APLIKASI *CHATTING* MENGGUNAKAN KRIPTOGRAFI BERBASIS ANDROID

Moch. Bahrul Ulum
Teknik Informatika, Institut Teknologi Nasional Malang
bahrul.ulum2310@gmail.com

ABSTRAK

Salah satu media sosial yang populer di kalangan masyarakat Indonesia adalah aplikasi *chatting*. Pada proses chatting tentu ada informasi rahasia yang terkandung. Ada kalanya seseorang ingin mengambil kesempatan untuk mendapatkan informasi rahasia tersebut. Pada acara tertentu yang memerlukan privasi tinggi, sebuah sistem keamanan sangatlah diperlukan untuk menjaga kerahasiaan informasi. Seperti pada acara pemilihan rektor universitas dan dekan fakultas yang memerlukan sistem keamanan jaringan dan informasi khusus untuk melindungi komunikasi yang terjadi antara panitia dan staff acara.

Kriptografi dapat digunakan untuk tujuan keamanan, tetapi teknik lain masih diperlukan untuk membuat komunikasi yang aman, terutama untuk memastikan integritas dan autentikasi dari sebuah pesan. Teknik kriptografi digunakan penulis untuk menjaga pesan agar aman. Sebuah algoritma kriptografi disebut *cipher*, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dimengerti selain orang yang dituju. Dekripsi adalah suatu upaya pengolahan informasi menjadi sesuatu yang dapat diutarakan secara jelas dan tepat dengan tujuan agar dapat dimengerti oleh orang yang dituju

Setelah dilakukan proses pengujian terhadap aplikasi, dapat disimpulkan bahwa aplikasi dapat mengirim pesan enkripsi kepada lebih dari 2 *client* yang terhubung dalam satu jaringan lokal yang sama dan aplikasi ini memiliki versi *mobile* dan *web*. Pesan enkripsi yang dikirimkan akan dilakukan proses dekripsi untuk mengetahui pesan yang sebenarnya disampaikan ke penerima.

Kata kunci : *kriptografi, android, chatting, base64, keamanan jaringan, group chat*

1. PENDAHULUAN

1.1 Latar Belakang

Media sosial sudah menjadi sesuatu yang penting di kalangan masyarakat Indonesia. Media sosial mempermudah kita dalam berhubungan sesama masyarakat tanpa mengenal ruang dan waktu. Informasi yang dipertukarkan pun bervariasi baik dari jenisnya maupun tingkat kerahasiaannya. Mulai dari data pribadi, data organisasi sampai data negara yang sangat rahasia. Hal inilah yang menuntut adanya pengamanan informasi tersebut sehingga tidak sampai tersadap oleh pihak ketiga. Salah satu media sosial yang populer di kalangan masyarakat Indonesia adalah aplikasi *chatting.* Dengan aplikasi *chatting* kita bebas mengobrol apa saja dan dimana saja. (Prisgunanto, 2015)

Pada tahun 2016 sebuah tim peretas mengklaim telah berhasil mengeksploitasi kelemahan yang tersemat pada jaringan telekomunikasi yang bernama SS7 (*Signalling System 7).* Mekanisme peretasannya terjadi dengan mengelabui jaringan operator agar terkoneksi ke *router* pada perangkat yang digunakan peretas. Mereka juga membuat akun duplikat dan mengeksploitasi SS7 lebih lanjut agar semua pesan komunikasi seperti di WhatsApp dan Telegram bisa dimata-matai. SS7 merupakan jaringan yang menghubungkan seluruh penyedia jasa telekomunikasi di dunia. Dengan memanfaatkan celah keamanan SS7 ini *hacker* seolah-olah menduplikasi nomer telepon korban. Sehingga perusahaan penyedia layanan telekomunikasi menganggap bahwa nomer *handphone* peretas adalah nomer *handphone* korban. Hal tersebut tentunya sangat merugikan para pengguna karena mereka merasa tidak aman lagi. (Ismail, 2016)

Semua aksi peretasan sangat merugikan terutama di kalangan perusahaan dan organisasi. Oleh karena itu, untuk mencegah terjadinya peretasan komunikasi dibutuhkan sebuah aplikasi *chatting* yang menggunakan jaringan khusus untuk berkomunikasi serta menerapkan metode kriptografi untuk mengamankan pesan. Pada acara tertentu yang memerlukan privasi tinggi, sebuah sistem keamanan jaringan dan informasi tersebut sangatlah diperlukan untuk menjaga kerahasiaan informasi. Seperti pada acara pemilihan rektor universitas dan dekan fakultas yang memerlukan sistem keamanan khusus untuk mengamankan proses komunikasi yang dilakukan oleh pihak panitia acara maupun staff acara. Informasi yang tidak boleh sampai bocor pada saat proses komunikasi contohnya adalah informasi tentang siapa saja calon-calon rektor, wakil rektor, dan dekan yang akan dipilih nanti, serta informasi mengenai siapa yang terpilih menjadi rektor, wakil rektor, dan dekan nantinya. Sistem keamanan jaringan dan informasi adalah suatu sistem yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan dan informasi agar terhindar dari berbagai ancaman luar yang mampu

meretas jalur komunikasi dan mengambil informasi yang ada.

Kriptografi adalah suatu teknik untuk menjaga informasi agar aman dengan cara mengenkripsi dan mendekripsi informasi tersebut. Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Dikarenakan enkripsi telah digunakan untuk mengamankan komunikasi di berbagai negara, hanya organisasi-organisasi tertentu dan individu yang memiliki kepentingan yang sangat mendesak akan kerahasiaan yang menggunakan enkripsi. Dekripsi adalah suatu upaya pengolahan data menjadi sesuatu yang dapat diutarakan secara jelas dan tepat dengan tujuan agar dapat dimengerti oleh orang yang tidak langsung mengalaminya sendiri. Pada umumnya dekripsi menegaskan sesuatu, seperti apa sesuatu itu kelihatannya, bagaimana bunyinya, bagaimana rasanya, dan sebagainya. (Nufus, 2009)

Salah satu metode kriptografi adalah base64. Dengan metode ini, keamanan data dapat lebih terjamin, karena pesan teks yang ditransfer dalam bentuk teks enkripsi. Sedangkan untuk mengamankan jalur komunikasi, sebuah sistem keamanan ganda sangat diperlukan yaitu menggunakan router mikrotik sebagai jalur komunikasi antar pengguna. Dengan menggunakan router mikrotik sebagai media penghubung, dapat digunakan untuk menerapkan filter keamanan dan *monitoring* jaringan.

Penelitian ini dilakukan berdasarkan latar belakang permasalahan yang sudah diuraikan pada paragraf diatas. Untuk menyelesaikan permasalahan tersebut maka penulis melakukan penelitian dengan membangun sebuah aplikasi *chatting* menggunakan kriptografi berbasis *mobile* dan *web* yang menggunakan jaringan *private* WLAN sebagai media penghubung.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan sebelumnya, maka penulis akan merumuskan masalah yang akan dibahas sebagai berikut :

1. Bagaimana membuat aplikasi *chatting* berbasis *mobile* dan *web* yang dapat mengamankan pesan ?
2. Bagaimana cara agar aplikasi dapat berkomunikasi secara *realtime* di jaringan *private* ?
3. Bagaimana cara agar *user* dapat berkomunikasi dengan lebih dari satu *user* dalam waktu yang bersamaan ?
4. Bagaimana memastikan pesan enkripsi yang dikirim dapat terbaca oleh penerima ?

1.3 Batasan Masalah

Dalam penyusunan penelitian ini agar menjadi sistematis dan mudah dimengerti, maka akan diterapkan beberapa batasan masalah. Batasan-batasan masalah itu antara lain.

1. Sistem ini digunakan untuk mengamankan komunikasi suatu kegiatan tertentu yang membutuhkan privasi untuk menjaga kerahasiaan informasi.
2. Sistem berkomunikasi menggunakan jaringan WLAN *(Wireless Local Area Network) private* dan harus mengkonfigurasi SSID (*Service set Identifier*) secara manual serta memasukkan *password login.*
3. Pengguna harus selalu berada di dalam aplikasi untuk menerima pesan dari pengguna lain.
4. *IP Address* perangkat harus dalam satu jaringan yang sama.
5. Data yang dienkripsi dalam sistem adalah data teks.
6. Pada aplikasi tidak dapat menyisipkan pesan rahasia di dalam *file audio, image,* dan *video.*
7. *Minimum requirement* OS Android 4.4 (KitKat) dan *Target requirement* OS Android 5.1 (Lollipop).
8. Metode kriptografi yang digunakan untuk men-enkripsi pesan adalah base64.
9. Perangkat lunak (*software*) yang digunakan untuk membuat aplikasi adalah Eclipse IDE Juno.
10. Perangkat lunak (*software*) yang digunakan untuk *web server* adalah Apache Tomcat 7.0.56.
11. Pengujian dilakukan menggunakan 2 jenis *browser* yaitu mozilla firefox, google chrome.
12. Aplikasi ini hanya berjalan di mode *potrait* pada perangkat *mobile* berbasis android.
13. Pada aplikasi ini tidak disertakan *logger* untuk merekam aktifitas *chatting* setelah keluar dari aplikasi.

1.4 Tujuan

Adapun tujuan yang ingin dicapai dari pembuatan aplikasi *chatting* ini adalah.

1. Untuk menghasilkan aplikasi *chatting* berbasis *mobile* dan *web* yang dapat mengenkripsi dan mendekripsi pesan.
2. Untuk menghasilkan aplikasi *chatting* berbasis *mobile* dan *web* di jaringan *private* agar komunikasi internal dapat dilakukan dengan cepat, aman, dan murah.
3. Untuk menghasilkan aplikasi *group chat* yang memudahkan pengguna berkomunikasi dengan lebih dari satu pengguna dalam satu *chat room.*
4. Menganalisa hasil dekripsi pesan, dimana keluaran pesan harus sama dengan pesan yang dikirim.

1.5 Manfaat

Adapun manfaat dari pembuatan aplikasi *chatting* ini adalah sebagai berikut.

1. Mengamankan pesan rahasia dari pihak ketiga yang dikirim oleh pengirim pesan kepada penerima pesan.
2. Memudahkan pengguna dalam penggunaannya karena berbasis *mobile* dan *web.*
3. Memudahkan pengguna untuk berkomunikasi dengan lebih dari satu pengguna lainnya dalam satu *chat room.*

2. TINJAUAN PUSTAKA

2.1. Penelitian Terkait

Dalam penelitiannya Yulianingsih (2014), membuat aplikasi *chatting* rahasia menggunakan algoritma *vigenere cipher.* Penelitian ini bertujuan untuk membuat suatu aplikasi kriptografi berbasis yang dapat menyandikan teks dan mengirimkan teks yang terenkripsi melalui jaringan berdasarkan algoritma *vigenere cipher.* Aplikasi ini melakukan kriptografi pada teks berupa huruf, angka dan simbol. Kunci yang digunakan berupa alfanumerik yang merupakan gabungan huruf, angka dan simbol. Setelah dilakukan implementasi, hasilnya adalah aplikasi dapat melakukan pengiriman pesan teks yang telah terenkripsi melalui jaringan LAN (*Local Area Network*) sehingga kerahasiaan dari pesan tersebut dapat terjaga keamanannya. Namun kekurangan dari aplikasi ini adalah masih berbasis *desktop,* sehingga kurang fleksibel untuk digunakan karena memerlukan instalasi untuk tiap-tiap *PC* yang akan digunakan untuk kegiatan operasional.

2.2. Aplikasi *Chatting*

Aplikasi *Chatting* sudah merambah kalangan anak-anak, remaja, dewasa bahkan orang tua sekalipun. Dengan *chatting,* kita bebas mengobrol apa saja mulai dari pekerjaan kantor, persahabatan, pelajaran sekolah, mata kuliah, sampai dengan hal yang bersifat pribadi sekali pun. *Chatting* adalah teknologi dalam sebuah jaringan untuk mengirim dan menerima pesan pengguna lain yang tersambung dalam suatu jaringan komputer. (Nasution, 2016).

2.3. Jaringan Komputer

Sebuah jaringan komputer dapat memiliki puluhan ribu atau bahkan jutaan node. Tiap komputer, printer atau periferal yang terhubung dengan jaringan disebut node. Sebuah jaringan biasanya terdiri dari 2 atau lebih komputer yang saling berhubungan diantara satu dengan yang lain, dan saling berbagi sumber daya, atau memungkinkan untuk saling berkomunikasi secara elektronik. (Santoso, 2012).

2.4. Protokol TCP/IP

TCP/IP (*Transmission Control Protocol/Internet Protocol*) digunakan untuk mengatur komunikasi data komputer di internet. TCP/IP menggunakan model komunikasi *client/server* dimana pengguna komputer (*client*) melakukan permintaan yang dikirim ke *server* dan *server* memberikan balasan berupa layanan seperti mengirim halaman *web* melalui jaringan. Komputer-komputer yang terhubung ke internet berkomunikasi dengan protokol ini. Karena menggunakan Bahasa yang sama, yaitu protokol TCP/IP, perbedaan jenis komputer dan sistem operasi tidak menjadi masalah. (Sarif, 2011).

2.5. Kriptografi

Kriptografi berfungsi untuk menjaga kerahasiaan informasi. Dalam menjaga kerahasiaan informasi, kriptografi mengubah *plaintext* ke dalam bentuk *ciphertext* yang tidak dapat dikenali. *Ciphertext* inilah yang kemudian dikirimkan oleh pengirim kepada penerima. Setelah sampai di penerima, *ciphertext* tersebut ditranformasikan kembali ke dalam bentuk *plaintext* agar dapat dikenali (Nufus, 2009).

2.6. Base64

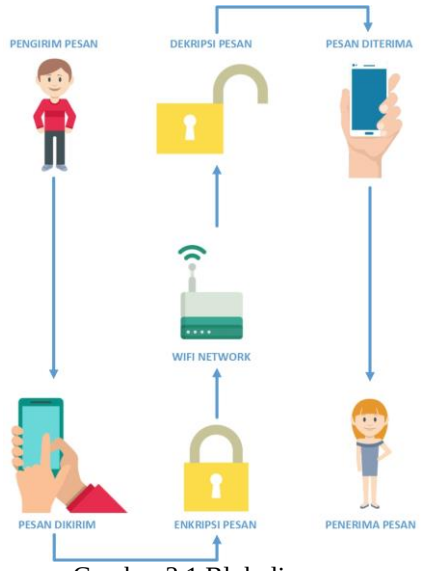
Algoritma Base64 merupakan salah satu algoritma untuk enkripsi dan dekripsi data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metode yang digunakan untuk melakukan enkripsi terhadap data binary. Prinsip enkripsinya adalah dengan memilih kumpulan dari 64 karakter yang dapat diprint (printable), dengan demikian data dapat disimpan dan ditransfer melewati media yang didesain untuk menangani data tekstual, penggunaan lain Base64 adalah untuk melakukan pengacakan data. (Nufus, 2009).

2.7. Android

Android merupakan sistem operasi yang berbasis Linux untuk telepon pintar dan computer tablet. Android menyediakan platform open source bagi para *developer* untuk menciptakan aplikasi mereka sendiri untuk digunakan oleh bermacam-macam *device.* Sebagai sebuah proyek yang bersifat open source, memungkinkan android untuk sepenuhnya dipahami dan dianalisis mengenai fitur, penyelesaian pada *bug* program hingga *hardware* (Ardiyanto, 2012).

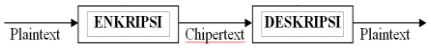
3. METODE PENELITIAN

Pada bagian ini akan dijelaskan tentang desain sistem yang terdiri dari blok diagram dan *flowchart.* Pada Gambar 3.1 dibawah ini merupakan gambaran diagram blok sistem.



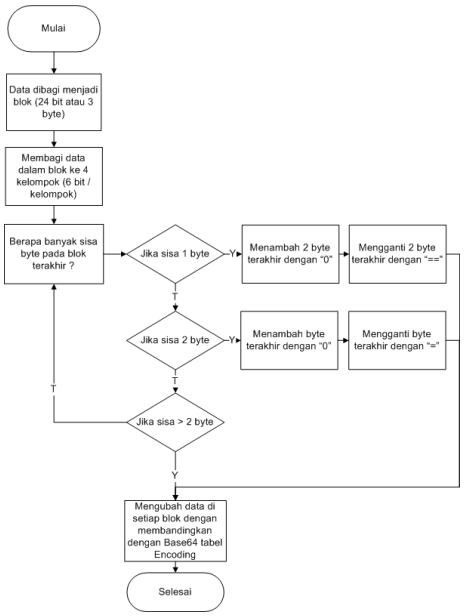
Gambar 3.1 Blok diagram

Pada Gambar 3.2 dibawah ini menjelaskan tentang proses enkripsi dan dekripsi pada pengiriman pesan. Dalam tahap perhitungan enkripsi pesan *plaintext* menggunakan algoritma base64.



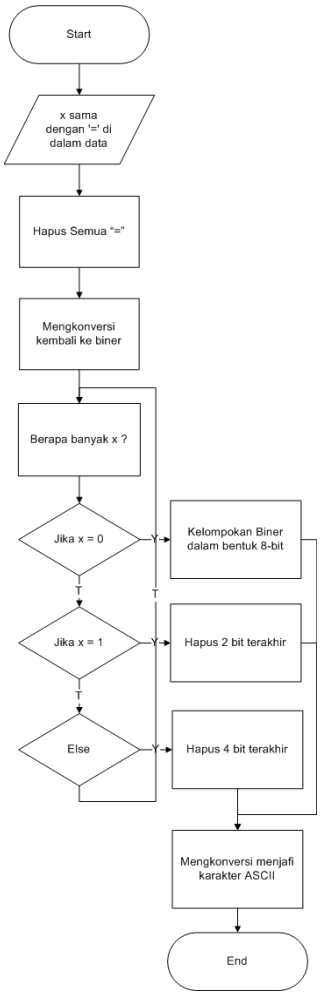
Gambar 3.2 Proses Enkripsi dan Dekripsi

Pada Gambar 3.3 dibawah ini adalah *flowchart* enkripsi data, dimana data yang masih berbentuk *plaintext* akan diubah menjadi data *ciphertext.*



Gambar 3.3 *Flowchart* enkripsi

Pada Gambar 3.4 dibawah ini adalah *flowchart* dekripsi data, dimana data yang masih berbentuk *ciphertext* akan diubah menjadi data *plaintext.*



Gambar 3.4 *Flowchart* dekripsi

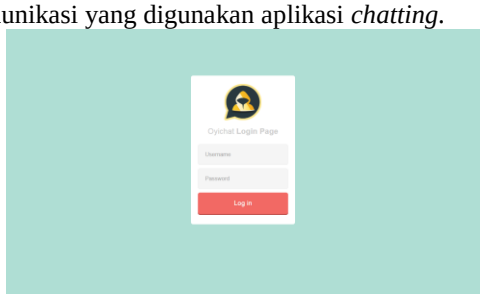
Dalam tahap enkripsi dan dekripsi akan dilakukan pembandingan dengan tabel base64 *encoding* seperti pada Gambar 3.5 berikut.

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	A	42	q	58	6
11	L	27	B	43	r	59	7
12	M	28	C	44	s	60	8
13	N	29	D	45	t	61	9
14	O	30	E	46	u	62	+
15	P	31	F	47	v	63	/

Gambar 3.5 Base64 *encoding*

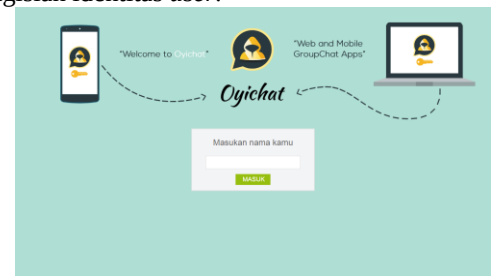
4. HASIL DAN PEMBAHASAN

Pada Gambar 4.1 merupakan tampilan halaman *login hotspot* untuk masuk ke dalam jaringan komunikasi yang digunakan aplikasi *chatting*.



Gambar 4.1 Halaman *login hotspot*

Pada Gambar 4.2 merupakan tampilan halaman *login* aplikasi versi *web* yang digunakan untuk pengisian identitas *user*.



Gambar 4.2 Halaman *login* aplikasi versi *web*

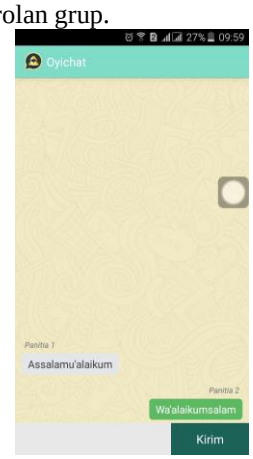
Pada Gambar 4.3 berikut ini merupakan tampilan halaman *chatting* versi *web* yang digunakan untuk melakukan obrolan grup.

Gambar 4.3 Halaman *chatting* versi *web*

Pada Gambar 4.3 merupakan tampilan halaman *login* aplikasi versi *mobile* yang digunakan untuk pengisian identitas *user*.

Gambar 4.4 Halaman *login* aplikasi versi *mobile*

Pada Gambar 4.5 merupakan tampilan halaman *chatting* versi *mobile* yang digunakan untuk melakukan obrolan grup.



Gambar 4.5 Halaman *chatting* versi *mobile*

Pada tahap pengujian dilakukan dengan menggunakan metode *blackbox* yaitu menguji fungsionalitas dari perangkat lunak saja. Fungsionalitas sistem diuji dalam beberapa sistem operasi dan *web browser*.

Tabel 4.1 berikut ini merupakan tabel hasil pengujian fungsionalitas dari aplikasi berdasarkan sistem operasi android yang digunakan.

Tabel 4.1 Pengujian Fungsional Sistem

No	Fungsi	*Android OS*		
		Kit Kat	Lolli pop	Marsh mallow
1	*Login* dengan memasukkan *user*name dan password pada halaman *login hotspot*	√	√	√
2	*Login* ke dalam aplikasi dengan memasukkan *username*	√	√	√
3	Men-enkripsi pesan yang hendak dikirim melalui sistem	√	√	√
4	Mendekripsi pesan yang diterima dari sistem	√	√	√
5	Menampilkan pesan diterima dan pesan terkirim	√	√	√
6	Menampilkan	√	√	√

	nama pengirim pesan di layar aplikasi			
7	Tombol *back* pada *smartphone* untuk keluar dari aplikasi	√	√	√
8	Menampilkan *user* yang bergabung ke dalam obrolan	√	√	√
9	Menampilkan *user* yang keluar obrolan	√	√	√

Tabel 4.2 berikut ini merupakan tabel hasil pengujian fungsionalitas dari aplikasi berdasarkan *web browser* yang digunakan.

Tabel 4.2 Pengujian Fungsional Sistem

No.	Fungsi	*Web Browser*	
		Firefox	Chrome
1	*Login* dengan memasukkan *user*name dan password pada halaman *login hotspot*	√	√
2	*Login* ke dalam aplikasi dengan memasukkan *username*	√	√
3	Men-enkripsi pesan yang hendak dikirim melalui sistem	√	√
4	Mendekripsi pesan yang diterima dari sistem	√	√
5	Menampilkan pesan diterima dan pesan terkirim di layar monitor	√	√
6	Menampilkan nama pengirim pesan di layar aplikasi	√	√
7	Tombol keluar untuk keluar dari aplikasi	√	√
8	Menampilkan *user* yang bergabung ke dalam obrolan	√	√
9	Menampilkan jumlah *user* yang berada di dalam obrolan	√	√
10	Menampilkan *user* yang keluar obrolan	√	√

Dari Tabel 4.2 dapat disimpulkan bahwa pengujian fungsional sistem dapat berjalan dengan baik dan lancar pada dua *web browser* yaitu mozilla firefox dan google chrome.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan pengujian dan pembahasan yang telah dilakukan maka dapat ditarik beberapa kesimpulan sebagai berikut.

1. Pesan dapat dienkripsi sesuai dengan metode yang digunakan dimana ditunjukkan dalam pengujian dan penerimaan pesan antar *client,* dimana dari 4 pengujian semua pesan berhasil dienkripsi dengan baik.
2. Pengiriman dan penerimaan pesan diantara aplikasi berbasis *mobile* dan *web* sudah berjalan lancar, dimana ditunjukkan pada pengujian *group chat.*
3. Aplikasi ini dapat melakukan fungsi *group chat* yang ditunjukkan dalam pengujian *group chat.*
4. Aplikasi ini telah dapat mendikripsi pesan enkripsi yang telah dikirim oleh perangkat pengirim dimana ditunjukkan dalam pengujian pengiriman dan penerimaan pesan antar *client*, dimana dari 4 pegujian semua pesan hasil deskripsinya telah sesuai.
5. Minimal versi *browser* yang dapat digunakan untuk menjalankan aplikasi *chatting* versi *web* adalah *google chrome* 4x/keatas dan *mozilla firefox* 3x/keatas.

5.2 Saran

Adapun saran yang dapat diberikan setelah melakukan pengujian sebagai berikut.

1. Mengintegrasikan aplikasi *chatting* dengan *google firebase* untuk membuat *push notification.*
2. Menambahkan fitur enkripsi dan dekripsi *file* dokumen, *video, audio,* animasi, maupun gambar.
3. Menambahkan fitur *emoticon support* untuk aplikasi *chatting* versi *mobile* maupun *web.*

DAFTAR PUSTAKA

[1] Ardiyanto, W., Anggraeni, W., Mukhlason, A., 2012. 'Pembuatan Sistem Pakar Untuk Pendeteksian dan Penanganan Dini Pada Penyakit Sapi Berbasis Android Dengan Kajian Kinerja Teknik *Knowledge Representation*.' Jurnal Teknik ITS, Vol. 1, No. 1, hh. A310-A315.

[2] Ismail, J. (2016). Hacker menjebol Whatsapp. Didapat dari: http://julismail.staff.telkomuniversity.ac.id/hacker-menjebol-whatsapp.html. (diakses pada 23 Juli 2016)

[3] Nasution, H., & Prihartini, N. (2016). Pengembangan media *chatting online* dengan fitur alih bahasa melalui pendekatan metode *rule based* dalam proses penerjemahan *chat*. *Jurnal Informatika Mulawarman (JIM)*, *7*(3), 94-104.

[4] Nufus, H. (2009). Pembuatan Aplikasi Kriptografi Algoritma Base64 Menggunakan Java JDK 1.6. *Universitas Gunadarma*. *Jurusan Sistem Informasi*.

[5] Prisgunanto, I. (2015). Pengaruh Sosial Media Terhadap Tingkat Kepercayaan Bergaul Siswa. Sekolah Tinggi Ilmu Kepolisian, Jakarta.

[6] Santoso, D. H. (2012). Pembangunan Jaringan Local Area Network Smp Negeri 2 Sumberlawang. *IJNS-Indonesian Journal on Networking and Security*, *1*(1).

[7] Sarif, A., Hidayanto, A., Santoso, I., 2011. *Analisis Kinerja Protokol TCP Pada Sistem WiMAX*, Tugas Akhir, Jurusan Teknik Elektro, Universitas Diponegoro, Semarang.

[8] Yulianingsih, P., Hamdani, Maharani, S., 2014. 'Aplikasi *Chatting* Rahasia Menggunakan Algoritma *Vigenere Cipher*.' Jurnal Informatika Universitas Mulawarman, Vol. 9, No. 1, hh. 19-22.