Penerapan *Message Diggest Algorithm MD5* untuk Pengamanan Data Karyawan PT. Swifect Berbasis *Desktop*

Muhammad Rafiq Zayana ^{1*}, Iskandar Fitri ², Fauziah ³, Aris Gunaryati ⁴

¹ Program Studi Informatika, Fakultas Teknologi Komunikasi dan Informatika, Universitas Nasional.

^{2,3,4} Program Studi Sistem Informasi, Fakultas Teknologi Komunikasi dan Informatika, Universitas Nasional.

article info

Article history:

Received 23 July 2021

Received in revised form

4 September 2021

Accepted 2 October 2021

Available online July 2022

DOI:

<https://doi.org/10.35870/jti.k.v6i3.446>

Keywords:

Message Diggest Algorithm

MD5; Data Security;

Employee; Desktop.

abstract

In the era of Society 5.0, technological progress is unstoppable. Technological advances in the era of society 5.0 have become the main needs of humans in helping daily work. Technology is used as a medium for finding information to transportation tools that are integrated with the intervention of digital technology. Almost every company has technology to support their business development needs. And especially in agencies in this era, employee data is also processed using technology, but with the integration of employee data into technology, a lot of sensitive data must be protected in order to avoid misuse by irresponsible people. Therefore, the main objective of this research is to develop the application of the Message Diggest Algorithm (MD5) Cryptography Algorithm in employee data applications. This application is very appropriate to make it easier for companies to manage their employee data and ensure data security. To secure sensitive data from each employee, the process carried out is by encrypting each sensitive data so that it is not easy to read by others who have no interest or authority over the data. And the desktop-based application was made using Visual Basic. The research was carried out with two methods, namely the method to test the compilation speed of MD5 and to test the validation of the decrypted data from the MD5. And from the results of the study, the average speed of 500-515 milliseconds and data consistency obtained valid results from all tests.

abstrak

Pada era Society 5.0 ini kemajuan teknologi sudah tidak dapat terbendung lagi. Kemajuan teknologi di era society 5.0 ini menjadi kebutuhan utama manusia dalam membantu pekerjaan sehari-hari. Teknologi digunakan sebagai media mencari informasi sampai kepada alat transportasi yang terintegrasi dengan campur tangan teknologi digital. Hampir setiap perusahaan memiliki teknologi untuk menunjang kebutuhan dalam pengembangan bisnis mereka. Dan khususnya pada instansi-instansi pada era ini data para karyawan pun diolah dengan menggunakan teknologi, namun dengan terintegrasinya data karyawan terhadap teknologi, banyak data-data sensitive yang harus dilindungi untuk bertujuan menghindari hal-hal penyalahgunaan oleh orang-orang yang tidak bertanggung jawab. Oleh karena itu tujuan utama dari penelitian ini ialah mengembangkan penerapan Algoritma Kriptografi Message Diggest Algorithm (MD5) pada aplikasi data karyawan. Aplikasi ini sangat tepat untuk mempermudah perusahaan dalam mengelola data-data karyawannya dan keamanan datanya terjamin. Untuk mengamankan data-data sensitive dari setiap karyawan, maka proses yang dilakukan adalah dengan cara mengenkripsi setiap data sensitive sehingga tidak mudah untuk dibaca orang lain yang tidak memiliki kepentingan atau wewenang atas data tersebut. Dan Aplikasi berbasis desktop tersebut dibuat menggunakan Visual Basic. Penelitian dilakukan dengan dua metode yaitu metode untuk menguji kecepatan kompilasi dari MD5 dan menguji validasi data yang di dekripsi dari MD5 tersenit. Dan dari hasil peneliiian tersebut diperoleh kecepatan rata-rata 500-515 milisecond dan konsistensi data mendapatkan hasil yang valid dari seluruh pengujian.

*Corresponding author. Email: rafiqzayana@gmail.com!

© E-ISSN: 2580-1643.

Copyright © 2022. Published by Lembaga Otonom Lembaga Informasi dan Riset Indonesia (KITA INFO dan Riset) (<http://creativecommons.org/licenses/by/4.0/>).

1. Latar Belakang

Bekerja adalah salah satu upaya yang dilakukan manusia untuk bertahan hidup untuk memenuhi kebutuhan hidup untuk menunjang keberlangsungan hidup, dan bekerja adalah salah satu cara manusia untuk mengimplementasikan keterampilan yang dimiliki seseorang untuk ikut serta berkontribusi dalam melakukan pengembangan serta memecahkan masalah yang ada pada lingkungan, di negara Indonesia sendiri teknologi sudah mengintegrasikan terhadap seluruh perusahaan yang ada di Indonesia khususnya di pulau jawa, dimana pengolahan data karyawan perusahaan sudah menggunakan teknologi aplikasi untuk manajemen data karyawan. Namun pada era society 5.0 ini penginputan data harus bisa dilakukan secara digital serta data-data yang diinputkan meliputi data data pribadi yang sensitive apabila disalah gunakan akan berimbas baik secara langsung maupun tidak langsung terhadap korban. Maka dari itu Tujuan dari penelitian ini adalah mengembangkan Aplikasi Data Karyawan berbasis desktop untuk meningkatkan keamanan data, metode yang akan diimplementasikan untuk penerapan keamanan dalam aplikasi ini adalah menggunakan Metode Enkripsi Hash Kriptografi dari Message Diggest Algorithm (*MD5*). Ada banyak metode untuk upaya pengamanan data yang digunakan menggunakan hash atau enkripsi kriptografi. Salah satunya adalah dengan menenkripsi data teks atau angka yang akan dienkrpsi menggunakan Panjang 32 bit, 64 bit, 128bit, dan seterusnya.

Berdasarkan dari penelitian sebelumnya telah dilakukan penelitian terkait metode *MD5* untuk system pengamanan data pada aplikasi mobile menggunakan java dengan judul “Implementasi Algoritma *MD5*, SHA1, dan RC4 Untuk System Kriptografi Pada Aplikasi Mobile Internet Berbasis Java”. Yang bertujuan untuk menghasilkan *Fingerprint* dari proses enkripsi. Dan fingerprint yang dihasilkan akan bertujuan untuk menjaga konsistensi data yang dikirimkan [1]. Penelitian terkait juga dilakukan dengan judul “Pemanfaatan Enkripsi *MD5* Pada Keamanan Login Sistem Informasi Manufaktur PT.Maruki International Indonesia” yang terapkan sebagai system keamanan informasi dari perusahaan tersebut untuk keamanan login administrator menggunakan Enkripsi *MD5* yang menghasilkan chiphertext sepanjang 128 bit [2].

Metode keamanan data menggunakan *MD5* juga di implementasikan sebagai system keamanan data pada basis data pada penilitan yang berjudul “Studi Implementasi Pengamanan Basis Data Menggunakan Metode Enkripsi *MD5*” yang memiliki tujuan utama mengamankan data-data hak akses login yaitu keamanan data chiphertext yang meliputi pada data-data *user* dan *password* login menggunakan *MD5* yang telah melewati berbagai macam pengujian enkripsi hash menggunakan *MD5* [3].

Aplikasi keamanan menggunakan *MD5* juga di implementasikan dalam penilitan yang berjudul “Aplikasi Kriptografi Dengan Algoritma Message Diggest (*MD5*)” yang didalam aplikasi tersebut menerapkan sebuah aplikasi desktop untuk mengenkripsi data text menjadi sebuah text sepanjang 128 bit secara acak yang bertujuan agar data tersebut tidak mudah dibaca orang lain diluar otoritas aplikasi tersebut sehingga keamanan data tersebut dapat terjaga dan kosnsisten [4].

Implementasi enkripsi *MD5* untuk keamanan data dalam penelitian yang berjudul “Analisis Kinerja Kombinasi Algoritma Message Diggest Algorithm 5 (*MD5*), Rivest Shamir Andleman (RSA) Dan Rivest Chipher 4 (RC4) Pada Keamanan E-Dokumen” pada penelitian tersebut mengimplementasikan *MD5* sebagai pengamanan data e-dokumen menggunakan enkripsi *MD5*, yang bertujuan untuk melakukan penerapan serta pengujian kecepatan *MD5* dalam enkripsi data tersebut terhadap informasi yang terkandung dalam e-dokumen [5].

Dari berbagai macam penelitian yang sudah terpublikasikan, oleh karena itu sebagai penulis melakukan penelitian serta menjelaskan dari setiap tahap pembuatan Aplikasi Keamanan data Karyawan PT. Swifect menggunakan metode *MD5*. Metode *MD5* dipilih sebagai metode pengamanan data karena dapat mengamankan data teks secara acak sepanjang 32 sampai 128 bit didalam *database* melalui aplikasi desktop sehingga apabila kita masukkan data-data sensitive dari karyawan data tersebut akan terolah menjadi enkripsi *MD5* lalu tersimpan ke data base, sehingga pada saat memunculkan data pada aplikasi data terdekripsi dengan *MD5* sehingga data dapat dibaca dengan mudah di dalam aplikasi. Namun Ketika di dalam *database* data berisi teks acak menggunakan *MD5*. Pembuatan Aplikasi Data

Karyawan PT. Swifect menggunakan *software* Visual Studio 2019, Framework .net serta menggunakan *database* Mysql untuk menyimpan data.

Kriptografi

Kriptografi (cryptographi) merupakan kata yang berasal dari Bahasa Yunani: “*cryptos*” berarti “*secret*” (rahasia). Sedangkan “*graphein*” memiliki arti “*writing*” (tulisan). Sehingga kriptografi adalah “*Secret Writing*” (Tulisan rahasia). Kriptografi merupakan ilmu dan seni dalam menjaga kerahasiaan pesan yang disampaikan dengan cara menyandikan pesan tersebut ke dalam bentuk yang tidak dapat dimengerti maknanya. Teknik kriptografi merupakan Teknik pengamanan suatu pesan atau informasi awal (*plaintext*) dengan menggunakan kombinasi suatu kunci enkripsi yang telah ditentukan, sehingga dapat menghasilkan sebuah informasi baru (*chipertext*) yang sulit untuk dibaca tanpa melalui proses dekripsi. *Chipertext* dapat dikembalikan Kembali menjadi *plaintext* dengan metode dekripsi [6].

Enkripsi

Enkripsi merupakan salah satu Teknik dari kriptografi, yang berfungsi mengacak menggunakan suatu kunci dekripsi. Secara garis besar, proses enkripsi merupakan sebuah proses pengacakan teks atau naskah asli (*plaintext*) menjadi naskah acak (*chipertext*) yang dapat menyulitkan seseorang dalam membacanya apabila seseorang tersebut tidak mempunyai kunci dekripsi. Sulit dibaca dengan kata lain adalah probabilitas mendapatkan Kembali naskah asli membutuhkan waktu yang cukup lama dan membutuhkan kombinasi yang akurat sesuai dengan kunci. Apabila seseorang yang mempunyai kunci tersebut maka tidak membutuhkan waktu lama untuk melakukan dekripsi [7].

Visual basic

Visual basic merupakan sebuah Bahasa pemrograman yang dikembangkan oleh Microsoft dalam halnya Bahasa visual basic ini dapat menghasilkan aplikasi berbasis Desktop yang hanya support dengan platform windows saja [8].

Message Digest 5 (MD5)

MD5 adalah salah satu dari sekian banyak metode hash untuk enkripsi, dan merupakan proyek lanjutan dari MD4, Professor Ronald Rivest adalah orang yang mengembangkan metode MD5 pada tahun

1991. MD5 ini merupakan versi pembaruan dari MD4 dikarenakan algoritma MD4 dirasa sudah mudah untuk ditebak kuncinya dalam kata lain sudah mendapat pola pasti dari MD4 yang menyebabkan adanya serangan yang melemahkan algoritma MD4. Algoritma MD5 ini bekerja dengan cara menerima input informasi dengan ukuran yang tidak menentu setelah itu menkonversikan informasi tersebut menggunakan metode hash message digest berukuran 128 bit, yaitu adalah salah satu dari rangkaian 32 digit karakter hexadecimal. Proses kerja MD5 adalah memproses informasi asli pada satuan blok-blok input sebesar 512 bit yang diproses secara berulang-ulang [9].

Gambar 1. Gambaran dari cara kerja MD5

Operasi dasar MD5 pada gambar diatas dapat dituliskan dengan persamaan berikut [10] :

$$a \leftarrow b + CLS_s (a + g(b, c, d) + X[k] + T[i])$$

Dimana:

a, b, c, d	= Empat buah pengubah penyangga 32-bit (berisi nilai penyangga A,B,C,D)
g	= Salah satu fungsi F, G, H, I
CLS_s	= Circular left shift sebanyak s bit.
$X[k]$	= Kelompok 32-bit ke-k dari blok 512 bit message ke-q. Nilai k = 0 sampai 15.
$T[i]$	= Elemen table T ke-I (32 bit)
+	= Operasi penjumlahan modulo 2^{32} .

Secara garis besar proses MD5 dijabarkan sebagai berikut [11] :

- 1) Menambahkan bit pengganjal (*Padding Bits*)
- 2) Menambahkan nilai Panjang informasi semula
- 3) Masukkan pesan diolah dalam blok yang memiliki ukuran 512 bit
- 4) Inisiasi penyangga (*Buffer*).

- 4) Pengembangan (*Development*)
- 5) Pengujian (*Testing*)

2. Metode Penelitian

Metode yang diterapkan dalam penelitian serta pembuatan Implementasi MD5 pada aplikasi karyawan PT. Swifect adalah menggunakan dua metode yaitu metode Enkripsi dan Dekripsi MD5, dan metode pengembangan aplikasi tersebut menggunakan SDLC (*Software Development Life Cycle*).

Enkripsi

Enkripsi merupakan sebuah proses menyembunyikan informasi asli dalam pesan yang hasil akhirnya akan tetap konsisten setelah di dekripsi. Yang mana enkripsi adalah sebuah proses pengubahan plaintext menjadi ciphertext. Tujuan dari enkripsi ialah membuat kriptanalisis sesulit mungkin untuk mendekripsi text yang telah di enkripsi (ciphertext) menjadi plaintext Kembali [12] .

Dekripsi

Dekripsi merupakan sebuah proses mengubah ciphertext menjadi plaintext. Dalam kata lain dekripsi adalah proses untuk membuka pesan asli dari sebuah enkripsi yang dimana informasi tersebut merupakan informasi asli dari sebuah pesan [13].

Software Development Life Cycle

Pada pembuatan aplikasi untuk keamanan data MD5 PT. Swifect menggunakan metode *software development life cycle* yaitu SDLC (*Software Development Life Cycle*) yang terdiri dari 5 tahapan, diantaranya adalah merancang Perencanaan (*Planning*), Analisis Kebutuhan (*Requirements*), Analisis & SRS Desain (*Design and Analysis*), Pengembangan (*Development*), dan tahapan terakhir ialah proses pengujian (*Testing Process*). Berikut adalah beberapa tahapan dalam penelitian yang mengimplementasikan metode SDLC.

- 1) Perencanaan (*Planning*)
- 2) Analisis Kebutuhan (*Requirement*)
- 3) Analisis SYS dan Design (*Design and analysis*)

Gambar 2. Metode SDLC

Berikut merupakan tahapan-tahapan pada penelitian menggunakan metode SDLC:

- 1) Perencanaan (*Planning*)

Proses perencanaan sendiri merupakan Langkah awal dari proses pengembangan serta penelitian ini, dengan tujuan menentukan penelitian menggunakan metode MD5 sebagai pengamanan dari data aplikasi Karyawan berbasis desktop PT. Swifect.

Proses perancangan dilakukan dari hasil perbandingan dari studi literatur terhadap pengamanan MD5 untuk mengenkripsi data-data sensitive. Perencanaan yang telah ditentukan tersebut menggunakan metode MD5 dalam proses pengamanan data yang bertujuan untuk tidak mudah terbaca apabila *database* teretas.

- 2) Analisis Kebutuhan (*Requirement Analysis*)

Analisa kebutuhan yang dibutuhkan dalam mengembangkan *software* aplikasi karyawan PT. Swifect tersebut merupakan hasil dari perencanaan yang dibuat terstruktur agar hasil akhir dari pengamanan data dengan MD5 dapat terlaksana sesuai dengan tujuannya yaitu mengenkripsi data pada saat disimpan dalam *database* dan didekripsi Kembali di dalam aplikasi agar *user* mendapatkan isi utama dari data yang terenkripsi.

- 3) Analisis system dan desain (*Analysis SYS and Design*)

Proses Analisa system bertujuan untuk

memenuhi kebutuhan yang dibutuhkan dari pengembangan aplikasi karyawan PT. Swifect untuk tujuan pengamanan data, dan setelah mendapat inti atau ide pokok dari sebuah system tersebut secara fungsional dalam mengamankan data menggunakan MD5 serta menggunakan VB untuk proses pembuatan aplikasi tersebut dan *database* MYSQL. Tahap selanjutnya adalah mendesain aplikasi tersebut agar menarik dan nyaman pada saat digunakan.

4) Pengembangan (*Development*)

Proses pengembangan merupakan suatu tahap setelah proses desain dan analysis system. Yaitu merealisasikan hasil dari system analisis agar aplikasi tersebut dapat berjalan sesuai yang diharapkan dan dapat mengamankan data-data sensitive tersebut menggunakan md5 lalu aplikasi tersebut dapat mendekripsi data-data penting yang sudah di enkripsi dalam *database* untuk ditampilkan terhadap *user*. Tahapan development ini menggunakan sebuah Integrated Development Environment (IDE) yaitu Microsoft Visual Studio 2019 dan menggunakan framework .Net core 4.0.

5) Pengujian (*Testing*)

Setelah tahap pengembangan aplikasi maka dilakukanlah tahap pengujian yang bertujuan untuk memeriksa keakuratan dari proses perancangan dan pengembangan sesuai dengan tujuan utamanya, serta menguji GUI(*Graphics User Interface*) yang terdapat dalam aplikasi, dan memvalidasi agar tidak ada bug atau error pada aplikasi tersebut.

Kebutuhan Sistem

Untuk memenuhi serta mendukung seluruh kebutuhan proses pembuatan serta pengembangan aplikasi Karyawan PT. Swifect dan penerapan MD5 dalam enkripsi serta dekripsi data, tentunya membutuhkan perangkat yang mendukung serta memadai dari segi *software* (Perangkat lunak) serta dari sisi *hardware* (Perangkat Keras). Oleh karena itu diperlukan perangkat yang mendukung kedua aspek tersebut.

Tabel 1. Spesifikasi *Hardware* yang digunakan

Perangkat	Spesifikasi
Processor	Intel® Core™ i7-10750H Processor (12M Cache, up to 5.00 GHz)
RAM/Memory	8 GB
SSD/Hardisk	500GB

Tabel 2. Spesifikasi *Software* yang digunakan

Perangkat	Spesifikasi
System Operasi Microsoft Windows 10 Professional 64 bit	System operasi PC yang digunakan oleh peneliti untuk mengembangkan <i>software</i> tersebut
Microsoft Visual Studio 2019 64-bit	Merupakan <i>software</i> yang digunakan untuk mengembangkan suatu aplikasi atau bisa disebut IDE (<i>Integrated Development Environment</i>) dan dapat dijalankan di windows maupun linux/mac os.
.Net Framework	Framework dedicated dari Bahasa pemrograman VB untuk memudahkan kerangka kerja dalam mengembangkan <i>software</i> Pengamanan Data karyawan dan sebagai wadah dari <i>algoritma</i> MD5.
MYSQL	Berfungsi untuk menyimpan data dari aplikasi karyawan tersebut apabila data-data tersebut sudah dienkripsi dan sebagai tempat mengambil data untuk ditampilkan dalam aplikasi.
Adobe Illustrator	Media pembuatan desain interface serta pembuatan icon yang ada pada aplikasi.
Navicat	Berfungsi untuk memudahkan dalam membuat query sql terhadap aplikasi <i>MYSQL</i> dalam membuat table serta keperluan query lainnya.
Visual Paradigm	Pembuatan <i>flowchart</i> atau diagram alir dalam menggambarkan system yang dikembangkan menggunakan MD5.

3. Hasil dan Pembahasan

Flowchart

Flowchart atau diagram alir Digunakan untuk media untuk menggambarkan dalam penggunaan atau system aplikasi yang akan paparkan dengan *flowchart*. Berikut adalah diagram alir yang ada pada aplikasi PT. Swifect.

Gambar 3. *Flowchart* dari aplikasi karyawan PT. Swifect dan implementasi MD5

Penerapan GUI (Graphical User Interface)

Pada pengembangan serta perancangan aplikasi tersebut, dilakukan proses pembuatan GUI (interface). Berikut adalah tampilan GUI pada aplikasi karyawan PT. Swifect.

Login

Tampilan awal dari aplikasi PT. Swifect ialah Login yang juga terdapat logo PT. Swifect, pada login ini *user* diharuskan untuk melakukan proses autentifikasi berupa *user* dan *password* sebagai proses untuk memasuki GUI Menu utama. Proses autentifikasi *password* melalui proses enkripsi menggunakan MD5 untuk mencegah pengiriman *password* kedalam *database* tanpa adanya pengamanan data [14].

Gambar 4. Tampilan Login

Main Menu

Pada tampilan main menu terdapat 2 pilihan menu, yaitu *Input Data*, dan *Data karyawan*.

Gambar 5. Tampilan Main Menu

Input Data

Dalam menu *Input Data* yang akan ditampilkan dalam menu textbox yang berfungsi agar *user* memberikan masukkan data-data karyawan yang akan di input, pada tombol save data yang diinputkan akan dikonversikan menjadi data chiphertext menggunakan algoritma MD5 lalu data baru akan disimpan kedalam *database*. Dalam implementasi MD5 terhadap basis data tersebut dapat membantu system meningkat keamanan sehingga data atau informasi dalam *database* tidak mudah untuk dibaca [15].

Gambar 6. Gambar *Input Data*

Data Karyawan

Pada *Data Karyawan user* akan diberikan pilihan untuk mengupdate data yang sudah dipilih dalam menu list tersebut dan data akan Kembali tersimpan dengan MD5, lalu proses pengembalian data dari chiphertext menjadi plaintext Kembali Ketika *user* memilih data yang akan di update lalu data tersebut akan muncul dengan plaintext

Gambar 7. Gambar *Data Karyawan*

Pengujian aplikasi

Pada aplikasi karyawan PT. Swifect dilakukan dua pengujian aplikasi antara lain menggunakan perangkat PC yang spesifikasinya berbeda.

Tabel 3. Perangkat Penguji

Perangkat	Spesifikasi
Processor	Intel® Core™ i7-10750H Processor (12M Cache, up to 5.00 GHz)
RAM/Memory	8 GB
SSD/Hardisk	500GB

1) Pengujian Kecepatan Enkripsi

Pengujian berdasarkan kecepatan compile aplikasi terhadap MD5 dikarenakan waktu compile sangat penting untuk efisiensi waktu dan memberikan kenyamanan dan keamanan dalam menggunakan MD5.

Tabel 4. Pengujian Waktu Compile dengan banyak 1-16 karakter

Panjang Karakter	Spesifikasi	Waktu Kompile
1-16 Karakter	Intel Core i7-10750H, 8GB RAM, 500GB SSD	513.3719 ms
	Intel i3 5005U, 12GB RAM, 1tb HDD	500.2124 ms
	AMD A4-9125, 4GB RAM, 500GB	515.2207 ms

Tabel 5. Pengujian Waktu Compile dengan banyak 16-32 Karakter

Panjang Karakter	Spesifikasi	Waktu Kompile
16-32 Karakter	Intel Core i7-10750H, 8GB RAM, 500GB SSD	503.7456 ms
	Intel i3 5005U, 12GB RAM, 1tb HDD	500.6021 ms
	AMD A4-9125, 4GB RAM, 500GB	502.4845 ms

Tabel 6. Pengujian Waktu Compile dengan banyak 32-64 Karakter

Panjang Karakter	Spesifikasi	Waktu Kompile
32-64 Karakter	Intel Core i7-10750H, 8GB RAM, 500GB SSD	510.012 ms
	Intel i3 5005U, 12GB RAM, 1tb HDD	500.95 ms
	AMD A4-9125, 4GB RAM, 500GB	508.4985 ms

2) Pengujian Konsistensi Data

Tabel 10. Tabel Simulasi Waktu Compile

Tabel 7. Pengujian Konsistensi Data Dari Dekripsi MD5 Sebanyak 1-16 Karakter

Panjang Karakter	Spesifikasi	Waktu Kompilasi	Konsistensi Data	Spesifikasi	Simulasi waktu Compile		
					1-16 karakter	16-32 karakter	32-64 karakter
1-16 Karakter	Intel Core i7-10750H, 8GB RAM, 500GB SSD	510.012 ms	Valid	Intel Core i7-10750H, 8GB RAM, 500GB SSD	513.3719 ms	503.7456 ms	510.012 ms
	Intel i3 5005U, 12GB RAM, 1tb HDD	500.95 ms	Valid	Intel i3 5005U, 12GB RAM, 1tb HDD	500.2124 ms	500.6021 ms	500.95 ms
	AMD A4-9125, 4GB RAM, 500GB	508.4985 ms	Valid	AMD A4-9125, 4GB RAM, 500GB	515.2207 ms	502.4845 ms	508.4985 ms

Tabel 8. Pengujian Konsistensi Data Dari Dekripsi MD5 Sebanyak 16-32 Karakter

Panjang Karakter	Spesifikasi	Waktu Kompilasi	Konsistensi Data
16-32 Karakter	Intel Core i7-10750H, 8GB RAM, 500GB SSD	503.7456 ms	Valid
	Intel i3 5005U, 12GB RAM, 1tb HDD	500.6021 ms	Valid
	AMD A4-9125, 4GB RAM, 500GB	502.4845 ms	Valid

Tabel 9. Pengujian Konsistensi Data Dari Dekripsi MD5 Sebanyak 32-64 Karakter

Panjang Karakter	Spesifikasi	Waktu Kompilasi	Konsistensi Data
32-64 Karakter	Intel Core i7-10750H, 8GB RAM, 500GB SSD	503.7456 ms	Valid
	Intel i3 5005U, 12GB RAM, 1tb HDD	500.6021 ms	Valid
	AMD A4-9125, 4GB RAM, 500GB	502.4845 ms	Valid

Tabel 11. Tabel Simulasi Konsistensi Data

Spesifikasi	Simulasi Konsistensi Data		
	1-16 karakter	16-32 karakter	32-64 karakter
Intel Core i7-10750H, 8GB RAM, 500GB SSD	Valid	Valid	Valid
Intel i3 5005U, 12GB RAM, 1tb HDD	Valid	Valid	Valid
AMD A4-9125, 4GB RAM, 500GB	Valid	Valid	Valid

4. Kesimpulan

Berdasarkan hasil dari penelitian yang telah dilakukan, maka dapat disimpulkan:

- 1) Implementasi *MD5* terhadap aplikasi karyawan PT. Swifect. dirancang sebagai pengamanan data-data sensitive pada karyawan yang bertujuan untuk bila data diretas, peretas tidak dapat melihat data plaintext dari database yang di retas karena terenkripsi menggunakan metode *MD5*.
- 2) Pengujian dilakukan dengan 2 metode, yaitu diukur dari kecepatan kompilasi data dan konsistensi data yang di dekripsi. Pada kedua pengujian tersebut minimum 1-16 karakter dan pada karakter maksimumnya adalah 32-64 karakter. Rata-rata waktu kompilasi yang

didapatkan adalah diantara 500-515 milisecond.

- 3) Aplikasi dikembangkan menggunakan software IDE Visual Studio 2019 dengan .Net Framework. Aplikasi Karyawan PT. Swifect dengan implementasi MD5 untuk keamanan data dapat berjalan pada platform Microsoft / Windows.
- 5. Daftar Pustaka**
- [1] Ardyanto Pamungkas, 2006. Implementasi Algoritma MD5, Sha1, Dan RC4 Untuk Sistem Kriptografi Pada Aplikasi Mobile Internet Berbasis Java. URL: www.tcpdf.org.
 - [2] Layuk, N.S., 2017, August. Pemanfaatan enkripsi md5 pada keamanan login sistem informasi manufaktur pt. Maruki international indonesia. In *SISITI: Seminar Ilmiah Sistem Informasi dan Teknologi Informasi* (Vol. 5, No. 1).
 - [3] S. Bahri, Diana, and S. D. PS, 2012. Studi Dan Implementasi Pengamanan Basis Data Menggunakan Metode Enkripsi MD5 (Message-Digest Algorithm 5), *J. Ilm.*, Vol. 5(5), pp. 1–15.
 - [4] Sofwan, A. and Susanto, T., 2006. Aplikasi Kriptografi Dengan Algoritma Message Digest 5 (Md5). *Transmisi*, 8(1), pp.22-27.
 - [5] Sumarno, S., 2018. Analisis Kinerja Kombinasi Algoritma Message-Digest Algorithm 5 (MD5), Rivest Shamir Adleman (RSA) dan Rivest Cipher 4 (RC4) Pada Keamanan E-Dokumen. *Jurnal Sistem Informasi dan Ilmu Komputer Prima (JUSIKOM PRIMA)*, 2(1).
 - [6] Prasetyo, T.F. and Hikmawan, A., 2016. Analisis Perbandingan Dan Implementasi Sistem Keamanan Data Menggunakan Metode Enkripsi RC4 SHA Dan MD5. *Infotech J*, 2(1), p.236705.
 - [7] Hayati, N., Budiman, M.A. and Sharif, A., 2017. Implementasi Algoritma RC4A dan MD5 untuk menjamin Confidentiality dan integrity pada file teks. *Sinkron*, 1(2).
 - [8] Qashlim, A., 2016. Implementasi Algoritma MD5 Untuk Keamanan Dokumen. *Jurnal Ilmiah Ilmu Komputer Fakultas Ilmu Komputer Universitas Al Asyariah Mandar*, 2(2), pp.10-15.
 - [9] SUTARNO, S.R.A., Mulya, M. and Marieska, M.D., 2020. *Pengamanan Integritas dan Otentikasi Data Pelanggan pada Sistem PT. Pos Indonesia menggunakan Algoritma MD5* (Doctoral dissertation, Sriwijaya University).
 - [10] Pattiasina, T.J. and Lysandra, A., 2013. Studi Literatur Kriptografi Dengan Algoritma Message Digest 5 (MD5). *Teknika*, 2(1), pp.59-69.
 - [11] Zein, Z. and Adil, A., 2016. Aplikasi Media Bantu Pembelajaran Kriptografi Dengan Menggunakan Algoritma Message Digest 5 (MD5). *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, pp.45-51.
 - [12] Nasrudin, K., 2018. *Penerapan Enkripsi Data Menggunakan Metode Kolaborasi Message Digest Algorithm 5 (Md5) Dan Sha3 Dengan Salt Function Pada Sistem Informasi Penjualan Dan Pembelian* (Doctoral dissertation, UNNES).
 - [13] Ginting, A.B.C., 2017. Perbandingan Algoritma Message Digest 5 (MD5) dan SHA256 pada Hashing File Dokumen. *J. Tek. Inform. Kaputama*, Vol 1 (1), pp. 50–61.
 - [14] Khairina, D.M., 2016. Analisis Keamanan Sistem Login. *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer*, 6(2), pp.64-67.
 - [15] Sibyan, H., 2017. Implementasi Enkripsi Basis Data Dengan Algoritma Md5 (Message Digest Algorithm 5) dan Vigenere Cipher. *Jurnal Penelitian dan Pengabdian Kepada Masyarakat UNSIQ*, 4(1), pp.114-121.