

IMPLEMENTASI ALGORITMA KRIPTOGRAFI DENGAN METODE DES, VERNAM DAN DIFFIE HELMAN PADA WEB SERVICE BERBASIS REST APLIKASI BLUCAMPUS FITUR PMB PADA UNIVERSITAS BUDI LUHUR

Riyan Sugiharto¹⁾, Painem²⁾

¹Tenik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur

^{1,2}Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260

E-mail: rivansghrt@gmail.com¹⁾, painem@budiluhur.ac.id²⁾

Abstrak

REST API semakin populer digunakan sebagai media pertukaran data, hal ini disebabkan semakin banyak aplikasi mobile yang bermunculan. Karena kelebihan REST API salah satunya adalah untuk mengintegrasikan dua atau lebih platform yang berbeda secara bersamaan. Karena banyaknya user yang akan menggunakan Aplikasi BluCampus untuk itu aplikasi BluCampus menggunakan API Rest sebagai Web service, oleh karena itu besar kemungkinan akan terjadinya pencurian data yang mungkin terjadi pada saat pengiriman data dari aplikasi BluCampus menuju Web service, jadi diciptakanlah algoritma - algoritma untuk enkripsi data dari metode Caesar hingga sekarang ini. Pada sistem aplikasi BluCampus diterapkan kombinasi metode Vernam, metode DES (Data Encryption Sistem) dan Deffie Helman. Penerapan Kombinasi Vernam dan DES pada API BluCampus dapat menyelesaikan kemungkinan terjadinya pencurian data. Pengujian dilakukan dengan cara mengenkripsikan semua data yang akan di kirim menuju API untuk di proses dan setelah API menerima data berbentuk ciphertext maka akan dilakukan dekripsi dan menghitung waktu saat pertukaran data dengan enkripsi dekripsi dan tanpa enkripsi. Enkripsi dilakukan dengan vernam terlebih dahulu dengan key dari deffie helman, setelah mendapat ciphertext maka dilakukan enkripsi lagi dengan metode DES. Pada penelitian ini dianalisis kecepatan enkripsi dekripsi pada data dari user yang berkarakter dari 80 hingga 260 karakter. Hasil penelitian menunjukkan rata rata waktu yang dibutuhkan untuk enkripsi dan dekripsi sebesar 440ms sedangkan jika tanpa enkripsi dekripsi sebesar 251ms, dari hasil penelitian bisa disimpulkan bahwa waktu yang dibutuhkan untuk pertukaran data lebih cepat jika tanpa enkripsi dekripsi dan waktu yang dibutuhkan server untuk enkripsi ataupun dekripsi berbanding lurus dengan spesifikasi server, semakin tinggi spesifikasi server maka waktu yang diperlukan akan semakin singkat

Kata Kunci: Data Encryption Standard(DES), Vernam, Diffie Helman, BluCampus, Fitur PMB, Webservice.

1. PENDAHULUAN

Keamanan data merupakan hal yang sangat penting dalam era teknologi seperti sekarang ini. Keamanan data adalah hal yang harus dimiliki dalam setiap sistem. Oleh karena itu, dengan adanya keamanan data maka sistem akan lebih terlindungi saat pertukaran data berlangsung dari aplikasi menuju *web service*. Namun, itu adalah saat yang mudah untuk diserang oleh para cracker jika tidak ada enkripsi yang mengamankan datanya.

Universitas Budi Luhur bagian PMB (Penerimaan Mahasiswa Baru) yang tugasnya melayani masyarakat yang ingin mendaftar sebagai mahasiswa baru. Saat ini memiliki kesulitan dalam menangani banyaknya orang yang ingin mendaftar sebagai mahasiswa di Universitas Budi Luhur. Namun, jumlah SDM(Sumber Daya Manusia) tidak sebanding dengan banyaknya orang yang ingin mendaftar, jika pendaftaran dilakukan secara online maka akan adanya kemungkinan pencurian data bisa terjadi. Dalam rangka membuat sistem *web*

Web service aplikasi BluCampus yang bisa digunakan sebagai sarana untuk mendaftar menjadi calon mahasiswa Universitas Budi Luhur. Untuk mengatasi itu, diperlukan keamanan data yang baik. Melihat kemungkinan semakin banyak user yang akan menggunakan aplikasi BluCampus, maka data harus di enkripsi terlebih dahulu sebelum dikirim dari aplikasi BluCampus menuju *web service* dan saat *web service* memberikan response kepada aplikasi BluCampus juga harus dilakukan enkripsi,

Karena itu diterapkannya enkripsi dengan kombinasi metode vernam DES sebagai salah satu cara untuk menjaga keamanan datanya. Untuk memperkuat sistem keamanan data, maka pada key menggunakan metode DES digunakan metode Deffie Helman agar data semakin terlindungi. Dengan menerapkan Enkripsi dengan kombinasi Metode vernam, Des dan Metode Deffie Helman sebagai pembangkitan keynya, diharapkan dapat melindungi saat pertukaran data

Web Service adalah suatu sistem perangkat lunak yang dirancang untuk mendukung interaction and interoperability antar sistem pada suatu

2. METODE PENELITIAN

2.1. Pengertian *Web Service*

jaringan [6]. Atau bisa juga didefinisikan sebagai sebuah software aplikasi yang tidak terpengaruh oleh platform, web service akan menyediakan method – method yang dapat diakses oleh network. Namun yang membedakan web service dengan web pada umumnya adalah interaksi yang diberikan oleh web service. Berbeda dengan URL web pada umumnya, URL web service hanya menggandung kumpulan informasi, perintah, konfigurasi atau sintaks yang berguna membangun sebuah fungsi-fungsi tertentu dari aplikasi. Web service dapat diartikan juga sebuah metode pertukaran data, tanpa memperhatikan dimana sebuah database ditanamkan, dibuat dalam bahasa apa, sebuah aplikasi yang mengkonsumsi data, dan di platform apa sebuah data itu dikonsumsi.

Web service sendiri dibentuk dari [2] :

- 1) Service provider adalah pemilik Web Service yang berfungsi menyediakan kumpulan operasi dari Web Service.
- 2) Service requestor adalah aplikasi yang bertindak sebagai klien.
- 3) Service registry adalah tempat dimana service mempublikasikan layanannya.

Keuntungan menggunakan web service antara lain :

- 1) Mudah dimengeri dan mudah di debug.
- 2) Dukungan interface yang stabil
- 3) Akselerasi
- 4) Pencapaian Modular
- 5) Mudah untuk menegahi pesan – pesan proses dan menambahkan nilai.
- 6) Mudah untuk mengembangkan dengan semantic transport tambahan.

2.2. Definisi REST

REST adalah gaya arsitektural yang memiliki aturan seperti antar muka yang seragam, sehingga jika aturan tersebut diterapkan pada web services akan dapat memaksimalkan kinerja web service terutama pada performa, skalabilitas, dan kemudahan untuk dimodifikasi. Pada arsitektur REST data dan fungsi dianggap sebagai sumber daya yang dapat diakses lewat Uniform Resource Identifier (URI), biasanya berupa tautan pada web [2]

REST adalah salah satu jenis webservices yang memiliki standar arsitektur komunikasi data antar aplikasi atau sistem berbasis web, yang memanfaatkan HTTP (Hypertext Transfer Protocol) sebagai protocol untuk komunikasi data dan memiliki Resource pada server dan client, yang dapat diakses lewat Uniform Resource Identifier (URI) . Berikut ini adalah method method yang mendukung REST :

- a. GET digunakan untuk resource yang hanya perlu dibaca (read only)
- b. PUT digunakan untuk membuat resource baru.
- c. DELETE digunakan untuk menghapus suatu resource.

- d. PUT digunakan untuk digunakan untuk memperbarui resource yang ada atau membuat resource baru
- e. OPTION digunakan untuk mendapatkan operasi yang disuport pada res

2.3. Algoritma Deffie Helman

Algoritma pertukaran kunci *Diffie-Hellman* salah satu algoritma yang dapat digunakan untuk melakukan enkripsi data sehingga data asli hanya dapat dibaca oleh seseorang yang memiliki kunci enkripsi tersebut dan juga bisa juga sebagai pertukaran kunci rahasia pada komunikasi data menggunakan kriptografi simetris. Ciri khas dari algoritma diffie helman adalah karena sulitnya melakukan perhitungan logaritma diskrit[4]. Langkah-langkahnya adalah sebagai berikut,

- a. Misalkan sarah dan doni adalah pihak-pihak yang berkomunikasi. Mula-mula sarah dan doni menyepakati dua buah bilangan yang besar (disarankan bilangan prima) P dan Q, sedemikian sehingga $P < Q$. Nilai P dan Q tidak perlu rahasia, bahkan sarah dan doni dapat membicarakannya melalui saluran yang tidak aman sekalipun.
- b. Sarah membangkitkan bilangan bulat acak x yang besar dan mengirim hasil perhitungan berikut kepada doni : $X = P^x \text{ mod } Q$.
- c. Doni membangkitkan bilangan bulat acak y yang besar dan mengirim hasil perhitungan berikut kepada sarah : $Y = P^y \text{ mod } Q$.

sarah menghitung $K = Y^x \text{ mod } Q$. Bob menghitung $K' = X^y \text{ mod } Q$.

Jika perhitungan dilakukan dengan benar, maka hasilnya $K = K'$. Dengan demikian maka sarah dan doni telah memiliki sebuah kunci yang sama tanpa diketahui pihak lain.

2.4. Algoritma Vernam

Algoritma kriptografi vernam cipher merupakan algoritma kriptografi berjenis symmetric key. Kunci yang digunakan untuk melakukan enkripsi dan dekripsi menggunakan kunci yang sama. Dalam melakukan proses enkripsi, algoritma vernam cipher menggunakan cara stream cipher dimana cipher berasal dari hasil operasi XOR antara bit plainteks dan bit key [1].

Vernam cipher merupakan algoritma kriptografi yang ditemukan oleh Mayor J. Maugborne dan G. Vernam. Algoritma Vernam cipher diadopsi dari one time pad cipher, dimana dalam hal ini karakter diganti dengan bit (0 atau 1). Dengan kata lain, vernam cipher merupakan versi lain dari one-time pad cipher.

2.5. Algoritma DES

salah satu algoritma kriptografi cipher block dengan ukuran blok 64bit dan ukuran kuncinya 56 bit. Algoritma DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis cipher blok. Kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit menggunakan metode diffie helman. Algoritma DES dibuat di IBM, dan merupakan modifikasi daripada algoritma terdahulu yang bernama Lucifer. Lucifer merupakan algoritma cipher block yang beroperasi pada blok masukan 64 bit dan kuncinya berukuran 128 bit .Pengurangan jumlah bit kunci pada DES dilakukan dengan alasan agar mekanisme algoritma ini bisa diimplementasikan dalam satu chip. DES pertama kali dipublikasikan di Federal Register pada 17 Maret 1975. Setelah melalui banyak diskusi, akhirnya algortima DES diadopsi sebagai algoritma standar yang digunakan oleh NBS (National Bureau of Standards) pada 15 Januari 1977. Sejak saat itu, DES banyak digunakan pada dunia penyebaran informasi untuk melindungi data agar tidak bisa dibaca oleh orang lain [3].

2.6. Layanan Web Service

Bagian ini berisikan berbagai layanan yang akan digunakan pada sistem *PMB*, beserta penjelasan dari masing-masing layanan seperti nama layanan, nama fungsi, parameter dan keluaran.

Tabel 1 : Daftar Layanan Web Service

Nama Layanan	Fungsi	Path	Parameter
Cek status tahun ajaran	Get	/tahun_ajaran	
Lihat pendaftar dari aplikasi berdasarkan no pendaftaran	Get	/show(daftar_mhs)	No_pendaftaran
Registrasi	Post	/signup	Request body parameter : nama, email, no_hp, provinsi, kota, jenjang, fakultas, program_studi, jenis daftar,
Calon mahasiswa	Get	/calonmhs	
Menampilkan informasi Ruang Tes berdasarkan no_pendaftar	Post	/ruang	Request body parameter : No_pendaftaran

Menampilkan Informasi Ordik berdasarkan NIM(Nomor Induk Mahasiswa)	Post	/ordik	Request body parameter : Nim
Melakukan validasi email pada saat registrasi	Post	/cekemail	Request body parameter : email
Melakukan validasi no_pendaftaran pada form di menu ruang tes	Post	/cekruang	Request body parameter : no_pendaftaran
Melakukan validasi NIM pada Form di menu ordik	Post	/ceknim	Request body parameter : nim
Menghapus data pendaftaran	Delete	/daftar{daftar_mhs}	Request body parameter : no_pendaftaran
Mengirim email	Post	/mailing	Parameter : no_pendaftaran

2.7. Spesifikasi Database

Berikut ini adalah spesifikasi basis data untuk menyimpan dan mengakses data dalam layanan web service

Tabel 2: daftar mhs

Field	Type	Length	Keterangan
No_Pendaftaran	Varchar	12	Nomor Pendaftaran
Nama	Varchar	50	Nama Mahasiswa
Email	Varchar	50	Email Mahasiswa
No_Hp	Varchar	12	No Handphone
Kota	Varchar	20	Kota Asal Mahasiswa
Provinsi	Varchar	20	Provinsi
Status	Varchar	15	Status Calon Mahasiswa
Kode_Pembayaran	Varchar	12	Kode Pembayaran
Id_tahun	Char	3	Nomor Tahun Ajaran
Created_At	Date Time	8	Tanggal Dibuat
Updated_At	Date Time	8	Tanggal Dirubah

Tabel 3 : Ruang Tes

Field	Type	Length	Keterangan
Id	Varchar	12	Id Ruang Tes
Hari	Varchar	50	Hari Tes
Tanggal	Varchar	50	Tanggal Tes
Gedung	Varchar	12	Gedung Tes
Ruangan	Varchar	20	Ruang Tes
Jam	Varchar	4	Jam Tes

Tabel 4 : Ordiks

Field	Type	Length	Keterangan
Id	Varchar	10	Id Ordik
Nim	Varchar	10	NIM Mahasiswa
Tanggal_Mulai	Date	8	Tanggal Mulai
Tanggal_Akhir	Date	8	Tanggal Akhir
Ruangan	Varchar	10	Ruang Ordik
Kelompok	Varchar	20	Kelompok Ordik
Id_Daftar	Int	9	Id Pendaftaran
Created_At	Date	8	Tanggal Pembuatan
Update_At	Date	8	Tanggal Perubahan

Tabel 5 : Tahun Ajaran

Field	Type	Length	Keterangan
Id	Varchar	11	Id Tahun Ajaran
Nama_Ajaran	Varchar	20	Nama Ajaran
Tahun	Varchar	20	Tahun Ajaran
Tgl_Mulai	Date	8	Tanggal Mulai
Tgl_Akhir	Date	8	Tanggal Akhir
Status_Aktif	Varchar	2	Status Aktif
Created_At	Date	8	Tanggal Pembuatan
Update_At	Date	8	Tanggal Perubahan

Tabel 6: User Tes

Field	Type	Length	Keterangan
Id	Varchar	10	Id User
Username	Varchar	10	Username
Password	Varchar	9	Password
Grade	Varchar	2	Nilai Tes
Id_Test	Int	8	Id Tes
Id_Daftar	Int	9	Id Daftar
Created_At	Date	8	Tanggal Pembuatan
Update_At	Date	8	Tanggal Perubahan

3.HASIL DAN PEMBAHASAN

3.1. Tampilan Layar

Pada Bagian ini, diuraikan mengenai tampilan layar aplikasi kriptografi mulai dari pertama kali dijalankan sampai selesai dijalankan. Berikut ini akan diberikan penjelasan dan gambar mengenai tampilan – tampilan yang ada pada aplikasi ini.

3.1.1 Tampilan Layar Menu Utama

Tampilan layar dari Menu utama merupakan menu pertama yang ditampilkan pada saat aplikasi pertama kali dibuka, pada menu ini terdapat 3 menu diantaranya menu registrasi, menu ruang tes, menu ordik.



Gambar 3.1 Tampilan Layar Menu Utama

3.1.2 Tampilan Layar Form Pendaftaran

Pada Tampilan Form Pendaftaran terdapat form yang harus di isi oleh user untuk mendaftar sebagai Calon Mahasiswa.



3.2 Tampilan Layar Form Pendaftaran



3.2b Tampilan Layar Form Pendaftaran



Gambar 3.2c Tampilan Layar Form Pendaftaran



Gambar 3.2d Tampilan Layar Form Pendaftaran

3.1.3 Tampilan Layar Form Ruang Tes

Pada Tampilan Menu Pendaftaran terdapat form yang harus di isi oleh user sesuai dengan no pendaftaran yang dimiliki untuk mengetahui informasi ruang tes.



Gambar 3.3 Tampilan Layar Form Ruang Tes

3.1.4 Tampilan Layar Form Ordik

Pada Tampilan Menu Ordik terdapat form yang harus di isi oleh user sesuai dengan NIM yang dimiliki, setelah user mengisi form maka akan ditampilkan informasi ordik sesuai dengan NIM yang dimiliki.



Gambar 3.4 Tampilan Layar Form Ordik

3.1.5 Tampilan Layar Hasil Pendaftaran

Pada Tampilan Layar hasil pendaftaran ini adalah tampilan jika form pada menu registrasi telah selesai di isi semua sesuai data user.



Gambar 3.5 Tampilan Layar Hasil Pendaftaran

3.1.6 Tampilan layar hasil ruang tes

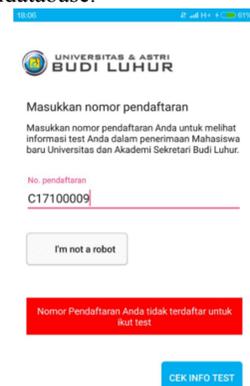
Pada Tampilan layar hasil ruang tes ini akan muncul ketika no pendaftaran user berhasil ditemukan didatabase.



Gambar 3.6 Tampilan Layar Hasil Ruang Tes

3.1.7 Tampilan Layar Gagal Ruang Tes

Pada tampilan layar gagal ruang tes ini akan muncul apabila no pendaftaran user tidak berhasil ditemukan didatabase.



Gambar 3.7 Tampilan Layar Gagal Ruang Tes

3.1.8 Tampilan Layar Hasil Ordik

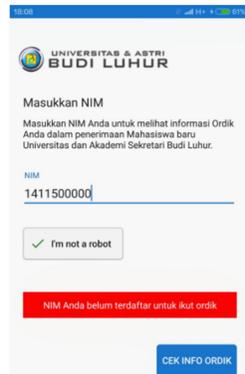
Pada tampilan layar hasil ordik ini akan muncul apabila NIM user berhasil ditemukan didatabase.



Gambar 3.8 Tampilan Layar Hasil Ordik

3.1.9 Tampilan Layar gagal Ordik

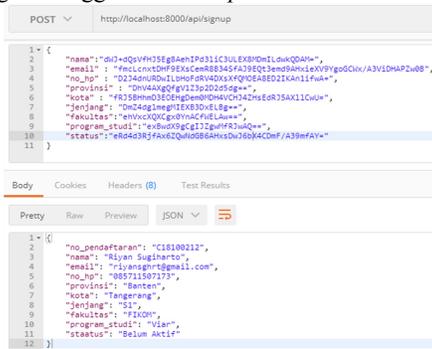
Pada tampilan layar hasil ordik ini akan muncul apabila NIM user tidak berhasil ditemukan didatabase.



Gambar 3.9 Tampilan Layar Gagal Ordik

3.1.10 Tampilan Layar Hasil Dekripsi

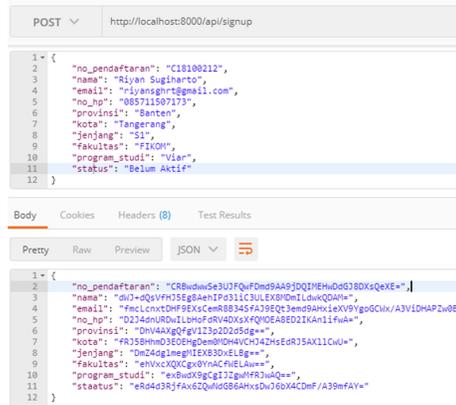
Tampilan ini berisi data *registrasi user* yang telah berhasil di dekripsi oleh API *BluCampus* dengan menggunakan *tool postman*.



Gambar 3.10 Tampilan Layar Berhasil Dekripsi

3.1.11 Tampilan Layar Berhasil Enkripsi

Tampilan ini berisi data registrasi ketika berhasil di enkripsi pada API *BluCampus* dengan menggunakan *tools postman*.



Gambar 3.11 Tampilan Layar Berhasil Enkripsi

3.2 Uji Coba Program

Pada bagian ini akan dilakukan pengujian terhadap layanan web service yang akan digunakan, dan terdapat pengujian proses enkripsi dan dekripsi untuk data Registrasi.

3.2.1 Uji Coba Layanan Web Service

Tabel dibawah ini merupakan hasil pengujian seluruh layanan *web service* yang sudah diimplementasikan pada aplikasi android.

Table 7 : Layanan Web Services

No	Nama Layanan	Status
1	Cek status tahun ajaran	Berhasil
2	Lihat pendaftar dari aplikasi berdasarkan no pendaftaran	Berhasil
3	Registrasi	Berhasil
4	Calon mahasiswa	Berhasil
5	Menampilkan informasi Ruang Tes berdasarkan no_pendaftaran	Berhasil
6	Menampilkan Informasi Ordik berdasarkan NIM(Nomor Induk Mahasiswa)	Berhasil
7	Melakukan validasi email pada saat registrasi	Berhasil
8	Melakukan validasi no_pendaftaran pada form di menu ruang tes	Berhasil
9	Melakukan validasi NIM pada Form di menu ordik	Berhasil
10	Menghapus data pendaftaran	Berhasil
11	Mengirim email	Berhasil

3.2.2 Pengujian Enkripsi dan Dekripsi Data Registrasi

Pada tabel dibawah ini adalah hasil pengujian dari enkripsi dan dekripsi dengan data registrasi untuk 10 user pada aplikasi *BluCampus* dengan iterasi 10 kali menggunakan *tool RestFull Stress*.

Tabel 8 menunjukkan hasil rata rata pengujian enkripsi dan dekripsi vernam des dengan parameter pengujian Encryption Time(ET), Dekryption

Time(DT), Ratio Enkripsi(RE) dan waktu tanpa enkripsi.

No	karakter	ET(ms)	RE(%)	DT(ms)	Waktu tanpa enkripsi (ms)
1	80	361	441.46	358	238
2	100	366	417.65	362	258
3	120	379	385.25	370	274
4	140	387	376.06	382	263
5	160	393	354.32	390	254
6	180	418	350.55	419	230
7	200	404	337.62	399	256
8	220	421	336.04	400	227
9	240	436	326.45	422	234
10	260	439	301.53	430	277

3.3 Evaluasi Program

Setelah dilakukan analisa dan hasil pengujian aplikasi dapat ditemukan beberapa kelebihan dan kekurangan dari aplikasi ini, yaitu sebagai berikut :

- a. Kelebihan Program
 - 1) Aplikasi mudah digunakan dan dipahami oleh user
 - 2) Data yang telah dienkripsi dapat diubah kembali menjadi data asli setelah di dekripsi
- b. Kekurangan Program
 - 1) Aplikasi ini masih dalam tahap pengembangan, belum sepenuhnya dapat bekerja dengan optimal
 - 2) data yang dibuat pada aplikasi ini masih berupa teks belum mendukung fitur gambar

4. KESIMPULAN

Berdasarkan perancangan, pembuatan, serangkaian uji coba, dan analisa program dari aplikasi ini, maka dapat diambil beberapa kesimpulan yaitu :

- Seluruh layanan web service yang dibuat dapat diimplementasikan pada aplikasi android dengan baik.
- Proses Enkripsi dan Dekripsi berjalan dengan baik pada web service.
- Rata – rata rasio enkripsi mencapai 335.17% dari data aslinya, hal ini membuat pertukaran data dengan menggunakan enkripsi dekripsi memerlukan waktu lebih lama dibandingkan jika tidak menggunakan enkripsi dekripsi.
- Waktu enkripsi dan dekripsi berbanding lurus dengan server, semakin bagus spesifikasi servernya maka waktu yang diperlukan untuk enkripsi dan dekripsi akan semakin meningkat.
- *Response time server* dengan menggunakan

teknik enkripsi lebih lama 6ms dibandingkan saat menggunakan teknik dekripsi

5. Daftar Pustaka

- [1]Jumeidi, M., Triyanto, D. And Brianorman Y. (2016). Implementasi Algoritma Kriptografi Vernam Cipher Berbasis Fpga, *Jurnal Coding*, 4(1), hal. 21-32.
- [2]Kurniawan, E. (2014). Implementasi Rest Web Service Untuk Sales Order Dan Sales Tracking Berbasis Mobile, *Jurnal Eksis*, 7, hal. 1–12.
- [3]Muzakir, A. (2014). Prototype Model Keamanan Data Menggunakan Kriptografi Data Encryption Standar (Des) Dengan Mode Operasi Chiper Block Chaining (Cbc). *Seminar Nasional Inovasi dan Tren. Universitas Bina Darma* : hal 33–36
- [4]Anwar, J., Nasution, S. M. And Purboyo, T. W. (2015). Perancangan Dan Implementasi Secure Cloud Dengan Menggunakan Diffie-Hellman Key Exchange Dan Triple Des. *e-Proceeding of Engineering*, 2(2), hal. 3808–3815.
- [5]Pressman, R. S. (2010) *Software Engineering*. 7th Ed. New York: Mcgraw-Hill.
- [6]Rahman, M. A., Kuswardayan, I. And Hariadi, R. (2013) ‘Perancangan Dan Implementasi Restful Web Service Untuk Game Sosial Food Merchant Saga Pada Perangkat Android’, *Jurnal Teknik Pomits*, 2(1), hal. 2–5.
- [7]Harisina, H. (2014). Aplikasi Steganografi Menggunakan File Mp3 Dengan Enkripsi DES (Data Encryption Standard) Dan Metode End Of File (EOF). *Skripsi*, Universitas Budi Luhur, Jakarta Selatan.