UNIVERSITAS BUDI LUHUR

SENAFTI
SEMINAR NASIONAL MAHASISWA FAKULTAS TEKNOLOGI INFORMASI
VOL. 1 NO. 1 SEPTEMBER 2022
E-ISSN: 2962-8628

PROSIDING

SEMINAR NASIONAL MAHASISWA FAKULTAS TEKNOLOGI INFORMASI (SENAFTI)

PERANAN ARTIFICIAL INTELLIGENCE
YANG CERDAS BERBUDI LUHUR
DALAM MENGHADAPI ERA SOCIETY 5.0

CYBER SECURITY

Supported by :
Ngampooz

STEERING COMMITE

Pelindung
Dr. Ir. Wendi Usino, M.Sc., M.M

Penanggung Jawab
Dr. Ir. Deni Mahdiana, S.Kom, M.M., M.Kom

Ketua Pelaksana
Dr. Rusdah, M.Kom

Sekretaris
Retno Wulandari, S.Kom., M.Kom.

Bendahara
Noni Juliasari, S.Kom., M.Kom.

Acara
Ratna Ujian Dari, S.Kom., M.M., M.Kom.

Pengelola Makalah dan Mitra Bestari
1. Atik Ariesta, S.Kom., M.Kom.
2. Samsinar, S.Kom., M.Kom.

Pengelola Editor dan Jurnal
1. Indah Puspasari Handayani, S.Kom., M.Kom.
2. Devit Setiono, S.Kom., M.Kom.
3. Anwar Rifa'i, S.Pd, M.Pd.
4. Reva Ragam Santika, S.Kom., M.Kom.
5. Kukuh Harsanto, S.Kom., M.Kom

Pengelola Teknologi Informasi
1. Sovan Dianarto, S.Kom.
2. Dolly Virgian Shaka Yudha Shakti, S.Kom., M.Kom.

Pengelola Undangan dan Desain
Wasiran

REDAKSI

MITRA BESTARI

1. Dr. Ir. Achmad Solichin, S.Kom., M.T.I (Universitas Budi Luhur)
2. Anita Ratnasari, S.Kom, M.Kom (Universitas Mercu Buana)
3. Prof. Dr. Anton Satria Prabuwono, ST., SSi., M.M (Universitas Budi Luhur)
4. Dr. Ir. Arief Wibowo, S.Kom., M.Kom (Universitas Budi Luhur)
5. Arif Bramantoro, Ph.D (Universitas Budi Luhur)
6. Bima Cahya Putra, S.Kom., M.Kom. (Universitas Budi Luhur)
7. Prof. Ir. Dana Indra Sensuse, Ph.D (Universitas Indonesia)
8. Denni Kurniawan, S.T., M.T.I., Ph.D (Universitas Budi Luhur)
9. Dian Anubhakti, S.Kom., M.Kom. (Universitas Budi Luhur)
10. Dolly Virgian Shaka Yudha Sakti, S.Kom., M.Kom. (Universitas Budi Luhur)
11. Dwi Pebrianti, S.T., M.Eng., Ph.D (Universiti Budi Luhur)
12. Dr. Emy Setyaningsih, S.Si., M.Kom (Institut Sains dan Teknologi AKPRIND Yogyakarta)
13. Dr. Gandung Triyono, M.Kom (Universitas Budi Luhur)
14. Dr. Ir. Goenawan Brotosaputro, S.Kom., M.Sc (Universitas Budi Luhur)
15. Grace Gata, S.Kom., M.Kom. (Universitas Budi Luhur)
16. Dr. Ir. Hari Soetanto, S.Kom., M.Sc (Universitas Budi Luhur)
17. Hendra Cipta, M.Si (Universitas Islam Negeri Sumatera Utara Medan)
18. Hendri Irawan, S.Kom., M.T.I. (Universitas Budi Luhur)
19. Dr. Imelda, M.Kom (Universitas Budi Luhur)
20. Indra Nugraha Abdullah, Ph.D (Universitas Budi Luhur)
21. Dr. Indra, S.Kom., M.T.I (Universitas Budi Luhur)
22. Ita Novita, S.Kom., M.T.I. (Universitas Budi Luhur)
23. Dr. Ir. Iwan Setiawan, MT, MCSA, CRM. (Universitas Nusa Putra)
24. Dr. Ir. Jan Everhard Riwurohi, M.T (Universitas Budi Luhur)
25. Kelik Sussolaikah, S.Kom., M.Kom (Universitas PGRI Madiun)
26. Dr. Krisna Adiyarta M, S.Kom., M.Sc (Universitas Budi Luhur)
27. Luhur Bayuaji, S.T., M.Eng., Ph.D (Universiti Malaysia Pahang)
28. Dr. Ir. Mardi Hardjianto, M.Kom (Universitas Budi Luhur)
29. Mayanda Mega Santoni, S.Komp., M.Kom. (Universitas Pembangunan Nasional Veteran Jakarta)
30. Prof. Dr. Moedjiono, M.Sc (Universitas Budi Luhur)
31. Dr. Mohammad Syafrullah, M.Kom., M.Sc (Universitas Budi Luhur)
32. Dr. Ir. Nazori A. Z., M.T (Universitas Budi Luhur)
33. Noni Juliasari, S.Kom., M.Kom. (Universitas Budi Luhur)
34. Rizky Pradana, S.Kom., M.Kom. (Universitas Budi Luhur)
35. Rohmat Indra Borman, M.Kom. (Universitas Teknokrat Indonesia)
36. Safitri Juanita, S.Kom., M.T.I. (Universitas Budi Luhur)
37. Dr. Samidi, S.Kom., M.M., M.Kom (Universitas Budi Luhur)
38. Setyawan Widyarto, M.Sc., Ph.D (Universiti Selangor, Malaysia)
39. Dr. Sofian Lusa, S.E., M.Kom (Universitas Budi Luhur)
40. Dr. Tenia Wahyuningrum, S.Kom., M.T (Institut Teknologi Telkom Purwokerto)
41. Titin Fatimah, S.Kom., M.Kom. (Universitas Budi Luhur)
42. Dr. Ir. Utomo Budiyanto, M.Kom., M.Sc (Universitas Budi Luhur)
43. Windarto, S.Kom., M.Kom. (Universitas Budi Luhur)
44. Dr. Yan Rianto, M.Eng (Badan Riset dan Inovasi Nasional/BRIN)

KATA PENGANTAR

Dengan memanjatkan puji syukur kehadirat Allah SWT dan hanya karena rahmat dan karunia-Nya, Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) 2022 telah terselesaikan dengan baik. Prosiding seminar ini merupakan kumpulan makalah hasil penelitian para akademisi dan peneliti yang sebelumnya telah dipresentasikan pada SENAFTI tahun 2022 yang dilaksanakan secara daring (online) pada tanggal 6 September 2022. Tema SENAFTI Tahun 2022 adalah "Peranan Artificial Intelligence yang Cerdas Berbudi Luhur Dalam Menghadapi Era Society 5.0"

Penyusunan prosiding ini dimaksudkan untuk penyebarluasan hasil-hasil penelitian dan kajian dalam bidang teknologi informasi. Selain itu, penyusunan prosiding ini juga dimaksudkan agar masyarakat luas dapat mengetahui berbagai informasi terkait dengan penyelenggaraan SENAFTI. Penyusunan prosiding ini dibagi menjadi 4 (empat) buku yaitu:

1. Buku 1 - Cyber Security
2. Buku 2 – Artificial Intelligence
3. Buku 3 – Programming
4. Buku 4 – Information System

Pada kesempatan ini kami menyampaikan terima kasih yang sebesar-besarnya kepada para akademisi dan peneliti atas hasil karya dan sumbangan pemikiran yang dipresentasikan dalam bentuk makalah dan presentasi ilmiah. Juga kami sampaikan terima kasih kepada para mitra bestari yang telah mereview semua makalah sehingga kualitas isi dari makalah dapat terjaga dan dipertanggungjawabkan. Tak lupa kepada semua pihak yang telah memberikan dukungan bagi terselenggaranya SENAFTI dan atas tersusunnya prosiding ini. Harapan kita bersama, semoga prosiding ini dapat menambah khasanah pengembangan ilmu pengetahuan dan teknologi informasi di Indonesia.

Jakarta, September 2022

Tim Penyusun

DAFTAR ISI

Aplikasi Pengamanan Dokumen Menggunakan Metode Rivest Code 4 (RC4) Berbasis Web Pada Yayasan Berkembang Mandiri Indonesia
Muhammad Farhansyah, Utomo Budiyanto 319-326

UNIVERSITAS BUDI LUHUR

SENAFTI SEMINAR NASIONAL MAHASISWA FAKULTAS TEKNOLOGI INFORMASI

SERTIFIKAT

F/UBL/FTI/000/044/09/22

Diberikan kepada

Dolly Virgian Shaka Yudha Sakti

Atas partisipasinya sebagai

PEMAKALAH

SEMINAR NASIONAL MAHASISWA FAKULTAS TEKNOLOGI INFORMASI
PERANAN ARTIFICIAL INTELLIGENCE YANG CERDAS BERBUDI LUHUR DALAM MENGHADAPI ERA SOCIETY 5.0

Diselenggarakan oleh Fakultas Teknologi Informasi Universitas Budi Luhur
Jakarta, 06 September 2022

Dekan Fakultas Teknologi Informasi

Dr. Ir. Deni Mahdiana, S.Kom., M.M., M.Kom.

Ketua Panitia

Dr. Rusdah, M.Kom.

PENERAPAN ALGORITMA AES128 DAN RC4 UNTUK PENGAMANAN DATABASE DAN *FILE* PADA PT. MAYAKSA MUGI MULIA

Mila Rismaya[1*], Dolly Virgian Shaka Yudha Sakti[2]

[1,2]Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia

Email: [1*]milarsmaya@gmail.com, [2*]dolly.virgianshaka@budiluhur.ac.id
(* : corresponding author)

Abstrak-PT. Mayaksa Mugi Mulia merupakan Perusahaan Swasta Nasional yang berfokus pada bidang perencanaan dan implementasi serta penyediaan Sistem Teknologi Informasi. Perusahaan ini memiliki data penting seperti manajemen data karyawan, data perusahaan, data keuangan beserta *file* yang masih disimpan secara manual dan berbentuk fisik, namun jika data dan informasi tersebut disimpan tanpa pengamanan yang baik, maka data dan informasi akan rentan terhadap pencurian atau pengubahan data oleh orang yang ingin mencuri atau mengubah data tersebut. Maka dibutuhkan aplikasi untuk pengamanan data berbasis Web dengan menggunakan teknik kriptografi. Pada aplikasi kriptografi ini bisa melakukan proses enkripsi dan proses dekripsi yang dapat mengamankan isi pada *file* berbentuk word,pdf, ppt dan excel, *file* yang telah melalui proses enkrip dan dekrip akan terjamin keutuhannya, dan tidak akan mengalami kerusakan dan perubahan pada isi *file*. Aplikasi kriptografi ini juga dapat mengamankan data isi *record* pada *file*. Pada penelitian ini dirancang dengan sebuah sistem Aplikasi Kriptografi berbasis Web dengan menarapkan Metode *Algoritma Advanced Encryption Standard* (AES 128) dan *Rivest Code* (RC4). Tujuan menggunakan kombinasi antara kedua algoritma ini diharapkan dapat melindungi data berupa *file* dan *file* perusahaan dengan keamanan yang tinggi, waktu yang cepat dan efisien, sehingga tidak perlu khawatir atas kebocoran data maupun pencurian data oleh pihak yang tidak berwenang.

Kata Kunci: kriptografi, RC4, AES 128, *file*

APPLICATION OF AES128 AND RC4 ALGORITHMS FOR SECURING FILES AND FILES ON PT. MAYAKSA MUGI MULIA

Abstract-*PT. Mayaksa Mugi Mulia is a National Private Company that focuses on the field of planning and implementation as well as the provision of Information Technology Systems. This company has important data such as employee data management, company data, financial data along with files that are still stored manually and in physical form, but if the data and information are stored without good security, then the data and information will be vulnerable to theft or alteration of data by people who want to steal or change the data. Then an application is needed for web-based data security using cryptographic techniques. In this cryptographic application, it can carry out an encryption process and decryption process that can secure the contents of files in the form of word, pdf, ppt and excel, files that have gone through the encryption and decryption process will be guaranteed their integrity, and will not experience damage and changes to the contents of the file. This cryptographic application can also secure the contents of the record data on the file. This study was designed with a Web-based Cryptographic Application system with the advanced encryption standard algorithm method (AES 128) and Rivest Code (RC4). The purpose of using a combination of these two algorithms is expected to be able to protect data in the form of files and company files with high security, fast and efficient time, so there is no need to worry about data leakage or data theft by unauthorized parties*.

Keywords*: cryptography, RC4, AES 128, file*

1. PENDAHULUAN

Pesatnya perkembangan teknologi informasi dan telekomunikasi saat ini dapat memudahkan manusia untuk melakukan aktifitas dalam bertukar informasi [1]. Keamanan informasi merupakan hal yang sangat penting [2]. Sangat pentingnya sebuah data menjadikan data hanya boleh diakses oleh orang-orang yang dipercaya saja [3]. Pencurian data merupakan salah satu dampak negatif dari perkembangan teknologi [4]. Data yang bersifat rahasia menjadi rentan untuk dicuri ataupun diakses oleh orang-orang yang tidak bertanggung jawab [5]. Untuk itu keamanan penyimpanan data yang digunakan haruslah terjamin keamanannya [6].

PT. Mayakasa Mugi Mulia memiliki data penting seperti manajemen data karyawan, data perusahaan, data keuangan beserta *file*. Penanganan sebelumnya pada PT. Mayaksa Mugi Mulia melakukan perlindungan *file* dan *file* tersebut dengan menggunakan cara manual dan berbentuk fisik, namun jika data dan informasi tersebut

disimpan tanpa pengamanan yang baik, maka data dan informasi tersebut akan rentan terhadap pencurian atau pengubahan data oleh orang yang ingin mencuri atau mengubah data tersebut [7].

Berdasarkan latar belakang pada masalah yang terjadi pada PT. Mayaksa Mugi Mulia, salah satu cara guna mengamankan data pada perusahaan, yaitu dibutuhkan aplikasi keamanan data berbasis Web dengan menggunakan teknik kriptografi. Kriptografi merupakan keahlian atau ilmu dalam penyandian atau pengamanan sebuah data atau informasi yang bersifat *privacy* [8]. Kriptografi merupakan seni untuk mengamankan data yang didalamnya terdapat algoritma tertentu yang bertujuan sebagai pengacakan, dengan cara mengubah teks asli (*plaintext*) menjadi teks yang tidak bisia dibaca (*ciphertext*) [8].

Pada penelitian ini dirancang dengan sebuah sistem Aplikasi Kriptografi berbasis Web menggunakan Metode Algoritma *Advanced Encryption Standard* (AES 128) dan *Rivest Code* (RC4). Berdasarkan penelitian sebelumnya yang dilakukan oleh[9] membahas, AES dikenal sebagai algoritma yang memiliki kelebihan yakni, kemampuan dengan tingkat keamananan yang cukup tinggi, dilihat dari segi kunci yang simetri maka kecepatan operasi lebih tinggi dibandingkan dengan algoritma asimetri, dan karena pada algoritma AES memiliki panjang kunci, yang paling sedikitnya sebesar 128 bit, maka algoritma AES akan tahan terhadap serangan *exhaustive key search* dengan teknologi saat ini, dan membutuhkan waktu selama 10^{10} tahun untuk mencoba seluruh kemungkinan kunci [9]

Sedangkan menurut penelitian sebelumnya yang dilakukan oleh[10] membahas, Algoritma Kriptografi *Rivest Code* 4 termasuk algoritma simetris, algoritma RC4 merupakan algoritma *stream cipher* dimana proses penyandiannya mengarah pada satu bit data, sehingga proses enkripsi dan dekripsi membutuhkan waktu yang singkat dan Algoritma RC4 juga memiliki tingkat efisiensi yang baik dalam menyimpan data.

Berdasarkan dari penelitian sebelumnya maka pada penelitian saat ini menggunakan kombinasi antara Algoritma *Advanced Encryption Standard* (AES 128) dan *Rivest Code* (RC4), diharapkan dapat melindungi data berupa *file* dan *file* perusahaan dengan keamanan yang tinggi, waktu yang cepat dan efisien, sehingga tidak perlu khawatir atas kebocoran data, maupun pencurian data penting pada perusahaan oleh pihak yang tidak memiliki wewenang, dan penelitian ini diharapkan dapat menjadi referensi bagi peneliti selanjutnya dalam penerapan Algoritma AES 128 dan RC4.

2. METODE PENELITIAN

2.1 Pengumpulan Data

Pada tahap pengumpulan data yang dilakukan pada penelitian ini yakni dengan melakukan wawancara dan observasi, dengan tujuan agar dapat berkomunikasi dengan pihak yang berhubungan dan mendapatkan informasi mengenai sistem aplikasi yang akan dibuat.

2.2 Penerapan Metode Kriptografi

a. Metode Algoritma *Advanced Encryption Standard* (AES 128)

Algoritma kriptografi AES 128 merupakan algoritma *block cipher* dengan menggunakan sistem permutasi dan subtitusi. Algoritma AES ini memiliki panjang kunci sebanyak 128 yang menggunakan 10 *round.*
Berikut ini merupakan tahapan Enkripsi pada algoritma AES 128 [11]:

1. AddRound*Key*, yaitu prose melakukan XOR antara awal *plaintext* dengan *cipher key*. Tahap ini disebut *initial round*
2. Round, yaitu putaran sebanyak Nr-1 kali. Proses yang ada dalam round, diantaranya adalah :
   a. *SubBytes*, yaitu subtitusi *byte* menggunakan tabel subtitusi *(S-Box).*
   b. *ShiftRows*, yaitu pergeseran baris-baris *array state* secara *wrapping*.
   c. *MixColumns*, yaitu mengacak data di masing-masing kolom *array state*.
   d. *AddRoundKey*, yaitu melakukan XOR antara *state* sekarang dengan *round key*.
3. Final round, yaitu proses untuk putaran terakhir:
   a. *SubBytes*
   b. *ShifRows*
   c. *Add RoundKey*

Berikut ini merupakan tahapan dekripsi pada algoritma AES 128 [11]:

1. *AddRoundKey*, yaitu proses melakukan XOR antara awal plaintext dengan *cipher key*. Tahap ini disebut *initial round*
2. Round, yaitu putaran sebanyak Nr-1 kali. Proses yang ada dalam round, diantaranya adalah :
   a. *SubBytes*, yaitu subtitusi *byte* menggunakan tabel subtitusi *(S-Box).*
   b. *ShiftRows*, yaitu pergeseran baris-baris *array state* secara *wrapping*.
   c. *MixColumns*, yaitu mengacak data di masing-masing kolom *array state.*

d. *AddRoundKey*, yaitu melakukan XOR antara state sekarang dengan *round key*.

3. *Final round*, yaitu proses untuk putaran terakhir:
   a. *SubBytes*
   b. *ShifRows*
   c. *Add RoundKey*

b. Metode Algoritma Rivest Code 4 (RC4)

Secara garis besar algoritma RC4 *Stream Cipher* ini terbagi dua bagian, yaitu : *key setup* dan *Key Scheduling Algorithm* (KSA) dan *stream generation* atau *Pseudo Random Generation Algorithm* (PRGA) dan proses XOR dengan *steam* data.

Tahapan proses Enkripsi pada algoritma RC4

1. *Key Setup / Key Scheduling Algorithm* (KSA)

   Pada bagian ini, terdapat tiga tahapan proses didalamnya yaitu: Inisialisasi *S-box*, Menyimpan kunci dalam *Key Byte Array*, Permutasi pada *S-Box*.

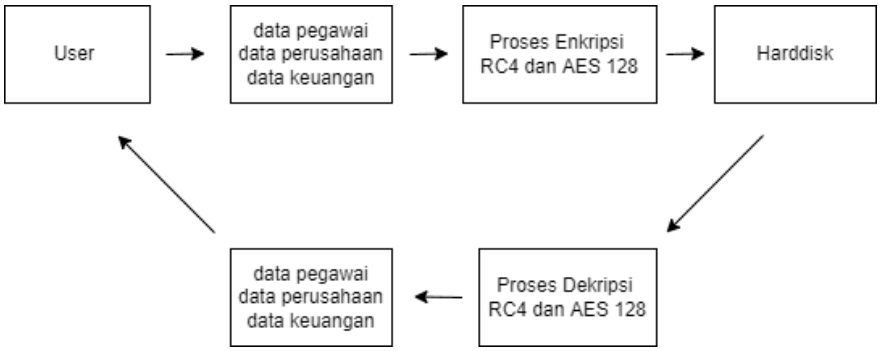
2. Stream Generation

   Pada tahapan ini akan menghasilkan *peseudorandom* yang menggunakan operasi XOR untuk menghasilkan *cipherhtext* menjadi *plaintext* ataupun sebaliknya [6].

Tahapan proses dekripsi pada algoritma RC4

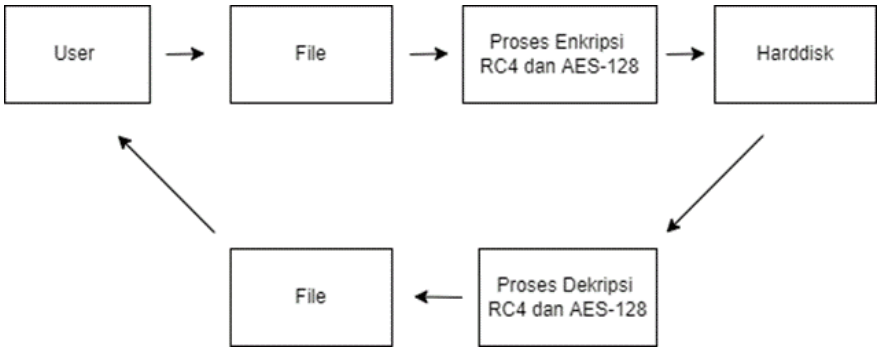
Algoritma dekripsi RC4 mirip dengan algoritma enkripsinya, perbedaan hanya pada saat *stream generation*, yaitu untuk menghasikan *plaintext* semula, maka *ciphertext*-nya akan dikenakan operasi XOR terhadap *pseurandom byte*nya [6].

Dari permasalahan pada penelitian ini, maka diperlukan sebuah aplikasi untuk mengamankan data dan *file* untuk menjaga keamanan dan kerahasiaannya. Pada keamanan data, *User* akan memasukan data pegawai, data perusahaan beserta data keuangan, lalu akan dienkripsi dengan menerapkan metode algoritma kriptografi RC4 dan AES 128 dengan menentukan kunci enkripsi agar data tidak dapat terbaca lalu data yang telah dimasukan akan tersimpan ke *file*. dan juga pada proses dekripsi, menggunakan kunci dekripsi yang sama seperti kunci enkripsi maka data bisa terbaca kembali. Dapat dilihat pada gambar 1.



Gambar 1. Penerapan Kriptografi Pegawai , Perusahaan, Keuangan

Pada keamanan *file* akan dienkripsi dengan menerapkan metode algoritma kriptografi RC4, *file* yang telah di*input* akan melalui proses enkripsi, lalu *file* akan tersimpan ke *harddisk*. *File* juga dapat di dekripsi kembali dengan menerapkan metode algoritma AES 128 dan RC4. Dapat dilihat pada gambar 2.



Gambar 2. Penerapan Metode Kriptografi *File*

2.3 Implementasi Sistem

Pada tahap implementasi sistem akan diimplementasikan kedalam bahasa pemprograman tertentu, dalam hal ini sistem aplikasi yang digunakan untuk mebuat aplikasi kriptografi menggunakan bahasa pemprograman PHP (*hypertext preprocessor*) dan DBMS (*file management system*) yang akan digunakan sebagai penyimpanan data adalah *MySQL* dan *Harddisk*

2.4 Pengujian Sistem dan Analisis Hasil Pengujian

Pada tahap pengujian sistem yang akan dilakukan, bertujuan untuk mengetahui sistem yang akan dibuat apakah sudah sesuai dengan hasil analisis dan rancangan sistem yang dibuat, serta apakah sudah sesuai yang diharapkan. Untuk mengetahui hal tersebut, maka diperlukan metode pengujian pada penelitian.

Pada penelitian ini, metode pengujian yang akan digunakan adalah *blackbox testing*, *blackbox testing* merupakan sebuah metode yang digunakan untu melakukan pengujian pada sebuah aplikasi apakah aplikasi terjadi kesalahan atau tidak dan apakah hasil sudah sesuai yang diharapkan.

3. HASIL DAN PEMBAHASAN

Pada tahap ini berisi implementasi metode, pengujian sistem dan *flowchart* enkripsi dan dekripsi AES 128, *flowchart* enkripsi dan dekripsi RC4, serta pembahasan topik penelitian, tahap ini dapat dilakukan setelah metodologi penelitian. Pada bagian ini juga berisi uraian yang berupa penjelasan, gambar, tabel, dan lainnya.

3.1 Implementasi Metode

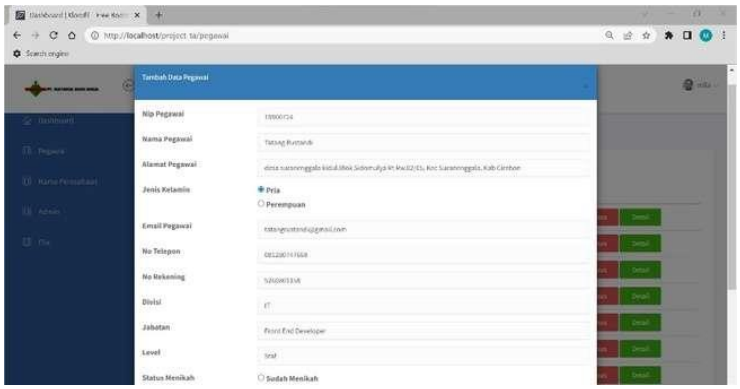
Berdasarkan metode yang akan dilakukan peneliti pada bab sebelumnya yaitu dengan menggunakan kriptografi AES 128 dan RC4 untuk mengamankan Data Pegawai, Data Admin, Data keuangan Perusahaan, dan *File*.

a. Data pegawai

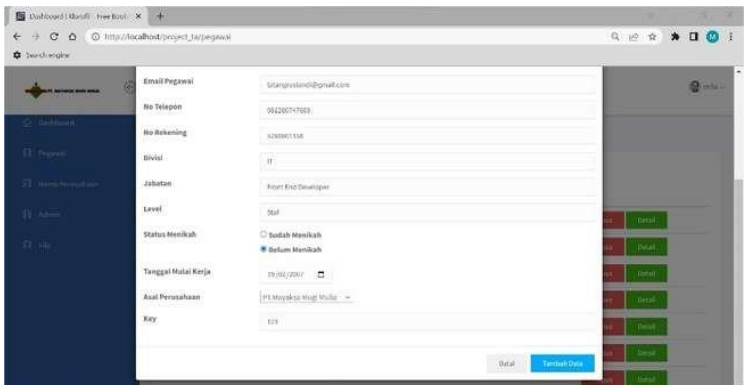
Pada halaman data pegawai, digunakan untuk menambah data pegawai perusahaan ke *file*, dan juga *user* dapat melihat isi dari data pegawai yang telah dienkripsi dengan cara mendekripsi data tersebut.

1. Enkripsi Data pegawai

   Pada tahapan ini *user* harus input terlebih dahulu data pegawai pada *form* tambah data pegawai. Setiap *field* yang tersedia di *form* harus terlebih dahulu dan data yang terenkripsi hanya data yang penting saja. *Form* data pegawai. Dapat dilihat pada gambar 3 dan gambar 4.

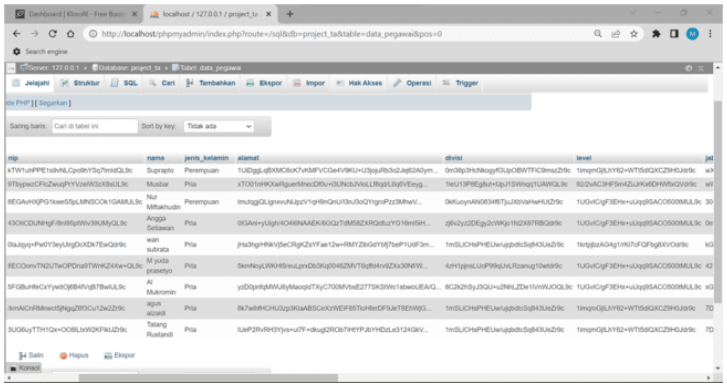


Gambar 3. Form Tambah Data Pegawai



Gambar 4. Form Tambah Data Pegawai

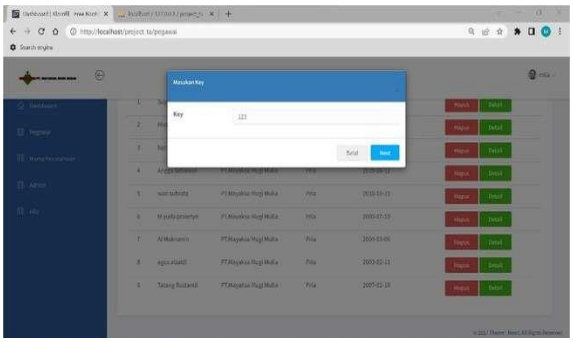
Setelah *user* berhasil mengisi *form* data pegawai maka data akan masuk ke *file*. Di dalam *file* data sudah terenkripsi dengan menggunakan metode kriptografi. Dapat dilihat seperti gambar 5.



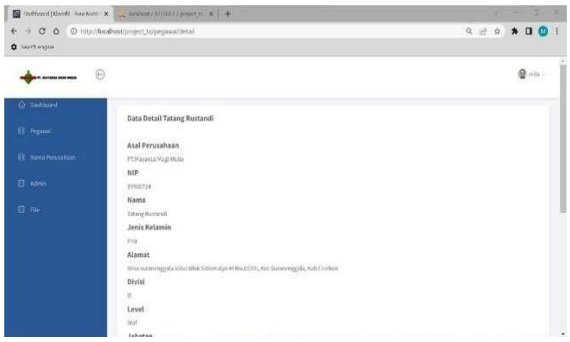
Gambar 5. Hasil Enkripsi Data Pegawai

2. Dekripsi Data pegawai

Pada tahap ini *user* akan melakukan dekripsi data yang terenkripsi dengan memilih data yang akan didekripsi lalu masukan *key* terlebih dahulu, *key* yang terisi harus benar agar bisa melanjutkan proses dekripsi. Dapat dilihat pada gambar 6 dan gambar 7.



Gambar 6. Masukan *Key* Untuk Dekripsi



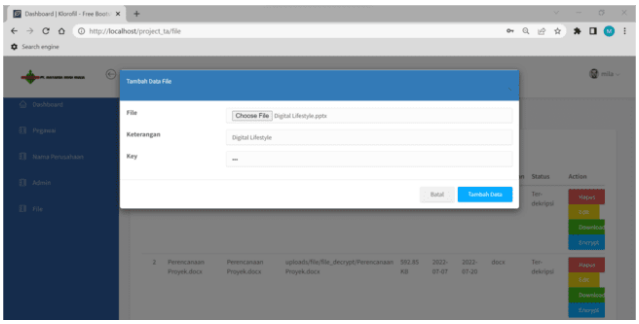
Gambar 7. Hasil Setelah Didekripsi

b. Data *File*

Pada halaman data *File* digunakan untuk menyimpan data *file* perusahaan. dan isi dari *file* tidak dapat dibuka. selain itu juga *user* dapat men-*download file*, baik *file* yang terenkripsi maupun *file* yang telah terdekripsi kembali.

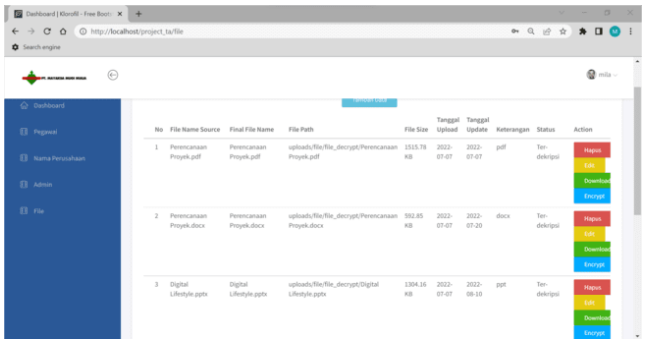
1. Enkripsi Data *File*

Pada tahapan ini *user* harus *input* terlebih dahulu *File*, pilih *file* yang ingin dienkripsi, isi keterangan dan *key*. Dapat dilihat pada gambar 8.



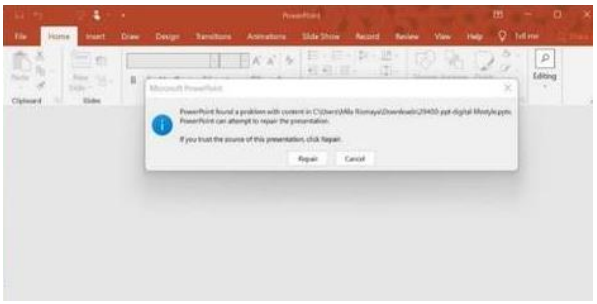
Gambar 8. Isi Form Data *File*

File yang telah di*input* akan masuk pada aplikasi. Dapat dilihat pada gambar 9.



Gambar 9. *File* Enkripsi

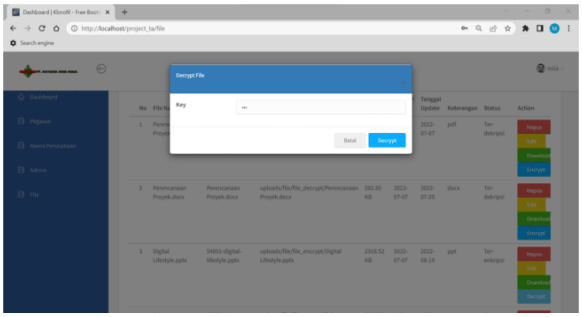
Download *file* yang terenkripsi, dan *file* tidak dapat terbuka.



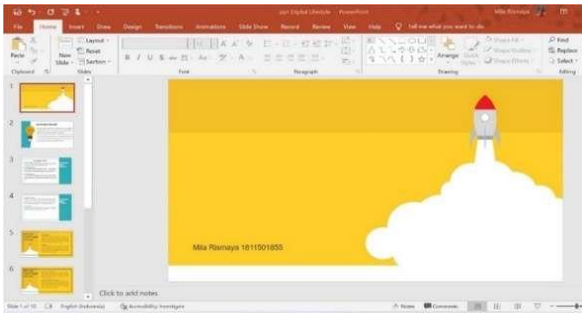
Gambar 10. *File* Terenkripsi

2. Dekripsi Data *File*

Pada tahap ini *user* akan melakukan dekripsi *file* yang terenkripsi dengan pilih *file* yang akan didekripsi, lalu menu dekripsi dan masukan *key* terlebih dahulu, *key* yang terisi harus benar agar bisa melanjutkan proses dekripsi. Dapat dilihat pada gambar 11. Download kembali *file* yang telah terdekripsi dan hasilnya. Dapat dilihat pada gambar 12.



Gambar 11. *Key* Dekripsi *File*



Gambar 12. *File* Terdekripsi

3.2 Flowchart Enkripsi dan Dekripsi AES 128

Pada *flowchart* enkripsi AES 128 menjelaskan alur atau proses enkripsi pada AES 128, yaitu mengubah *plaintext* menjadi *ciphertext*. Pada *flowchart* dekripsi menjelaskan alur atau proses dekripsi pada AES 128, yaitu mengembalikan *ciphertext* menjadi *plaintext*. Dapat dilihat pada gambar 13.

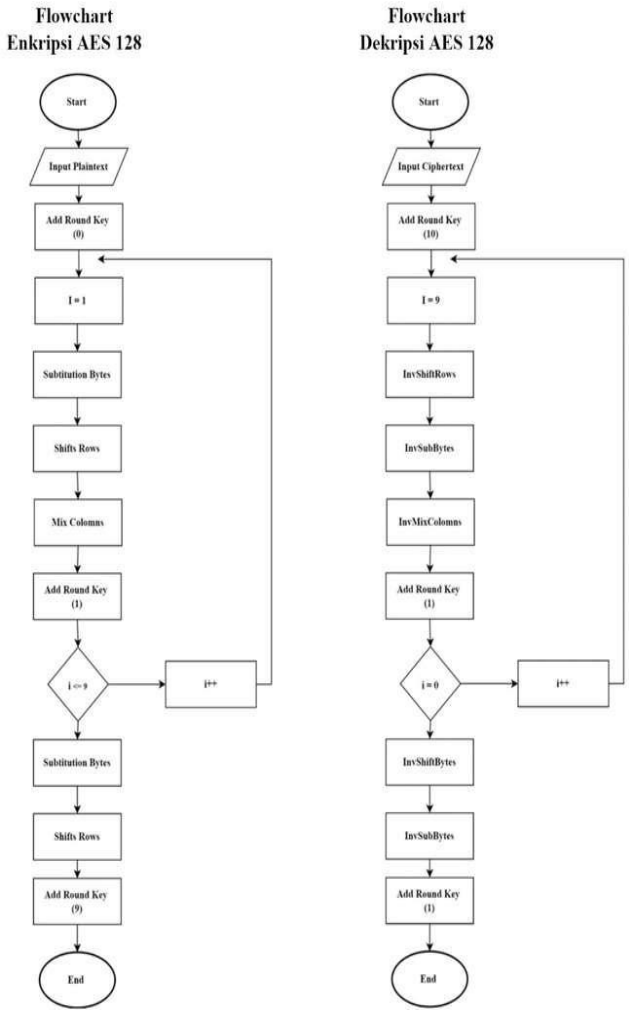
3.3 Flowchart Enkripsi dan Dekripsi RC4

Pada *flowchart* enkripsi RC4 menjelaskan alur atau proses enkripsi pada RC4, yaitu mengubah *plaintext* menjadi *ciphertext*. Pada *flowchart* dekripsi menjelaskan alur atau proses dekripsi pada RC4, yaitu mengembalikan *ciphertext* menjadi *plaintext.* Dapat dilihat pada gambar 14.

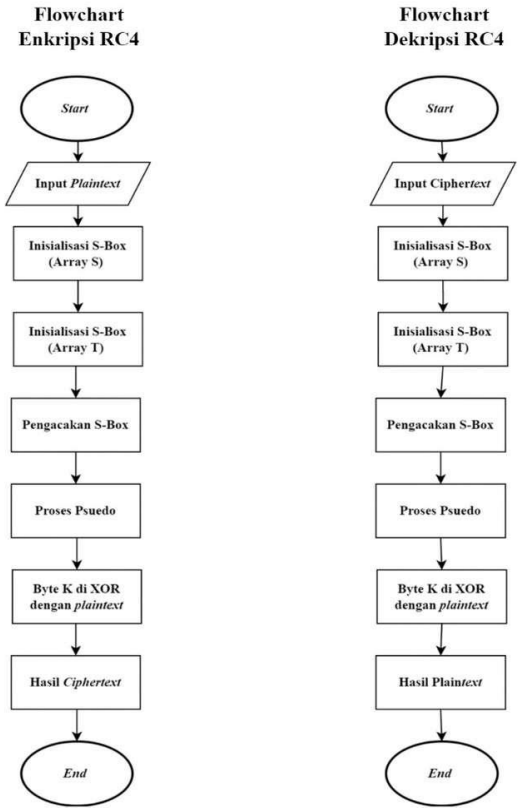
3.4 Pengujian Sistem

Pada pengujian sistem, peneliti menggunakan *blackbox* sebagai metode pengujian. *Blackbox* merupakan metode yang akan dilakukan pada penelitian ini yang bertujuan untuk mengecek terjadinya kesalahan dan melakukan percobaan pada aplikasi serta mengetahui apakah input yang diterima, dan *output* yang dihasilkan, sudah sesuai dengan apa yang diharapkan. Berdasarkan penelitian sebelumnya metode pengujian *blackbox* memiliki kelebihan, yakni dapat mengetahui mengenai fungsi *input* dan *output* pada suatu perangkat lunak [7].

Pada pengujian *blackbox* ini, juga digunakan untuk melakukan pengujian dari sisi panjang *teks* asli, dengan hasil *text* setelah dilakukan proses enkripsi dan proses dekripsi beserta lamanya waktu pada proses enkripsi dan proses dekripsi. Begitupun pada pengujian *file*, dapat melakukan pengujian ukuran *file*, beserta waktu pada proses enkripsi dan proses dekripsi. Tabel 1 menyajikan hasil pengujian enkripsi dan dekripsi data pegawai dan data keuangan.



Gambar 13. Flowchart Enkripsi dan Dekripsi AES 128



Gambar 14. Flowchart Enkripsi dan Dekripsi RC4

Tabel 1. Hasil Pengujian Enkripsi Dan Dekripsi Data Pegawai Dan Data Keuangan

Karakter Asli	Jumlah Karakter	Hasil Enkripsi	Jumlah Karakter Hasil Enkripsi	Waktu Enkripsi	Waktu Dekripsi	Akurasi (%)
Data Pegawai						
Nip: 19900724	8	3UG6uyTTH1Q x+OO8lLtxW2K FlktJZr9c	32	0,06 Sec	0,02 Sec	100%
Alamat : desa suranenggala kidul.Blok Sidomulya Rt Rw.02/05, Kec Suranenggala, Kab Cirebon	76	lUeP2RvRH3Yjv s+ui7F+dkugl2R Ob7IHtYPJbYH DzLe3124GkV8 322FANUk7uqv Fi48SotfADDG/ 46Pfy9iQIKeoq6 zkgMSHtBo0rb DnuTyWuc0PfH a9i7Oa55ql0Yv9 Z/tf7bItqvBJWa OTwbgJx3zPgK	172	0,06 Sec	0,02 Sec	100%

Karakter Asli	Jumlah Karakter	Hasil Enkripsi	Jumlah Karakter Hasil Enkripsi	Waktu Enkripsi	Waktu Dekripsi	Akurasi (%)
		wNlZvPAZsyw5i7MNs=				
Jabatan: Front End Developer	19	7Da4qxniDHNm/MO7n49YUFSAlENUU/MWmLztftHv/Zyq4ms462A99VlfREM=	60	0,06 Sec	0,02 Sec	100%
		Data Keuangan				
Judul : Harga Pokok Produksi	19	0WCQowf/AGl5zJqDgp9ba3KMylcIUPgMg7/dPqPo/MGT3nQUzgcL/WRwbkM=	60	0,00 Sec	0,01 Sec	100%
Jumlah: Rp.30.000.000	13	9F6IhAfMKHUM5M21ka1/VWL9xlAZQL9c	32	0,00 Sec	0,01 Sec	100%
Total Akurasi						100%

Tabel 2 menyajikan hasil pengujian *file*.

Tabel 2. Hasil Pengujian *File*

Nama *File*	Ukuran *File*			Waktu		Akurasi (%)
	Asli	Enkripsi	Dekripsi	Enkripsi	Dekripsi	
Perencanaan Proyek.pdf	1516 Kb	2694,73 Kb	1515,78 Kb	23,71 Sec	28,54 Sec	100%
Perencanaan Proyek.docx	593 Kb	1053,96 Kb	592,85 Kb	10,06 Sec	10,74 Sec	100%
Jadwal Proyek.xls	21 Kb	35,88 Kb	20,17 Kb	0,47 Sec	0,34 Sec	100%
Digital Lifestyle.ppt	1305 Kb	2318,52 Kb	1304,16 Kb	22,29 Sec	26,99 Sec	100%
Project Bulan Mei.docx	13,6 Mb	24,2 Mb	13,9 Mb	504,50 Sec	427,89 Sec	100%
Rekap Dokumentasi .docx	30,0 Mb	53,3 Mb	-	609,97 Sec	-	0%
Total Akurasi						83%

Berdasarkan dari hasil uji coba menggunakan metode *blackbox testing* pada penelitian ini yakni pada tabel hasil pengujian enkripsi dan dekripsi data pegawai dan data keuangan memiliki total akurasi keberhasilan 100%. Sedangkan pada tabel hasil pengujian enkripsi dan dekripsi data *file*, ditemukannya kegagalan pada proses dekripsi dengan nama *file*: Rekap Dokumentasi.docx sehingga total akurasi keberhasilan pada data *file* sebesar 83%.

4. KESIMPULAN

Dengan adanya aplikasi pengamanan *file* dan *file* ini, menjadikan data pada perusahaan lebih aman, aplikasi ini dapat mengamankan database berupa data pegawai, data keuangan dan *file* penting pada perusahaan dengan

menerapkan proses enkripsi dan proses dekripsi menerapkan metode algoritma AES 128 dan RC4. Aplikasi ini dapat mengamankan *file* dengan menerapkan proses enkripsi dan dekripsi menerapkan metode algoritma kriptografi AES 128 dan RC4, dalam bentuk ekstensi .docx, .pdf, .xlsx, .pptx, ukuran *file* dapat mempengaruhi lamanya waktu enkripsi dan dekripsi, namun *file* yang di enkripsi dan dekripsi akan terjamin keutuhannya, dan tidak akan mengalami kerusakan dan perubahan pada isi *file*.

DAFTAR PUSTAKA

[1] D. Widyawan and Imelda, "Pengamanan *File* Menggunakan Kriptografi Dengan Metode AES-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi," *SKANIKA*, vol. 4, no. 1, pp. 15–22, 2021.

[2] M. Fahri, H. Damanik, et al, "Pemanfaatan Algoritma AES Untuk Keamanann Data Karyawan PT. Telkom Indonesia Pematangsiantar," *Jurnal Ilmiah Teknik dan Ilmu Komputer*, vol. 1, no. 1, pp. 32–37, 2022.

[3] F. Akbar and S. Waluyo, "Sistem Keamanan Database Menggunakan Algoritma Advanced Encryption Standard (AES-128) Studi Kasus: Red Avenue Indonesia," *SKANIKA*, vol. 1, no. 2, pp. 821-828, 2018.

[4] H. Kusniyati, S. Diansyah, and R. Yusuf, "Penerapan Algoritma Rivert Code 4 (RC4) Pada Aplikasi Kriptografi Dokumen," *Jurnal PETIR*, vol. 11, no. 1, pp. 38-47, 2018.

[5] T. Erlangga and D. Kusumaningsi, "Implementasi Algoritma Advanced Encryption Standard-128 (AES-128) Untuk Pengamanan Database Berbasis Desktop Pada Icaltoys," *SKANIKA*, vol. 1, no. 2, pp. 565-569, 2018.

[6] L. Risnanda and N. Juliasari, "Penerapan Algoritma Kriptografi Vignere Cipher Dan RC4 (Rivest Code 4) Pada Databease Berbasis Java," *SKANIKA*, vol. 1, no. 3, pp. 1100-1107, 2018.

[7] A. kodir and W. Pramusinto, "Implementasi Kriptografi Dengan Menggunakan Metode RC4 dan Base64 Untuk Mengamankan Database Sekolah Pada SDN Grogol Utara 10," *SKANIKA* , vol. 4, no. 1, pp. 7–14, 2021.

[8] F. Ahmad Sitorus, N. Budi Nugroho, and U. Fatimah Sari Sitorus Pane, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit Untuk Keamanan Data Transaksi Penjualan Pada PT. Mitsubishi Electric Indonesia," Jurnal SAINTIKOM, vol. 4, no. 5, pp. 1-14, 2020.

[9] Asriyanik, "Studi Terhadap Advanced Encyption Standard (AES) Dan Algoritma Knapsack Dalam Pengamanan Data," *Jurnal SANTIKA: Jurnal Ilmiah Sains dan Teknologi*, vol. 7, no. 1, pp. 553-561, 2017.

[10] A. Setiawan and T. Fatimah, "Implementasi Algoritma Kriptografi RC4 Untuk Keamanan Database Aplikasi Penggajian Karyawa Berbasis Web Pada PT. Trans Asia," *JANUARI*, vol. 4, pp. 66–71, 2021.

[11] S. Waluyo, Ferdiansyah, and firman, "Sistem Keamanan Management *File* Menggunakan Algoritma Advanced Encryption Standard (AES-128) Studi Kasus : Tabitha Indonesia," vol. 1, pp. 639-644, 2018.