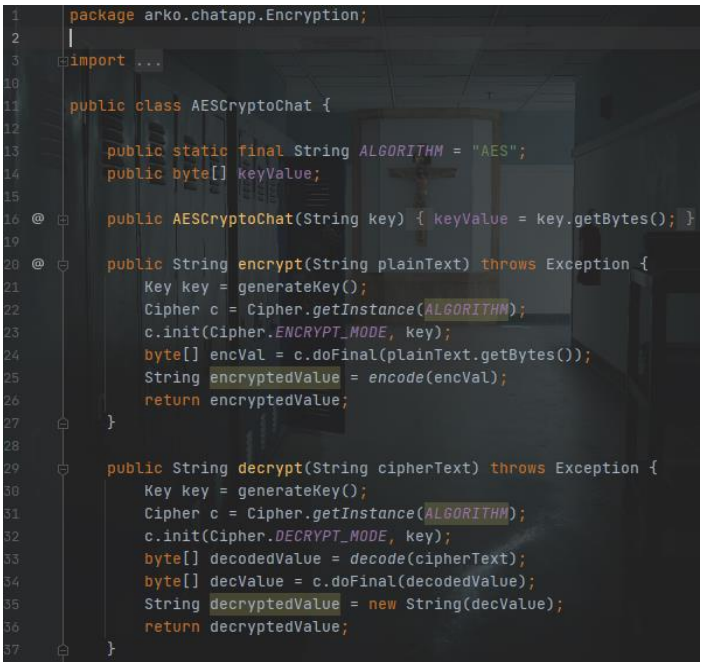
Gambar 8. Kode Program *Key*

Kode program yang tertera adalah *key* untuk menjalankan enkripsi dan dekripsi AES seperti pada Gambar 9.



Gambar 9. Kode Program *Generate Key*

Kode program yang tertera adalah *object generate* yang dipanggil dari k*ey value* dan algoritma AES untuk menghasilkan enkripsi dan dekripsi seperti pada Gambar 10.



Gambar 10. Kode Program Enkripsi dan Dekripsi

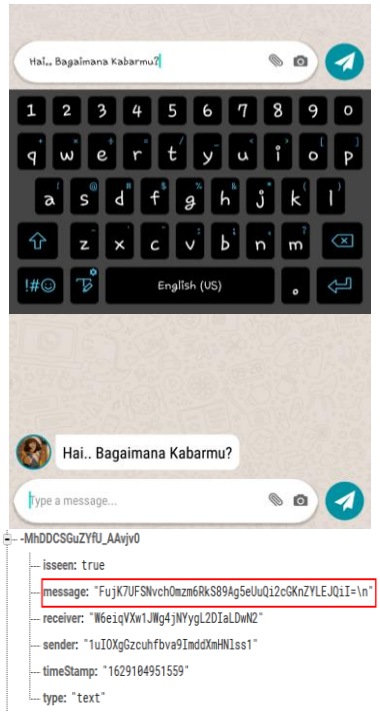
Baris 20 – 27 adalah kode program deklarasi *method* Enkripsi untuk dipanggil ke bagian input pesan dan menjadikan *plaintext* input pesan menjadi *chipertext*. Baris 29 – 37 adalah kode program deklarasi *method* Dekripsi untuk dipanggil ke bagian *class adapter* penampil pesan dan menjadikan *chipertext* menjadi *plaintext*.

e-ISSN: 2685-5615
p-ISSN: 2715-5315

Hasil Pengujian Sistem

Testing Enkripsi

Tabel 1. *Black Box Testing* Enkripsi

Pengujian Enkripsi	Hasil yang Diharapkan
Mengisi pesan *plaintext* dengan kata "Hai.. Bagaimana Kabarmu?" pada salah satu *User* didalam *Chat room* dan menampilkan data pesan yang sudah dienkripsi dalam bentuk Json pada Firebase *database*.	Hasil Pengujian : 
Status Pengujian	Valid

Pengujian *compatibility*

Dilakukan dengan cara menggunakan beberapa macam perangkat *mobile* dengan berbagai *device* menggunakan Android versi 5.1 Lollipop hingga Android versi 8.0 Oreo dengan fitur uji fungsional sistem. Pengujian dilakukan dengan menggunakan 3 *device* Android yang tersaji dalam gambar 11.

No	Model	Spesifikasi	
1	Redmi 3S	Versi OS	5.1.1 Lollipop
		CPU	Qualcomm octa-core 1,4 GHz
		RAM	3GB
		Layar	5" Beresolusi (1.280x720 px)
	Status	Valid	
2	Samsung Galaxy Note 5	Versi OS	7.0 Nougat
		CPU	Exynos 7420 octa-core 2.1 GHz
		RAM	4GB
		Layar	5.7" Beresolusi (1440x2560 px)
	Status	Valid	
3	Sony Xperia X Compact	Versi OS	8.0 Oreo
		CPU	Snapdragon 650 1.4 GHz
		RAM	3GB
		Layar	4.6" Beresolusi (720x1280 px)
	Status	Valid	

Gambar 11. Pengujian *Compability*

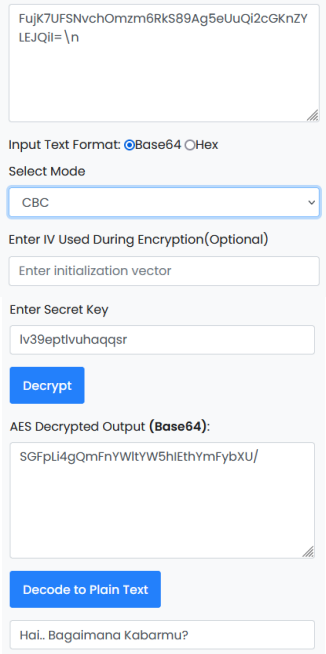
e-ISSN: 2685-5615
p-ISSN: 2715-5315

Pengujian *Usability*

Pengujian usability digunakan untuk mengukur *learnability* (seberapa mudah mencari fitur utama, menu, dan menggunakan semua fasilitas yang ada pada aplikasi), *efficiency* (seberapa efisien sistem sehingga user yang telah mempelajari sistem dapat mencapai tingkat produktivitas yang tinggi), *memorability* (seberapa mudah diingat fitur sistem sehingga user telah biasa menggunakan sistem), *error* (kesalahan-kesalahan yang dilakukan oleh user selama berinteraksi dengan aplikasi) dan *satisfaction* (kepuasan dari User selama menggunakan aplikasi). Untuk pengujian *usability* dilakukan dengan menggunakan metode kuisioner. Kuisioner nantinya akan menggunakan 10 responden setelah menggunakan aplikasi ini, kemudian responden diminta mengisi kuisioner, hasil dari kuisioner yang telah diisi nantinya akan diolah untuk dianalisis

Testing Dekripsi

Tabel 2**.** *Black Box Testing* Dekripsi

Pengujian Dekripsi	Hasil yang Diharapkan
Melakukan *Testing* Dekripsi pada *chipertext* yang sudah terenkripsi AES, memasukkan dan melakukan *Generate* Secret *Key* dan melakukan *decode to plaintext* maka akan menampilkan kembali pesan yang dienkripsi AES.	Hasil Pengujian : 
Status Pengujian	Valid

Pembahasan

Berdasarkan hasil dari pengujian *usability*, aplikasi MyChat *messenger* setelah dilakukan pengujian dengan mengukur *learnability* (seberapa mudah aplikasi), *efficiency* (kecepatan dalam pengoperasian aplikasi), *memorability* (kemampuan pengguna dapat menghafal fitur aplikasi ketika sudah tidak menggunakanya), *error* (sistem memberikan interaksi *feedback* pada *user*) dan *satisfaction* (kepuasan pengguna setelah menggunakan aplikasi). Dilakukan pengujian langsung kepada 10 responden *user* menggunakan aplikasi, kemudian responden diminta mengisi kuisioner. Berdasar data kuisioner didapatkan total untuk jawaban dari 10 responden adalah: sangat setuju = 53, untuk jawaban setuju = 35, jawaban netral = 10, jawaban tidak setuju = 1 dan sangat tidak setuju = 0. Kemudian total jawaban tersebut diolah dalam perhitungan presentase *usability*, dari hasil perhitungan tersebut didapatkan bahwa jumlah untuk persentase usability yakni sebesar 97%. Maka

kesimpulan dari hasil perhitungan kuantitatif menurut Arikunto untuk hasil persentase 97% termasuk ke dalam kualifikasi baik dan berhasil.

Simpulan

Aplikasi yang dikembangkan dapat mengamankan pesan teks sehingga terjaga kerahasiaannya dari pihak yang tidak bertanggung jawab, yang tidak berkepentingan, dan yang tidak berhak mengetahui apa isi pesan tersebut. Sistem enkripsi yang stabil dan terjaga, dengan kata lain pesan tidak akan berkurang atau mengalami kerusakan saat disimpan pada *database*. Keseluruhan data-data pesan tidak akan hilang walaupun aplikasi sudah dihapus dari *smartphone* pengguna, karena pesan-pesan yang terkirim terkirim dan terenkripsi akan disimpan pada Firebase *database.*

Daftar Pustaka

Abdulloh, Rohi. (2020). Menguasai React JS Untuk Pemula Panduan Belajar Javascript Dari Dasar Hingga Membuat Aplikasi Web Modern. Rohi Abdullah.

Aida, Nur Rohmi. 12 Januari 2021. Galau karena Kebijakan Baru WhatsApp, Setujui atau Pindah Aplikasi? Kompas.com. Diunduh pada tanggal 22 Juni 2021. Pukul 22.04 WIB. https://www.kompas.com/tren/read/2021/01/12/195200565/galau-karena-kebijakan-baru-whatsapp-setujui-atau-pindah-aplikasi?page=all

Enterprise, Jubilee. (2015). Mengenal Dasar-Dasar Pemrograman Android. Elex Media Komputindo: Jakarta

Haqi, Bay. 2019. Aplikasi SPK Pemilihan Dosen Terbaik Metode *Simple Additive Weighting* (SAW) Dengan Java. Deepublish: Yogyakarta

Herlinah dan Musliadi. (2019). *Pemrograman Aplikasi Android Dengan Android Studio,Photoshop, dan Audition,* Elex Media Computindo: Jakarta

Hermawan, Stephanus. (2011). Mudah Membuat Aplikasi Android. Penerbit Andi: Yogyakarta.

Hadi, Wahyu Krishna dan Mulyati, Sri. (2017). Pengamanan Aplikasi *Chatting* Pada Perangkat Android Menggunakan Kriptografi Dengan Metode *Advanced Encryption Standard* (AES) 128. P*ada PT. Salam Medina Indonesia,* BIT , Volume 14, No. 2. September 2017, ISSN: 1693-9166.

Jubilee Digital. (2016). Kursus Singkat Dan Cepat Internet. Jubilee Enterprise: Yogyakarta

Kroenke, David M. (2005). *Database Processing* (Dasar-Dasar, Desain, Dan Implementasi). Erlangga: Jakarta

Mukhtar, Harun. (2018). Kriptografi Keamanan Untuk Data. Deepublish: Yogyakarta

Mohammad Arifin, Mufti. (2018). Implementasi Kriptografi *Chatting* Menggunakan Metode *Vigenere Dan AES 128 Bebasis Web*, SKANIKA, Volume 1, No. 1. Maret 2018.

Prasetyo, Didik Dwi. (2006). Pemrograman Aplikasi *Database* Dengan VB Net 2005. Elex Media Computindo: Jakarta

Purnomo, Rosyana Fitria, Purbo, Onno W, dan Aziz, RZ. Abd. (2021). *Firebase* Membangun Aplikasi Berbasis Android. Andi: Yogyakarta

Rozaq, Afifur. (2017). Pembangunan Aplikasi Brawijaya Messenger Dengan Menggunakan *Platform* Firebase *Pada Universitas Brawijaya.*