IMPLEMENTASI METODE ALGORITMA AES PADA PERLINDUNGAN DATA SISTEM LOGIN

Lie Clara [1] dan Akhmad Budi [2]
[1]Alumni Program Studi Teknik Informatika
[2]Staff Pengajar Program Studi Teknik Informatika
Institut Bisnis dan Informatika Kwik Kian Gie
Jl. Yos Sudarso Kav. 87, Sunter, Jakarta Utara, 14350
56160336@student.kwikkiangie.ac.id
akhmad.budi@kwikkiangie.ac.id

ABSTRACT

At present the development of digital technology and telecommunications is progressing very rapidly throughout the world, making almost in every country always closely related to technology in their daily lives, including Indonesia. Utilization of computer applications in everyday life has become a necessity. For this reason, the issue of security and confidentiality of data and information is very important. Personal data should not be known by others to suppress the occurrence of data that is misused and used. It needs to be protected and restricted from anyone who can access important data.

In this study, the authors developed a login data security system application with the AES algorithm method to assist individuals in maintaining important data, especially passwords they have. In addition this application uses a MySQL database as a means of storing data, and PHP, HTML as a programming language, and CodeIgniter as a framework for supporting system development.

This research was conducted by utilizing the methods in collecting data, namely, literature study and documentation. And utilizing the AES algorithm as a data analysis and measurement technique

The design of the application that the authors propose will include a system architecture, a system description using UML diagrams, namely use case diagrams, activity diagrams, and class diagrams, there is also a design interface and program flow design to explain how the program can run and how the program displays when viewed by the user, and there is a system implementation that covers hardware specifications, installation guides, and usage guides.

The cryptographic application that the authors produced through this research is intended to be able to provide a security system solution that can maintain data security on the login system so that users can stop using passwords that are weak and repetitive, so users can keep their passwords safer.

Keyword : Information System, Data, Login System, AES Algorithm, Cryptography.

1. PENDAHULUAN

Saat ini perkembangan teknologi digital dan telekomunikasi mengalami kemajuan yang sangat pesat di seluruh dunia, membuat hampir di setiap negara selalu berhubungan erat dengan teknologi dalam kehidupan sehari-harinya, termasuk juga Indonesia. Pemanfaatan komputer yang semakin canggih dan pemanfaatan aplikasi komputer yang semakin banyak dan beraneka ragam. Selain itu dengan berkembangnya teknologi dan internet, juga mempermudah serta memperluas penyebaran informasi ke segala penjuru.

Pemanfaatan aplikasi komputer dalam kehidupan sehari-hari sudah menjadi suatu kebutuhan. Karena penggunaan komputer dinilai dapat menghasilkan pengolahan data yang lebih akurat dan pencarian data yang lebih cepat pada teknologi berkembang saat ini.

Untuk itu pemanfaatan aplikasi komputer dan teknologi tentunya sangat berkaitan erat dengan data. Pada bidang dan pekerjaan apapun, data menjadi salah satu bagian terpenting di dalam hidup. Segala hal yang dilakukan oleh masyarakat melibatkan sejumlah data dalam prosesnya. Data-data yang bersifat personal tidak sepatutnya diketahui oleh orang lain untuk menekan terjadinya data tersebut disalahgunakan dan dimanfaatkan tanpa ijin pengguna selaku yang berhak atas data-data tersebut.

Maka itu data perlu dilindungi dan dibatasi siapa saja yang dapat mengakses data-data tersebut. Sehingga masalah keamanan dan kerahasiaan data dan informasi merupakan suatu hal yang sangat penting. Dengan semakin berkembangnya teknologi membuat penyebaran informasi menjadi lebih mudah, sehingga membuat segala hal yang kita lakukan yang berkaitan dengan

teknologi dan internet menjadi lebih rentan dan dapat berpotensi untuk dicuri dan disalahgunakan oleh pihak lain.

Dalam aplikasi komputer baik untuk kebutuhan personal maupun bisnis diperlukan suatu sistem yang dilengkapi dengan kemampuan untuk mengenkripsi data khususnya data-data yang berkaitan dengan sistem login yaitu kata sandi/ password. Kata sandi atau password merupakan hal yang paling sering ditemukan dalam kehidupan sehari-hari dan merupakan benteng pertahanan terkuat terhadap serangan dan pencurian data. Karena kasus-kasus kebocoran dan pencurian data terjadi akibat kata sandi yang digunakan bersifat lemah dan memiliki suatu pola tertentu sehingga menjadikan kata sandi tersebut mudah untuk ditebak serta memiliki unsur yang sama dengan kata sandi yang pernah digunakan sebelumnya. Namun apabila kata sandi yang digunakan bersifat unik untuk setiap keperluan dan akun yang dimiliki maka akan banyak sekali kata sandi yang dimiliki, dan akan sulit untuk mengelola dan menyimpan kata sandi tersebut di tempat yang berbeda-beda dan di tempat yang dapat diakses oleh orang lain.

2. LANDASAN TEORI

2.1. Data

Menurut Hutahaean (2014:8), "Data adalah bahan mentah bagi informasi, dirumuskan sebagai kelompok lambang-lambang tidak acak. Menunjukan jumlah, tindakan-tindakan, hal-hal dan sebagainya."

Selain itu menurut Rainer dan Prince (2016:10), "Data merupakan deskripsi dasar tentang berbagai hal, peristiwa, aktivitas, dan transaksi yang direkam, diklasifikasi, dan disimpan tetapi belum disusun atau diolah untuk menyampaikan suatu makna tertentu."

2.2. Informasi

Pengertian sistem menurut Romney dan Steinbart (2015:4), "Informasi (information) adalah data yang telah dikelola dan diproses untuk memberikan arti dan memperbaiki proses pengambilan keputusan. Sebagaimana perannya, pengguna membuat keputusan yang lebih baik sebagai kuantitas dan kualitas dari peningkatan informasi."

Menurut Rainer dan Prince (2016:10), "Informasi mengacu pada data yang telah disusun sehingga memiliki makna dan nilai bagi penerima." Informasi dapat juga dikatakan sebagai sebuah pengetahuan yang diperoleh dari pembelajaran, pengalaman, dan instruksi. Sehingga dapat disimpulkan bahwa informasi merupakan data hasil pengolahan sistem maupun teknologi informasi yang memiliki nilai dan berguna bagi pengguna/ penerimanya.

2.3. Sistem

Menurut Romney dan Steinbart (2015:3), Sistem adalah suatu rangkaian yang terdiri dari dua atau lebih komponen yang saling berhubungan dan saling berinteraksi satu sama lain untuk mencapai tujuan dimana sistem biasa nya terbagi dalam sub system yang lebih kecil yang mendukung system yang lebih besar.

Definisi sistem menurut Mulyadi (2016:5), "Sistem adalah suatu jaringan prosedur yang dibuat menurut pola yang terpadu untuk melaksanakan kegiatan pokok perusahaan."

Dari kedua informasi yang telah dijabarkan di atas, secara sederhana sistem dapat diartikan sebagai suatu kumpulan atau himpunan dari unsur, komponen, atau variabel yang terorganisir, saling berinteraksi, saling tergantung satu sama lain, dan terpadu.

1. Pendekatan sistem pada prosedurnya

Suatu sistem adalah suatu jaringan dan prosedur yang saling berkaitan, dan bekerja sama untuk melakukan suatu pekerjaan atau menyelesaikan suatu masalah tertentu.

2. Pendekatan sistem pada komponennya

Suatu sistem adalah sekumpulan dari beberapa elemen yang saling berinteraksi dengan teratur sehingga membentuk suatu totalitas untuk menyelesaikan suatu masalah tertentu. Berdasarkan beberapa pendapat yang dikemukakan diatas dapat ditarik kesimpulan bahwa sistem adalah kumpulan bagian-bagian atau sub sistem - sub sistem yang disatukan dan dirancang untuk mencapai suatu tujuan.

2.4. Sistem Informasi

Menurut Kenneth C Laudon dan Jane P Laudon (2014:45), "Suatu sistem informasi dapat didefinisikan secara teknis sebagai seperangkat komponen yang saling terkait yang mengumpulkan (atau mengambil), memproses, menyimpan, dan mendistribusikan informasi untuk mendukung pengambilan keputusan dan kontrol dalam suatu organisasi."

Menurut Yakub dan Hisbanarto (2014:32) "Sistem informasi merupakan hal yang sangat penting bagi manajemen dalam pengambilan keputusan dalam sebuah organisasi yang berhubungan dengan proses penciptaan dan aliran informasi."

Sementara menurut R. Kelly Rainer dan Casey G. Cegielski (2015:5), "Sistem Informasi merupakan sistem yang mengumpulkan, mengolah, menyimpan, menganalisa, dan menguraikan informasi untuk tujuan spesifik."

2.5. Keamanan Informasi

Menurut Whitman dan Mattord (2011:41), Keamanan informasi merupakan upaya untuk melindungi informasi dan elemen-elemen penting yang ada didalamnya, baik berupa sistem atau perangkat keras yang digunakan untuk menyimpan dan mengirimkan informasi.

Keamanan informasi menggambarkan usaha untuk melindungi komputer dan non peralatan komputer, fasilitas, data, dan informasi dari penyalahgunaan oleh orang yang tidak bertanggung jawab. Keamanan informasi dimaksudkan untuk mencapai kerahasiaan, ketersediaan, dan integritas di dalam sumber daya informasi baik bagi kebutuhan personal maupun kebutuhan bisnis perusahaan.

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi, sayang sekali masalah keamanan ini seringkali kurang mendapat perhatian dari pemilik dan pengelola sistem infromasi. Jatuhnya informasi ke pihak lain (misal pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi. Untuk itu keamanan dari sistem informasi yang digunakan harus terjamin dalam batas yang diterima. Web server dan database Server bagaikan jantung dan otak dari organisme internet. Dua komponen ini menjadi komponen pokok dari sebuah aplikasi internet yang tangguh dan tepatlah keduanya menjadi target hacker. Dalam beberapa kasus kita harus dapat menentukan titik-titik lemah dalam aplikasi tersebut yang bisa menjadi sasaran penyerang. Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi.

Keamanan informasi dimaksudkan untuk mencapai tiga sasaran utama yaitu:

- Melindungi data dan informasi personal dan bisnis dari penyingkapan orang-orang yang tidak berhak. Inti utama dari aspek kerahasiaan adalah usaha untuk menjaga informasi dari orang-orang yang tidak berhak mengakses. Privacy lebih kearah data-data yang sifatnya privat. Serangan terhadap aspek privacy misalnya usaha untuk melakukan penyadapan. Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy adalah dengan menggunakan teknologi kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, serta autentikasi data.
- Ketersediaan. Aspek ini berhubungan dengan metode untuk menyatakan bahwa informasi benar-benar asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. Masalah pertama untuk membuktikan keaslian dokumen dapat dilakukan dengan teknologi watermarking dan digital signature.Watermarking juga dapat digunakan untuk menjaga intelektual property, yaitu dengan menandatangani dokumen atau hasil karya pembuat. Masalah kedua biasanya berhubungan dengan akses control, yaitu berkaitan dengan pembatasan orang-orang yang dapat mengakses informasi. Dalam hal ini pengguna harus menunjukkan bahwa memang dia adalah pengguna yang sah atau yang berhak menggunakannya.
- Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa izin. Sistem informasi perlu menyediakan representasi yang akurat dari sistem fisik yang direpresentasikan.

2.6. Unified Modelling Language (UML)

UML (Unified Modelling Language) adalah sekumpulan alat yang digunakan untuk melakukan abstraksi terhadap sebuah sistem atau perangkat lunak berbasis objek. UML juga menjadi salah satu cara untuk mempermudah pengembangan aplikasi yang berkelanjutan. Aplikasi atau sistem yang tidak terdokumentasi biasanya dapat menghambat pengembangan karena developer harus melakukan penelusuran dan mempelajari kode program. UML juga dapat menjadi alat bantu untuk transfer ilmu tentang sistem atau aplikasi yang akan dikembangkan dari satu developer ke developer lainya. Tidak hanya antar developer terhadap orang bisnis dan siapapun dapat memahami sebuah sistem dengan adanya UML.

a. Use Case Diagram

Use Case Diagram adalah gambaran grafis dari beberapa atau semua actor, use case, dan interaksi diantaranya yang memperkenalkan suatu sistem.

Simbol-simbol yang digunakan dalam use case diagram, yaitu :

- Use case menggambarkan fungsionalitas yang disediakan sistem.
- Aktor adalah orang, proses, atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat.
- Asosiasi adalah komunikasi antara aktor dan use case yang berpartisipasi pada use case diagram atau use case yang memiliki interaksi dengan aktor.
- Include adalah relasi use case tambahan ke sebuah use case dimana use case yang ditambahkan membutuhkan use case ini untuk

menjalankan fungsinya atau sebagai syarat dijalankan use case ini.
- Extend adalah relasi use case tambahan ke sebuah use case dimana use case yang ditambahkan dapat berdiri sendiri meski tanpa use case tambahan itu.
- Hubungan generalisasi dan spesialisasi (umum - khusus) antara dua buah use case dimana fungsi yang satu merupakan fungsi yang lebih umum dari lainnya.

b. Activity Diagram

Diagram ini menggambarkan tentang aktifitas yang terjadi pada sistem. Dari pertama sampai akhir, diagram ini menunjukkan langkah – langkah dalam proses kerja sistem yang dibuat.

c. Class Diagram

Class Diagram menggambarkan serta deskripsi atau penggambaran dari class, atribut, dan objek disamping itu juga hubungan satu sama lain seperti pewarisan, containmet, asosiasi dan lainnya.

2.7. Sistem Basis Data

Menurut Rosa dan Shalahuddin (2015:43) "Basis data merupakan salah satu bagian dalam rekayasa perangkat lunak yang terkomputerisasi dan bertujuan utama memelihara data yang sudah diolah atau media penyimpanan informasi agar dapat diakses dengan mudah dan cepat."

Sedangkan menurut Yakub dan Hisbanarto (2015:25) menjelaskan, "Basis data merupakan kumpulan data yang saling berhubungan atau punya relasi".

Dari teori ahli di atas, dapat disimpulkan bahwa sistem basis data merupakan kumpulan dari data yang saling berhubungan (relasi) antara satu dengan yang lainnya yang diorganisasikan berdasarkan skema atau struktur tertentu sehingga menghasilkan suatu informasi.

Pada penelitian ini, sistem basis data yang penulis gunakan adalah MySQL. MySQL merupakan sistem basis data yang menggunakan perintah dasar SQL (Structured Query Language). SQL sendiri merupakan suatu bahasa yang dipakai di dalam pengambilan data pada relational database atau sistem basis data yang terstruktur. Jadi MySQL adalah database management system yang menggunakan bahasa SQL sebagai bahasa penghubung antara perangkat lunak aplikasi dengan database server.

Berikut adalah kelebihan dari mysql yang membuat penulis menggunakan sistem basis data mysql dalam penelitian ini :

- Program yang multi-threaded, sehingga dapat dipasang pada server yang memiliki mulit-CPU
- Didukung bahasa pemrograman umum seperti C, C++, Java, Perl, PHP, Python, TCL, APls dls.
- Bekerja pada berbagai platform
- Memiliki jenis kolom yang cukup banyak sehingga memudahkan konfigurasi system database
- Memiliki jenis kolom yang cukup banyak sehingga memudahkan konfigurasi sistem database
- Memiliki system sekuriti yang cukup baik dengan verifikasi host
- Mendukung ODBC untuk OS Microsoft Windows
- Mendukung record yang memiliki kolom dengan panjang tetap
- Software yang free

2.8. Kriptografi

Menurut Dan Boneh dan Victor Shoup (2015:2), "Kriptografi adalah alat yang sangat diperlukan untuk melindungi informasi dalam sistem komputasi."

Perkembangan komunikasi telah mendorong manusia untuk menyembunyikan informasi yang dimilikinya dari orang lain demi alasan keamanan dan privasi, untuk itu ditemukanlah konsep kriptograf. Kriptografi telah dikenal sejak 4000 tahun yang lalu. Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana.

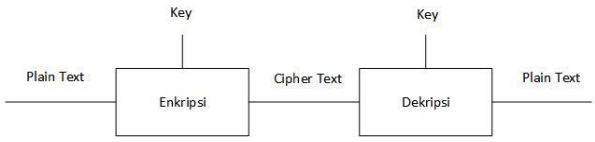
Kriptografi merupakan seni dan keahlian mengamankan pesan atau data menghasilkan suatu pesan atau data yang asli berubah menjadi tidak dikenali lagi. Secara umum kriptografi dapat diartikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu pesan.

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

1. Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
2. Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.

3. Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
4. Non-repudiasi., adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat. Istilah-istilah yang digunakan dalam bidang kriptografi :
   a. Plaintext (M) adalah pesan yang hendak dikirimkan (berisi data asli).
   b. Ciphertext (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
   c. Enkripsi (fungsi E) adalah proses pengubahan plaintext menjadi ciphertext.
   d. Dekripsi (fungsi D) adalah kebalikan dari enkripsi yakni mengubah ciphertext menjadi plaintext, sehingga berupa data awal/asli.

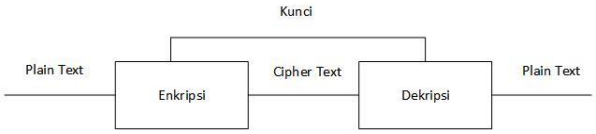
Kriptografi pada dasarnya terdiri dari dua proses, yaitu proses enkripsi dan proses dekripsi. Proses enkripsi adalah proses penyandian pesan terbuka menjadi pesan rahasia (ciphertext). Pada saat ciphertext diterima oleh penerima pesan, maka pesan rahasia tersebut diubah lagi menjadi pesan terbuka melalui proses deskripsi sehingga pesan tadi dapat dibaca kembali oleh penerima pesan. Secara umum, proses enkripsi dan dekripsi dapat digambarkan sebagai berikut:



Gambar 2. 1 Proses Enkripsi dan Dekripsi
Sumber : AES, Algoritma Rijndael

Algoritma Kriptografi Ada 2 jenis kriptografi berdasar jenis kuncinya yaitu algoritma simetri (konvensional/secret key) dan algoritma asimetri (kunci publik/public key).

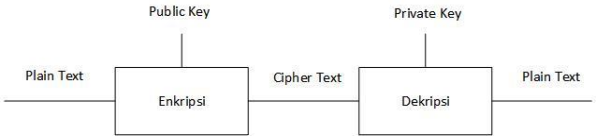
a. Kriptografi Simetri (Secret Key) Kriptografi secret key adalah kriptografi yang hanya melibatkan satu kunci dalam proses enkripsi dan dekripsi. Kriptografi secret key seringkali disebut sebagai kriptografi konvensional atau kriptografi simetris (Symmetric Cryptography) dimana proses dekripsi adalah kebalikan dari proses enkripsi dan menggunakan kunci yang sama.



Gambar 2. 2 Kriptografi Simetris
Sumber : AES, Algoritma Rijndael

Yang termasuk dalam kriptografi algoritma kunci simetri adalah OTP, DES, RC2, RC4, RC5, RC6, IDEA, AES, Twofish, Blowfish, Magenta, FEAL, SAFER, CAST, GOST, A5, LOKI, dan lain-lain

b. Kriptografi Asimetri (Public Key) Kriptografi public key sering disebut dengan kriptografi asimetris. Berbeda dengan kriptografi secret key, kunci yang digunakan pada proses enkripsi dan proses dekripsi pada kriptografi public key ini berbeda satu sama lain. Jadi dalam kriptografi public key, suatu key generator akan menghasilkan dua kunci berbeda dimana satu kunci digunakan untuk melakukan proses enkripsi dan kunci yang lain digunakan untuk melakukan proses dekripsi. Yang termasuk dalam algoritma asimetri adalah ECC, LUC, RSA, El Gamal, dan DH.

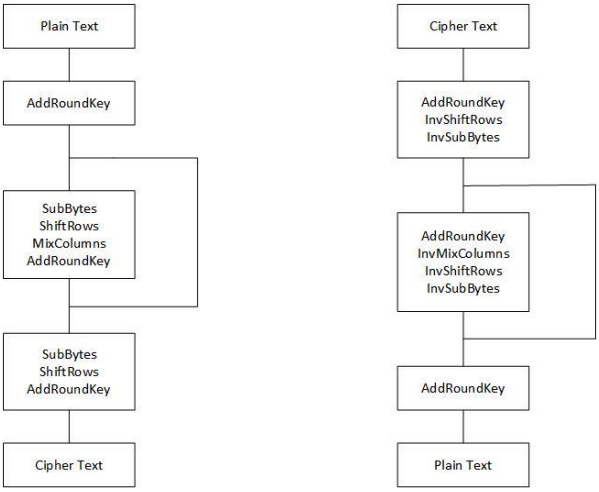


Gambar 2. 3 Kriptografi Asimetris
Sumber : AES, Algoritma Rijndael

2.9. Enkripsi

Menurut Dan Boneh dan Victor Shoup (2015:18), “Enkripsi adalah kasus bagaimana dua pihak dapat berkomunikasi secara rahasia di Internet dengan adanya kehadiran penyadap.”

Proses enkripsi pada algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Pada awal proses enkripsi, input yang telah dikopikan ke dalam akan mengalami transformasi byte AddRoundKey. Setelah itu, State akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai round function.



Gambar 2. 4 Diagram Alir Proses Enkripsi dan Dekripsi
Sumber : AES, Algoritma Rijndael

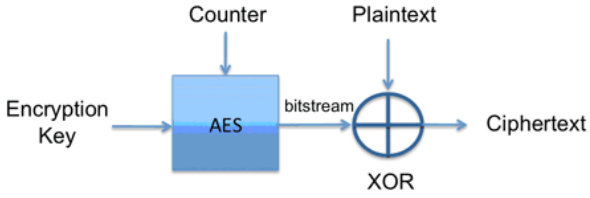
2.10. Dekripsi

Dekripsi Transformasi cipher dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse cipher yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers cipher adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey.

2.11. Algoritma AES

AES adalah lanjutan dari algoritma enkripsi standar DES yang pada 2 Maret tahun 2001 ditetapkanlah algoritma baru Rijndael sebagai AES. Kriteria pemilihan AES didasarkan pada 3 kriteria utama yaitu: keamanan, harga, dan karakteristik algoritma beserta implementasinya.

Rijndael termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan cipher block. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu.



Gambar 2. 5 Algoritma AES
Sumber : AES, Algoritma Rijndael

Rijndael mendukung berbagai variasi ukuran blok dan kunci yang akan digunakan. Namun Rijndael mempunyai ukuran blok dan kunci yang tetap sebesar 128, 192, 256 bit. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi. Proses enskripsi adalah kebalikkan dari deskripsi. Berikut penjelasannya :

1. Key Schedule

Proses key schedule diperlukan untuk mendapatkan subkey-subkey dari kunci utama agar cukup untuk melakukan enkripsi dan dekripsi. Proses ini terdiri dari beberapa operasi, yaitu :

a. Operasi Rotate, yaitu operasi perputaran 8 bit pada 32 bit dari kunci.
b. Operasi SubBytes, pada operasi ini 8 bit dari subkey disubstitusikan dengan nilai dari S-Box.
c. Operasi Rcon, operasi ini dapat diterjemahkan sebagai operasi pangkat 2 nilai tertentu dari user. Operasi ini menggunakan nilai-nilai dalam Galois field. Nilai-nilai dari Rcon kemudian akan di-XOR dengan hasil operasi SubBytes.
d. Operasi XOR dengan w[i-Nk] yaitu word yang berada pada Nk sebelumnya.

2. AddRoundKey

Pada proses ini subkey digabungkan dengan state. Proses penggabungan ini menggunakan operasi XOR untuk setiap byte dari subkey dengan byte yang bersangkutan dari state. Untuk setiap tahap, subkey dibangkitkan dari kunci utama dengan menggunakan proses key schedule. Setiap subkey berukuran sama dengan state yang bersangkutan.

3. SubBytes

Rijndael hanya memiliki satu S-box. Kriteria desain untuk kotak S yang dibuat sedemikian rupa sehingga tahan terhadap diferensial linear yang dikenal sebagai pembacaan sandi dan menyerang menggunakan manipulasi aljabar. Koordinat x merupakan digit pertama sedangkan y yang kedua dari bilangan hexadecimal

4. ShiftRows

Proses ShiftRows akan beroperasi pada tiap baris dari tabel state. Proses ini akan bekerja dengan cara memutar byte-byte pada 3 baris terakhir (baris 1, 2, dan 3) dengan jumlah perputaran yang berbeda-beda. Baris 1 akan diputar sebanyak 1 kali, baris 2 akan diputar sebanyak 2 kali, dan baris akan diputar sebanyak 3 kali. Sedangkan baris 0 tidak akan diputar.

5. MixColums

Proses MixColumns akan beroperasi pada tiap kolom dari tabel state. Operasi ini menggabungkan 4 bytes dari setiap kolom tabel state dan menggunakan transformasi linier Operasi Mix Columns memperlakukan setiap kolom sebagai polinomial 4 suku dalam Galois field dan kemudian dikalikan dengan c(x) modulo (x4+1), dimana c(x)=3x3+x2+x+2. Kebalikkan dari polinomial ini adalah c(x)=11x3+13x2+9x+14.

Operasi MixColumns juga dapat dipandang sebagai perkalian matrix.

Sebagai varian dari Square Cipher, Rijndael memiliki kemampuan untuk bekerja sangat baik pada platform apapun. Ditambah dengan operasi yang menggunakan table lookup dan operasi XOR membuat prosesnya menjadi tidak terlalu rumit.

2.12. Tolak Ukur Kata Sandi yang Kuat dan Lemah

Kata sandi yang kuat adalah kata sandi yang dirancang untuk sulit ditemukan oleh seseorang atau program. Karena tujuan kata sandi adalah untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses informasi, kata sandi yang mudah ditebak menjadi suatu risiko keamanan. Komponen penting dari kata sandi yang kuat mencakup panjang yang cukup dan campuran jenis karakter. Kata sandi yang lemah biasanya pendek dan hanya terdiri dari huruf kecil atau besar.

Ketika orang membuat kata sandi, seringkali menggunakan hal-hal yang mudah ditebak seperti bagian dari nama mereka, nama hewan peliharaan mereka, atau bahkan kata "kata sandi," itu sendiri, yang merupakan kata sandi yang paling umum digunakan selama bertahun-tahun. Kata sandi dapat dibuat lebih sulit untuk dipecahkan dengan menggunakan lebih banyak karakter, menggabungkan huruf besar dan kecil, dan termasuk angka dan karakter khusus. Menurut panduan keamanan dari Texas A&M University's Research Foundation, kata sandi enam karakter, satu kasus memiliki 308 juta kemungkinan kombinasi, yang semuanya dapat diakses oleh cracker kata sandi hanya dalam beberapa menit. Menggabungkan huruf besar dan kecil dan menggunakan delapan karakter meningkatkan kemungkinan kombinasi menjadi 53 triliun; mengganti angka dengan salah satu huruf menghasilkan 218 triliun kemungkinan; dan mengganti karakter khusus atau tanda baca dengan yang lain menghasilkan 6.095 triliun kemungkinan kombinasi.

2.13. Perbandingan Algoritma AES dan DES

Factors	DES	AES
Key Length	56 bits	128, 192 or 256 bits
Block Size	64 bits	128, 192, or 256 bits
Cipher Text	Symmetric block cipher	Symmetric block cipher
Developed	1977	2000
Security	Proven inadequate	Considered secure
Cryptanalysis Resisteance	Vulnerable to differential and linear cryptanalysis; weak substitution tables	Strong against differential, truncated differential, linear, interpolation and square attacks
Possible keys	2^{56}	2^{128},2^{192} and 2^{256}
Possible ASCII printable character key	95^{7}	95^{16}, 95^{24} or 95^{32}

Tabel 2. 1 Perbandingan Algoritma AES dan DES

Sumber : Analysis and Comparison between AES and DES Cryptographic Algorithm, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012

Kesimpulannya algoritma AES dibandingkan dengan DES, algoritma AES memiliki banyak variasi panjang kunci dan block yang lebih banyak sehingga dapat dicocokkan sesuai kebutuhan, selain itu sudah dibuktikan bahwa DES memiliki kinerja yang lebih buruk dalam hal keamanan dibandingkan AES, DES lebih rentan terhadap serangan dibandingkan AES.

3. ANALISIS SISTEM YANG BERJALAN

3.1. Gambaran Umum Objek Penelitian

Objek penelitian yang digunakan oleh penulis dalam penelitian ini adalah para individu yang tidak memiliki sistem secara independen layaknya perusahaan untuk mengamankan kata sandi dan dokumen serta data-data penting yang bersifat rentan terhadap seranga. Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi, sayang sekali masih banyak pihak yang kurang peka dan perhatian dalam masalah keamanan ini.

Saat ini dunia tengah berada dalam era informasi, pada era informasi keberadaan suatu informasi mempunyai arti dan peranan yang sangat penting bagi semua aspek kehidupan, serta merupakan salah satu kebutuhan hidup bagi semua orang baik individual maupun organisasi, sehingga dapat dikatakan bahwa dalam masyarakat informasi, informasi telah berfungsi sebagaimana layaknya aliran darah sumber kehidupan bagi

tubuh manusia. Salah satu temuan yang memberikan pengaruh paling besar dalam masyarakat informasi adalah ditemukannya internet. Hadirnya internet sebagai bentuk teknologi baru menyebabkan manusia tidak mampu terlepas dari arus komunikasi dan informasi. Internet telah menyebabkan terjadinya satu lompatan besar dalam kehidupan. Sama halnya dengan teknologi lainnya, internet tidak bebas nilai. Teknologi akan menjadi efektif jika kita memberi perhatian pada kegunaan dari teknologi yang disesuaikan dengan nilai-nilai sosial maupun pribadi serta adanya peraturan pemerintah yang melindungi masyarakat dari dampak negatif yang ditimbulkannya.

Berdasarkan berbagai kejadian pada beberapa tahun ke belakang, Indonesia merupakan negara yang lemah cyber-securitynya. Hal ini dapat diketahui dari maraknya berbagai kejadian, salah satunya adalah peretasan terhadap data kartu debit nasabah sebuah bank karena hacker berusaha menyusup ke sistem pengamanan kartu nasabah bank yang terjadi pertengahan Mei 2014 menjadikan catatan betapa buruknya cyber-security di Indonesia.

3.2. Analisis Sistem yang Berjalan/ Analisis Kesenjangan

Indonesia sebenarnya saat ini tengah dalam keadaan mendesak cyber-security atau keamanan dunia maya karena melihat kenyataan bahwa tingkat kejahatan di dunia maya atau cyber crime di Indonesia sudah mencapai tahap memprihatinkan. Namun berbeda dengan penangganan kejahatan lainnya, cyber-security membutuhkan pemikiran yang komprehensif untuk menangganinya.

3.3. Metodologi Penelitian

Pada penelitian ini penulis menggunakan teknik pengumpulan data dan analisis data kualitatif. Data yang dibutuhkan berupa sejumlah data-data rahasia yang bersifat nyata seperti username/ email dari kata sandi sejumlah akun yang sering digunakan pada umumnya.

1. Teknik Pengumpulan Data

Untuk mendukung keperluan penelitian ini, penulis memerlukan sejumlah data pendukung. Teknik pengumpulan data yang digunakan dalam penelitian ini adalah teknik kualitatif.

a. Data yang dibutuhkan oleh penulis

- Data primer

Data primer adalah data yang diperoleh langsung dari lapangan seperti dengan melalui metode observasi.

- Data sekunder

Data sekunder adalah dokumen-dokumen atau literatur-literatur dari buku, internet, jurnal, dan lain sebagainya. Pengumpulan data sekunder dilakukan dengan mengambil seluruh/ sebagian dari sekumpulan data yang telah dicatat atau dilaporkan.

b. Teknik pengumpulan data yang digunakan

- Studi Pustaka

Studi pustaka adalah jenis pengumpulan data yang meneliti berbagai macam dokumen yang berguna yang berhubungan dengan penelitian, studi pustaka yang dilakukan dalam penelitian ini adalah studi pustaka sekunder. Dimana studi pustaka sekunder adalah dokumen yang ditulis berdasarkan oleh laporan/ cerita orang lain seperti biografi dan jurnal serta buku-buku berisikan teori-teori yang menjadi landasan penelitian ini.

- Dokumentasi

Pada penelitian ini, penulis membutuhkan data berupa sampel-sampel data yang nyata yang digunakan oleh penulis yang nantinya akan disimpan di dalam database dengan metode kriptografi algoritma AES dan digunakan untuk proses testing dan autentikasi pada sistem.

1. Teknik Analisis Data

a. Metode Algoritma AES

Penulis akan menganalisis efektivitas sistem dan penggunaannya terhadap data yang ada, sehingga proses login dapat dibuat menjadi lebih efisien dan aman.

2. Teknik Pengukuran Data

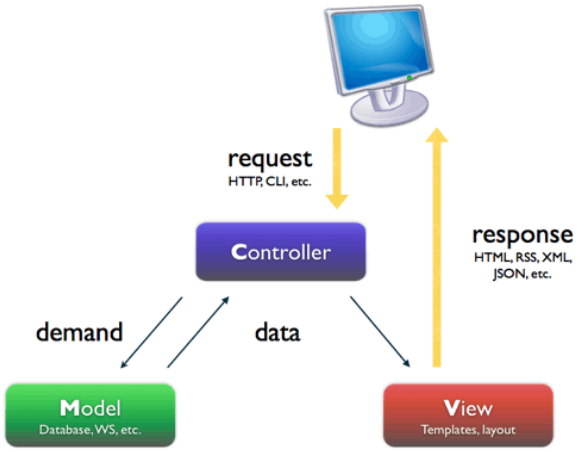
Teknik pengukuran data yang digunakan oleh penulis adalah berdasarkan parameter dari enkripsi AES atau yang lebih dikenal dengan Rijndael. Metode enkripsi ini menyimpan informasi menggunakan algoritma penyandian blok. Blok menyusun masukan teks biasa dan keluaran ciphertext (teks tersandikan), yang diukur dalam bit. Secara keseluruhan, AES terdiri dari tiga penyandian blok yaitu AES-128, AES-192 dan AES-256. Masing-masing penyandian AES mengenkripsi dan dekripsi data dalam blok 128 bit menggunakan kunci kriptografi untuk 128, 192 dan 256-bit, dengan 256-bit merupakan yang paling aman. Untuk kunci 128-bit, ada 10 putaran proses enkripsi, 12 putaran untuk kunci 192-bit dan 14 putaran untuk kunci 256-bit. Berikut ini adalah operasi Rijndael (AES)

1. Ekspansi kunci utama.
2. Pencampuran subkey.
3. Ulang dari i=1 sampai i=10 Transformasi : ByteSub (subtitusi per byte) ShiftRow (Pergeseren byte perbaris) MixColumn (Operasi perkalian GF(2) per kolom).
4. Pencampuran subkey (dengan XOR).
5. Transformasi : ByteSub dan ShiftRow.
6. Pencampuran subkey.

Teknik pengukuran data yang digunakan penulis dalam sistem ini adalah 256-bit. Penulis menggunakan kriptografi aes dengan panjang kunci 256-bit karena semakin panjang kunci enkripsi, semakin sulit untuk membukanya, selain itu AES256 sudah dianggap sangat aman dan secara teoritis tahan terhadap serangan paksa komputer quantum.

4. PERANCANGAN SISTEM YANG DIUSULKAN

4.1. Arsitektur Sistem

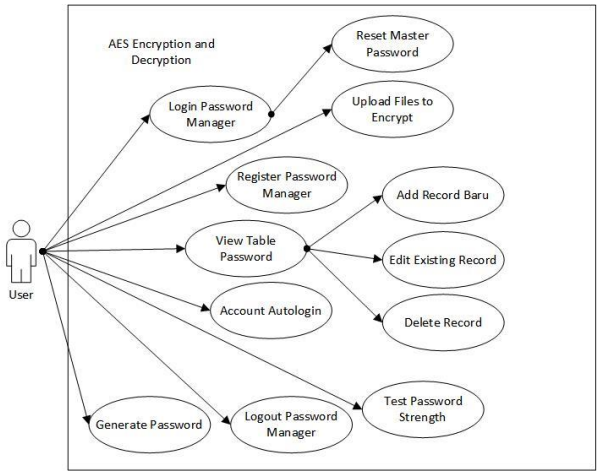


Gambar 4. 1 Arsitektur Sistem

Sumber : Olahan Penulis

Gambar 4.1 di atas, menunjukkan arsitektur sistem yang diajukan penulis dalam penelitian ini. Penulis menggunakan prinsip MVC dari CodeIgniter berbasis PHP dan HTML yang terdiri dari Model, View, dan Controller. Dimulai dari Model yang akan mengambil data yang disimpan di dalam database MySQL, lalu data tersebut dioper ke Controller yang kemudian akan ditampilkan di Web Browser sesuai pengaturan pada View.

4.2. Use Case Diagram

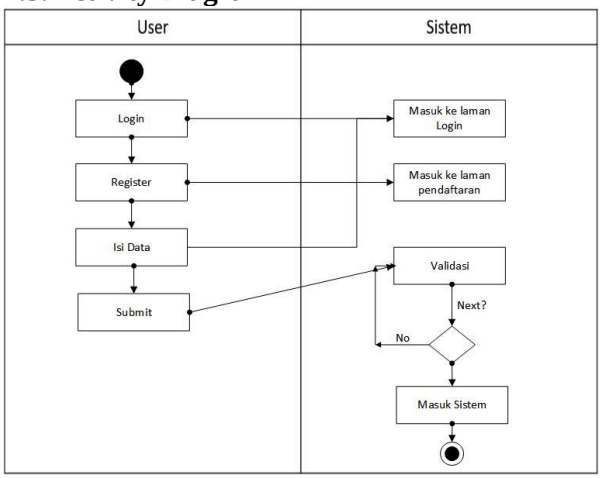


Gambar 4. 2 Use Case Diagram

Sumber : Olahan Penulis

Gambar 4.2 di atas merupakan pemodelan untuk menggambarkan sistem yang diusulkan. Bagaimana sistem berjalan dari awal hingga akhir dan terdapat fungsi -fungsi apa saja dalam sistem aplikasi yang diusulkan.

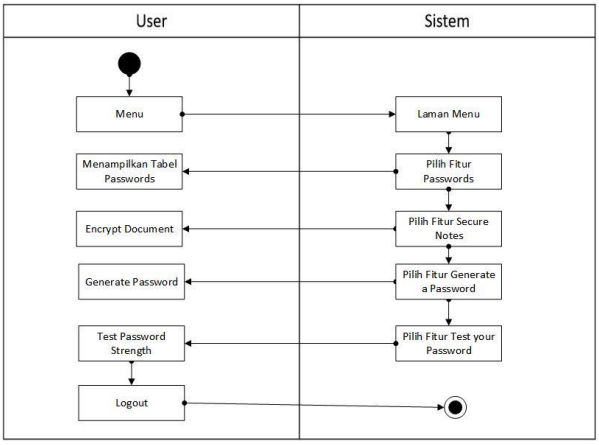
4.3. Activity Diagram



Gambar 4. 3 Activity Diagram Login dan Register

Sumber : Olahan Penulis

Berdasarkan Gambar 4.3 di atas, user memulai dengan masuk ke dalam sistem yaitu dengan login dan registrasi. Tahapannya dari user mulai akses ke laman login dan register sistem, mengisi data di antaranya username, email, dan master password, lalu data-data tersebut akan melalui proses validasi. Bila proses validasi berhasil maka user akan berhasil masuk ke dalam sistem

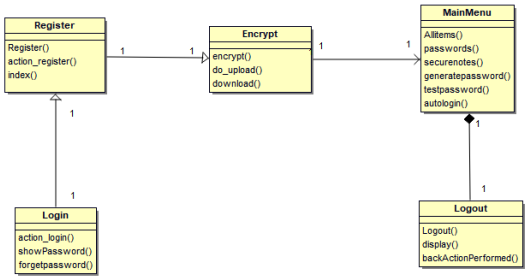


Gambar 4. 4 Activity Diagram Fitur Menu

Sumber : Olahan Penulis

Berdasarkan Gambar 4.4 di atas, user dapat menggunakan fitur-fitur yang terdapat dalam menu sistem di antaranya untuk insert, update, dan delete data kata sandi yang tersimpan, mengenkripsi dokumen penting, generate password, dan test password strength.

4.4. Class Diagram

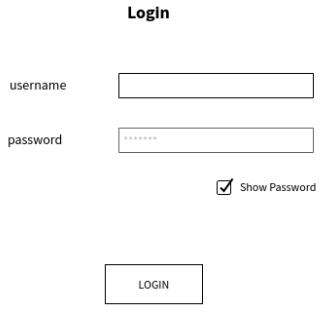


Gambar 4. 5 Class Diagram

Sumber : Olahan Penulis

Berdasarkan Gambar 4.5 di atas, merupakan class diagram dari sistem yang diusulkan oleh penulis.

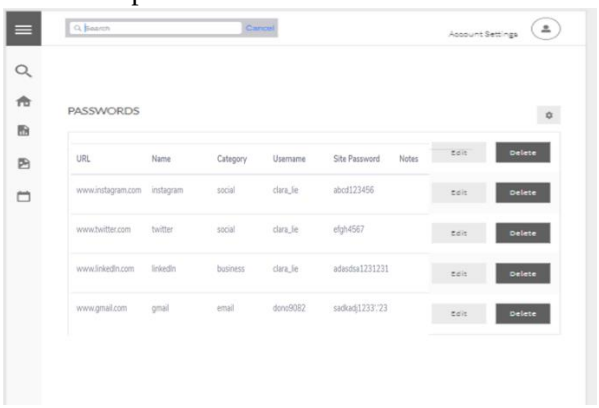
4.5. Rancangan Tampilan Antar Muka



Gambar 4. 6 Rancangan Tampilan Antar Muka Laman Login

Sumber : Olahan Penulis

Gambar 4.6 di atas merupakan rancangan tampilan antar muka dari laman Login, dimana di dalamnya pengguna dapat memasukkan username dan password yang dimilikinya untuk dapat masuk ke dalam aplikasi.



Gambar 4. 7 Rancangan Tampilan Antar Muka Main Menu

Sumber : Olahan Penulis

Gambar 4.7 di atas merupakan rancangan tampilan antar muka dari laman menu password manager.

4.6. Rancangan Alur Program

Dalam membuat dan mengembangkan sebuah aplikasi tentunya perlu membuat rancangan alur program agar aplikasi dapat berjalan dengan baik. Berikut adalah rancangan alur program yang dibuat penulis

1. Login

Start

Input username, input password
Database connect

If input username = database username AND input master password = database master password Then

Login = true
Redirect to main menu

Else Then

Login = false
Display Error Message

End If

End

2. Register

Start

Input email, username, input password
Database connect

If input username != database username AND input email != database email Then

Register = true
Redirect to login

Else Then

Register = false
Display Error Message

End If

End

3. Forget Password

Start
Click forget your password
Input Email Address
If Input Email Address = Registered Email Then
Reset Password Email Sent
End If
Click Link Reset Password
Input New Password
If New Password Format = Regex Then
Password Changed = True
End If
End

4. Main Menu

Start
Select Passwords
Display Table Passwords
Insert | Update | Delete Data
Select Secure Notes
Select Document to encrypt
Document.encrypt = True
Select Document to decrypt
Document.decrypt = True
Select Generate a Password
Determine Password Length
Click Generate
echo $RandomPasswordString
Select Test your Password
Insert Password
Validate
Password = "weak | medium | strong"
End

5. Logout

Start
Click Back Button
Go To Login Form
Hide this Form
End

4.7. Implementasi Sistem

1. Spesifikasi Perangkat Keras

Dalam pengembangan dan uji coba aplikasi yang penulis rancang ini, penulis menggunakan perangkat dengan spesifikasi sebagai berikut

Nama Perangkat : HP Pavilion Notebook
Processor : Intel® Core™ i5-6200U CPU @2.30 GHz 2.40 GHz
Installed RAM : 4 GB
Storage Capacity : 1T
System Type : 64-bit operating system, x64-based processor
Operating System : Windows 10

2. Panduan Instalasi

Pada dasarnya, project yang terbentuk pada java akan membentuk sebuah package yang terdiri dari library, modules, class, dan form yang dapat penulis manfaatkan dalam mengembangkan aplikasi. Selain itu penulis juga menggunakan MySQL sebagai sistem basis datanya yang berfungsi untuk menampung data-data yang diperlukan.

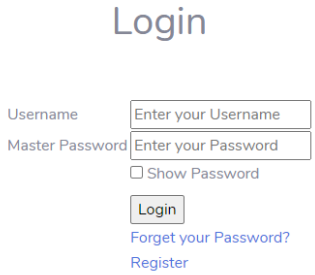
Berikut cara-cara dalam menginstalasi XAMPP untuk menjalankan MySQL :

- Buka website Apache Friends, kemudian download installer XAMPP sesuai dengan sistem operasi yang dimiliki
- Setelah selesai didownload, lakukan instalasi XAMPP, dengan cara klik kanan pada file instalasi kemudian pilih Open.
- Selanjutnya akan tampil pilihan aplikasi apa yang akan dapat diinstal, centanglah MySQL dan phpMyAdmin.
- Selanjutnya, pilih folder dimana file instalasi disimpan.
- Seperti prosedur instalasi pada umumnya, selesaikan instalasi XAMPP
- Untuk menjalankannya, jalankan control panel dan nyalakan Apache dan MySQL.

Selanjutnya, cara-cara dalam menginstalasi Framework CodeIgniter :

- Buka halaman download berikut ini https://codeigniter.com/en/download
- Download
- Buka file ZIP dan extract di folder root xampp yaitu htdocs.
- Konfigurasi config dan database sesuai project

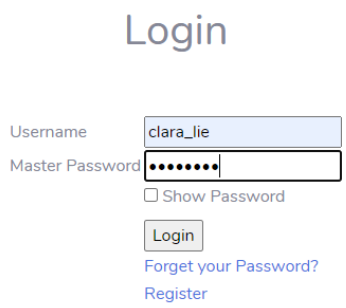
3. Panduan Penggunaan



Gambar 4. 8 Tampilan Awal Login

Sumber : Olahan Penulis

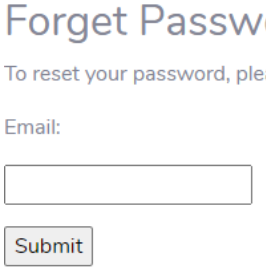
Pada Gambar 4.8 di atas, menunjukkan tampilan yang terlihat ketika awal aplikasi di buka dan merupakan tampilan awal dari laman login.



Gambar 4. 9 Tampilan Pengisian Laman Login

Sumber : Olahan Penulis

Pada Gambar 4.9 di atas, menunjukkan tampilan yang terlihat ketika pengguna mengisi laman login.



Gambar 4. 10 Tampilan Laman Forget Password

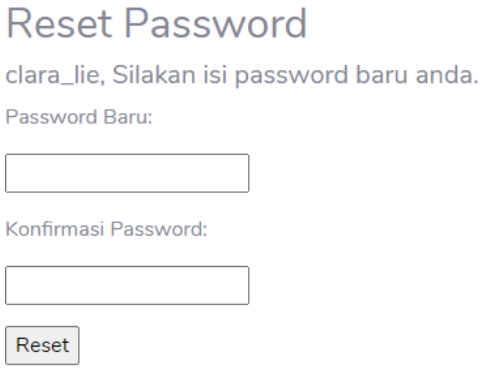
Sumber : Olahan Penulis

Pada Gambar 4.10 di atas, menunjukkan tampilan yang terlihat ketika pengguna menekan pilihan Forget your Password? Pada laman Login.

Gambar 4. 11 Tampilan Laman Send Email Reset Password

Sumber : Olahan Penulis

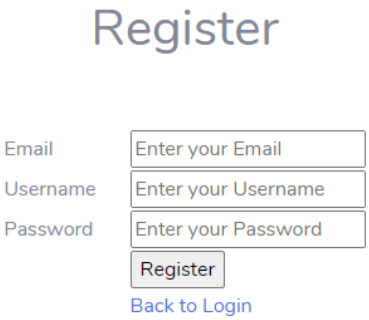
Pada Gambar 4.11 di atas, menunjukkan tampilan yang terlihat ketika email berhasil dikirimkan sesuai dengan email yang terdaftar dan dimasukkan user.



Gambar 4. 12 Tampilan Laman Input New Password

Sumber : Olahan Penulis

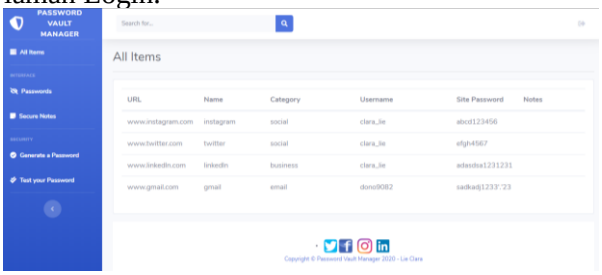
Pada Gambar 4.12 di atas, menunjukkan tampilan yang terlihat ketika pengguna menekan link yang dikirimkan melalui email.



Gambar 4. 13 Tampilan Laman Register

Sumber : Olahan Penulis

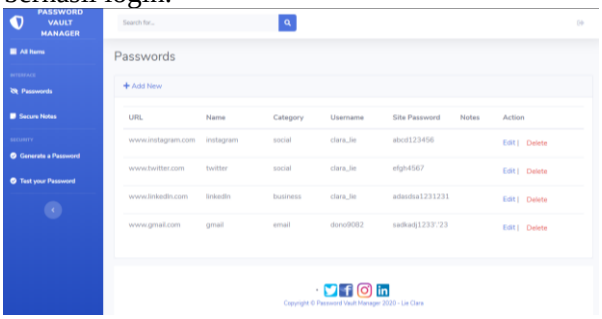
Pada Gambar 4.13 di atas, menunjukkan tampilan yang terlihat ketika pengguna membuka laman register dengan memilih pilihan Register pada laman Login.



Gambar 4. 14 Tampilan Laman Menu Utama

Sumber : Olahan Penulis

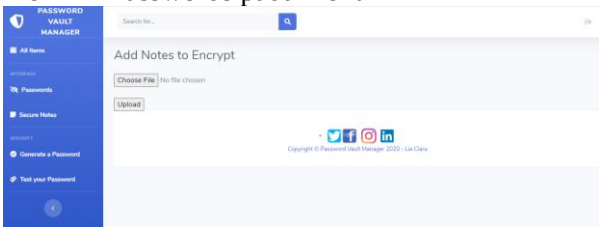
Pada Gambar 4.14 di atas, menunjukkan tampilan menu utama yang terlihat setelah pengguna berhasil login.



Gambar 4. 15 Tampilan Laman Menu Utama Passwords

Sumber : Olahan Penulis

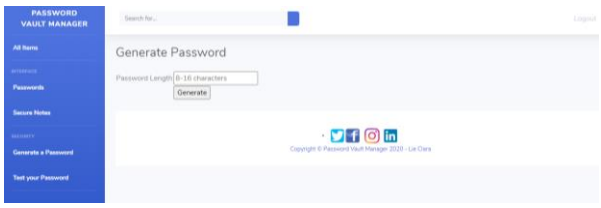
Pada Gambar 4.15 di atas, menunjukkan tampilan menu utama yang terlihat setelah pengguna memilih Passwords pada menu



Gambar 4. 16 Tampilan Laman Menu Utama Secure Notes

Sumber : Olahan Penulis

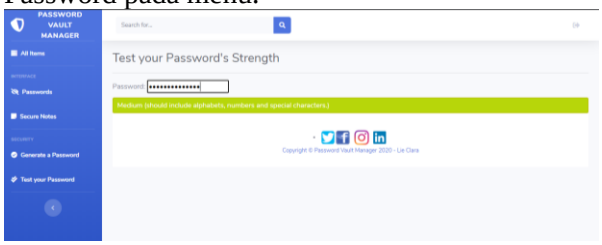
Pada Gambar 4.16 di atas, menunjukkan tampilan yang terlihat Ketika pengguna memilih Secure Notes pada menu.



Gambar 4. 17 Tampilan Laman Menu Utama Generate a Password

Sumber : Olahan Penulis

Pada Gambar 4.17 di atas, menunjukkan tampilan yang terlihat Ketika pengguna memilih Generate a Password pada menu.



Gambar 4. 18 Tampilan Laman Menu Utama Test your Password

Sumber : Olahan Penulis

Pada Gambar 4.18 di atas, menunjukkan tampilan yang terlihat Ketika pengguna memilih Test your Password pada menu.

5. SIMPULAN DAN SARAN

5.1. Simpulan

Berdasarkan hasil penelitian yang telah dilakukan penulis mengenai Pengamanan Data Sistem Login dengan password manager berbasis PHP dan HTML dengan memanfaatkan framework CodeIgniter dengan menerapkan metode Algoritma AES, maka dapat disimpulkan sebagai berikut :

1. Dengan menerapkan sistem ini, pengguna dapat lebih sadar betapa pentingnya keamanan data dan membuat pengguna untuk semakin berhati-hati dalam penyimpanan kata sandi dan data penting.
2. Kata sandi yang digunakan pengguna cenderung bersifat lemah dan rentan terhadap serangan. Untuk itu dengan menggunakan sistem ini dapat menjadi tolak ukur pengguna atau pemilik akun untuk mengetahui seberapa kuat atau lemah kata sandi yang dimilikinya.
3. Mencegah penggunaan kata sandi yang memiliki unsur yang sama dengan kata sandi yang pernah digunakan sebelumnya. Karena dengan password manager ini dapat menyimpan kata sandi dengan jumlah banyak, sehingga dengan menggunakan kata sandi yang berbeda-beda pun pengguna tidak perlu takut akan melupakan kata sandi tersebut.
4. Sistem ini membuat penyimpanan dan penggunaan kata sandi menjadi lebih efektif, efisien dan aman
5. Ancaman kebocoran data dapat ditekan seminim mungkin dengan menggunakan kriptografi dalam sistem keamanannya sehingga untuk memperoleh data asli, seseorang harus memiliki kunci dan akses ke dalam aplikasi untuk dapat melakukan enkripsi maupun dekripsi. Dengan begitu dapat menekan kemungkinan data perusahaan untuk dicuri dan disalahgunakan oleh pihak lain.

5.2. Saran

Berdasarkan simpulan yang telah diuraikan di atas, serta mengingat masalah keamanan dalam sistem login sering dianggap hal yang sepele dan masih banyak pihak yang belum menyadari betapa pentingnya pengamanan data dalam sistem login, maka hal-hal yang dapat disarankan adalah sebagai berikut :

1. Diharapkan penelitian ini dapat bermanfaat dan dapat dijadikan sebagai bahan pembelajaran. Sistem ini sudah dapat diterapkan khususnya untuk penggunaan setiap individu untuk menyimpan masing-masing password yang dimilikinya, namun agar sistem ini dapat bekerja lebih optimal, dapat terus dikembangkan lebih lanjut baik dari segi fungsionalitas maupun fitur-fiturnya.
2. Bagi peneliti selanjutnya, diharapkan dapat lebih mengembangkan penelitian ini dengan aspek yang lebih banyak dan lebih beragam.

6. DAFTAR PUSTAKA

[1] Dan Boneh, Victor Shoup (2017), A Graduate Course in Applied Cryptography.

[2] Eka Adhitya Dharmawan, Erni Yudaningtyas, M. Sarosa. (2013), Perlindungan Web pada Login Sistem Menggunakan Algoritma Rijndael. Jurnal EECCIS, Volume 7

[3] Hutahaean, J. (2014), Konsep Sistem Informasi, Yogyakarta: CV Budi Utama.

[4] Kenneth J. Laudon, Jane P. Laudon. (2014), Management Information Systems 13th edition. New Jersey: Pearson

[5] Mulyadi (2016), Sistem Informasi Akuntansi, Jakarta: Salemba Empat.

[6] Patrick Grässle, Henriette Baumann, Philippe Baumann (2005), UML 2.0 in Action. Birmingham: Packt Publishing Ltd

[7] R. Kelly Rainer, Casey G. Cegielski (2015), Introduction to Information System. Vancouver: Langara College

[8] R. Kelly Rainer, Brad Prince (2016), Introduction to Information System 6th edition. New Jersey: Wiley.

[9] Romney, Marshall B. dan Steinbart (2015), Sistem Informasi Akuntansi, Edisi 13. Jakarta : Salemba Empat.

[10] Rosa AS dan M. Shalahuddin (2015), Rekayasa Perangkat Lunak Terstruktur Dan Berorientasi Objek. Bandung : Informatika.

[11] Shraddha Soni, Himani Agrawal, Monisha Sharma. (2012), Analysis and Comparison between AES and DES Cryptographic Algorithm. International Journal of Engineering and Innovative Technology (IJEIT)

[12] Surian, Didi. (2006), Algoritma Kriptografi AES Rijndael. Universitas Tarumanagara, Jakarta

[13] Whitman, Michael E., and Herbert J. Mattord (2011), Principles of Information Security. Independence 4th Edition. KY: Cengage.

[14] Widiasari, R.I. (2012), Combining Advanced Encryption Standard (AES) and One Time Pad (OTP) Encryption for Data Security. International Journal of Computer Applications, Volume 57.

[15] Yakub dan Hisbanarto, Vico (2014), Sistem Informasi Manajemen Pendidikan. Yogyakarta: Graha Ilmu