3rd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
30 Agustus 2023 – Jakarta, Indonesia
Volume 2, Nomor 2, September 2023 - ISSN 2962-8628 (*online*)

IMPLEMENTASI ALGORITMA *AES*-128 DENGAN *BLOCKCHAIN* UNTUK PENGAMANAN *FILE* PADA SDN PASAR BARU 3

Rizky Uki Indriani[1*], Mardi Hardjianto[2]

1*,2 Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, DKI Jakarta, Indonesia
Email: [1*]rizkyukiindriani@gmail.com, [2]mardi.hardjianto@budiluhur.ac.id
(* : corresponding author)

Abstrak-Dalam era digital yang semakin maju, pertukaran data menjadi semakin penting dalam berbagai aspek kehidupan, termasuk bisnis, layanan keuangan, pendidikan, dan lainnya. Namun, dengan pertukaran data yang semakin sering terjadi akan meningkatkan potensi risiko keamanan data, seperti peretasan dan kebocoran data. Pengelolaan data pada Sekolah Dasar Negeri Pasar Baru 3 sudah tersimpan secara sistematis, tetapi data yang berada di sekolah masih disimpan dalam *file* asli yang dapat dengan mudah tersebar oleh orang lain. Untuk mengatasi masalah ini, teknologi kriptografi *Advanced Encryption Standard* (AES)-128 dengan *blockchain* berbasis web hadir sebagai solusi yang kuat untuk melindungi keamanan data. *B*lockchain itu sendiri hadir sebagai tambahan penguat keamanan *file* dalam blok, sedangkan enkripsi AES-128 dapat digunakan untuk melindungi data di tingkat *file*. Untuk memastikan keberhasilan keamanan data enkripsi dan dekripsi dengan mengintegrasikan AES-128 dalam proses enkripsi data yang disimpan dalam blok, serta selama proses data yang terjadi di dalam jaringan blockchain. Proses ini memastikan bahwa blok yang disimpan dalam jaringan blockchain tidak berubah, jika terdapat perubahan pada blok enkripsi maka data tidak bisa didekripsi maupun sebaliknya. Hasil penelitian ini menunjukkan bahwa aplikasi ini memberikan tingkat keamanan yang tinggi dalam mengamankan data pada SDN Pasar Baru 3. Hasil akhir pengujian dari file SDN Pasar Baru 3 berukuran 1.063 Kb memiliki waktu enkripsi 255 detik dan dekripsi memiliki waktu 252 detik. Kesimpulan dari hasil implementasi, bahwa algoritma kriptografi menggunakan metode AES-128 dengan *Blockchain* dapat menjaga keamanan *file* pada SDN Pasar Baru 3.

Kata Kunci: AES-128, *Blockchain*, Dekripsi, Enkripsi, *File*, Kriptografi.

IMPLEMENTATION OF ALGORITHM AES-128 *USING BLOCKCHAIN FOR FILE SECURITY AT SDN PASAR BARU 3*

Abstract- *In this increasingly advanced digital era, data exchange is becoming increasingly important in various aspects of life, including business, financial services, education, and others. However, the more frequent exchange of data will increase the potential for data security risks, such as hacking and data leakage. Data management at Pasar Baru 3 Public Elementary School has been stored systematically, but the data at the school is still stored in the original file which can be easily spread by other people. To solve this problem, Advanced Encryption Standard (AES)-128 cryptographic technology with web-based blockchain comes as a powerful solution to protect data security. The blockchain itself comes as an additional reinforcement of file security in blocks, while AES-128 encryption can be used to protect data at the file level. To ensure successful encryption and decryption data security by integrating AES-128 in the process of encrypting data stored in blocks, as well as during data processing that occurs in the blockchain network. This process ensures that the block stored in the blockchain network does not change, if there is a change in the encryption block, the data cannot be decrypted and vice versa. The results of this study indicate that this application provides a high level of security in securing data at SDN Pasar Baru 3. The final test result of the SDN Pasar Baru 3 file measuring 1,063 Kb has an encryption time of 255 seconds and a decryption time of 252 seconds. The conclusion from the implementation results is that the cryptographic algorithm using the AES-128 method with Blockchain can maintain file security at Pasar Baru 3 Elementary School.*

Keywords*: AES-128, Blockchain, Decryption, Encryption, Files, Cryptography.*

1. PENDAHULUAN

Perkembangan teknologi saat ini berkembang sangat pesat dan telah mengalami perubahan yang signifikan dalam hal keamanan data. Ancaman dalam keamanan data seperti peretasan, pencurian identitas, dan kebocoran data merupakan masalah yang dapat merugikan individu maupun organisasi. Informasi dan data adalah sebuah

aset yang penting untuk sebuah instansi maupun individu [1]. Oleh karena itu, teknologi pengamanan *file* menjadi sangat penting untuk melindungi data dan menjaga kerahasiaan.

Pengelolaan data pada SDN Pasar Baru 3 sudah tersimpan secara sistematis, tetapi data yang berada di sekolah masih berupa *file* asli yang dapat dengan mudah tersebar luas. Pihak sekolah memiliki kebutuhan untuk menyimpan data siswa, guru, dan penilaian yang bersifat rahasia dan penting. Permasalahan yang ada adalah dalam data-data tersebut bisa dilihat oleh siapa saja padahal tidak seharusnya orang lain dapat melihat dan mengakses. Solusi dari permasalahan ini adalah dengan mengimplementasikan pengamanan *file* menggunakan metode kriptografi yang bisa mengunci data sehingga data menjadi lebih aman. Kontribusi penelitian ini adalah mengimplementasikan kriptografi dengan mengkombinasikan dua metode enkripsi *Advanced Encryption Standard* (AES) dengan *blockchain* untuk mengamankan *file*.

Kriptografi adalah ilmu yang mempelajari teknik matematika yang berkaitan dengan informasi dan aspek keamanan informasi seperti validitas data, integritas dan otentikasi data [2]. Berdasarkan kunci yang digunakan, algoritma enkripsi dapat dibedakan menjadi dua kelompok, yaitu algoritma simetris dan asimetris. Sistem ini menggunakan algoritma simetris, yaitu algoritma enkripsi yang menggunakan kunci yang sama untuk enkripsi dan dekripsi [3].

Berdasarkan paparan dari kriptografi, *Advanced Encryption Standard* (AES) adalah algoritma kriptografi yang menjadi standar algoritma enkripsi kunci simetris pada saat ini [4]. AES bekerja dengan blok sekitar 128-bit atau 16 karakter dan dapat digunakan untuk enkripsi.

Blockchain adalah sekumpulan blok yang terdiri dari lebih dari satu blok yang terhubung. Setiap blok terdiri dari tiga elemen, yaitu data, nilai hash blok, dan nilai hash blok sebelumnya [3]. Blockchain digunakan untuk memastikan tingkat keamanan yang tinggi dan mencegah manipulasi data yang tidak sah [5]. Data di dalam blockchain diamankan dengan menggunakan kriptografi, di mana setiap data yang terjadi akan dienkripsi dan dihubungkan dengan data sebelumnya melalui mekanisme hashing. Seluruh jaringan juga memverifikasi data [6], sehingga upaya untuk melakukan perubahan atau manipulasi data oleh pihak yang tidak berwenang menjadi sulit dilakukan.

Inilah sebabnya mengapa *blockchain* adalah cara yang efektif untuk menjaga keamanan data. Namun, metode ini masih rentan terhadap serangan pasif di mana penyerang dapat mengakses datanya, karena data di blok blockchain masih belum terenkripsi [3]. Oleh karena itu, penelitian ini menggabungkan metode *Advanced Encryption Standard* (AES)-128 yang dapat mengenkripsi data, dengan metode blockchain untuk meningkatkan keamanan sistem pengamanan data agar tahan terhadap serangan aktif maupun pasif.

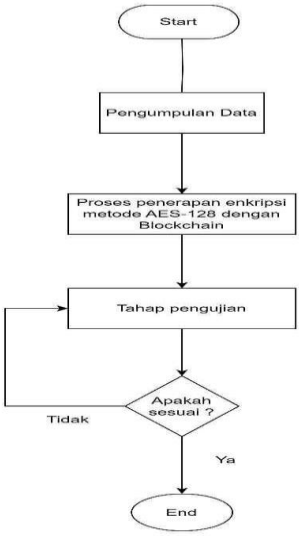
Penelitian terdahulu telah ada pembahasan tentang kriptografi dengan metode AES dan *Blockchain* berbasis android dari "Dhiya Calista, dkk" dengan judul "*Sistem Pengamanan Data Menggunakan Kriptografi AES dan Blockchain Berbasis Android*" pada penelitian ini pengamanan data berbasis android menggunakan metode AES dan *blockchain* di ruang lingkup sekolah [3]. Sehingga muncul penelitian baru untuk membuat aplikasi berbasis web pengamanan informasi akademik. Perbedaan dari jurnal diatas, yaitu berbasis android dan web serta akan menambahkan fitur input kunci saat proses enkripsi dan dekripsi. Adapun penelitian dengan judul "*Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)*", oleh Azhari, dkk yang implementasinya hanya menggunakan 1 metode yaitu AES sedangkan penelitian ini menambahkan metode tambahan yaitu *Blockchain*.

Berdasarkan uraian permasalahan di SDN Pasar Baru 3, solusi yang didapatkan adalah penggunaan kriptografi algoritma AES-128 dengan *Blockchain* berbasis *Web* untuk pengamanan *file* untuk menjamin keamanan data informasi akademik. Jenis dokumen yang akan diuji adalah laporan bulanan sekolah pada bulan Maret 2023 dengan format .xls.

2. METODE PENELITIAN

2.1 Penerapan Metode

Penerapan metode ini digunakan sebagai panduan utama untuk memastikan bahwa tujuan yang telah dibuat sebelumnya tetap berjalan. Untuk tahapan penelitian ini dapat dilakukan pada gambar 1 sebagai berikut :



Gambar 1 Penerapan Metode

Dalam penerapan metode enkripsi dan dekripsi AES-128 menambahkan metode blockchain digunakan untuk memberikan tingkat keamanan yang tinggi dan mencegah manipulasi data yang tidak sah. Karena dalam simpul menyimpan salinan lengkap dari seluruh rantai blok, bagi penyerang akan sulit untuk merusak atau mengubah data di blockchain. Selain itu, jika beberapa simpul terganggu atau diserang, simpul-simpul lain masih dapat memverifikasi dan mempertahankan keaslian data. Serta penggunaan fungsi hash seperti SHA-256 untuk menghasilkan hash blok yang unik.

2.2.1. Kriptografi

Kriptografi adalah disiplin ilmu yang mempelajari metode untuk menjaga keamanan informasi, termasuk otentikasi, kerahasiaan data, keabsahan data, dan integritas data. Kriptografi juga bisa dianggap sebagai seni menjaga kerahasiaan pesan [7]. Terdapat 4 tujuan kriptografi [8], yaitu :

1. Kerahasiaan (*confidentiality*) adalah Layanan yang dirancang untuk mencegah pesan dibaca oleh orang yang tidak berwenang.
2. Integritas data (data *integrity*) adalah layanan yang menjamin bahwa pesan masih asli atau belum pernah dimanipulasi selama pengiriman.
3. Otentikasi (*authentication*) adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication)*.
4. *Non-repudiation* adalah layanan yang mencegah entitas komunikasi melakukan penolakan

2.2.2. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) adalah sebuah algoritma *block cipher* yang memiliki sifat simetris, di mana menggunakan kunci simetris saat proses enkripsi dan dekripsi [4]. Algoritma AES memungkinkan enkripsi dan dekripsi data dengan panjang kunci yang dapat bermacam-macam, yaitu 128 bit, 192 bit, dan 256 bit. Perbedaan antara ketiga panjang kunci tersebut adalah jumlah putaran (round) yang dilakukan oleh AES. AES-128 menggunakan 10 putaran, AES-192 menggunakan 12 putaran, dan AES-256 menggunakan 14 putaran [9]. Terdapat 4 transformasi putaran pada proses enkripsi dan dekripsi :

a. Pada proses enkripsi algoritma AES [10] :
   1. Tahap *Sub Bytes substitution* dengan tabel (S-Box).
   2. Tahap *Shift Rows* melakukan pergeseran pada baris array, menyesuaikan dengan nilai baris.
   3. Tahap *MixColumns* melakukan perkalian dengan kolom tiap array *state*.
   4. Tahap *Add Round Key* akan melakukan XOR antara *state* yang paling terbaru sampai mencapai akhir
b. Pada proses dekripsi algoritma AES:
   1. Tahap *InvShiftRows* melakukan pergeseran bit ke kanan pada setiap blok baris.
   2. Tahap *InvSubBytes* setiap elemen pada *state* dipetakan dengan tabel Inverse S-Box.
   3. Tahap *InvMixColumn* setiap kolom dalam *state* dikalikan dengan matriks AES.
   4. Tahap *AddRoundKey* mengkombinasikan *state array* dan *round key* dengan hubungan XOR

2.2.3. *Blockchain*

Blockchain adalah suatu bentuk basis data yang terdistribusi atau terdesentralisasi yang menggunakan node independen untuk menyimpan dan mengambil data [11]. Teknologi *blockchain* menghubungkan berbagai blok data secara berurutan dalam suatu buku besar yang tersebar. Setiap blok berisi berbagai konten, termasuk "*hash*", yaitu pengidentifikasi unik dari blok tersebut. *Hash* ini berfungsi untuk mengidentifikasi dan menghubungkan blok tersebut dengan semua blok lainnya, baik blok sebelumnya maupun blok selanjutnya. Dengan demikian, dapat disimpulkan bahwa *blockchain* merupakan kumpulan blok-blok yang berisi data transaksi yang saling terhubung dan diurutkan. *Blockchain* dapat dianggap sebagai sebuah sistem penyimpanan data digital di mana setiap blok terbaru atau blok terakhir selalu memiliki informasi *hash* dari blok sebelumnya. Setiap blok merujuk pada blok sebelumnya dan membentuk rantai (*chain*) yang terus berlanjut [12].

2.2 Pengumpulan Data

Pada tahap pengumpulan data ini, data yang digunakan dalam penelitian melibatkan beberapa metode layanan data yaitu :

a. Wawancara
   Proses wawancara dengan tanya jawab langsung dengan kepala sekolah dari SDN Pasar Baru 3 agar mendapatkan informasi tentang profil sekolah dan sistem kerja yang sudah ada.
b. Observasi
   Proses observasi ini dilakukan pada SDN Pasar Baru 3 secara langsung dengan tujuan mengetahui sistem atau proses keamanan yang dilakukan oleh sekolah.
c. Studi Literatur
   Proses studi literatur juga dilakukan melalui pembacaan berbagai buku teks, jurnal, dan karya tulis ilmiah yang berkaitan dengan masalah yang akan dibahas, terutama dalam bidang kriptografi dengan fokus pada metode kriptografi AES dan *blockchain*. Hal ini bertujuan untuk memperoleh dasar referensi yang tepat dalam memecahkan permasalahan yang akan diteliti.

2.3 Tahap Pengujian

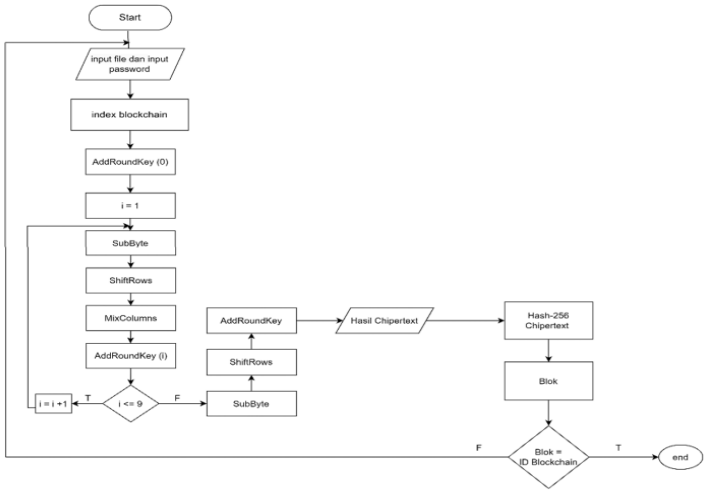
Tujuan pada tahap pengujian ini untuk menjamin sistem yang telah dibuat sesuai dan berjalan sesuai dengan perancangan dan hasil analisis serta menghasilkan suatu kesimpulan apakah sistem yang telah dibuat sesuai dengan harapan dari permasalahan yang ada. Untuk mencapai tujuan tersebut diperlukan penggunaan metode pengujian yang akan menjadi kesimpulan bahwa sistem telah berjalan sesuai dengan perencanaan. Metode pengujian yang digunakan adalah *black box*, yang merupakan metode untuk menemukan kesalahan dan menguji fungsi dari sistem aplikasi saat dijalankan.

2.4 *Flowchart*

Untuk menjelaskan metode dengan menggambarkan urutan prosess pada aplikasi ini, akan digunakan *Flowchart* sebagai gambaran skema proses program. Berikut ini adalah beberapa *Flowchart* dari masing-masing proses.

2.4.1. *Flowchart* Enkripsi AES-128 dengan *Blockchain*

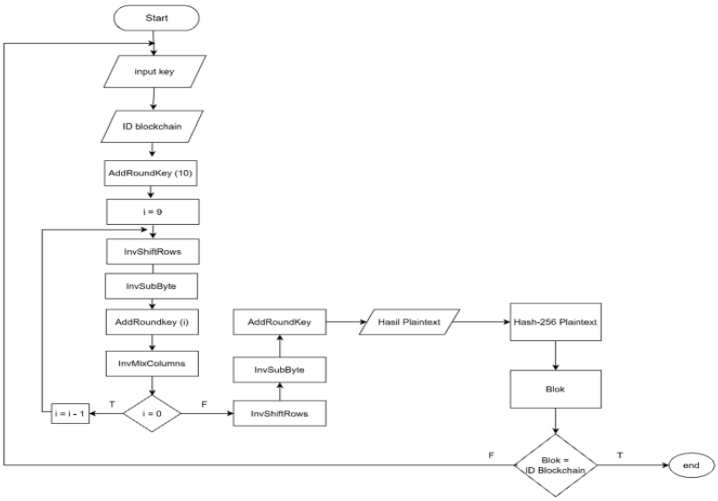
Proses enkripsi metode AES-128 dengan *blockchain* dapat dilihat bentuk *Flowchart* pada gambar 2 pertama yang dilakukan adalah admin menginput *file* dan *key*, lalu *file* tersebut akan diinisialisasikan kembali pada sebuah ID dalam *blockchain* dan membuat blok baru dalam *blockchain*. Selanjutnya *plaintext* akan dienkripsi terlebih dahulu pada proses *AddRoundKey*, *SubByte*, *ShiftRows*, *MixColumns*, setelah itu dilakukan lagi pada proses *AddRoundKey*. Selanjutnya jika telah selesai melakukan proses perulangan sebanyak 10 kali putaran maka program akan melakukan proses *final round* yang terdiri dari *SubByte*, *ShiftRows*, *AddRoundKey*. Setelah proses AES selesai hasil pada enkripsi berupa *chipertext* akan di hashing dan membuat blok baru, blok ini akan diverifikasi integrasi blockchain untuk memastikan bahwa blok yang baru ditambah valid. Proses enkripsi AES-128 dengan *blockchain* selesai dan *file* akan tersimpan.



Gambar 2 *Flowchart* enkripsi AES-128 dengan *blockchain*

2.4.2. *Flowchart* Dekripsi AES-128 dengan Blockchain

Proses dekripsi metode AES-128 dengan *blockchain* dapat dilihat pada *flowchart* gambar 3. Pertama yang dilakukan pada proses dekripsi adalah input *password* yang sama pada *password* dan memanggil ID dari *blockchain*. Selanjutnya proses *AddRoundKey*, *InvShiftRows*, *InvSubBytes*, dan *AddRoundKey* kembali, lalu *InvMixColumns*. Proses akan terulang selama putaran (Nr) masih sama dengan Nr-1. Setelah putaran mencapai 0 putaran, maka program akan melanjutkan proses *final round* yang terdiri dari proses *InvShiftRows*, *InvSubBytes* dan *AddRoundKey*. Setelah proses selesai maka hasil pada dekripsi berupa *plaintext*, *plaintext* selanjutkan akan dilakukan hash dan disimpan dalam blok. Verifikasi integrasi blok tersebut dengan *blockchain* jika valid maka dekripsi berhasil.



Gambar 3 *Flowchart* dekripsi AES-128 dengan *blockchain*

3. HASIL DAN PEMBAHASAN

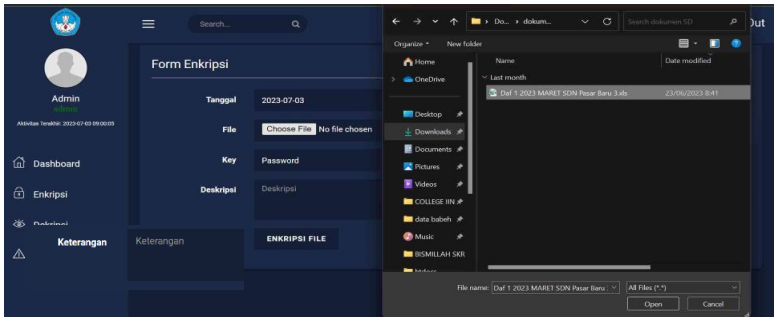
Pada bagian ini pengujian hasil yang diperoleh melalui uji coba mencakup implementasi, dan pengujian hasil. Selain itu, disampaikan penjelasan mendalam dengan tabel, teks, dan gambar guna memahami hasil dari uji coba.

3.1 Implementasi Metode

Berikut ini akan dijelaskan serangkaian langkah yang menjelaskan bagaimana metode AES-128 dengan Blockchain bekerja dalam proses implementasinya dalam bentuk Flowchart.

3.1.1. Proses Enkripsi *File*

Pada proses enkripsi ini admin harus masuk terlebih dahulu ke menu *form* enkripsi yang terletak di bagian sidebar. Kemudian admin pilih *file* yang ingin dienkripsi, setelah memilih *file* admin memasukan *password* dan terakhir diberi keterangan di setiap enkripsi. Jika sudah semua *form* enkripsi diisi dengan baik dan benar bisa klik *button* enkripsi *file*, maka proses enkripsi sedang berlangsung.



Gambar 4 Proses enkripsi *file*

Jika proses enkripsi berhasil akan ada *pop up* enkripsi berhasil lalu klik *button* ok.

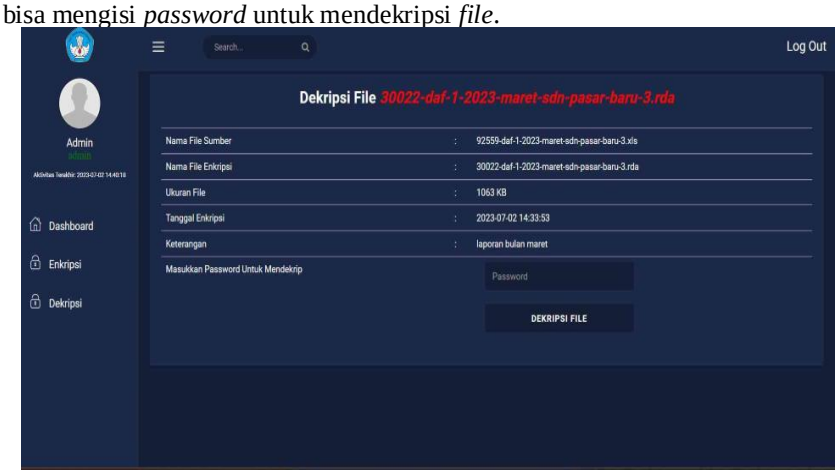
Gambar 5 *Pop up* enkripsi berhasil

3.1.2. Proses Dekripsi *File*

Sebelum proses dekripsi pengguna bisa pilih menu dekripsi pada sidebar, pada halaman ini pengguna dapat melihat *file* yang telah dienkripsi dan yang akan di deskripsi dalam tampilan tabel. Jika pengguna mengklik *button* dekripsi *file* makan akan pindah ke halaman *Form* Dekripsi pada gambar 7 dan ketika mengklik enkripsi *file* makan akan pindah ke halaman *form* Enkripsi.

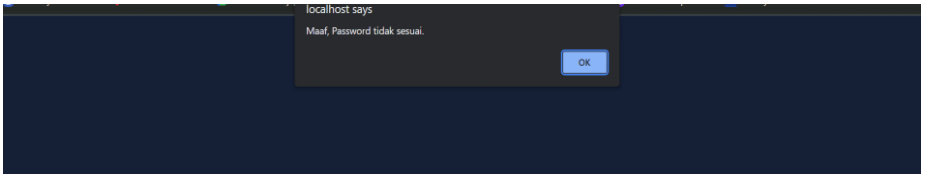
Gambar 6 Tabel Dekripsi

Form dekripsi ini akan muncul setelah pengguna mengklik button dekripsi *file* pada tabel di halaman dekripsi. Setelah itu pengguna bisa mengisi *password* untuk mendekripsi *file*.

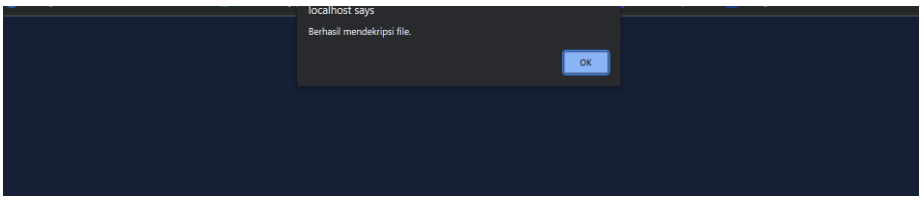


Gambar 7 Proses Dekripsi *File*

Jika *password* yang diinput salah maka akan muncul *pop up* “Maaf, Password tidak sesuai” “Ok” seperti gambar 7 , tetapi jika *password* benar akan muncul *pop up* “Berhasil mendekripsi file” “Ok” seperti gambar 8 maka proses dekripsi pada file berhasil.



Gambar 8 *Pop Up* Password Salah



Gambar 9 *Pop Up* Dekripsi Berhasil

3.2 Hasil Pengujian

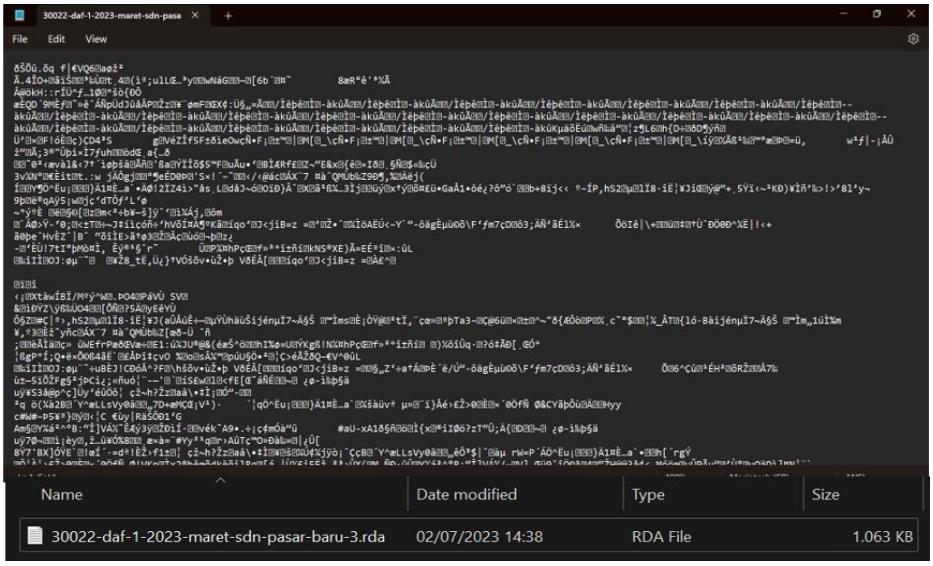
Pengujian program ini menggunakan metode *black box*. Metode black box adalah pendekatan pengujian yang berfokus pada input dan output program memudahkan dalam pemodelan dan analisis sistem yang kompleks tanpa perlu memperhatikan detail internal kode program.

Table 1 Pengujian Fungsional Sistem

No	Rancangan Proses	Hasil yang diharapkan	Hasil Pengujian	Kesimpulan
1.	Melakukan form *Login*	Berhasil *Login*	Sesuai harapan	Ketika pengguna berhasil *Login* akan pindah ke halaman *Dashboard*
2.	Klik menu sidebar di *Dashboard*	Muncul halaman *Dashboard*	Sesuai harapan	Ketika pengguna mengklik menu *Dashboard*, pengguna akan dapat melihat jumlah data yang telah di enkripsi dan dekripsi
3.	Klik menu enkripsi di sidebar	Muncul halaman form enkripsi	Sesuai harapan	Ketika pengguna mengklik menu enkripsi pada sidebar, pengguna dapat mengisi form enkripsi
4.	Klik tombol enkripsi	Berhasil mengenkripsi *File*	Sesuai harapan	Proses data akan dienkripsi
5.	Klik tombol dekripsi	Muncul halaman untuk dekripsi *File*	Sesuai harapan	Ketika pengguna mengklik menu dekripsi, pengguna akan melihat tabel dari data yang telah dienkripsi
6.	Klik tombol dekripsi *File*	Berhasil mendekripsi *File*	Sesuai harapan	Ketika pengguna mengklik tombol dekripsi pada tabel halaman dekripsi akan muncul halaman dekripsi *File*
7.	Klik tombol enkripsi *File*	Maka akan pindah ke halaman enkripsi	Sesuai harapan	Ketika pengguna mengklik tombol enkripsi *File* pada tabel halaman dekripsi akan pindah ke halaman enkripsi
8.	Klik menu panduan di sidebar	Muncul halaman panduan program	Sesuai harapan	Ketika pengguna mengklik menu panduan, maka akan muncul halaman panduan
9.	Klik *logout* menu untuk keluar	Berhasil keluar dari aplikasi	Sesuai harapan	Ketika pengguna mengklik menu *logout*, maka pengguna akan keluar dari aplikasi dan kembali ke halaman *login*

3.2.1. Hasil Pengujian Enkripsi

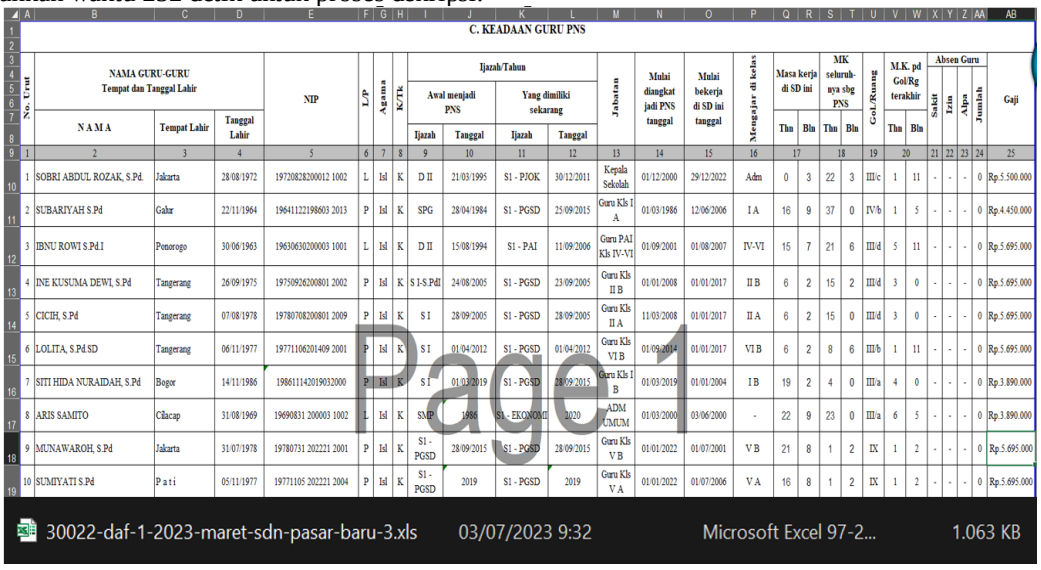
Pada *file* yang telah enkripsi akan mengalami perubahan pada penambah angka acak di depan nama *file* asli, format berubah menjadi .rda, akan tetapi ukuran *file* tidak berubah tetap 1.063 Kb dan membutuhkan waktu enkripsi 255 detik.



Gambar 10 Hasil Pengujian Enkripsi

3.2.2. Hasil Pengujian Deskripsi

Jika proses dekripsi telah selesai format pada *file* kembali ke asli dan tidak mengalami perubahan ukuran file, membutuhkan waktu 252 detik untuk proses dekripsi.



Gambar 10 File Dekripsi

3.2.3. Hasil *Output* Blockchain

Hasil *output* pada *blockchain*, block index dimulai dari angka 0, data pada awal belum ada karena belum ada data yang disimpan dalam blok, *timestamp* adalah waktu pembuatan blok, *previous hash* pertama kali tidak terdefinisi (0000000000000), hash hasil *chipertext* yang di *hash* dengan SHA256 sebanyak data yang dibutuhkan, *nonce* diinisialisasi dengan nilai 00. Dilanjutkan kembali pada *block index* selanjutnya (*block index* 2) dan seterusnya, data yang sudah disimpan dalam blok sudah terisi, menampilkan *previous hash* dari hash awal, menghasilkan *hash* baru, dilakukan terus menerus hingga jumlah *hash*ing yang dilakukan untuk menemukan nonce yang valid dan bergantung pada tingkat kesulitan. Semakin tinggi tingkat kesulitannya, semakin banyak percoba an *hash*ing yang diperlukan untuk menemukan *nonce* yang memenuhi syarat dan tingkat kesulitannya bisa diatur.

Block Index: 0 Timestamp: 1689702231 Data: Genesis Block Previous Hash: Hash: abf4ecc28b2af1a13768bbb19808e9af61a[illegible]c71de30a2d41b142c296d29f936a Nonce: 0
Block Index: 1 Timestamp: 1689702231 Data: S[illegible]×ul½"<±[illegible]NKê« Previous Hash: abf4ecc28b2af1a13768bbb19808e9af61abc71de30a2d41b142c296d29f936a Hash: 644c9c0987457fd83556b4469835e3653501cffae11f3364a7296a9c5b5d6ce3 Nonce: 0
Block Index: 2 Timestamp: 1689702231 Data: Žúxçß[illegible]Z¯H'¥[illegible]„s\o Previous Hash: 644c9c0987457fd83556b4469835e3653501cffae11f3364a7296a9c5b5d6ce3 Hash: 596c095ebcbf5d49092c63f48e8702160b6c747ff3941e744329027cd5436add Nonce: 00

Gambar 11 Hasil *Output Blockchain*

4. KESIMPULAN

Berdasarkan penjelasan dan uraian yang telah dibahas, maka dapat disimpulkan pada SDN Pasar Baru 3 dapat diimplementasikan aplikasi kriptografi pengamanan file berbasis web menggunakan algoritma *Advanced Encryption Standard* (AES-128) dengan *Blockchain*. Aplikasi berbasis *web* ini dapat membantu SDN Pasar Baru 3 dalam mengamankan *file* laporan bulanan sekolah. Program ini berhasil melakukan proses enkripsi dan dekripsi dan tidak mengubah ukuran pada file asli. Pengembangan aplikasi ini diharapkan dapat ditambahkan beberapa aksi pada tabel dekripsi seperti button hapus untuk langsung menghapus *file*. Penelitian selanjutnya diharapkan dapat dikembangkan sistem pengamanan pada metode blockchain dalam database.

DAFTAR PUSTAKA

[1] N. U. Baidoi, M. Hardjianto, and A. Wibowo, "Implementasi Algoritma Advanced Encryption Standard Untuk Pengamanan File Pada Smp Negeri 189 Jakarta Barat Implementation Of The Advanced Encryption Standard Algorithm For Securing Files At Smp Negeri 189 West," vol. 2, no. April, pp. 1–9, 2023.

[2] I. Rahim, N. Anwar, A. M. Widodo, K. Karsono Juman, and I. Setiawan, "Komparasi Fungsi Hash Md5 Dan Sha 256 Dalam Keamanan Gambar Dan Teks," *Ikraith-Informatika*, vol. 7, no. 2, pp. 41–48, 2022, doi: 10.37817/ikraith-informatika.v7i2.2249.

[3] D. Calista, A. Farissi, and M. D. Marieska, "Sistem Pengamanan Data Menggunakan Kriptografi AES dan Blockchain Berbasis Android," *J. JUPITER*, vol. 13, no. 2, pp. 220–226, 2021.

[4] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Inform.*, vol. 8, no. 1, p. 52, 2020, doi: 10.30864/eksplora.v8i1.139.

[5] L. Wikarsa, T. Suwanto, and C. Lengkey, "Implementasi Algoritma Konsensus Proof-of-Work dalam Blockchain terhadap Rekam Medis Implementation of Proof-of-Work Consensus Algorithm in Blockchain for Medical Records," *Jurnal_Pekommas_Vol._7_No._1*, vol. 2022, pp. 41–52, 2022, doi: 10.30818/jpkm.2022.2070105.

[6] U. Rahardja, Q. Aini, M. Yusup, and A. Edliyanti, "Penerapan Teknologi Blockchain Sebagai Media Pengamanan Proses Transaksi E-Commerce," *CESS (Journal Computer. Eng. Syst. Sci.*, vol. 5, no. 1, p. 28, 2020, doi: 10.24114/cess.v5i1.14893.

[7] D. Widyawan and I. 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, doi: 10.36080/skanika.v4i1.2216.

[8] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Inform. Mulawarman J. Ilm. Ilmu Komputer.*, vol. 10, no. 1, p. 20, 2019, doi: 10.30872/jim.v10i1.23.

[9] A. Eka Putri, A. Kartika dewi, 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.

[10] A. Nugrahantoro, A. Fadlil, and I. Riadi, "Optimasi Keamanan Informasi Menggunakan Algoritma Advanced Encryption Standard (AES) Mode Cipher Block Chaining (CBC)," *J. Ilm. FIFO*, vol. 12, no. 1, p. 12, 2020, doi: 10.22441/fifo.2020.v12i1.002.

[11] T. P. Utomo, "Implementasi Teknologi Blockchain Di Perpustakaan: Peluang, Tantangan Dan Hambatan," *Bul. Perpus.*, vol. 4, no. 2, pp. 173–200, 2022.

[12] B. E. Atmomintarso and W. Wirawan, "Sistem Pelaporan Pajak Pertambahan Nilai pada Web dengan Menggunakan Teknik Blockchain," *J. Tek. ITS*, vol. 10, no. 2, 2021, doi: 10.12962/j23373539.v10i2.65827.