

Aplikasi Keamanan Group Chat Menggunakan Kombinasi Metode RSA dan ELGAMAL

Group Chat Security Application Using a Combination of RSA and ELGAMAL Methods

Yedutun Bill Situmorang^a, Lili Tanti^b

^aMahasiswa Universitas Potensi Utama, Jl.K.L. Yos Sudarso KM 6.5 Tj.Mulia, Medan, 20241, Indonesia

^bDosen Universitas Potensi Utama, Jl.K.L. Yos Sudarso KM 6.5 Tj.mulia, Medan, 20241, Indonesia

bg.yedutun@gmail.com ¹, lilitanti@gmail.com ²

ABSTRAK

Pada aktifitas chat didalam suatu group chat sangat diwaspadai adanya akun tidak dikenal yang dapat mengakses dan mengetahui setiap aktifitas. Untuk menjaga keamanan suatu grup atau instansi dalam melakukan aktifitas chat dapat menggunakan teknik enkripsi dan dekripsi sehingga menghindari adanya akun tidak dikenal mengakses grup chat. Aplikasi keamanan Group chat ini menggunakan sistem berbasis web sehingga dapat diakses dengan mudah oleh seluruh user dari suatu group/instansi baik menggunakan smartphone ataupun PC. Metode yang dipakai ialah kombinasi algoritma RSA dan ELGAMAL. Sistem akan membangkitkan kunci publik dan kunci privat untuk mengamankan group chat menggunakan generate RSA dan kunci ELGAMAL acak secara otomatis pada saat pembuatan group chat. Setelah selesai pembuatan maka seluruh anggota group harus menggunakan kunci tersebut untuk masuk kedalam group chat. Pengamanan ini juga meng-enskripsikan setiap pesan di dalam group chat. Dalam penelitian ini memberikan simpulan yang mengimplementasikan pengamanan data menggunakan teknik kriptografi pada pengamanan group chat berbasis web menggunakan algoritma RSA dan ELGAMAL.

Kata Kunci : Web, AjaxJS, PHP, Group Chat, RSA, ELGAMAL, Kriptografi

ABSTRACT

In chat activities in a group chat, be very wary of unknown accounts that can access and know every activity. To maintain the security of a group or agency in carrying out chat activities, you can use encryption and decryption techniques so as to avoid having unknown accounts accessing group chats. This group chat security application uses a web-based system so that it can be easily accessed by all users from a group/agency using either a smartphone or a PC. The method used is a combination of the RSA and ELGAMAL algorithms. The system will generate public keys and private keys to secure group chats using random RSA and ELGAMAL generated keys automatically when creating group chats. After completing the creation, all group members must use the key to enter the group chat. This security also encrypts every message in the group chat. This study provides conclusions that implement data security using cryptographic techniques in securing web-based group chats using the RSA and ELGAMAL algorithms.

Keywords : Web, AjaxJS, PHP, Group Chat, RSA, ELGAMAL, Cryptography

Info Artikel :

Disubmit: 2 Februari 2023

Direview: 13 Maret 2023

Diterima : 20 April 2023

Copyright © 2023 - Journal UPU. All rights reserved.

1. PENDAHULUAN

Tidak semua hal yang dikomunikasikan bersifat umum sehingga bisa diketahui oleh banyak orang. Ada kalanya hal yang dikomunikasikan tersebut bersifat private atau rahasia sehingga hanya orang-orang tertentu yang bisa mengetahuinya. Terjadi penyadapan terhadap pesan yang disampaikan saat komunikasi, tentunya menjadi masalah apabila pesan tersebut bersifat rahasia[1].

Hal tersebut dapat mengakibatkan proses pengiriman data menjadi tidak aman karena dapat dimanfaatkan oleh pihak lain yang tidak bertanggung jawab untuk mengambil data maupun informasi di tengah jalan. Masalah keamanan data merupakan suatu aspek penting dalam pengiriman data teks maupun informasi melalui jaringan seluler. Oleh karena itu, dibutuhkan suatu sistem keamanan data yang dapat menjaga kerahasiaan suatu data teks maupun informasi. Untuk mencapai

tujuan terjaganya kerahasiaan tersebut, berbagai macam teknik keamanan telah dikembangkan. Untuk melindungi dan menjaga kerahasiaan data agar terhindar dari orang yang tidak berhak mendapatkan informasi tersebut, yaitu menggunakan metode kriptografi. Kriptografi adalah suatu ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi[2].

Pada penelitian ini peneliti menggunakan metode RSA. RSA adalah algoritma pertama yang sesuai dengan *digital signature* seperti halnya enkripsi, dan menjadi salah satu algoritma yang paling maju di bidang kriptografi public key. Sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor bilangan prima merupakan kunci keamanan algoritma RSA. Pada penelitian ini peneliti menggunakan metode RSA. RSA adalah algoritma pertama yang sesuai dengan digital signature seperti halnya enkripsi, dan menjadi salah satu algoritma yang paling maju di bidang kriptografi public key. Sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor bilangan prima merupakan kunci keamanan algoritma RSA. Pemfaktoran digunakan untuk mendapatkan kunci yang khusus. Selama pemfaktoran bilangan dengan nilai yang besar menjadi faktor-faktor prima belum ditemukan, maka selama itu pula keamanan algoritma RSA tetap terjamin [3].

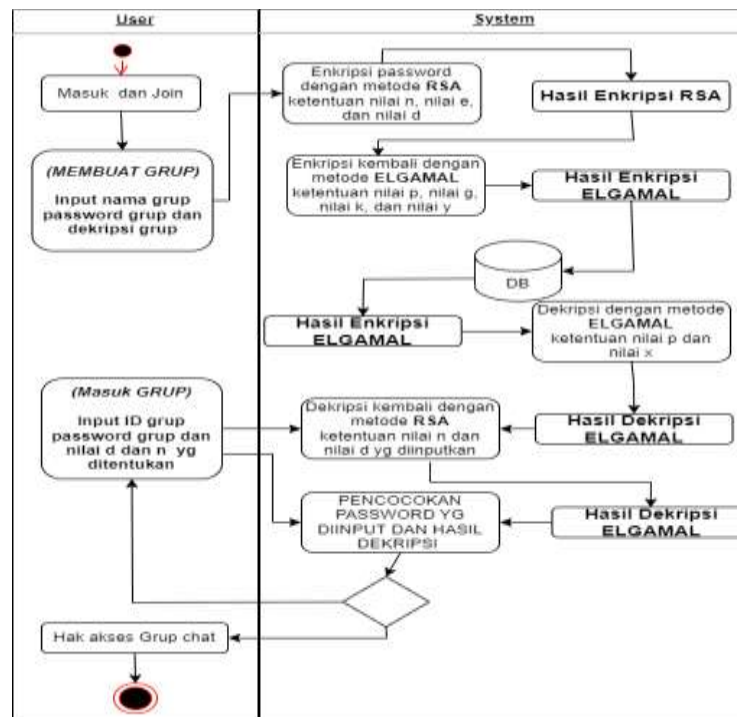
Peneliti menambahkan algoritma ELGAMAL untuk memperkuat hasil enkripsi algoritma Algoritma Elgamal merupakan sepasang kunci yang dibangkitkan dengan memilih bilangan prima p dan dua buah bilangan acak (random) g dan x , dengan syarat bahwa nilai g dan x lebih kecil dari p yang memenuhi persamaan [4].

Untuk menyelesaikan masalah tersebut penulis merancang aplikasi keamanan group chat berbasis web menggunakan kombinasi RSA dan ELGAMAL. Rivest Shamir Adlmen (RSA) sering digunakan karena sulitnya pemfaktoran bilangan besar ke bilangan prima dan didasarkan pada teorema Euler sehingga sangat sulit untuk memecahkan sandi [5], sedangkan Algoritma ELGAMAL ini merupakan cipher blok, yaitu melakukan proses enkripsi pada blok-blok plainteks dan menghasilkan blok-blok cipherteks yang kemudian dilakukan proses dekripsi dan hasilnya tentu saja sama sulitnya dengan algoritma RSA[6].

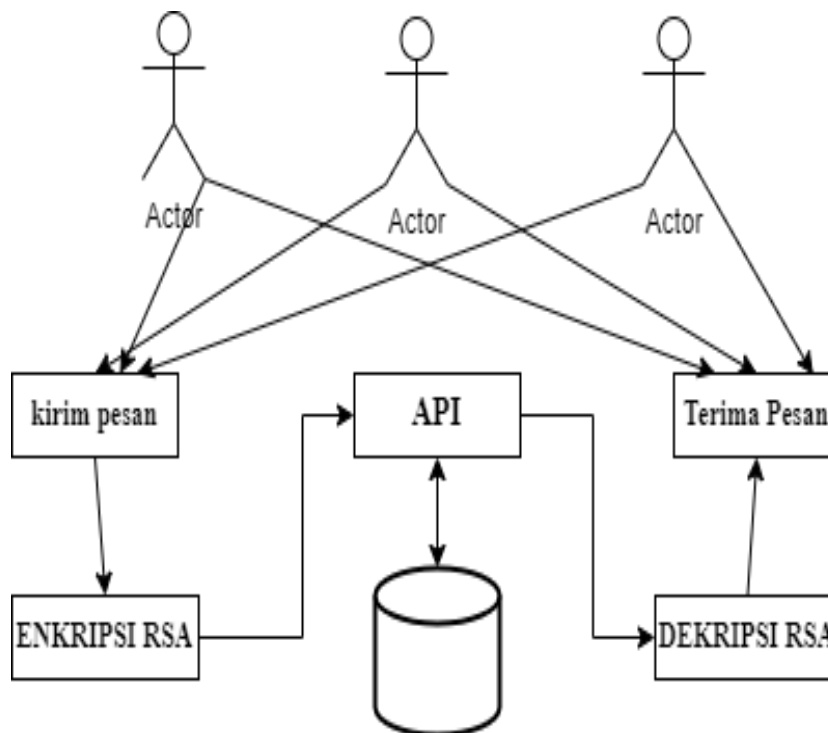
2. METODE

Metode penelitian merupakan tahapan-tahapan dalam membangun Aplikasi keamanan Group chat berbasis web dengan menggunakan metode RSA dan ELGAMAL.

A. Arsitektur Sistem



Gambar 1. Flowchart Kombinasi Metode RSA dan ELGAMAL Membuat dan Akses Masuk Dalam Group Chat



Gambar 2. Arsitektur Aktivitas pengiriman Pesan Pada Group Chat

Berdasarkan gambar 1 dapat terlihat bahwa penelitian menggunakan kombinasi metode RSA dan ELGAMAL untuk membangun aplikasi keamanan group chat berbasis web. Proses Pembuatan group chat ditandai dengan melakukan proses enkripsi memakai metode RSA dan kemudian dienkripsikan kembali memakai metode ELGAMAL, setelah proses enkripsi selesai maka dapat

dipastikan maka group chat sudah berhasil dibuat, Sebaliknya proses masuk kedalam group chat ditandai dengan melakukan proses dekripsi memakai metode ELGAMAL terlebih dahulu dilanjutkan memakai metode RSA. Berdasarkan gambar 2 dapat dilihat bahwa penelitian menggunakan metode Algoritma RSA untuk mengamankan informasi dan seluruh aktifitas didalam group chat dalam bentuk chat

B. Metode Algoritma RSA

Algoritma ini adalah salah satu algoritma asimetris dimana algoritma ini menggunakan kunci public dan private, sehingga proses algoritma ini terbagi menjadi 3 bagian, membangkitkan kunci, proses enkripsi dan terakhir proses dekripsi. Berikut nilai untuk membangkitkan kunci pada RSA:

1. P dan q bilangan prima acak yang sifatnya rahasia dan disarankan bilangan besar.
2. $n = p \cdot q$, bersifat tidak rahasia
3. $m = (p-1)(q-1)$, sifat bilangan ini adalah rahasia.
4. e (kunci enkripsi), tidak rahasia.
5. d (kunci dekripsi), bersifat rahasia.
6. P (plaintext), informasi awal yang ingin di enkripsikan.
7. C (ciphertext), informasi yang telah dienkripsi

- **Mencari nilai n** ($n = p \times q = 17 \times 11 = 187$)
- Mencari nilai m ($m = (17 - 1) \times (11 - 1) = 16 \times 10 = 160$)
- **Menentukan nilai e**, $e = 7 \dots$
 $160 \bmod 7 = 6$
 $7 \bmod 6 = 1$
 $6 \bmod 1 = 0$
Mencari nilai d ($d \cdot e \equiv 1 \pmod{160} + 1$) ($d = 23$, karena $23 \times 7 = 161 = (1 \times 160) + 1$)
 nilai e = 7 dan nilai d = 23
- Enkripsi contoh $Y = 89$ ($C = P^e \bmod n = 89^7 \bmod 187 = 166$)
- Dekripsi, ($M = C^d \bmod n = 166^{23} \bmod 187 = 89 = Y$)

C. Metode Algoritma ELGAMAL

Algoritma ini sama seperti algoritma RSA menggunakan 3 proses dikarenakan sesama algoritma asimetris dan memakai bilangan prima sebagai dasar perhitungannya, perbedaannya algoritma ini melakukan proses enkripsi pada blok-blok, sehingga jika ada yang ingin melakukan brute force akan sangat kesulitan memecahkan enkripsi algoritma ELGAMAL. Berikut nilai untuk membangkitkan kunci pada RSA:

- Pilih sembarang bilangan prima (p), contoh 131
- Pilih dua buah bilangan acak, g dan x, dengan syarat $g < p$ dan $1 \leq x \leq p - 2$, contoh $g = 3$ dan $x = 5$
- Hitung $y = g^x \bmod p \Rightarrow y = 3^5 \bmod 131 = 112$
 maka Kunci publik: triplet ($y = 112, g = 3, p = 131$) Kunci privat: pasangan ($x = 5, p = 131$)
- Susunan plaintext menjadi blok, $m_1, m_2, m_3, \dots$, contoh 166, ciphertext Y dari enkripsi RSA sebelumnya.
- Kemudian pilih lagi bilangan acak k, yang dalam hal ini $1 \leq k \leq p - 2$, contoh $k_1 = 23$
- Setiap blok m dienkripsi dengan rumus $a = g^k \bmod p$; $b = y^k \cdot m \bmod p$
 contoh $a = 3^{23} \bmod 131 = 91$ $b = 112^7 \cdot 89 \bmod 131 = 49$
 maka ciphertext dari 166 = 7,46
- **Dekripsinya**
 $(a^x)^{-1} = a^{p-1-x} \bmod p$
 $(a^x)^{-1} = 91^{131-1-5} \bmod 131 = 91^{125} \bmod 131$

$$\begin{aligned} &= (91^5 \bmod 131)^{25} \bmod 131 \\ &= 80^5 \bmod 131 \\ &= (80^5 \bmod 131)^5 \bmod 131 \\ &= 60^5 \bmod 131 = \mathbf{113} \\ m1 &= b. (a^x)^{-1} \bmod p = 46. 113 \bmod 131 = 89 = Y \end{aligned}$$

D. Ajax js

Ajax merupakan solusi untuk permasalahan pada web tradisional, dimana ketika client mengirim permintaan ke server harus menunggu respon dari server, baru bias melanjutkan aktivitas berikutnya. Permasalahan muncul ketika terjadi suatu hal pada jaringan atau banyaknya pengunjung yang sedang membuka aplikasi web, sehingga respon dari server sangat lambat. Berbeda dengan menggunakan teknologi Ajax, user tidak berkomunikasi langsung dengan server tetapi berkomunikasi dengan system Ajax, selanjutnya system Ajax yang akan melanjutkan komunikasi tersebut ke server. Komunikasi dengan Ajax menggunakan Javascript dan tanggapan dari Ajax berupa HTML, CSS dan Data. Sedangkan komunikasi Ajax dengan server menggunakan HTTP-request dan tanggapan dari server berupa data XML. Hebatnya, selama Ajax menunggu respon dari server user tetap bias berkomunikasi dengan Ajax.

E. PHP

PHP biasa digunakan untuk membuat halaman web yang diampilkan bersifat dinamis atau tidak tetap, sehingga memungkinkan untuk menyimpan data ke dalam database, membuat halaman yang berubah-ubah sesuai input dari user, dan sebagainya

F. MySQL

MySQL adalah sebuah struktur database yang terstruktur dan termasuk database digital yang menggunakan database management system (DBMS. Dimana DBMS dapat membuat dan maintenance data serta pencairan akses lain.

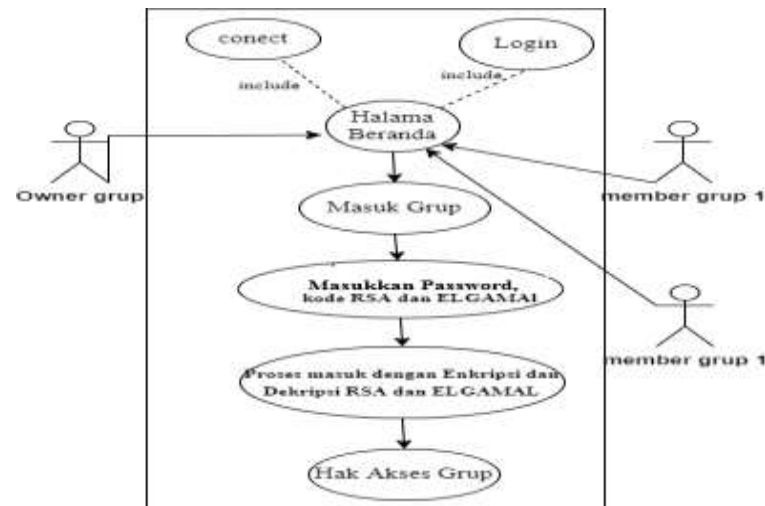
G. Unified Modeling Language (UML)

UML dapat juga dikatakan sekumpulan konvensi permodelan yang dapat digunakan menentukan atau menggambarkan sebuah sistem aplikasi yang terkait dengan objek. UML merupakan suatu kumpulan teknik terbaik yang telah terbukti sukses dalam memodelkan system yang besar dan kompleks. UML tidak hanya digunakan dalam proses pemodelan dalam membuat aplikasi, namun hampir dalam semua bidang yang membutuhkan pemod

3. HASIL DAN PEMBAHASAN

A. Perancangan Sistem

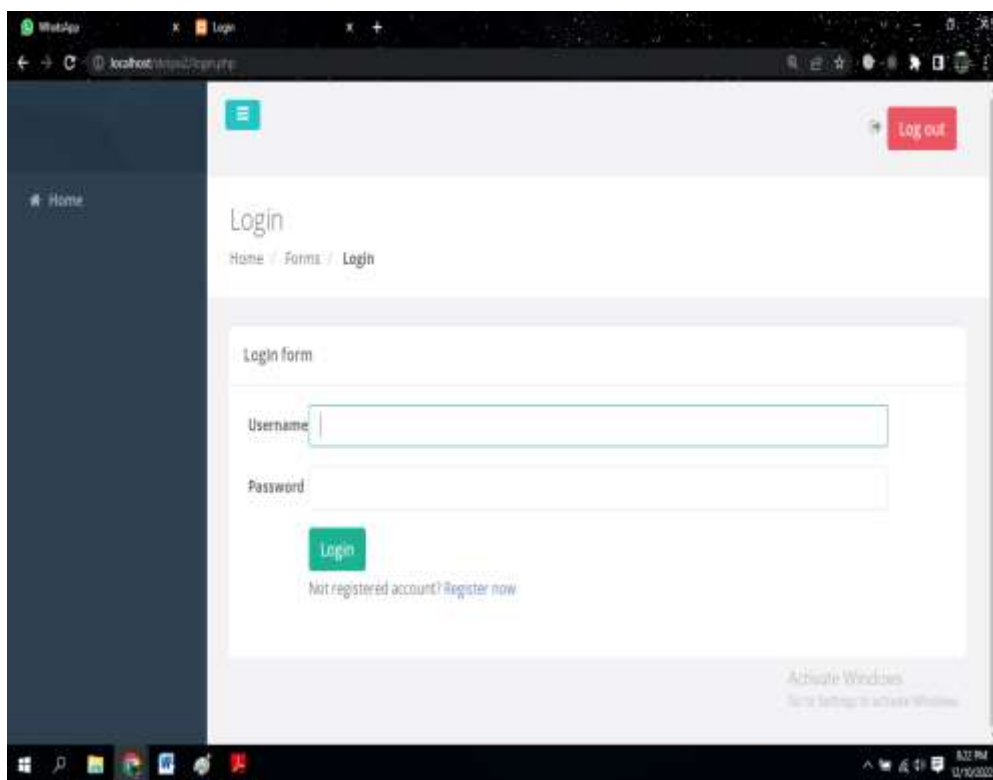
Secara garis besar proses sistem yang akan dirancang digambarkan dengan *usecase diagram* yang terdapat pada gambar 3:



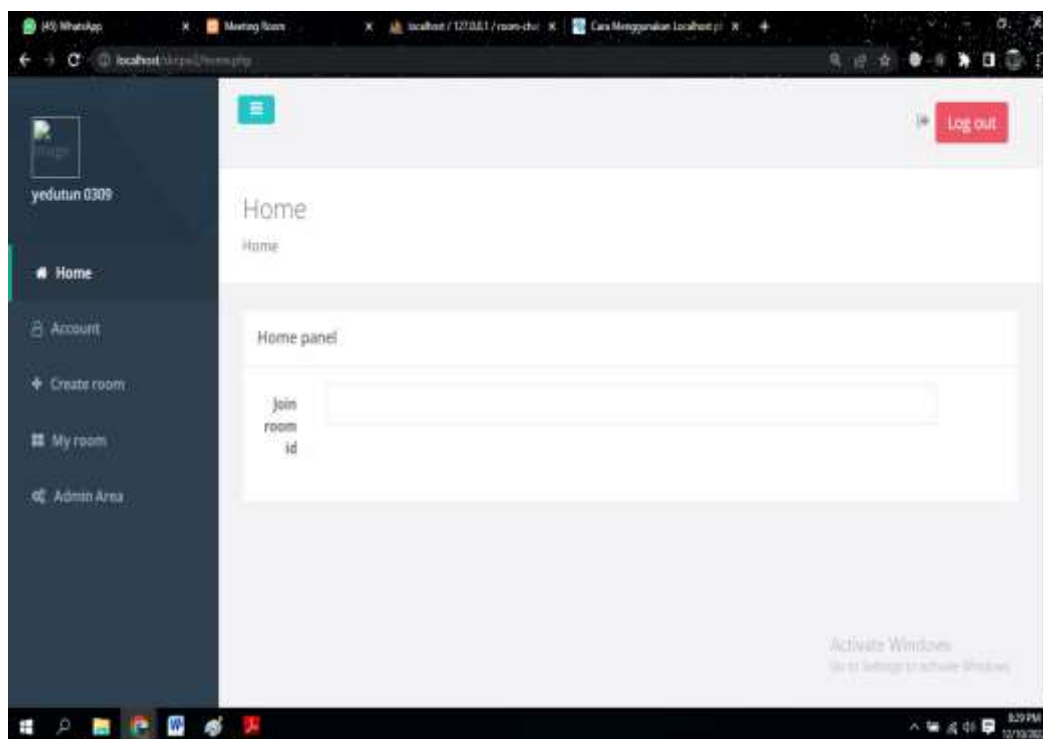
GAMBAR 3. Aplikasi Enkripsi Dan Dekripsi Menggunakan Metode Rsa Dan Elgamal Pada Group Chat

B. Tampilan Hasil Sistem

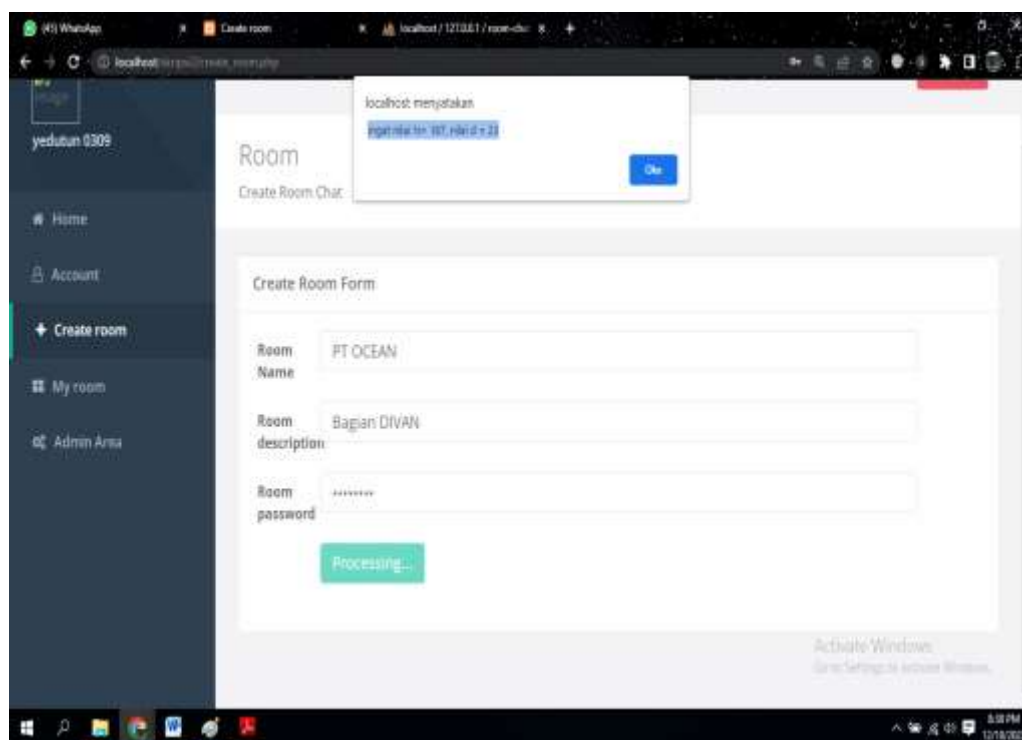
Adapun tampilan hasil dari hasil pembangunan sistem dalam mengimplementasikan aplikasi keamanan group chat dengan menggunakan metode RSA dan ELGAMAL adalah sebagai berikut



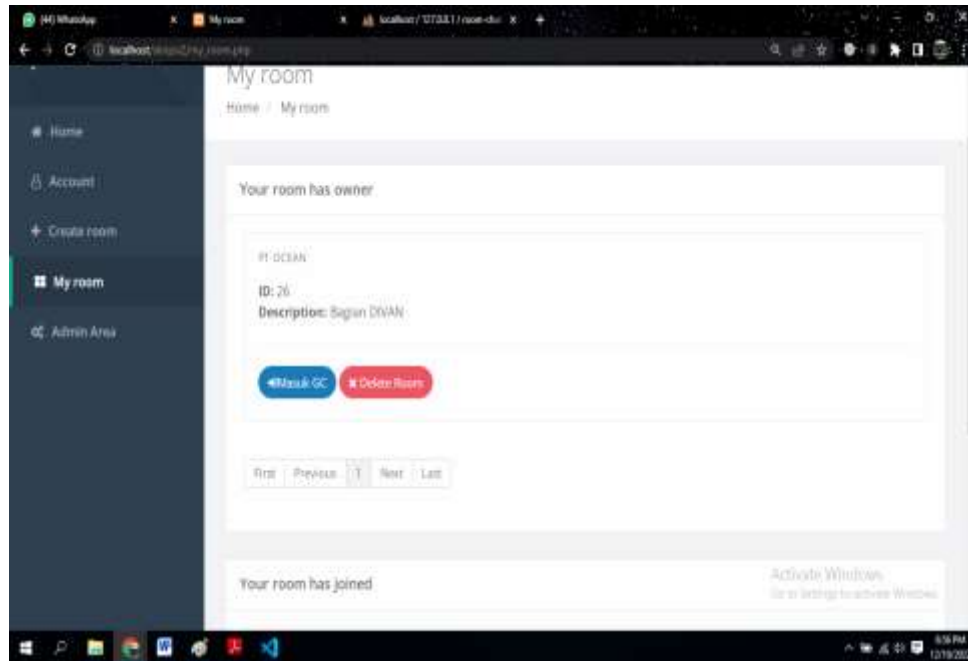
Gambar 5. Tampilan Login Setiap User



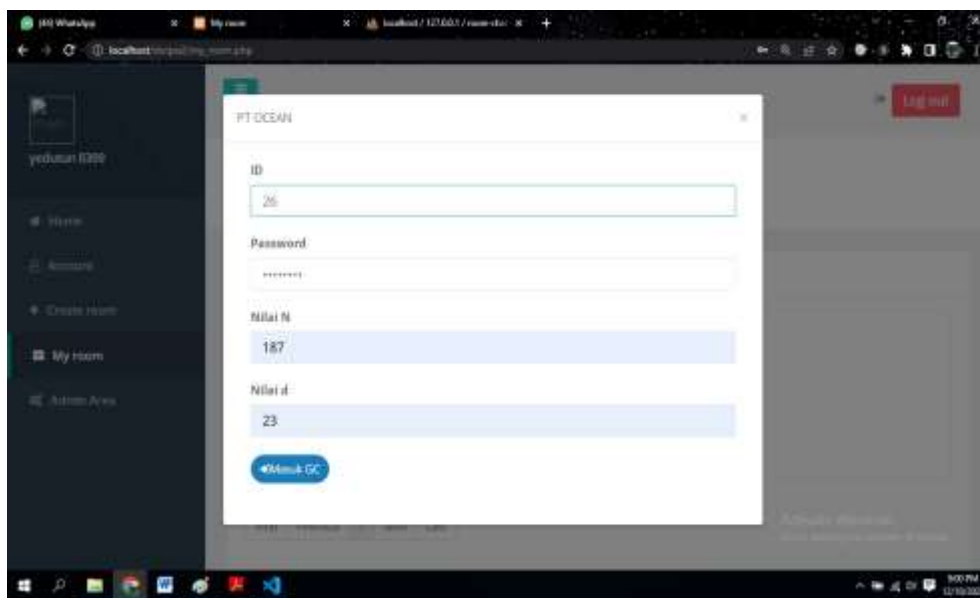
Gambar 6. Tampilan halaman Beranda Setiap User



Gambar 7 . Tampilan halaman Membuat Group Chat



Gambar 8. Tampilan halaman group chat terbentuk



Gambar 9. Tampilan halaman masuk ke dalam group chat



C. Uji Coba Aplikasi

Uji coba yang dipakai pada pembuatan aplikasi ini ialah blackbox testing, dan uji coba aplikasi keamanan group chat dengan menggunakan metode RSA dan ELGAMAL dapat dilihat dari tabel-tabel berikut:

Tabel.1. *Blackbox Testing Form Login*

No.	Form Login	Hasil	Validitas
1.	Masukkan data anda	Jika sandi benar, maka sistem menampilkan <i>form</i> menu utama. Jika sandi salah, maka aplikasi menampilkan pesan kesalahan	Valid

Table.2. *Blackbox Testing Menu Beranda*

No.	Form Menu	Hasil	Validitas
1.	Klik Home	Sistem menampilkan <i>ke</i> menu beranda setiap user	Valid
2.	Klik Acount	Sistem menampilkan data akun setiap user	Valid
3.	Klik Create Room	Sistem menampilkan <i>form</i> yang digunakan untuk membuat grup chat	Valid
4.	My room	Sistem menampilkan <i>seluruh grup chat</i> setiap user	Valid

Tabel. 3 *Blackbox Testing Fungsi Tombol*

No.	Fungsi Tombol	Hasil	Validitas
1.	Login	System menghasilkan halaman beranda setiap user	Valid
2	Register	System membuat akun baru user	Valid
3	Masuk GC	System menampilkan Form untuk masuk kedalam grup chat	Valid
4	masukGc(pada form masuk gc)	System akan menampilkan aktifitas grupchat	Valid
5	Delete room	System akan menghapus grupchat	Valid

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan selama membuat aplikasi ini, maka dapat ditarik beberapa kesimpulan sebagai berikut :

- a) Aplikasi ini dapat mengamankan privasi setiap user dalam melakukan aktifitas grup chat .
- b) Aplikasi dapat dipakai untuk semua kalangan, baik hanya untuk kelompok kecil, maupun kelompok besar.
- c) Aplikasi dapat digunakan pada berbagai instansi untuk melakukan meeting dan tidak takut adanya penyusup.

Saran untuk pengembangan aplikasi pada waktu mendatang adalah:

Untuk kedepannya diharapkan melakukan pengembangan aplikasi pengaman grup chat lebih luas sehingga banyak kalangan kelompok yang akan merasa aman dalam melakukan aktifitas grup chat yang dianggap rahasia.

- a. Pada aplikasi ini perlu adanya pengembangan fitur seiring dengan perkembangan teknologi terus menerus dan beberapa perbaikan *User Interface* yang lebih baik guna mempermudah penggunaan
- b. aplikasi ini dengan menggunakan *native apps* atau dengan *framework* yang lebih responsive

UCAPAN TERIMA KASIH

Saya mengucapkan terimakasih kepada Tuhan YME, Universitas Potensi Utama, Dosen Pembimbing, sahabat serta keluarga serta kepada dewan Jurnal Info Digit yang membantu menjadi Reviewers dalam penerbitan Volume 1 Nomor 1 januari 2023

REFERENSI .

- [1] Arista, T., & Murdani, M. (2020). Perancangan Aplikasi Pengamanan Pesan Menggunakan Algoritma Elgamal Berbasis Android. KAKIFIKOM (Kumpulan Artikel Karya Ilmiah Fakultas Ilmu Komputer), 43-48, doi :10.54367/kakifikom.v2i1.667
- [2] Yusfrizal, Y. (2019). Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android. JTIK (Jurnal Teknik Informatika Kaputama), 3(2), 29-37
- [3] Setiawan, D. R. (2018). *Peningkatan keamanan grup chat menggunakan kombinasi metode RSA, Elgamal dan Viginere Cipher* (Doctoral dissertation, Universitas Islam Negeri Maulana Malik Ibrahim).
- [4] Alfiah, F., Sudarji, R., & Al Fatah, D. T. (2020). *Aplikasi Kriptografi Dengan Menggunakan Algoritma Elgamal Berbasis Java Desktop Pada Pt. Wahana Indo Trada Nissan Jatake*. ADI Bisnis Digital Interdisiplin Jurnal, 1(1 Juni), 22-34.
- [5] Aufa, F. J. (2018). *Sistem Keamanan dengan Metode Enkripsi RSA dan Digital Signature Algorithm untuk Komunikasi Bergerak pada Aplikasi Intelligent Transportation System* (Doctoral dissertation, Institut Teknologi Sepuluh Nopember)
- [6] Setiawan, D. R. (2018). *Peningkatan keamanan grup chat menggunakan kombinasi metode RSA, Elgamal dan Viginere Cipher* (Doctoral dissertation, Universitas Islam Negeri Maulana Malik)