INOTEK, Vol.8 Agustus 2024
ISSN: 2580-3336 (Print) / 2549-7952 (Online)
Url: https://proceeding.unpkediri.ac.id/index.php/inotek/

Sistem Keamanan Data Menggunakan Metode Base 64 Dan Salt

Diterima:
10 Juni 2024
Revisi:
10 Juli 2024
Terbit:
1 Agustus 2024

[1*]Ahmad Rifai, [2]Rini Indriati, [3]M. Najibulloh Muzaki
[1-3]Universitas Nusantara PGRI Kediri
[1]ahmadrifaiunpkediri@gmail.com,[2]rini.indriati@unpkediri.ac.id,
[3]m.n.muzaki@gmail.com

Abstrak— Abstrak ini menyajikan sistem keamanan data yang menggunakan metode Base 64 dan Salt untuk melindungi informasi sensitif. Base 64 digunakan untuk mengubah data agar dapat disimpan dan ditransmisikan secara aman, sementara Salt digunakan untuk meningkatkan keamanan password dengan menambahkan nilai acak. Penelitian ini mengevaluasi efektivitas metode tersebut dalam mengamankan data dari akses yang tidak sah atau pencurian. Hasilnya menunjukkan bahwa kombinasi Base 64 dan Salt mampu meningkatkan tingkat keamanan secara signifikan dibandingkan dengan metode enkripsi tunggal. Kesimpulan ini menekankan pentingnya penerapan teknologi keamanan yang kuat dalam sistem informasi untuk melindungi privasi pengguna dan keberlangsungan operasional.
Kata kunci—keamanan data; Base 64; Salt, enkripsi; privasi.

Abstract— *This abstract presents a data security system that uses Base 64 and Salt methods to protect sensitive information. Base 64 is used to transform data so that it can be stored and transmitted securely, while Salt is used to increase password security by adding random values. This research evaluates the effectiveness of these methods in securing data from unauthorized access or theft. The results show that the combination of Base 64 and Salt can significantly increase the level of security compared to a single encryption method. This conclusion emphasizes the importance of implementing strong security technologies in information systems to protect user privacy and operational continuity.*
Keywords*—data security; Base 64; Salt, encryption; privacy*.

Penulis Korespondensi:

Nama Penulis: Ahmad Rifai
Departemen Penulis: Sistem Informasi
Institusi Penulis: Universitas Nusantara PGRI Kediri
Email: ahmadrifaiunpkediri@gmail.com
ID Orcid: 0009-0003-0269-8342
Handphone: 081554445566

I PENDAHULUAN

keamanan menggunakan Base 64 dan salt sering kali mencakup pemahaman yang mendalam tentang kebutuhan akan teknologi enkripsi yang handal dalam mengamankan data sensitif. Dalam era digital ini, keamanan informasi menjadi perhatian utama di berbagai sektor, termasuk pendidikan, bisnis, dan pemerintahan. Teknik enkripsi seperti Base 64, yang mengubah data biner menjadi format teks ASCII, dan penggunaan salt sebagai tambahan nilai acak untuk menghasilkan enkripsi yang unik, telah terbukti efektif dalam melindungi data dari akses yang tidak sah.

Dengan fokus pada keamanan Base 64 dan salt bertujuan untuk mengatasi tantangan keamanan data yang semakin kompleks di berbagai lingkungan kerja. Pendahuluan dari pengabdian ini menggarisbawahi pentingnya mengamankan data karyawan dalam sistem HRMS atau sistem manajemen lainnya untuk melindungi informasi sensitif dari ancaman siber. Isu-isu terkait mencakup peningkatan insiden peretasan data dan kebutuhan akan perlindungan yang lebih kuat terhadap privasi individu.

Sebelumnya, beberapa penelitian telah mengkaji implementasi teknik enkripsi dalam konteks aplikasi dan keamanan data. Studi-studi ini memberikan wawasan yang berharga tentang penggunaan Base 64 dan salt dalam berbagai skenario, menyoroti tantangan dan solusi dalam implementasi teknologi ini untuk memastikan keamanan informasi yang efektif. Latar belakang ini memberikan konteks yang memadai untuk memahami pentingnya pengabdian ini dalam menjawab kebutuhan aktual dalam mengelola dan melindungi data sensitif secara efisien dan aman.

II METODE

Mengamankan data dalam sistem informasi menggunakan Base 64 dan salt, metode yang digunakan harus mencakup langkah-langkah teknis dari proses enkripsi dan dekripsi data. Pertama, metode ini akan memulai dengan menjelaskan proses input data karyawan oleh administrator melalui antarmuka aplikasi sistem informasi. Setelah data dimasukkan, langkah berikutnya adalah proses enkripsi menggunakan algoritma Base 64 yang diterapkan dengan salt yang unik untuk setiap data. Enkripsi ini bertujuan untuk mengubah data sensitif seperti NIK, nomor telepon, dan alamat email menjadi format yang tidak mudah dibaca secara langsung oleh pihak yang tidak berwenang.

Selanjutnya, setelah data terenkripsi, metode tersebut akan menggambarkan bagaimana data yang telah dienkripsi dikirimkan dan disimpan ke dalam database sistem. Di sini, penting untuk mencatat bahwa data yang tersimpan dalam database tetap dalam format terenkripsi untuk memastikan keamanan maksimal. Proses terakhir adalah ketika data tersebut didekripsi kembali saat diakses melalui aplikasi oleh pengguna yang berwenang, seperti administrator atau staf HR. Metode ini harus dijelaskan dengan detail untuk menunjukkan bagaimana sistem mengelola kunci enkripsi, mengintegrasikan proses enkripsi-dekripsi dengan fungsionalitas aplikasi, dan memastikan bahwa data hanya dapat diakses oleh pihak yang memiliki otorisasi yang tepat, sesuai dengan prinsip keamanan informasi yang baik.

Desain eksperimen untuk mengamankan data sistem informasi menggunakan Base 64 dan salt dapat dijelaskan sebagai berikut:

1. **Prosedur Eksperimen:**

- **Input Data Karyawan:** Eksperimen dimulai dengan administrator menginputkan data karyawan melalui antarmuka sistem informasi yang telah dirancang. Data yang dimasukkan meliputi NIK, nomor telepon, dan alamat email.
- **Enkripsi Data:** Sebelum data dimasukkan ke dalam database, sistem akan menerapkan proses enkripsi menggunakan Base 64 dengan tambahan salt yang dihasilkan secara acak. Langkah ini bertujuan untuk mengamankan data sensitif sebelum disimpan di dalam basis data.
- **Penyimpanan ke Database:** Data yang telah dienkripsi akan disimpan ke dalam basis data sistem. Penting untuk memastikan bahwa proses penyimpanan dilakukan dengan aman dan terstruktur sesuai dengan kebutuhan aplikasi.

2. **Survei dan Wawancara:**
   - **Survei Keamanan Sistem:** Untuk mengukur keefektifan sistem dalam mengamankan data, survei dapat dilakukan terhadap pengguna atau administrator. Survei ini bertujuan untuk mengumpulkan umpan balik tentang persepsi mereka terhadap tingkat keamanan data setelah implementasi sistem.
   - **Wawancara dengan Pengguna:** Wawancara dengan pengguna aplikasi, seperti administrator atau staf HR, dapat dilakukan untuk mendapatkan pandangan langsung tentang pengalaman mereka dalam menggunakan fitur keamanan data yang diimplementasikan.
3. **Karakteristik Pengamatan:**
   - **Pengamatan Keamanan Data:** Karakteristik utama pengamatan adalah proses enkripsi dan dekripsi data dalam aplikasi. Pengamatan ini melibatkan monitoring bagaimana sistem mengelola dan melindungi data sensitif dari akses yang tidak sah.
   - **Ketersediaan Data:** Penting untuk memantau ketersediaan data yang terdekripsi saat diakses melalui aplikasi, memastikan bahwa proses dekripsi berjalan dengan lancar dan data ditampilkan dengan akurat.

Dengan mengikuti desain eksperimen ini, penelitian dapat memvalidasi efektivitas sistem dalam menjaga keamanan data sensitif dalam aplikasi HRMS. Pendekatan ini juga memungkinkan untuk mengumpulkan bukti empiris tentang performa dan keamanan sistem, serta memperoleh masukan langsung dari pengguna tentang kepuasan mereka terhadap fitur keamanan yang telah diimplementasikan.

Table 4.1 Tabel Karyawan

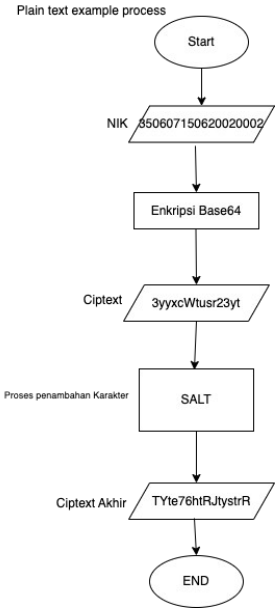
No	Field_name	Type	size	Description
1	Id_karyawan	int	4	Id_karyawan (Primery key)
2	Nik_karyawan	int	20	NIK Karyawan
3	Nama_karyawan	varchar	50	Data nama karyawan
4	Gmail_karyawan	varchar	50	Data gmail karyawan
5	No_hp	int	15	Data No HP Karyawan
6	Ttl_karyawan	varchar	100	Data Alamat Karyawan
7	Gaji_karyawan	varchar	20	Data Gaji Karyawan

Table 4.2 Gaji Karyawan

No	Field_name	Type	size	Description
1	Id_gaji	int	4	Id_gaji (Primery key)
2	Nik_Karyawan	varchar	25	NIK Karyawan

3	Nama_karyawan	varchar	50	Nama Karyawan
2	Jml_gaji	varchar	20	Jumlah Gaji

III HASIL DAN PEMBAHASAN



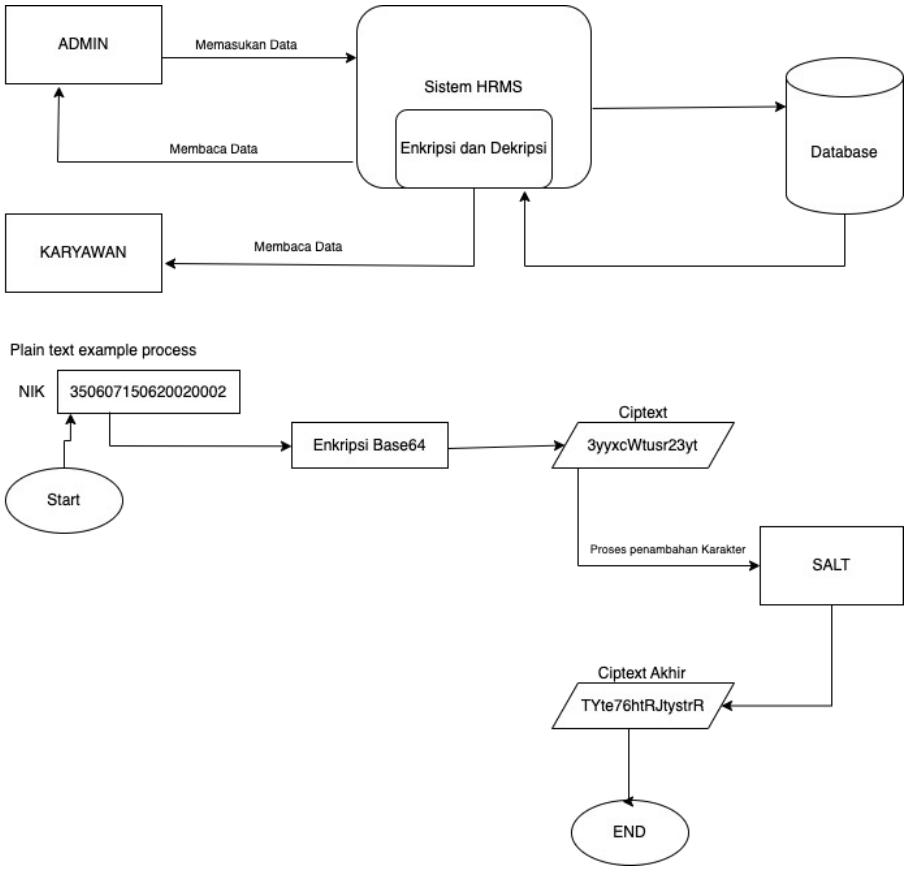
Gambar Flowchart Proses Engkripsi

Sistem keamanan data yang dikembangkan menggunakan metode Base 64 dan salt bertujuan untuk mengamankan informasi sensitif yang disimpan dalam sebuah database. Sistem ini dibangun dengan dua hak akses utama: admin dan karyawan. Admin memiliki kewenangan untuk memasukkan data karyawan setelah berhasil melakukan login dengan menggunakan username dan password yang telah terdaftar.

Proses Input Data oleh Admin

Setelah proses login berhasil, admin dapat memasukkan data karyawan ke dalam sistem. Data yang dimasukkan akan melalui proses enkripsi sebelum disimpan ke dalam database. Proses enkripsi dilakukan dengan menggunakan metode Base 64, yang memberikan tingkat keamanan tambahan dengan cara mengubah teks menjadi format yang sulit dibaca jika dilihat langsung.

Penggunaan Salt dalam Enkripsi



Gambar Proses Bisnis Sistem Keamanan Base 64 dan Salt

Sebelum proses enkripsi dilakukan, sistem menggunakan salt sebagai tambahan keamanan. Salt merupakan nilai acak yang ditambahkan ke data sebelum proses enkripsi dimulai. Hal ini membantu dalam meningkatkan kompleksitas hasil enkripsi dan mencegah serangan dengan teknik-teknik kriptografi yang sederhana.

Penyimpanan Data Terenkripsi dalam Database

Setelah data karyawan terenkripsi dengan menggunakan Base 64 dan salt, hasil enkripsi tersebut disimpan ke dalam database oleh sistem. Langkah ini memastikan bahwa data yang tersimpan dalam database tidak mudah diakses secara langsung tanpa melalui proses dekripsi yang tepat.

Tampilan Data pada Halaman Admin

Ketika admin ingin melihat data karyawan yang tersimpan, sistem akan melakukan proses dekripsi terlebih dahulu sebelum menampilkan informasi tersebut pada halaman admin. Proses dekripsi ini memastikan bahwa data yang ditampilkan dalam bentuk aslinya dan dapat dibaca dengan jelas oleh admin yang berwenang.

Pembahasan Aspek Baru dan Penting

1. **Penerapan Metode Base 64 dan Salt**: Penggunaan Base 64 sebagai metode enkripsi menambahkan lapisan keamanan yang cukup untuk melindungi data sensitif seperti

informasi karyawan. Penggunaan salt juga menjadi penting karena mempersulit proses dekripsi oleh pihak yang tidak berwenang.

2. **Proses Enkripsi Sebelum Penyimpanan**: Langkah untuk mengenkripsi data sebelum disimpan ke dalam database merupakan praktik terbaik dalam memastikan keamanan data. Dengan demikian, bahaya akses ilegal terhadap informasi sensitif dapat diminimalisir.
3. **Tampilan Data yang Didekripsi**: Meskipun data disimpan dalam bentuk terenkripsi, sistem mampu mengembalikan data ke bentuk aslinya ketika ditampilkan kepada admin. Hal ini menunjukkan bahwa keamanan tidak mengorbankan ketersediaan dan kegunaan informasi bagi pengguna yang sah.

Dengan mengimplementasikan sistem ini, organisasi dapat memastikan bahwa informasi sensitif mereka aman dari ancaman keamanan yang mungkin timbul, sambil tetap memberikan akses yang diperlukan kepada pihak yang berwenang.

IV KESIMPULAN

Berdasarkan berbagai penjelasan dan hasil penelitian yang telah dilakukan, mengenai cara mengamankan Data. Dapat disimpulkan beberapa hal, diantaranya:

Dengan diterapkannya cara pengamanan ini, Data dapat disamarkan. Hal tersebut dapat mengatasi serangan yang mengancam keamanan data pada suatu *Data*. Integritas dari Data yang telah dienkripsi akan lebih terjaga, karena metode *Base64* tidak dapat diterapkan pada Data yang telah dienkripsi.

DAFTAR PUSTAKA

[1] Rahardjo, Budi. (2001). Keamanan Sistem Informasi Berbasis Internet. Bandung: PT Insan Komunikasi

[2] Mukhtar, H. (2018). HRMSUntuk Keamanan Data. Bandung : Deepublish
Digdo, G. P. (2017). Panduan Audit Keamanan Komputer Bagi Pemula. Jakarta: Elex Media Komputindo.

[3] Gunawan, I. (2021). Keamanan Data: Teori Dan Implementasi . Sukabumi: Cv Jejak
Huda, M. (2020). Keamanan Informasi. Mandiri Nulis Buku. Hutahaean, J. (2017). Konsep Sistem Informasi. Bandung: Deepublish. Raharjo, B. (2017). Keamanan Informasi. Bandung : Pt Insan Infonesia.

[5] Susilo, A. (2010). Teknik Cepat Memahami Keamanan Kompuer Dan Internet. Jakarta: Elex Media Komputindo

[6] Sutabri, T. (2012). Konsep Sistem Informasi. Yogyakarta: Penerbit Andi.
Ditkaminfo, Ditjen Aptika, KEMKOMINFO. (2011). Panduan Keamanan Webserver. Jakarta. http:// publikasi.kominfo.go.id/handle/54323613/120

[7] Kurniawan, Yusuf. (2017). Kriptografi Keamanan Internet dan Jaringan Komunikasi. Bandung

[8] Sariasih, Christine. 2019. Rancangan Keamanan Data Sistem Smart Card Kesehatan Sesuai Kebutuhan di Indonesia. Fakultas Ilmu Komputer Universitas Indonesia.

[9] Stallings, William. 2003. Cryptography and Network Security : Principles and Practice. Prentice-Hall, New Jersey.

[10] Syaputra, Hendri dkk. 2012. Aplikasi Enkripsi Data pada File Text dengan Algoritma RSA. Jurusan Teknik Informatika, Sekolah Tinggi Teknik Musi, Palembang.

[11] Triorizka, Adrianus. 2010. Penerapan Algoritma RSA untuk Pengamanan Data dan Digital Signature dengan .Net. Sekolah Tinngi Manajemen Informatika dan Komputer AMIKOM, Yogyakarta.