IMPLEMENTASI WEB SERVICE BERBASIS REST MENGGUNAKAN ALGORITMA AES 128 DAN AFFINE CIPHER FITUR BLUACADEMIC APLIKASI BLUCAMPUS

Tomi Hartanto[1)], **Painem**[2)]
[1]Tenik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : tomihartanto96@gmail.com[1)], painem@budiluhur.ac.id[2)]

Abstrak

Saat ini perkembangan teknologi sudah sangat pesat, terutama teknologi dalam bidang informasi dan komunikasi. Aplikasi smartphone dengan fitur informasi membutuhkan data yang dinamis seiring dengan perubahan data. Oleh karena itu solusi yang diperllukan yaitu dengan cara menyimpan data pada satu database server. Selanjutnya aplikasi akan melakukan request untuk mendapatkan data yang diinginkan, begitupun saat terjadinya pengiriman data. Untuk mendukung scalability diperlukan teknologi RESTful Web Service sebagai solusi dari pertukaran data tersebut. Dengan memanfaatkan RESTful Web Service aplikasi pada smartphone yang menggunakan jaringan internet dapat mengakses layanan data dari server. Namun seiring bertambahnya pengguna aplikasi yang melakukan pertukaran data, aspek keamananpun menjadi penting, terlebih jika data yang dikirim bersifat rahasia. Oleh karena itu solusi yang dibutuhkan yaitu dengan menambahkan algoritma kriptografi pada aplikasi. Metode yang digunakan yaitu kriptografi AES 128 dikombinasikan dengan Affine Cipher. Pada proses enkripsi, pertama data akan dienkripsi dengan AES 128 kemudian dienkripsi menggunakan Affine Cipher begitupun pada saat proses dekripsi, pertama ciphertext akan didekripsi dengan Affine cipher kemudian didekripsi menggunakan AES 128. Hasil pengujian rata–rata waktu yang diperlukan saat proses enkripsi adalah 1253,5 ms dan proses dekripsi membutuhkan rata-rata waktu 1320,5 ms, dengan demikian waktu yang dibutuhkan saat enkripsi data lebih cepat dibandingkan waktu dekripsi data.

Kata kunci: RESTful, *Web Service*, AES 128, Affine Cipher, enkripsi, dekripsi

1. PENDAHULUAN

Saat ini perkembangan teknologi sudah sangat pesat, terutama teknologi dalam bidang informasi dan komunikasi. Aplikasi *smartphone* dengan fitur informasi promosi dan fitur tersebut sudah pasti membutuhkan data yang dinamis seiring dengan perubahan data yang dinamis. Solusi yang dibutuhkan yaitu menyimpan data di satu database *server*. Selanjutnya aplikasi akan melakukan *request* untuk mendapatkan data yang diinginkan dari *server,* begitu pula dengan pengiriman data. Untuk mendukung *scalability* maka diperlukan teknologi RESTful *web service* sebagai solusi dari pertukaran data. Dengan memanfaatkan RESTful *web service* maka setiap *platform* perangkat *mobile* yang menggunakan jaringan internet dapat mengakses layanan data.

Namun seiring bertambahnya pengguna aplikasi yang mengirim data ke *server,* keamanan dalam penyimpanan data dan pengiriman data atau informasipun menjadikan hal yang sangat penting dan tidak dapat diabaikan, terlebih jika data yang disimpan dan dikirim bersifat penting dan rahasia. Dengan makin berkembangnya teknologi informasi maka bertukar data atau informasi menjadi lebih mudah dengan menggunakan jaringan internet sebagai media pertukaran data. Selain dampak positif dari perkembangan teknologi maka adapun dampak negatif dari perkembangan teknologi ini, salah satu dampak negatif dari perkembangan teknologi ini adalah adanya pencurian data atau informasi yang biasa disebut menyadap. Dengan adanya pencurian data maka aspek keamanan dalam pertukaran informasi dan penyimpanan data dianggap penting, karena suatu komunikasi data jarak jauh belum tentu aman terhadap pencurian.

Oleh karena itu, dilakukan penelitian guna mendapatkan solusi dari permasalahan diatas. penulis bertujuan untuk mengimplementasikan RESTful *web service* dalam pertukaran data tersebut. Sedangkan untuk keamanan data, penulis menggunakan algoritma kriptografi *Advanced Encryption Standard*-128(AES-128) dan algoritma kriptografi *Affine Cipher* untuk mengamankan data yang dikirimkan oleh *smartphone* ke jaringan *server*. Dengan dikombinasikan dua algoritma kriptografi keamanan data saat melakukan pertukaran data akan menjadi lebih aman.

2. METODE PENELITIAN

2.1. Metode Penelitian

Untuk dapat mengimplementasikan *rest Web Service* diatas, maka secara garis besar digunakan beberapa metode sebagai berikut :

- Studi literatur dan teori Penunjang untuk memperoleh informasi dengan mempelajari buku-buku literatur atau karya lainnya yang membahas tentang kriptografi atau untuk menunjang pembuatan RESTful *web service* yang berhubungan dengan materi penulisan tugas akhir.

- Penerapan metode algoritma AES-128 dan Affine Cipher dalam RESTful *web service*.
- Analisa permasalahan untuk menentukan metode algoritma yang akan digunakan pada fitur BluAcademic.
- Pembuatan RESTful *web service* untuk android setelah menganalisa permasalahan, selanjutnya dilakukan perancangan atau pembuatan sistem dengan menggunakan model perancangan sistem yang telah diterapkan agar API hasilnya akan maksimal dan dapat digunakan oleh development android dengan mudah.
- Evaluasi RESTful *web service* dengan melakukan pengujian dan pengoperasian sistem secara keseluruhan evaluasi program dan pengujian pada suatu sistem sangat diperlukan untuk mengetahui kestabilan sistem yang telah dibuat.

2.2. REST

REST (*Representational State Transfer*) merupakan kumpulan aturan yang apabila diaplikasikan pada desain sistem akan menciptakan suatu arsitektur perangkat lunak. Jika ita mengimplementasikan semua pedoman REST. kita akan sampai pada sistem yang memiliki data, komponen, hyperlink, protokol komunikasi dan data consumer yang memiliki peranan khusus. Empat metoda yang paling umum adalah GET, PUT, DELETE dan POST [2].

2.3. Web Sevice

Web Service adalah suatu sistem perangkat lunak yang dirancang untuk mendukung interoperabilitas dan interaksi antar sistem pada suatu jaringan. Web Service digunakan sebagai suatu fasilitas yang disediakan oleh suatu website untuk menyediakan layanan (dalam bentuk informasi) kepada sistem lain, sehingga sistem lain dapat berinteraksi dengan sistem tersebt melalui layanan-layanan (service) yang disediakan oleh suatu sistem yang menyediakan Web Service. Web Service menyimpan data informasi dalam bentuk XML, sehingga data ini dapat diakses oleh sistem lain walaupun berbeda platform, sistem operasi, maupun bahasa compiler [4].

2.4. Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek-aspek keamanan informasi seperti kerahasiaan, integritas data, otantikasi dan anti penyangkalan [3].

2.5. Algoritma AES

Advanced Encryption Standard adalah sebuah algoritma kriptografi simetris yang dapat digunakan untuk mengamankan data. Algoritma ini merupakan standar enkripsi dengan kunci-simetris. Algoritma AES dengan blok ciphertext simetris dapat mengenkripsi dan mendekripsi pada sebuah informasi. Jenis Algoritma ini terbagi menjadi 3 yaitu AES-128, AES-192 dan AES-256. Masing-masing jenis algoritma AES tersebut dapat mengenkrip dan dekrip data pada blok 128 bit, blok 128 bit adalah ukuran tetap blok chiper yang digunakan pada algoritma AES [1].

pada algoritma *Advanced Encryption Standard* (AES), jumlah blok *input*, blok *output* dan *state* adalah 128 bit. Dengan besar data 128 bit, berarti *Nb* = 4 yang menunjukkan panjang data tiap baris adalah 4 *byte.* Dengan blok *input* atau blok data sebesar 128 bit, *key* yang digunakan pada algoritma AES dapat menggunakan kunci yang memiliki panjang 128 bit, 192 bit, atau 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah *round* yang akan diimplementasikan pada algoritma AES tersebut [5].

2.6. Affine Cipher

Affine *Cipher* adalah perluasan dari metode Caesar *Cipher* yang menggunakan teknik substitusi dengan menggunakan fungsi linier ap+b untuk enkripsi teks asli p dan a-1 c-b untuk dekripsi teks sandi c pada z26. Kunci pada sandi Affine adalah 2 integer yaitu a dan b. Nilai a yang dapat dipakai adalah anggota elemen pada z26 yang memiliki invers yaitu yang memenuhi gcd(a,26) = 1 [6].

2.7. Layanan Web Service

Bagian ini berisikan berbagai layanan yang akan digunakan pada sistem *BluAcademic*, 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
List dari semua data surat	GET	/surat	
Buat surat mahasiswa	POST	/suratmahasiswa	*Request body* parameter : nama_instansi, alamat_instansi, telepon_instansi, nim_mahasiswa1, nama_mahasiswa1, nim_mahasiswa2, nama_mahasiswa2. nim_mahasiswa3, nama_mahasiswa3, prodi, id_surat, jumlah_cetak
List dari semua data surat mahasiswa	GET	/suratmahasiswa	
List data surat mahasiswa dari *user* telah buat surat mahasiswa	GET	/user/suratmahasiswa	
List data detail surat	GET	/suratmahasiswa/de	*Path* parameter: *id_user*

mahasiswa dari *user* yang telah buat surat mahasiswa untuk admin melihat detail pesan		tail/{id?}	
Hapus surat mahasiswa	DELETE	/suratmahasiswa/delete/{id?}	*Path* parameter: *id_user*

2.8. Spesifikasi Basis Data

Berikut ini adalah spesifikasi basis data yang digunakan untuk menyimpan dan mengakses data dalam layanan *web service.*

Tabel 2. User

Nama *Field*	Tipe Data	Ukuran	Keterangan
id	int	10	Id user
username	varchar	20	Username user
nama	varchar	100	Nama user
email	varchar	191	Email user
password	varchar	191	Password user
tanggal_lahir	date	10	Tanggal lahir user
jenis_kelamin	enum	2	Jenis_kelamin user
alamat	text	255	Alamat user
foto	varchar	191	Foto user
token	varchar	191	Token user
status_aktif	tinyint	4	Status aktif user
telepon	varchar	15	Telepon user
ni	varchar	14	Ni (NIM/NIP) user
id_status	int	10	status user
id_otorisasi	int	10	Otorisasi user
id_daftar	int	10	Daftar KKP atau TA user
remember_token	varchar	100	Remember token user
created_at	timestamp	20	Waktu pembuatan user
updated_at	timestamp	20	Waktu perubahan user

Tabel 3. Surat Mahasiswa

Nama *Field*	Tipe Data	Ukuran	Keterangan
id	int	10	Id surat mahasiswa
nama_instansi	varchar	191	Nama instansi
alamat_instansi	varchar	191	Alamat_instansi
telepon_instansi	varchar	191	Telepon_instansi
nim_mahasiswa1	varchar	191	Nim mahasiswa 1
nama_mahasiswa1	varchar	191	Nama mahasiswa 1
nim_mahasiswa2	varchar	191	Nim mahasiswa 2
nama_mahasiswa2	varchar	191	Nama mahasiswa 2
nim_mahasiswa3	varchar	191	Nim mahasiswa 3
nama_mahasiswa3	varchar	191	Nama mahasiswa 3
prodi	varchar	191	Prodi
id_surat	varchar	191	Jenis surat
kode_pembayaran	varchar	191	Kode pembayaran
jumlah_cetak	varchar	191	Jumlah cetak
id_statsurat	int	10	Jenis status surat
otal_bayar	varchar	191	Total yang harus dibayar
created_at	timestamp	20	Waktu pembuatan user
updated_at	timestamp	20	Waktu perubahan user
id_user	int	10	Id user yang login

Tabel 4. Surat

Nama *Field*	Tipe Data	Ukuran	Keterangan
id	int	10	Id surat
nama_surat	varchar	191	Jenis surat
harga	varchar	191	Harga surat
created_at	timestamp	20	Waktu pembuatan
updated_at	timestamp	20	Waktu perubahan

Tabel 5. Status Surat

Nama *Field*	Tipe Data	Ukuran	Keterangan
id	int	10	Id status surat
jenis_status	varchar	191	Jenis status
created_at	timestamp	20	Waktu pembuatan
updated_at	timestamp	20	Waktu perubahan

Tabel 6. Mahasiswa Daftar

Nama *Field*	Tipe Data	Ukuran	Keterangan
id	int	10	Id mhs daftar
jenis_daftar	varchar	191	Jenis daftar
created_at	timestamp	20	Waktu pembuatan
updated_at	timestamp	20	Waktu perubahan

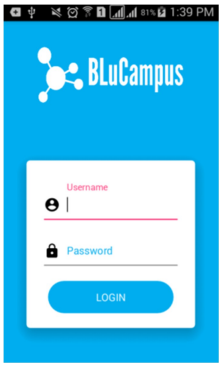
3. HASIL DAN PEMBAHASAN

3.1. Tampilan Layar

Pada bagian ini dijelaskan mengenai proses pada fitur *BluAcademic* pada aplikasi *BluCampus* mulai dari pertama kali dijalankan sampai selesai. Berikut ini akan di berikan penjelasan dan gambar mengenai tampilan-tampilan yang ada pada aplikasi ini.

3.1.1. Tampilan Menu Login

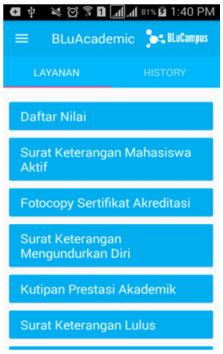
Pada tampilan ini menggunakan layanan data *user* untuk dapat *login* menuju menu BluAcademic.



Gambar 1. Menu Login

3.1.2. Tampilan Menu Layanan

Pada tampilan ini menggunakan layanan data surat untuk menampilkan beberapa pilihan surat yang ingin dipesan.



Gambar 2. Menu Layanan

3.1.3. Tampilan Layanan Surat

Pada tampilan ini menggunakan layanan buat surat mahasiswa, untuk mengirimkan inputan membuat sebuah surat yang akan dipesan.

Gambar 3. Layanan Surat

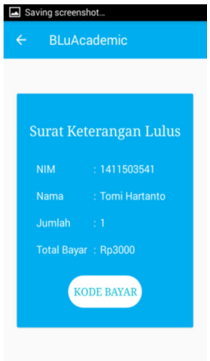
3.1.4. Tampilan Menu *History*

Pada tampilan ini menggunakan layanan surat mahasiswa, untuk menampilkan semua surat yang sudah dipesan oleh *user*.

Gambar 4. Menu History

3.1.5. Tampilan Detail *History*

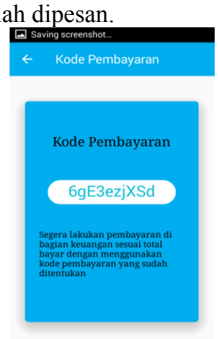
Pada tampilan ini menggunakan layanan surat mahasiswa, untuk menampilkan detail dari surat mahasiswa.



Gambar 5. Detail History

3.1.6. Tampilan Kode Pembayaran

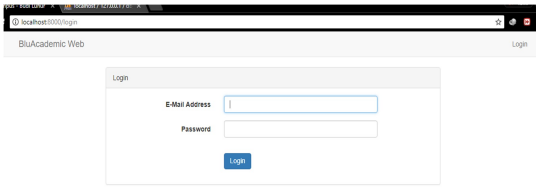
Pada tampilan ini menggunakan layanan data surat mahasiswa, untuk menampilkan kode pembayaran dari surat yang telah dipesan.



Gambar 6. Kode Pembayaran

3.1.7. Tampilan *Login Web*

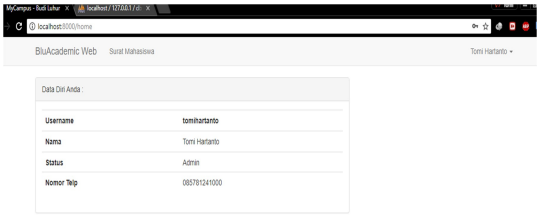
Pada tampilan ini menggunakan data user, untuk dapat *login* menuju halaman awal website BluAcademic.



Gambar 7. Login Web

3.1.8. Tampilan Menu Utama *Web*

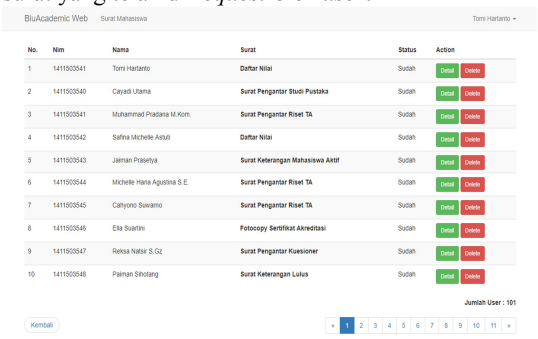
Pada tampilan ini menggunakan layanan user, untuk menampilkan detail user yang melakukan *login*.



Gambar 8. Menu Utama Web

3.1.9. Tampilan Menu Surat Mahasiswa *Web*

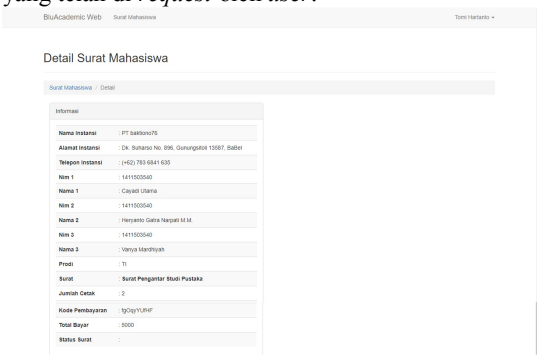
Pada tampilan ini menggunakan layanan data surat mahasiswa, untuk menampilkan semua data dari surat yang telah di *request* oleh *user*.



Gambar 9. Menu Surat Mahasiswa Web

3.1.10. Tampilan Detail Surat Mahasiswa

Pada tampilan ini menggunakan layanan data surat mahasiswa, untuk menampilkan detail dari surat yang telah di *request* oleh *user*.



Gambar 10. Detail Surat Mahasiswa

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 pesan surat mahasiswa.

3.2.2. Uji Coba Layanan Web Service

Tabel dibawah ini merupakan hasil pengujian dari seluruh layanan *web service* yang telah diimplementasikan pada aplikasi android dan website BluAcademic.

Tabel 7. Layanan Web Service

No	Nama Layanan	Hasil
1	List dari semua data *Request* surat	Berhasil
2	Buat *request* surat baru	Berhasil
3	Detail *request* surat	Berhasil
4	List data profil dari user	Berhasil
5	List data jenis surat	Berhasil
6	Hapus data *request* melalui admin	Berhasil
7	List status *request* surat	Berhasil

3.2.2. Pengujian Enkripsi dan Dekripsi Data Surat Mahasiswa

Pada tabel dibawah ini adalah hasil pengujian dari enkripsi data pada menu layanan surat, data layanan surat keterangan magang, surat keterangan riset TA, dan surat keterangan riset KKP dengan mengubah data text dengan metode *Advance Encrypt Standard – 128 (AES-128)* dan Affine Cipher.

Tabel 4.2 menunjukkan hasil dari enkripsi dan dekripsi dengan AES-128 dan Affine Cipher dengan parameter pengujian *Encryption Time* (ET) dan *Decryption Time* (DT) setelah itu dirata-ratakan waktu dalam proses enkripsi dan dekripsi seperti pada tabel dibawah ini.

Tabel 8. Hasil pengujian Proses Enkripsi dan Dekripsi

Plaintext	Output AES-128	Output Affine Cipher	Output AES-128 & Affine Cipher	ET (ms)	DT (ms)
Data Layanan Surat NIM: 1411503541 Nama: Tomi Hartanto	NIM: 9ad1bd45e29fb4302aef42ffdd969391 Nama: 41bba431e3c00c03e49d1f3801e418e2	NIM: <4=$7=-0@'<C7-*!'4@C-'CC==<3<*<$ Nama: -$774-*$@*:!!:!*@-<=$C*9!$@-$9@'	NIM: <4=$7=-0@'<C7-*!'4@C-'CC==<3<*<$ Nama: -$774-*$@*:!!:!*@-<=$C*9!$@-$9@'	281	303
Data Layanan Surat Keterangan Magang Nama Instansi : PT fathonah.wijaya Alamat Instansi : Ds. Baya Kali Bungur No. 801, Bengkulu 22512,	Nama Instansi : 465a847f9d6e6d21c925cc38347b2c5cb2f5e5dc1a33d0337f17a88be64e8b2f Alamat Instansi : 64a2408fe59f3cc86fc248f057097acc908fdf8064dde442f8c0177af83685b977fd2c7345b61f03747ffa9f8262316a7ad678e4ed2fec680	Nama Instansi : -3049-6C<=3@3='$:<'0::*9*-67':0:7'C0@0=:$4**=!**6C$64997@3-@97'C Alamat Instansi : 3-4'-!9C@0<C*::93C:'-9C!06!<64::<!9C=C9!3-==@--'C9:!$664C9*3907<66C=':6*-	Nama Instansi : -3049-6C<=3@3='$:<'0::*9*-67':0:7'C0@0=:$4**=!**6C$64997@3-@97'C Alamat Instansi : 3-4'-!9C@0<C*::93C:'-9C!06!<64::<!9C=C9!3-==@--'C9:!$664C9*3907<66C=':6*-073$C!*6-6CC4<C9'3'*$3464=369@-@='C@:39	237	312

BaBel Telepon Instansi : (+62) 319 4555 255 NIM: 14115 03541 Nama: Tomi Hartanto	63d80e39f191ca8 Telepon Instansi : f8b5b9edc910ef5f22852ccafd8a3cb711d0eea729d7926fe7e9f7ea02f3a8ab NIM: 9ad1bd45e29fb4302aef42ffdd969391 Nama: 41bba431e3c00c03e49d1f3801e418e2	073$C!*6-6CC4<C9'3'*$3464=369@-@='C@:39!3*=9!@*<C$<$:49 Telepon Instansi : C9707<@=:<$!@C0C"90'::4C=94*:76$$=!@@46'<=6<'3C@6@<C6@4!'C*4947 NIM: <4=$7=-0@'<C7-*!'4@C-'CC==<3<*<$ Nama: -$774-*$@*:!!:!*@-<=$C*9!$@-$9@'	!3*=9!@*<C$<$:49 Telepon Instansi : C9707<@=:<$!@C0C"90'::4C=94*:76$$=!@@46'<=6<'3C@6@<C6@4!'C*4947 NIM: <4=$7=-0@'<C7-*!'4@C-'CC==<3<*<$ Nama: -$774-*$@*:!!:!*@-<=$C*9!$@-$9@'		
Data Layanan Surat Keterangan Riset TA Nama Instansi : PT fathonah.wijaya Alamat Instansi : Ds. Baya Kali Bungur No. 801, Bengkulu 22512, BaBel Telepon Instansi : (+62) 319 4555 255 NIM: 14115 03541 Nama: Tomi Hartanto	Nama Instansi : 465a847f9d6e6d21c925cc38347b2c5cb2f5e5dc1a33d0337f17a88be64e8b2f Alamat Instansi : 64a2408fe59f3cc86fc248f057097acc908fdf8064dde442f8c0177af83685b977fd2c7345b61f03747ffa9f8262316a7ad678e4ed2fec68063d80e39f191ca8 Telepon Instansi : f8b5b9edc910ef5f22852ccafd8a3cb711d0eea729d7926fe7e9f7ea02f3a8ab NIM: 9ad1bd45e29fb4302aef42ffd	Nama Instansi : -3049-6C<=3@3='$:<'0::*9*-67':0:7'C0@0=:$4**=!**6C$64997@3-@97'C Alamat Instansi : 3-4'-!9C@0<C*::93C:'-9C!06!<64::<!9C=C9!3-==@--'C9:!$664C9*3907<66C=':6*-073$C!*6-6CC4<C9'3'*$3464=369@-@='C@:39!3*=9!@*<C$<$:49 Telepon Instansi : C9707<@=:<$!@C0C"90'::4C=94*:76$$=!@@46'<=6<'3C@6@<C6@4!'C*4947 NIM: <4=$7=-0@'<C7-*!'4@C-'CC==<3<*<$ Nama: -$774-*$@*:!!:!*@-<=$C*9!$@-$9@'	Nama Instansi : -3049-6C<=3@3='$:<'0::*9*-67':0:7'C0@0=:$4**=!**6C$64997@3-@97'C Alamat Instansi : 3-4'-!9C@0<C*::93C:'-9C!06!<64::<!9C=C9!3-==@--'C9:!$664C9*3907<66C=':6*-073$C!*6-6CC4<C9'3'*$3464=369@-@='C@:39!3*=9!@*<C$<$:49 Telepon Instansi : C9707<@=:<$!@C0C"90'::4C=94*:76$$=!@@46'<=6<'3C@6@<C6@4!'C*4947 NIM: <4=$7=-0@'<C7-*!'4@C-'CC==<3<*<$ Nama: -$774-*$@*:!!:!*@-<=$C*9!$@-$9@' Prodi : =!-*='0:C@$*<!9=!*94<999$$'CC3*CCC$9-:37:!-0$4<99-9$6'9C:3:'99*6	264	346
Data Layanan Surat Keterangan Riset KKP Nama Instansi : PT fathonah.wijaya Alamat Instansi : Ds. Baya Kali Bungur No. 801, Bengkulu 22512, BaBel Telepon Instansi : (+62) 319 4555 255 NIM1: 14115 03541 Nama 1: Tomi Hartanto NIM2: 14115 02477 Nama	Nama Instansi : 465a847f9d6e6d21c925cc38347b2c5cb2f5e5dc1a33d0337f17a88be64e8b2f Alamat Instansi : 64a2408fe59f3cc86fc248f057097acc908fdf8064dde442f8c0177af83685b977fd2c7345b61f03747ffa9f8262316a7ad678e4ed2fec68063d80e39f191ca8 Telepon Instansi : f8b5b9edc910ef5f22852ccafd8a3cb711d0eea729d7926fe7e9f7ea02f3a8ab NIM: 9ad1bd45e29fb4302aef42ffdd969391 Nama: 41bba431e3c00c03e49d1f38	Nama Instansi : -3049-6C<=3@3='$:<'0::*9*-67':0:7'C0@0=:$4**=!**6C$64997@3-@97'C Alamat Instansi : 3-4'-!9C@0<C*::93C:'-9C!06!<64::<!9C=C9!3-==@--'C9:!$664C9*3907<66C=':6*-073$C!*6-6CC4<C9'3'*$3464=369@-@='C@:39!3*=9!@*<C$<$:49 Telepon Instansi : C9707<@=:<$!@C0C"90'::4C=94*:76$$=!@@46'<=6<'3C@6@<C6@4!'C*4947 NIM: <4=$7=-0@'<C7-*!'4@C-'CC==<3<*<$ Nama: -$774-*$@*:!!:!*@-<=$C*9!$@-$9@' Prodi : =!-*='0:C@$*<!9=!*94<999$$'CC3*CCC$9-:37:!-0$4<99-9$6'9C:3:'99*6	Nama Instansi : -3049-6C<=3@3='$:<'0::*9*-67':0:7'C0@0=:$4**=!**6C$64997@3-@97'C Alamat Instansi : 3-4'-!9C@0<C*::93C:'-9C!06!<64::<!9C=C9!3-==@--'C9:!$664C9*3907<66C=':6*-073$C!*6-6CC4<C9'3'*$3464=369@-@='C@:39!3*=9!@*<C$<$:49 Telepon Instansi : C9707<@=:<$!@C0C"90'::4C=94*:76$$=!@@46'<=6<'3C@6@<C6@4!'C*4947 NIM1: <4=$7=-0@'<C7-*!'4@C-'CC==<3<*<$ Nama1: -$774-*$@*:!!:!*	232	321

2: Lia Amelli a Putri NIM3: 14115 04077 Nama 3: Mocha mmad Andik a Putra	01e418e2 NIM2: 7172f102 f7c750da b5181fdc 23e0d688 Nama2: c4e30935 e1a31d02 781db04 1a820ea9 f92082e5 2809253 73f16f38 b04a9370 b9i NIM3: c791feb4 bc14e134 028bb28 2221520 9b Nama3: 2a977b0f 191eba6b 2d32e095 266bb2b 5118d30e 7105b79 97ee0ad6 4c11bdca 95	NIM1: <4=$7=-0@'<C7-*!'4@C-'CC==<3<*<$ Nama1: -$774-*$@*:!!:!*@-<=$C*9!$@-$9@' NIM2: 6$6'C$!'C6:60!=470$9$C=:'*@!=399 Nama2: :-@*!<*0@$4*$=!'69$=7!-$49'!@4<C<'!9'@0'9!<'0*6*C$3C*97!-4<*6!7< NIM3: :6<$C@7-7:$-@$*-!'977'9'"$0'!<7 Nama3: '4<667!C$<$@7437'=*'@!<0'3377'70$$9=*!@6$!076<<6@@!4=3-:$$7=:4<0	@-<=$C*9!$@-$9@' NIM2: 6$6'C$!'C6:60!=470$9$C=:'*@!=399 Nama2: :-@*!<*0@$4*$=!'69$=7!-$49'!@4<C<'!9'@0'9!<'0*6*C$3C*97!-4<*6!7< NIM3: :6<$C@7-7:$-@$*-!'977'9'"$0'!<7 Nama3: '4<667!C$<$@7437'=*'@!<0'3377'70$$9=*!@6$!076<<6@@!4=3-:$$7=:4<0		
			Rata - Rata	253,5	320,5

3.3. Evaluasi Program

Setelah dilakukan analisa dan pengujian aplikasi, maka ditemukan beberapa kelebihan dan kekurangan dari aplikasi yang telah dibuat, berikut adalah beberapa kelebihan dan kekurangan dar aplikasi BluAcademic :

Kelebihan Program :

- Aplikasi mudah dipahami dan digunakan oleh *user*.
- Semua layanan *web service* dapat berfungsi dengan baik.
- Data *request* dapat dienkripsi sehingga dapat mengamankan data saat terjadinya pertukaran data di *server*.

Kekurangan Program :

- *User* masih dapat melakukan *request* pesan sesuai yang *user* inginkan.
- Semua *user* dapat melakukan *request*, karena belum adanya validasi status *user* tersebut.

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 pada algoritma AES 128 membutuhkan satu kunci, sedangkan pada Affine Cipher membutuhkan dua kunci dan satu nilai pergeseran. Sehingga dengan mengkombinasikan algoritma AES 128 dan Affine Cipher maka kemanan data menjadi lebih aman.
- Jumlah data saat proses enkripsi dan dekripsi dilakukan pada server membutuhkan waktu yang lebih lama dibandingkan dengan tidak menggunakan enkripsi dan dekripsi.
- Hasil pengujian rata-rata waktu proses enkripsi adalah 1253,5 ms dan proses dekripsi membutuhkan waktu 1320,5 ms. maka waktu proses enkripsi sedikit lebih cepat dibandingkan dengan proses dekripsi.

5. DAFTAR PUSTAKA

[1] Abidin, A. M., Hardianti, F., & Setiani, I. N. (2016). Analisa Dan Implementasi Proses Kriptografi Encryption-Decryption Dengan Algoritma Advanced Encryption Standard (Aes-128). *Jurnal Sarjana Teknik Informatika, Keamanan Komputer*, `.

[2] Maulidiansyah, R., Rakhman, D. F., & Ramdhani, M. A. (2017). Aplikasi Pelaporan Kerusakan Jalan Tol Menggunakan Layanan Web Service Berbasis Android, *X*(1), 117–123.

[3] Menezes, J.A, 1996, Handbook of Applied Crypthography, USA, CRC Press LLC.

[4] Nuari, N. (2014). Perancangan Aplikasi Layanan Mobile Informasi Administrasi Akademik Berbasis Android Menggunankan Webservice (Studi Kasus Reg. B Universitas Tanjungpura). *Jurnal Sistem Dan Teknologi Informasi (JustIN)*, *1*, 1–7.

[5] Permatasari, D., 2016. Aplikasi Kriptografi Menggunakan Algoritma AES-128 (Advanced Encryption Standard-128) Berbasis Web Pada Laboratorium ICT Terpadu Universitas Budi Luhur.

[6] Rachmawati, D., & Candra, A. (2015). Implementasi Kombinasi Caesar dan Affine Cipher untuk Keamanan Data Teks. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *1*(2), 60–63.