PENERAPAN ALGORITMA AES PADA KEAMANAN URL STUDI KASUS *WEBSITE* MAHASISWA ATMA LUHUR

Asih Indriati
Fakultas Teknologi Informasi
Program Studi Teknik Informatika, ISB Atma Luhur
E-mail: asihindriati77@gmail.com

Abstrak

AES merupakan standar enkripsi dengan kunci simetris yang terdiri dari tiga penyandian blok, yaitu AES-128, AES-192, dan AES-256, yang awalnya diterbitkan sebagai Rijndael. *Website* mahasiswa Atma Luhur memiliki banyak halaman yang diakses melalui *Link* untuk membuka halaman web yang terkait dengan data akademik mahasiswa, contohnya foto maupun nilai akademik mahasiswa. Masing-masing halaman tersebut akan membentuk suatu URL dengan menyebut *File* yang digunakan, sebagai contoh https://mahasiswa.atmaluhur.ac.id /v3/index.php?hal=khs akan membaca *File* khs.php sehingga *File* tersebut akan rentan menjadi target serangan. Penelitian ini mengusulkan penggunaan algoritma AES untuk mengenkripsi URL yang dimaksud dengan tujuan mengamankan URL *website* mahasiswa Atma Luhur. Pengujian dilakukan terhadap 34 URL *website* mahasiswa Atma Luhur, menghasilkan tingkat keberhasilan enkripsi sebesar 100%. Adapun metode pengumpulan data yang digunakan pada penelitian ini menggunakan metode observasi, wawancara, dan studi literatur, untuk metode pengembangan sistem pada penelitian ini menggunakan metode *iterative*. Metode *iterative* terdiri dari beberapa tahapan, yaitu: analisis, desain, implementasi, dan pengujian. Dalam pengembangan sistem juga penulis mengacu pada metode OOP (*Object Oriented Programming*). Dari hasil pengujian yang dilakukan terhadap 34 URL *website* mahasiswa Atma Luhur, menghasilkan tingkat keberhasilan enkripsi sebesar 100%.
Kata Kunci: *AES, Kriptografi, URL*

Abstract

AES is a standard encryption method that uses a symmetric key and consists of three encoding blocks: AES-128, AES-192, and AES-256. The method was first published as Rijndael. The Atma Luhur student website contains several pages that can be accessed by clicking on Links, which provide student academic data such as photos and grades. When accessing any of these pages, a URL is formed by specifying the relevant File, for instance, https://mahasiswa.atmaluhur.ac.id/v3/index.php?hal=khs, which reads the khs.php File. This creates a vulnerability whereby the File can be targeted by attacks. To secure the URL of Atma Luhur's student website, this study recommends using the AES algorithm to encrypt the intended URL. We carried out tests on 34 URLs of the Atma Luhur student website and achieved a 100% encryption level. To collect data in this study, we employed observation, interviews, and literature study. We developed the system in an iterative way, involving analysis, design, implementation, and testing. The iterative method comprises the stages of analysis, design, implementation, and testing. In system development, the author also uses the OOP (Object Oriented Programming) method. The test results from 34 URLs of the Atma Luhur student website indicate a 100% encryption level.
***Keywords**: AES, Kriptografi, URL*

1. Pendahuluan

Dalam era digital saat ini, internet telah menjadi salah satu media komunikasi dan transaksi yang sangat populer. Dalam lingkungan perkuliahan, banyak universitas dan perguruan tinggi yang menggunakan *website* untuk memudahkan mahasiswa dalam mengakses informasi, seperti jadwal kuliah, nilai, dan lain sebagainya.

Maka dari itu, diperlukan tindakan preventif untuk meningkatkan keamanan data yang tersimpan pada *website*, salah satunya dengan menerapkan teknologi kriptografi. *Advanced Encryption Standard* (AES) merupakan salah satu teknik kriptografi yang dapat digunakan untuk meningkatkan keamanan URL. Dengan menerapkan AES pada URL, maka informasi yang dikirim melalui URL akan terenkripsi dan sulit untuk dibaca.

Beberapa penelitian terdahulu yang menjadi acuan penelitian ini antara lain penelitian yang dilakukan oleh Dede Rusman[1] pada tahun 2021 yang berjudul "Implementasi Enkripsi Keamanan URL (*Uniform Resource Locator*) Menggunakan Algoritma AES" menghasilkan kesimpulan URL masih dalam bentuk plainteks dan tidak menjadi cipherteks, sistem sudah aman dari serangan SQL Injection, sedangkan untuk kecepatan hasil percobaan dari 100 pengguna di dapat 16.1/detik dengan waktu terima rata-rata 200.84 kb/detik dan waktu kirim rata-rata 3.11 kb/detik.

Penelitian serupa juga pernah dilakukan oleh Ridwan Andriyanto, dkk.[2] pada tahun 2020 yang berjudul "Penerapan Kriptografi AES Class Untuk Pengamanan URL *Website* Dari Serangan SQL Injection" menghasilkan kesimpulan Algoritma AES dapat mengenkripsi dan mendekripsi data URL sebuah *website* dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit, sehingga dapat menyamarkan informasi yang terdapat pada URL. Enkripsi URL menghasilkan keluaran berupa URL yang tidak menampilkan variabel asli melainkan cipherteks hasil enkripsi.

Selain itu, penelitian yang dilakukan oleh Aghistina Kartikadewi, dkk.[3] pada tahun 2021 yang berjudul "Implementasi Kriptografi dengan Algoritma *Advanced Encryption Standard* (AES) 128 Bit dan Steganografi menggunakan Metode *End of File* (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang" menghasilkan kesimpulan tindakan pencurian, penyalahgunaan dan manipulasi data tidak dapat terjadi karena isi *File* dokumen sudah teracak, dengan menggunakan kunci yang berbeda saat enkripsi dan dekripsi maka keamanan data rahasia semakin terjaga dan aman. Proses dekripsi dengan kunci yang asli akan mengembalikan *File* menjadi *File* semula tanpa mengalami perubahan sedikitpun. Waktu yang digunakan untuk melakukan proses enkripsi dan dekripsi berbanding lurus dengan ukuran *File* yang diproses (semakin kecil ukuran *File* yang diproses, semakin cepat proses enkripsi dan dekripsi dilakukan, semakin besar ukuran *File* yang diproses, semakin lama proses enkripsi dan dekripsi dilakukan).

Penelitian Aprizaldi., dkk.[4] pada tahun 2023 yang berjudul "Aplikasi Keamanan Data Berbasis Web Menggunakan Algoritma AES 128 Untuk Enkripsi Dan Dekripsi Data" menghasilkan kesimpulan dengan adanya sistem keamanan dalam penguncian data dan *File* dapat menghindari terjadinya penipuan dalam pembocoran data proses dan produksi. Selain itu, mengenkripsi *File* dan menyimpannya ke dalam database dalam suatu program dapat membantu melindungi program dari pengguna yang tidak bertanggung jawab.

Penelitian Yusuf Jordan El Anwar, dkk.[5] pada tahun 2022 yang berjudul "Penerapan Metode Kriptografi AES Untuk Mengamankan *File* Dokumen" menghasilkan kesimpulan sistem pengamanan dokumen elektronik berbasis web dapat mengenkripsi dan mendekripsi dokumen menggunakan metode AES.

Oleh karena itu, penelitian ini bertujuan untuk menerapkan AES pada URL untuk meningkatkan keamanan *website* mahasiswa Atma Luhur. Penelitian ini diharapkan dapat memberikan solusi yang tepat dalam meningkatkan keamanan data akademik terkait mahasiswa pada *website* tersebut. Selain itu, penerapan AES pada URL juga dapat memberikan manfaat lainnya, seperti meningkatkan privasi data akademik mahasiswa dan mencegah akses yang tidak sah ke informasi

yang terdapat pada *website*.

a. Rumusan Masalah

Rumusan masalah pada penelitian ini adalah "Bagaimana cara menerapkan algoritma AES untuk keamanan URL yang digunakan pada *website* Mahasiswa Atma Luhur?"

b. Tujuan Penelitian

Tujuan dari penelitian ini adalah menerapkan algoritma AES untuk keamanan URL yang digunakan pada *website* Mahasiswa Atma Luhur.

c. Manfaat Penelitian

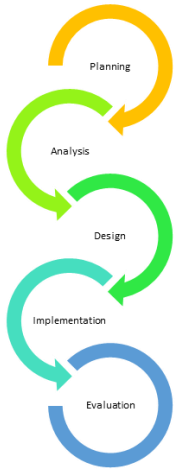
Adapun manfaat yang didapatkan dari penelitian ini antara lain:

1. Meningkatkan kerahasiaan *File* yang diakses pada suatu halaman *website*.
2. Menyamarkan informasi yang dikirimkan pada URL *website*.

2. Metodologi Penelitian

A. Metode Penelitian

Pada penelitian ini, digunakan model pengembangan perangkat lunak *iterative*. Model ini dipilih karena memungkinkan pengembang untuk mengembangkan perangkat lunak secara bertahap dan melakukan perubahan pada setiap tahapan. Setiap iterasi pada model ini memiliki tahapan analisis, desain, implementasi, dan pengujian. Dengan model *iterative*, pengembang dapat menyesuaikan perangkat lunak sesuai dengan kebutuhan pengguna dan memastikan keamanan perangkat lunak dalam setiap tahapan. Berikut adalah tahapan pengembangan perangkat lunak dengan model *iterative*:



Gambar 1. Model *Iterative*[6]

1. Perencanaan

Tahapan ini dimulai dengan mengidentifikasi masalah yang ada dan kebutuhan dari pengguna sistem, yaitu saat akan mengakses *website* mahasiswa atmaluhur, kemudian selanjutnya menentukan tujuan yang hendak dicapai, yaitu mengamankan URL dengan metode kriptografi menggunakan algoritma AES. Pada tahap ini juga dilakukan perencanaan untuk menentukan jumlah iterasi yang diperlukan dan waktu yang dibutuhkan untuk menyelesaikan setiap iterasi.

2. Analisis

Pada tahap ini, tim pengembang melakukan analisis kebutuhan pengguna dan mempelajari sistem yang akan dikembangkan. Analisis ini bertujuan untuk mengidentifikasi masalah atau kekurangan dalam sistem dan menentukan fitur yang dibutuhkan oleh pengguna.

3. Desain

Tahapan desain dilakukan untuk merancang arsitektur sistem, dimulai dari merancang *use case diagram*, *activity diagram*, *sequence diagram*, dan *class diagram*, lalu dilanjutkan dengan membuat desain antarmuka sistem keamanan URL.

4. Pengembangan

Tahapan ini merupakan bagian dari implementasi sistem, dimana sistem dibangun berdasarkan hasil dari tahap analisis dan desain. Pada tahap ini, tim pengembang membuat kode program menggunakan bahasa pemrograman php dan menguji fitur enkripsi dan dekripsi dari

URL di beberapa menu di *website* mahasiswa atma luhur. Setiap iterasi dilakukan untuk memastikan bahwa fitur yang dibuat sesuai dengan kebutuhan pengguna.

5. Pengujian

Pada tahap ini, tim pengembang melakukan pengujian untuk mengevaluasi kinerja dan keamanan sistem. Pengujian dilakukan dengan metode *blackbox* yang menguji fungsionalitas dari sistem kriptografi dalam melakukan enkripsi dan dekripsi terhadap URL.

6. Evaluasi

Tahapan evaluasi dilakukan untuk mengevaluasi setiap iterasi dan menentukan apakah sistem sudah mencapai tujuan yang diinginkan. Jika hasil dari evaluasi memuaskan, maka pengembangan dilanjutkan ke iterasi selanjutnya. Namun, jika ada kekurangan atau perbaikan yang perlu dilakukan, maka tahap analisis dan desain dilakukan kembali sebelum dilanjutkan ke iterasi berikutnya.

B. Teknik Pengumpulan Data

Adapun teknik pengumpulan data yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Observasi

Pada tahap observasi ini peneliti melakukan pengamatan terhadap *website* Sistem Informasi Akademik dengan *URL:* mahasiswa.atmaluhur.ac.id, dengan cara mencoba mengakses beberapa menu yang ada di dalamnya.

2. Wawancara

Wawancara merupakan metode yang digunakan untuk memperoleh informasi dengan cara melakukan sesi tanya jawab kepada pengelola dari *website* yang menjadi objek ujicoba, yakni Direktur Pengembangan Sistem Informasi, ISB Atma Luhur Pangkalpinang.

3. Studi Pustaka (*Literatur*)

Teknik studi pustaka (literatur) merupakan metode yang digunakan untuk mengumpulkan data dengan cara mencari refrensi melalui *e-book* atau mencari jurnal penelitian lima tahun terakhir yang sesuai dengan penelitian yang akan berguna dalam pembuatan penelitian ini.

C. Alat Bantu Pengembangan Sistem

Adapun *tools* yang digunakan dalam pengembangan sistem jaringan pada penelitian ini menggunakan UML (*unified modeling language*). UML (*unified modeling language*) merupakan sebagai alat perancang sistem berorientasi objek. Secara filosofis, lahirnya UML terinspirasi dari konsep yang sudah ada yaitu konsep pemodelan berorientasi objek, karena konsep tersebut dianalogikan seperti sistem kehidupan nyata, dikendalikan oleh objek dan digambarkan atau ditunjukkan dengan simbol-simbol yang sangat spesifik, karena itu pemoodelan berorientasi objek memiliki proses standar dan bersifat independe n[7]. Adapun *tools-tools* yang digunakan dalam penelitian ini sebagai berikut:

1. *Use case diagram*

Use case diagram merupakan sekumpulan atau gambaran dari suatu kelompok yang saling berhubungan satu sama lain dan membentuk suatu sistem yang teratur yang dilaksanakan atau dikendalikan oleh suatu aktor[8].

2. *Activity diagram*

Activity diagram merupakan diagram yang menjelaskan tentang operasi yang dapat dilakukan entitas atau pengguna yang berlaku untuk aplikasi[9].

3. Sequence diagram

Sequence diagram mengambarkan bagaimana suatu objek dapat dilakukan seperti pesan yang dilakukan pada antar mitra yang nantinya akan berguna di dalam membuat model interaksi yang kompleks dan sesuai dengan urutan.[10].

4. *Class diagram*

Class diagram mendeskripsikan sistem dari definisi kelas-kelas yang dirancang. *Class diagram* memiliki 3 area pokok, diantaranya yaitu :

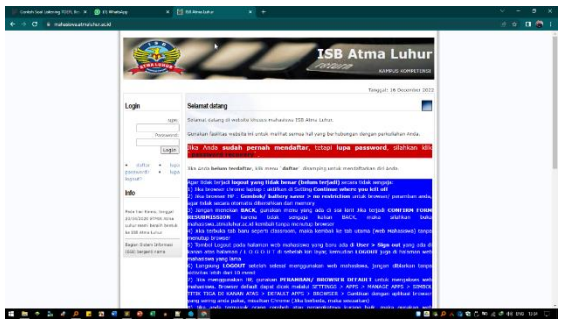
a. Nama Kelas
   Sebuah kelas harus mempunyai nama agar dapat dikenal oleh pengembang.
b. Atribut
   Atribut adalah variabel-variabel sebagai kelengkapan dari suatu kelas.
c. Operasi atau Metode
   Operasi atau metode merupakan fungsi yang dapat dilakukan oleh sebuah kelas [10].

A. Rancangan Sistem Kriptografi

Pada tahap perancangan sistem kriptografi menggunakan algoritma AES ini ada beberapa tahapan yang dilakukan sesuai dengan model pengembangan yang digunakan, antara lain :

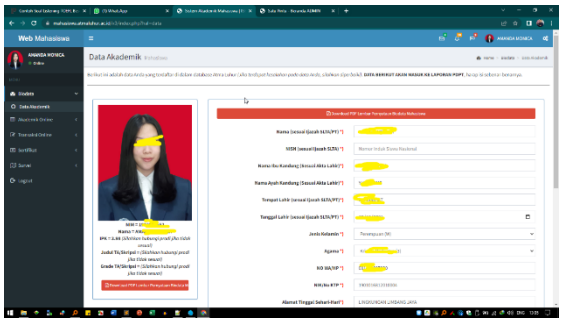
a. Analisa Sistem Berjalan

Mahasiswa ISB Atma Luhur Pangkalpinang setiap kali akan mengakses data akademiknya, perlu membuka dan *Login* di *website* mahasiswa Atma Luhur di domain https://mahasiswa.atmaluhur.ac.id.



Gambar 3. Tampilan halaman *Login Website* Mahasiswa

Setelah mahasiswa berhasil melakukan *Login*, mahasiswa dapat mengakses fitur terkait data akademiknya mulai dari KRS, Jadwal Kuliah, Kartu Ujian, Soal Ujian, Pembayaran, Nilai, Pendaftaran Sidang, foto, dan masih banyak lagi.



Gambar 2. Tampilan *Website* Mahasiswa Setelah *Login*

Pada gambar 2, menunjukkan halaman data akademik seorang mahasiswa dengan *Link* menuju ke URL halaman tersebut adalah https://mahasiswa.atmaluhur.ac.id/v3/index.php?hal=data. Sembari mengklik *Link* lainnya pada menu yang tersedia, misalnya Jadwal Kuliah, maka diperoleh URL https://mahasiswa.atmaluhur.ac.id/v3/index.php?hal=jadwal. Dari percobaan sederhana seperti ini, dapat disimpulkan jika parameter "hal" akan berisi nilai "data", "jadwal", "soalujian", dan sebagainya dimana nilai tersebut mengacu pada *File* yang digunakan untuk menampilkan halaman *website*. Dengan mengetahui info seperti ini, pihak yang "jahil" pasti akan menargetkan serangan ke *File-File* yang berisikan data penting, misalnya nilai.

Selain itu, saat foto akademik mahasiswa di klik kanan, dan dipilih *open image in new tab*, maka akan tampil URL dari foto mahasiswa tersebut, yakni https://mahasiswa.atmaluhur.ac.id/foto/1922500162.jpg. Jika nama *File* foto diganti dengan angka lainnya, misalnya 1922500007.jpg, maka akan menampilkan foto akademik dari mahasiswa yang lain.

b. Analisa Sistem Usulan

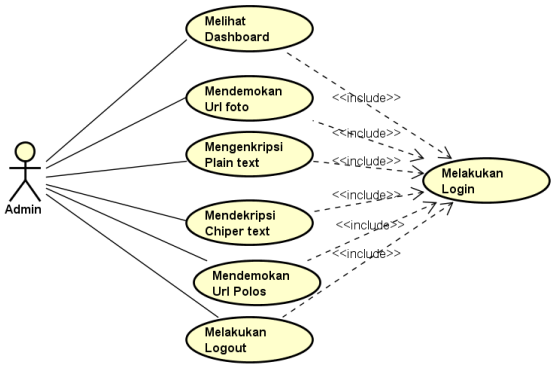
Dalam sistem usulan ini, penulis akan membuat sebuah sistem sebagai pengamanan terhadap URL agar data yang tampil di URL seperti *Link* foto pada contoh kasus ini bisa disembunyikan kedalam format yang terenkripsi menggunakan teknik kriptografi

dengan algoritma AES.

Dalam sistem usulan ada beberapa diagram yang dirancang agar dalam pembuatan sistem sesuai dengan kebutuhan pengguna, antara lain:

a. *Use case diagram* Usulan

Pada tahap ini penulis mendesain *use case diagram* usulan untuk memberi gambaran aktivitas pengguna yaitu admin *website* mahasiswa atmaluhur saat sedang menggunakan sistem. Dapat dilihat pada gambar 4. sebagai berikut.

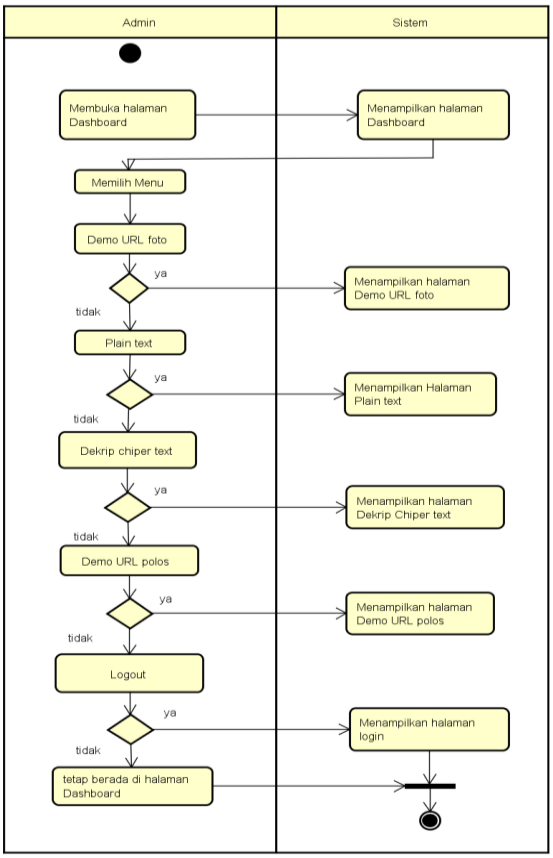


Gambar 4. *Use case diagram* Usulan

Pada gambar 3. dapat dilihat terdapat beberapa menu yang bisa diakses setelah masuk kedalam sistem yang dibuat. Cara kerja sistem kriptografi teradap URL *Website* mahasiswa atmaluhur menggunakan algoritma AES ini bisa di lihat pada *activity diagram* usulan yang mana sistem ini akan melakukan enkripsi dan dekripsi terhadap URL yang diinputkan.

b. *Activity diagram* Usulan

Pada tahap ini, penulis mendesain *activity diagram* untuk memberi gambaran bagaimana aktivitas admin sebagai pengguna dan sistem keamanan url ketika sedang beroperasi. Adapun hasil dari desain yang telah dibuat dapat dilihat pada gambar 5. sebagai berikut.

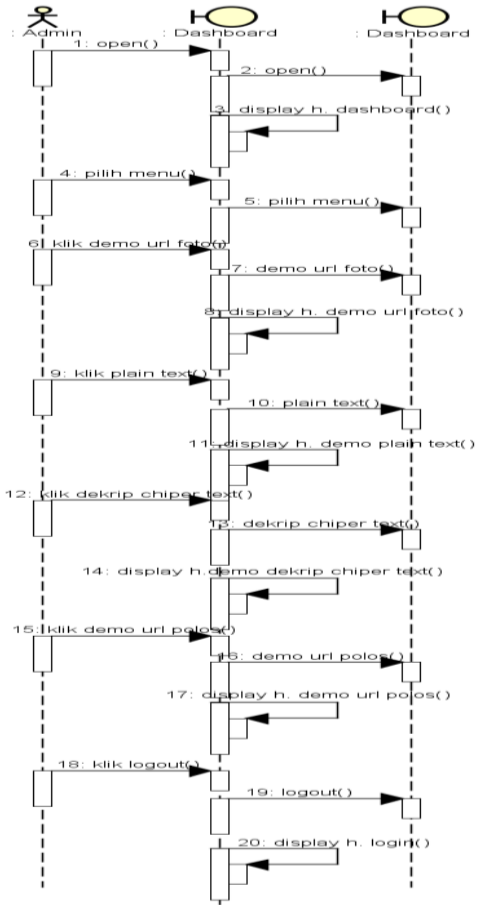


Gambar 5. *Activity diagram* Usulan

Gambar 4 diatas menggambarkan tampilan halaman *Dashboard* pada aplikasi web untuk mengamankan URL. Ketika aplikasi dijalankan, pengguna akan melihat halaman *Dashboard*. Di halaman *Dashboard* ini, pengguna diberikan beberapa pilihan seperti Demo URL Foto, Plain Text, Dekrip Cipher Teks, Demo URL Polos dan *Logout*. Jika pengguna memilih menu Demo URL Foto, aplikasi akan menampilkan halaman Demo URL Foto. Jika pengguna memilih menu Plain Teks, aplikasi akan menampilkan halaman Plain Teks. Menu Dekrip Cipher Teks akan menampilkan halaman Dekrip Cipher Teks. Menu Demo URL Polos akan menampilkan halaman Demo URL Polos. Terakhir, jika pengguna memilih menu *Logout*, aplikasi akan ditutup dan pengguna akan kembali ke halaman *Login*.

c. *Sequence diagram* Usulan

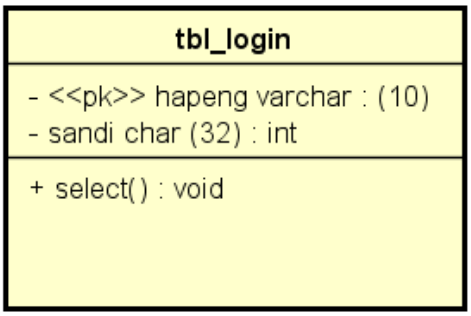
Pada tahap ini, penulis mendesain *Sequence diagram* usulan untuk memberi gambaran tentang proses yang terjadi pada saat sistem digunakan oleh admin. Adapun *sequence diagram* pada *Dashboard admin* dapat dilihat pada gambar 6. sebagai berikut.



Gambar 6. *Sequence diagram* Usulan

Dalam Gambar 5, dapat dijelaskan langkah-langkah yang diambil oleh pengguna untuk mengakses halaman *Login*. Ketika pengguna membuka aplikasi aplikasi akan menampilkan halaman Demo URL Foto. Jika pengguna memilih menu Plain Teks, aplikasi akan menampilkan halaman Plain Teks. Menu Dekrip Cipher Teks akan menampilkan halaman Dekrip Cipher Teks. Menu Demo URL Polos akan menampilkan halaman Demo URL Polos. Terakhir, jika pengguna memilih menu *Logout*, aplikasi akan ditutup dan pengguna akan kembali ke halaman *Login*.

d. Class Diagram



Gambar 7. *Class diagram* Usulan

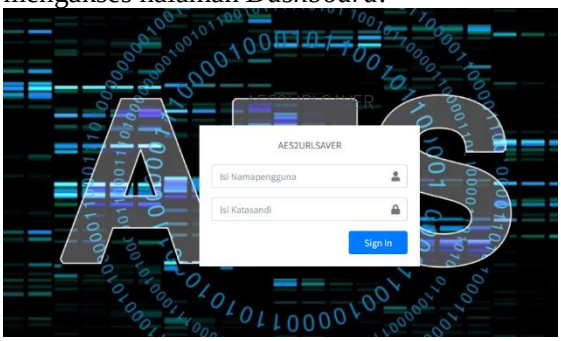
3. Hasil dan Pembahasan

Setelah melakukan desain sistem melalui alat bantu UML, tahapan selanjutnya adalah implementasi dan pengujian.

A. Implementasi

Ada beberapa Langkah awal untuk mengamankan URL pada *website* mahasiswa atmaluhur menggunakan sistem kriptografi yang dibangun, adapun tahapan yang dilalui sebagai berikut:

Ketika aplikasi dijalankan, pengguna akan melihat halaman *Login* seperti yang ditunjukkan dalam gambar 6. Pengguna akan diminta untuk memasukkan username dan password agar dapat mengakses halaman *Dashboard*.

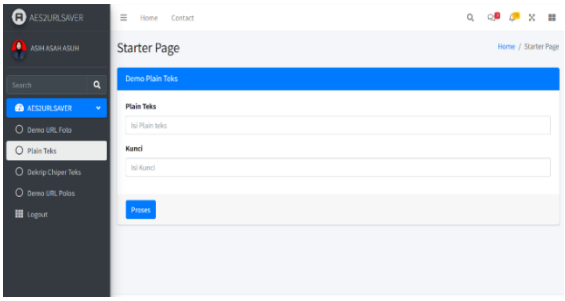


Gambar 8. Tampilan *Login*

Setelah berhasil *Login*, pengguna akan diarahkan ke halaman *Dashboard*. Di halaman ini, terdapat beberapa menu yang dapat dipilih oleh pengguna, yaitu Demo URL foto, Plain Teks, Dekrip Cipher Teks, Demo URL Polos. Jika pengguna memilih Demo URL Foto, aplikasi akan menampilkan halaman Demo URL

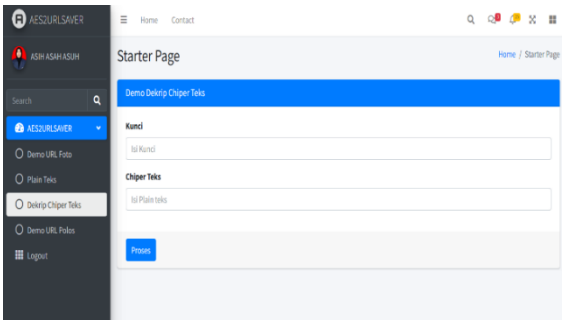
Foto. Jika pengguna memilih menu Plain Teks, aplikasi akan menampilkan halaman Demo Plain Teks. Jika pengguna memilih menu Dekrip Cipher Teks, aplikasi akan menampilkan halaman Demo Dekrip Cipher Teks. Jika pengguna memilih menu Demo URL Polos, aplikasi akan menampilkan halaman Demo URL Polos. Dan jika pengguna memilih menu *Logout*, aplikasi akan menutup dan kembali ke halaman *Login*.

Halaman Demo URL Foto yang berfungsi untuk melakukan proses enkrip dan dekrip pada foto. Sedangkan Halaman Plain Teks yang berfungsi untuk melakukan proses dekripsi. Pada halaman ini, pengguna dapat memilih Plain Teks yang ingin didekripsi, memasukkan plain teks dan kunci yang digunakan saat melakukan enkripsi dengan mengklik tombol "Proses".



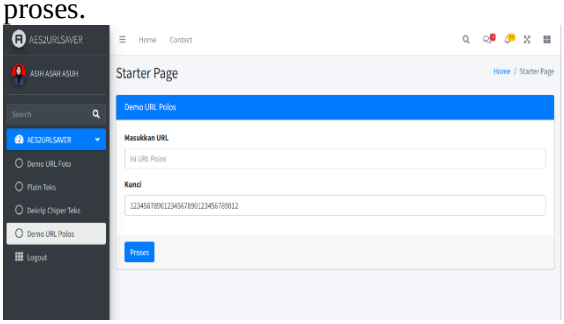
Gambar 9. Tampilan Layar Plain Teks

Halaman Dekrip Cipher Teks yang berfungsi untuk melakukan proses enkripsi. Pada halaman ini, pengguna dapat memilih yang ingin dienkripsi, memasukkan isi kunci dan isi plain teks yang digunakan saat melakukan dekripsi dengan mengklik tombol "Proses".



Gambar 10. Tampilan Dekrip Cipher Teks

Halaman Demo URL Polos yang berfungsi untuk menampilkan hasil Enkripsi *Link*. Admin berada di halaman Demo URL Polos, lalu Menginput URL dan kunci lalu mengklik tombol proses.



Gambar 11. Tampilan Halaman Demo URL Polos

B. Hasil Uji Coba

Adapun hasil dari pengujian didapatkan bahwa sistem mampu melakukan dekripsi dengan baik, sehingga meskipun URL telah di enkrip, akan tetapi data yang dibutuhkan tetap bisa di akses, terlihat dari Tabel 1, ada 7 menu yang diuji, antara lain: Menu data akademik, ganti password dan email, kalender akademik, jadwal kuliah, KHS, HSK, dan *history* pembayaran.

Tabel 1. Menu Pengujian

No	Nama Menu	URL Web	Link (Plain Teks)	Panjang Plain Teks (N Karakter)
1.	Data Akademik	https://mahasiswa.atmaluhur.a[redacted]al=data	[redacted]=data	21
2.	Ganti Password & E-mail	https://mahasiswa.atmaluhur.a[redacted]	[redacted]	12
3.	Kal. Akademik	https://mahasiswa.atmaluhur.a[redacted]mik.php	[redacted].php	20
4.	Jadwal Kuliah	https://mahasiswa.atmaluhur.a[redacted]al=jadwal	[redacted]=jadwal	23
5.	Kartu Hasil Studi	https://mahasiswa.atmaluhur.[redacted]hp?id=2	[redacted]?id=2	22
6.	HSK Online	https://mahasiswa.atmaluhur.ac.id/mhs_hsk.php	[redacted]	11
7.	Hist. Pembayaran	https://mahasiswa.atmaluhur.[redacted]hp?id=6	[redacted]?id=6	22

Dari URL web yang diakses, dapat dilihat nama data seperti id, jadwal dan *Link* lain, kemudian panjang karakter dari *Link* yang ingin di enkrip dihitung per karakter, kemudian dimasukkan kunci yang digunakan untuk melakukan enkripsi, maka dapat terlihat hasilnya seperti pada tabel 2

Tabel 2. Hasil Enkripsi

Kunci (Key)	Panjang Kunci (N Karakter)	Link (Cipher Teks)	Panjang Cipher Teks (N Karakter)	Hasil Dekrip
1234567890123456 7890123456789012	32	DQOsxGUDumSuPj6L [redacted] csA64Kal=	40	sukses
1234567890123456 7890123456789012	32	[redacted] RIBtG8VDhA=	28	sukses
1234567890123456 7890123456789012	32	QgLgvAEtvmONGNn [redacted] g4TRw==	40	sukses
1234567890123456 7890123456789012	32	TQDJk90gvmTTMsB6 [redacted] W52TcV+g==	44	sukses
1234567890123456 7890123456789012	32	hgF93L8lvmTlV2Abtc [redacted] RoAkK	40	sukses
1234567890123456 7890123456789012	32	kAKEvrAnvmQX3X6p [redacted]	28	sukses
1234567890123456 7890123456789012	32	wwFUAG8uvmTBn+s [redacted] Ka1kGRjWgt	40	sukses

4. Kesimpulan dan Saran

Berdasarkan pembahasan yang telah dilakukan, penelitian ini berhasil menerapkan algoritma AES untuk keamanan URL yang digunakan pada *website* Mahasiswa Atma Luhur, sehingga dapat:

1. Meningkatkan kerahasiaan *File* yang diakses pada suatu halaman *website*.
2. Menyamarkan informasi yang dikirimkan pada URL *website*.

Adapun beberapa saran yang dapat disampaikan untuk penelitian lebih lanjut diantaranya sebagai berikut:

1. Algoritma AES sebagai enkripsi URL dapat digabungkan dengan algoritma steganografi untuk hasil yang lebih aman.
2. Studi kasus dapat diperluas ke *website* lain sebagai objek penelitian.

Daftar Pustaka

[1] D. Rusman, "Implementasi Enkripsi Keamanan URL (*Uniform Resource Locator*) Menggunakan Algoritma AES," no. January, 2021.

[2] R. Andriyanto, K. Khairijal, and D. Satria, "Penerapan Kriptografi AES Class Untuk Pengamanan URL *WEBSITE* Dari Serangan SQL INJECTION," J. Unitek, vol. 13, no. 1, pp. 34–48, 2020, doi: 10.52072/unitek.v13i1.153.

[3] A. Eka Putri, A. Kartikadewi, and L. A. Abdul Rosyid, "Implementasi Kriptografi dengan Algoritma *Advanced Encryption Standard* (AES) 128 Bit dan Steganografi menggunakan Metode *End of File* (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang," Appl. Inf. Syst. Manag., vol. 3, no. 2, pp. 69–78, 2021, doi: 10.15408/aism.v3i2.14722.

[4] N. A. Ilham, "Implementasi Konsep Pemrograman Berorientasi Objek Pada Aplikasi Sistem Parkir Menggunakan Bahasa Pemrograman Java," J. Edukasi Elektro, vol. 3, no. 2, pp. 63–69, 2020, doi: 10.21831/jee.v3i2.28293.

[5] Y. J. El Anwar, R. Habibi, and N. Riza, "Penerapan Metode Kriptografi AES Untuk Mengamankan *File* Dokumen," J. Tekno Insentif, vol. 16, no. 2, pp. 92–104, 2022, doi: 10.36787/jti.v16i2.852.

[6] T. Oktarina and U. B. Darma, "APPLICATION OF THE *ITERATIVE* MODEL IN DESIGNING AN ACADEMIC E- PENERAPAN MODEL *ITERATIVE* DALAM PERANCANGAN SISTEM E- KONSELING AKADEMIK UNTUK MAHASISWA PADA UNIVERSITAS BINA," vol. 4, no. 1, pp. 117–124, 2023.

[7] S. Dharwiyanti and R. S. Wahono, "Pengantar Unified Modeling LAnguage (UML)," IlmuKomputer.com, pp. 1–13, 2003, [Online]. Available: http://www.unej.ac.id/pdf/yanti-uml.pdf

[8] M. Korkmaz, O. K. Sahingoz, and B. DIri, "Detection of Phishing *Website*s by Using Machine Learning-Based URL Analysis," 2020 11th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2020, no. June 2021, 2020, doi: 10.1109/ICCCNT49239.2020.9225561.

[9] F. Huzaeni, I. Gunawan, D. Cahya, M. Yanti, and N. Krisdayanti, "Analisis Keamanan Data Pada *Website* Dengan Wireshark," JES (Jurnal Elektro Smart), vol. 1, no. 1, pp. 13–17, 2021, [Online]. Available: https://www.sttrcepu.ac.id/jurnal/index.php/jes/article/view/161

[10] Y. Findawati, Buku Ajar Rekayasa Perangkat Lunak. 2018.

[11] G. G. Putri, W. Setyorini, and R. D. Rahayani, "Analisis Kriptografi Simetris AES dan Kriptografi Asimetris RSA pada Enkripsi Citra Digital," ETHOS (Jurnal Penelit. dan Pengabdian), vol. 6, no. 2, pp. 197–207, 2018, doi: 10.29313/ethos.v6i2.2909.