Jurnal Widya
Volume 4, Nomor 1, April 2023: halaman 87-96
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id / editor.jurnalwidya@gmail.com

P-ISSN: 2746-5411
E-ISSN: 2807-5528

Pengembangan Aplikasi Keamanan Data Agen Kapal Dengan Menggunakan Metode MD5 Berbasis Web

Development Of Ship Agent Data Security Application Using Web-Based MD5 Method

Rini Oktari Batubara

[1]*Fakultas Informatika Universitas Potensi Utama*
[1]*Universitas Potensi Utama, K.L. Yos Sudarso KM 6,5 No. 3ATj. Mulia - Medan*

Email : rini.admmedan@gmail.com

Received: 17 Februari 2023, **Revised:** 08 April 2023, **Accepted:** 14 April 2023

ABSTRAK

Di Kantor Distrik Navigasi Kelas I Belawan Bagian yang terkait dengan agel kapal adalah perwakilan kapan yang ditambahkan di pelabuhan dengan menyerahkan PNBP (Penerimaan Negara Bukan Pajak) ke Kantor Distrik Navigasi Kelas I Belawan. Keuntungan Keselamatan kapal dalam linntar dan lintas kapal di daerah tertentu. Masalah yang saya temui di Kantor Kecamatan Navigasi Kelas I Belawan adalah saya memiliki data agen kapal yang berisi ID agen, tetapi karena keamanan data tidak diterapkan maka informasi dalam data tersebut dapat bocor. Ini mengkhawatirkan nama pemilik data agen kapal. Ia takut identitasnya diambil alih oleh orang lain.

Kata Kunci: Kantor Distrik Navigasi Kelas I Belawan, Data Agen

ABSTRAK

At the Belawan Class I Navigation District Office, the part related to ship agent is the representative of ships moored at the port by submitting PNBP (Non-Tax State Revenue) to the Belawan Class I Navigation District Office. ship safety advantages in the passage and passage of ships in certain areas. The problem I encountered at the Belawan Class I Navigation District Office was that I had ship agent data containing the agent ID, but because data security was not implemented, the information in the data could be leaked. This concerns the name of the data owner, the ship's agent. He is afraid that his identity will be taken over by someone else.

Keyword: Belawan Class I Navigation District Office, Agent Data

Jurnal Widya
Volume 4, Nomor 1, April 2023: halaman 87-96
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id / editor.jurnalwidya@gmail.com
P-ISSN: 2746-5411
E-ISSN: 2807-5528

1. Pendahuluan

Menjaga kerahasiaan suatu data merupakan hal yang sangat penting untuk dilakukan, maka dari itu keamanan informasi dapat menjadi hal yang sangat penting, yang tentunya dapat menimbulkan kenyamanan kepada pemiliknya. Data berisi informasi penting sangat mudah diretas jika tidak adanya keamanan yang diterapkan. Salah satu alternatif yang dapat dilakukan untuk menjaga kerahasiaan informasi tersebut adalah dengan menyamarkan menjadi bentuk tersandi yang tidak bermakna, hal tersebut dapat dilakukan dengan kriptografi.

Pada Kantor Distrik Navigasi Kelas 1 Belawan merupakan bagian memiliki kaitan dengan Agen kapal yang merupakan sebuah perwakilan suatu kapal yang akan berhenti di suatu pelabuhan dengan membayar PNBP (Penerimaan Negara Bukan Pajak) pada Kantor Distrik Navigasi Kelas 1 Belawan untuk menjamin kepentingan dan keselamatan pelayaran kapal pada alur dan perlintasan kapal di wilayah tertentu.

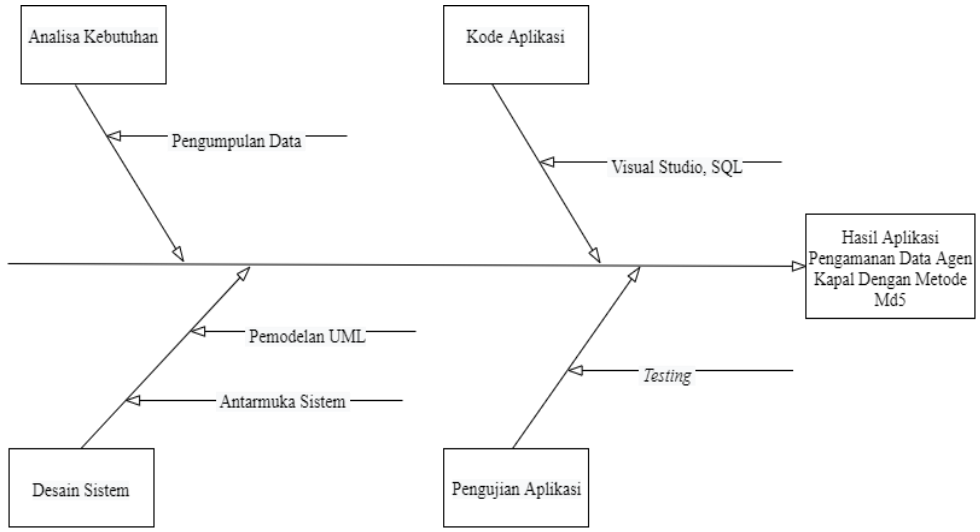
Permasalahan sedang terjadi di Kantor Distrik Navigasi Kelas 1 Belawan terdapat pada data agen kapal didalamnya memuat identitas agen, akan tetapi belum diterapkan keamanan data sehingga informasi didalam data tersebut bisa jadi mengalami kebocoran data. Hal ini memuat pemilik data tersebut yaitu nama agen kapal menjadi tidak merasa aman karena merasa cemas identitas mereka diambil oleh orang lain. Selain itu data agen kapal tersebut masih ditulikan didalam sebuah buku, dimana bisa saja buku tersebut hilang, rusak, atau dengan mudah dicuri oleh orang lain.

Dari permasalahan tersebut penulis berharap dapat membantu mengamankan data agen sehingga setiap agen merasa aman dan tidak perlu cemas lagi karena identitas mereka tetap aman dan dapat membantu kerja pegawai agar lebih efektif serta efisien. Oleh karena itu penulis bertekad mengangkat judul “Pengembangan Aplikasi Keamanan Data Agen Kapal Dengan Menggunakan Metode Md5 Berbasis Web”

Jurnal Widya
Volume 4, Nomor 1, April 2023: halaman 87-96
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id / editor.jurnalwidya@gmail.com
P-ISSN: 2746-5411
E-ISSN: 2807-5528

2. Metodologi Penelitian.

Langkah-langkah yang diperlukan untuk mencapai tujuan perancangan dapat dilihat pada *diagram fishbone* gambar 1.



Gambar I. Diagram *FishBone* Pengembangan Aplikasi Kemanan Data Agen Kapal Dengan Menggunakan Metode Md5 Berbasis Web

Informasi dalam diagram grafik *Fishbone* adalah sebagai berikut :

1. Analisa Kebutuhan.

Setelah melalui tahap proses perancangan, tahap selanjutnya adalah analisis kebutuhan yaitu yang dibutuhkan untuk merancang sistem sebagai perangkat lunak, yaitu PHP digunakan untuk merancang aplikasi Perencanaan untuk perangkat keras seperti komputer atau laptop yang dibutuhkan untuk membangun aplikasi.

2. Desain System.

Pada tahap ini dibangun sebuah *Design* sistem dari suatu aplikasi keamanan data agen kapal dengan menggunakan metode MD5. Penulis menggunakan pemodelan UML yaitu *use case diagram, class diagram, activity diagram* dan *sequence diagram* untuk perancangan sistem.

Jurnal Widya
Volume 4, Nomor 1, April 2023: halaman 87-96
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id / editor.jurnalwidya@gmail.com
P-ISSN: 2746-5411
E-ISSN: 2807-5528

3. Penulisan Kode Aplikasi.

Pada tahap ini rancang bangun aplikasi keamanan data agen kapan dengan metode MD5 dituangkan kedalam bahasa pemprograman dan mulai dibangun menggunakan visual studio code untuk menghasilkan sebuah aplikasi sesuai dengan perancangan.

4. Pengujian Aplikasi.

Pada tahap ini dilakukan pengujian aplikasi keamanan data agen kapal menggunakan metode MD5 secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan aplikasi. Pengujian fungsional dilakukan untuk mengetahui bahwa aplikasi keamanan data agen kapal menggunakan metode MD5 telah berjalan sesuai dengan perancangan.

5. Hasil.

Pada tahap ini akan diambil kesimpulan dari perancangan aplikasi keaamanan data agen kapal menggunakan metode MD5 yang telah dihasilkan, seperti apa saja kelebihan dan kekurangan dari apikasi perancangan aplikasi keamanan data agen kapal menggunakan metode MD5. Sehingga didapatkan kesimpulan untuk menambahkan fungsi-fungsi tertentu sesuai dengan kebutuhan kedalam aplikasi.

3. Hasil dan Pembahasan.

3.1. Analisis Masalah.

Pada saat ini kantor distrik navigasi kelas I Belawan masih memiliki Sistem secara manual, dimana agen kapal yang datang ke kantor tersebut mengurus data tamu kedatangan kapal masih dituliskan kedalam buku besar dan diletakkan begitu saja tanpa adanya pengawasan yang ketat, hal ini akan menjadi kekhawatiran yang bisa saja membuat buku tersebut hilang, rusak, atau dengan mudah dicuri oleh orang lain dan memanipulasi data-data yang ada dibuku tersebut dan dalam sistem kerja nya menjadi tidak efektif dan efisien.

Untuk menjaga kamanan suatu data dari ancaman yang dijelaskan diatas, maka diperlukan suatu aplikasi pengamanan dengan memverifikasi data *file* agar terhindar dari gangguan oknum yang tidak bertanggung jawab. Sehingga oknum yang tidak bertanggung jawab tidak dapat mengetahui isi *file* tersebut. Dalam penlitian ini sistem yang akan dibangun adalah mengubah *file* yang terdapat didalam sebuah *file* kedalam bentuk yang tidak dapat dikenali agar kerahasiaannya dapat terjaga. Oleh karena itu salah satu metode yang akan digunakan dalam keamanan verifikasi *password* pada suatu data *file* ini adalah menggunakan metode MD5 atau *message-Digest* algoritma MD5.

Jurnal Widya
Volume 4, Nomor 1, April 2023: halaman 87-96
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id / editor.jurnalwidya@gmail.com
P-ISSN: 2746-5411
E-ISSN: 2807-5528

3.2. Penerapan Metode.

Penerapan algoritma *message Digest5* (MD5) pada pengamanan data agen kapal pada kantor Distrik Navigasi Kelas I Belawan, ini akan mengenkripsi sebuah data agen kapal dan disimpan didalam system yang didalamnya menerapkan keamanan MD5. Sebelum mengenkripsi plaintext, pertama-tama kita perlu mengetahui berapa banyak fungsi hash yang dapat digunakan sebagai kunci untuk mengenkripsi pesan. Perhitungan algoritma MD5 ada;ah sebagai berikut :

1. Tentukan teks yang akan di Hash.
   Teks (String) : Teknik.
   Teks (Hex) :74 65 6b 6e 69 6b.
2. Tambahkan bit pesan yang ditambahkan dengan bit blok hingga kongruen dengan 448 modulo 512 bit.
   Pesan : 74 65 6b 6e 69 6b
   Pesan terdiri dari 6 karakter atau 6 byte= 6 x 8 = 48 bit,
   Maka diperlukan 448 – 48 = 400 bit.
3. Bit terakhir 64 bit diisi dengan nilai panjang pesan, dimana panjang pesan adalah 6 byte = 6 x 8 = 48 bit atau dalam Hex = 30.
4. Pemprosesan pesan dalam blok 16 kata pada MD5 juga mengandung 4 fungsi nonlinear yang masing – masing digunakan pada setiap operasi, yaitu :
   F (X,Y,Z)=XY v not (X) ZG (X,Y,Z) = XZ v Y langkah (Z) H(X,Y,Z) = X x r Y x rZ I(X,Y,Z) = Y x r (Xv langkah (Z)) Pemprosesan pesan dilakukan dalam 4 putaran, setiap putaran dilakukan 16 kali operasi dasar, sebagai berikut : Loop (1,16) A = 2249092517 dalam Hex = 860E6DA5 B = 2931300306 dalam heksadesimal = AEB817D2 C = 712877834 dalam heksadesimal = 2A7DA70A D = 229885237 dalam Hex = 0DB3C535 Round (2,16) A = 3914487489 dalam Hex = E95256C1 B = 2441348034 dalam Hex = 918403C2 C = 3652998760 dalam heksadesimal = D9BC5668 D = 27302740 dalam Hex = 01AFDD94 Putaran (3,16) A= 4131823715 dalam Hex = F646A063 B = 3065820097 dalam Hex = B6BCB3C1 C = 1815224134 dalam Hex = 6C321F46 D = 73124886 dalam Hex = 045BCC16 Putaran (4,16) A = 1331224407 dalam Hex = 4F58DF57 (AA) B = 2605068873 dalam Hex = 9B463249 (BB) C = 3006515519 dalam Hex = B333C93F (CC) D = 2079023797 dalam Hex = 7BEB62B5 (DD).
5. Inisialisasi Buffer / MD5 Buffer.
   Dalam perhitungan ini menggunakan buffer (dalam Hex) :
   A = 67452301.
   B = efcdab89.
   C = 98badcfe.
   D = 10325476.
   Hasil Akhir dari pemprosesan pesan dengan 4 putaran kemudian ditambahkan ke nilai buffer MD5 :
   A = A + AA
   B = B + BB
   C = C + CC

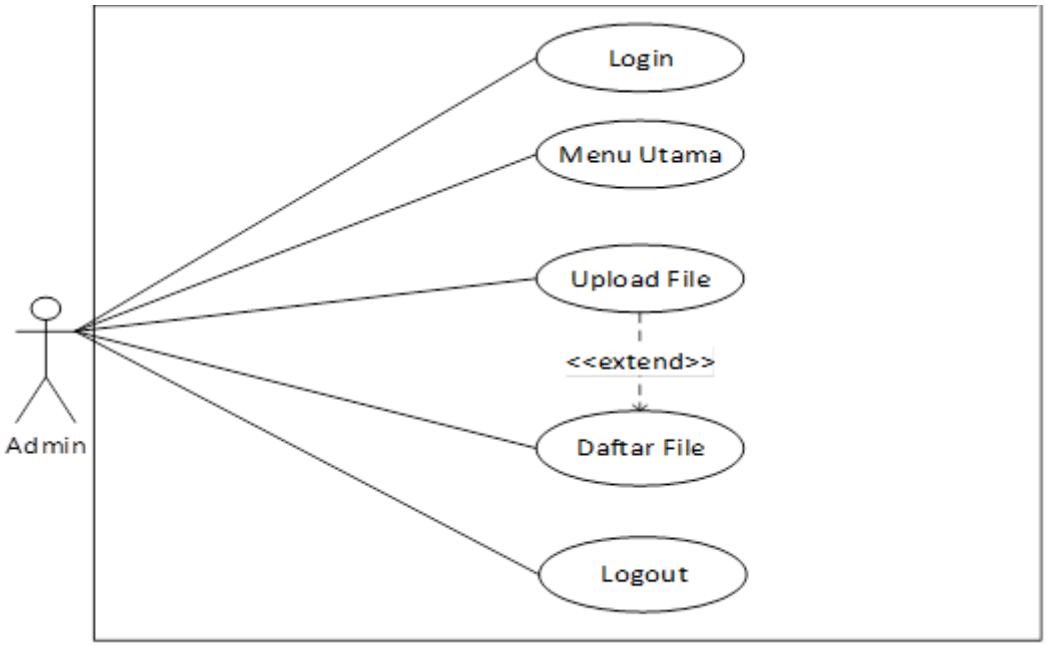
Jurnal Widya
Volume 4, Nomor 1, April 2023: halaman 87-96
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id / editor.jurnalwidya@gmail.com
P-ISSN: 2746-5411
E-ISSN: 2807-5528

D = D + DD
Hasil
A = 3063808600 dalam Hex = B69E0258
B = 2333334994 dalam Hex = 8B13DDD2
C = 1273931325 dalam Hex = 4BEEA6D3
D = 2350757675 dalam Hex = 8C1DB72
Nilai Pesan pertama adalah 58, pesan kedua adalah 02, pesan ketiga adalah 9E, dan seterusnya. Di urutkan di tabel sampai mendapatkan 32 karakter dari pesan MD5 yaitu "58029EB6D2DD138B3DA6EE4B2BB71D8C".

3.3. Desain Sistem.

1. *Use Case Diagram.*

Diagram use case menggambarkan aktor, use case, dan hubungannya sebagai urutan tindakan yang memberikan nilai terukur kepada aktor. Sebuah use case direpresentasikan dengan elips horizontal pada use case diagram UML, yang dapat dilihat pada Gambar 2:



Gambar 2. *Use Case Diagram*

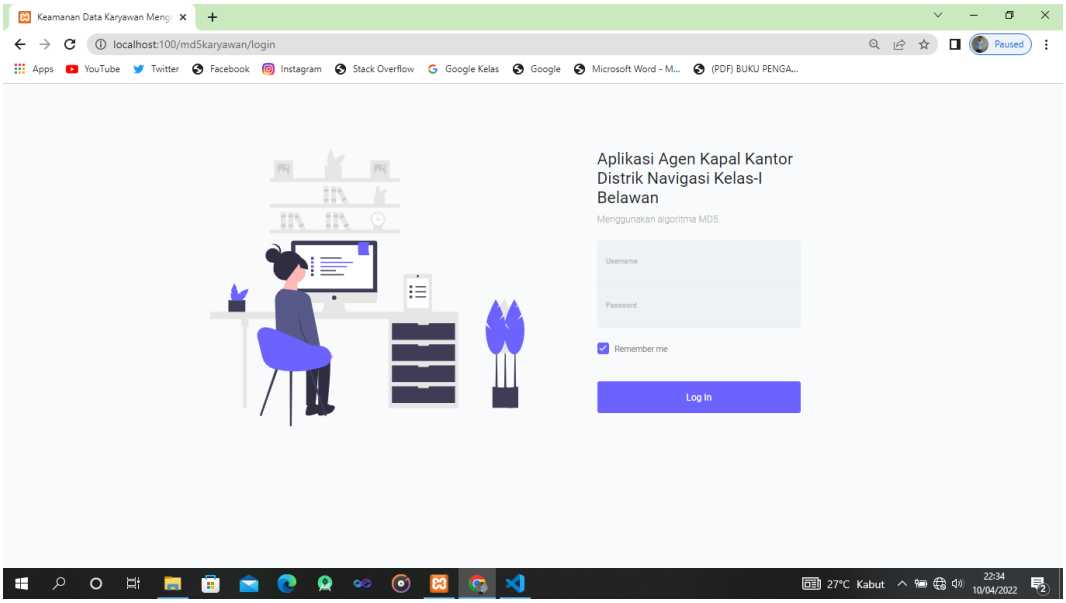
3.4. Tampilan Desain.

Aplikasi Pengembangan Aplikasi Keamanan Data Agen Kapal Dengan Menggunakan Metode MD5 Berbasis Web dalam mengamankan sebuah data *file*.

3.4.1. Tampilan Form Desain.

Form Login adalah antarmuka program untuk metode MD5, dimana dengan menggunakan aplikasi ini Anda dapat melalui antarmuka form login. dapat dilihat pada 3. di bawah ini :

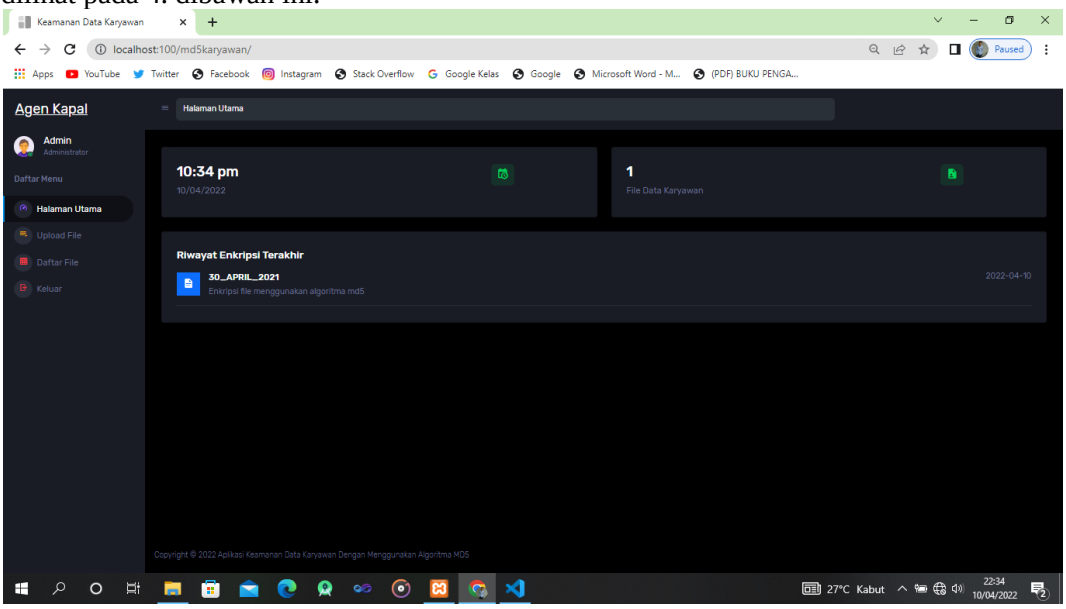
Jurnal Widya
Volume 4, Nomor 1, April 2023: halaman 87-96
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id / editor.jurnalwidya@gmail.com
P-ISSN: 2746-5411
E-ISSN: 2807-5528



Gambar 3. Tampilkan Form Login

3.4.2. Menampilkan Form Menu Utama.

Form utama adalah antarmuka global dari program kriptografi. Untuk menggunakan aplikasi kripto ini Anda dapat melalui antarmuka formulir utama. Untuk lebih jelasnya tampilan form utama dapat dilihat pada 4. dibawah ini.

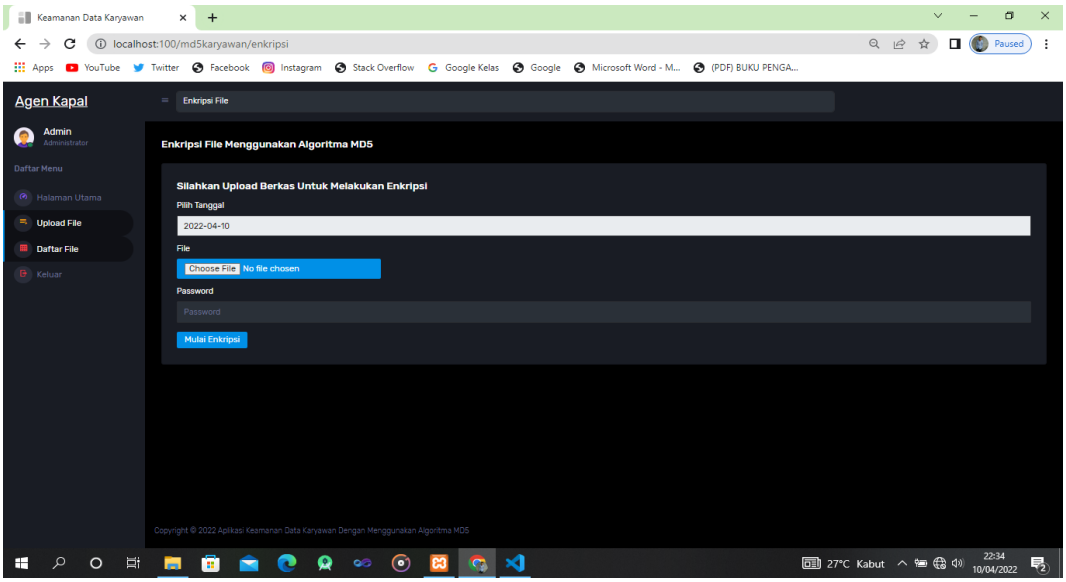


Gambar 4. Tampilan Form Utama

Jurnal Widya
Volume 4, Nomor 1, April 2023: halaman 87-96
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id / editor.jurnalwidya@gmail.com
P-ISSN: 2746-5411
E-ISSN: 2807-5528

3.4.3. Tampilan Form Upload File.

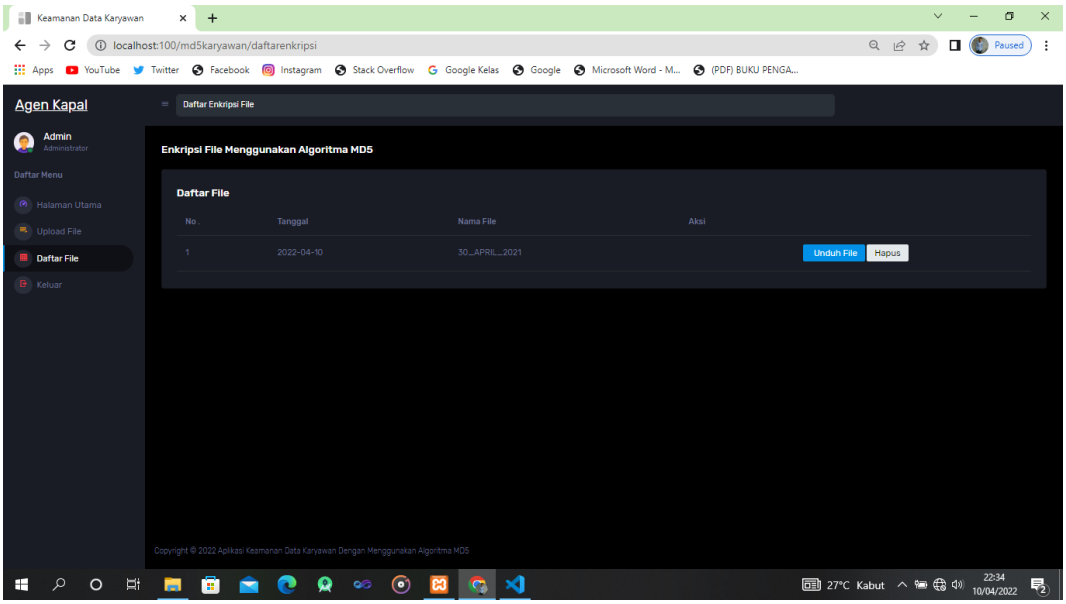
Formulir Unggah file ini digunakan untuk menyimpan konten file data menggunakan enkripsi kata sandi. Berikut adalah rendering form upload file, yang dapat dilihat pada Gambar 5 di bawah ini:



Gambar 5. Tampilan Form Upload File

3.4.4. Tampilan Form Daftar File.

Form daftar file ini berfungsi untuk melihat data bentuk *file* yang sudah terenkripsi *password.* Berikut ini tampilan *form* daftar *file* dapat dilihat pada gambar 6. berikut ini:



Gambar 6. Tampilan *Form* Daftar *File*

Jurnal Widya
Volume 4, Nomor 1, April 2023: halaman 87-96
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id / editor.jurnalwidya@gmail.com
P-ISSN: 2746-5411
E-ISSN: 2807-5528

Setelah melakukan uji coba terhadap sistem, maka dapat disimpulkan hasil yang didapatkan yaitu :

Tabel 1. Hasil Uji Coba

No	Skenario Pengujian	Hasil yang diharapkan	Hasil Pengujian	Kesimpulan
1	Klik Home	Aplikasi memproses Menu dan akan muncul *sub menu*	Sesuai dengan yang diharapkan	*Valid*
2	Klik *Upload File*	Ketika menu *upload file* dan akan muncul *form* menu *file* yang mau di enkripsi	Sesuai dengan yang diharapkan	*Valid*
3	Klik Daftar *File*	Ketika menu daftar file, maka akan mucul daftar *file* yang sudah dienkripsi *password*	Sesuai dengan yang diharapkan	*Valid*
4	Klik Keluar	Keluar pada sistem	Sesuai dengan yang diharapkan	*Valid*

Kelebihan sistem yang dapat diambil dari sistem keamanan data menggunakan algoritma MD5 adalah :

1. Sistem bawaan dapat mengamankan data file dan konten file dengan sistem enkripsi kunci algoritma MD5.
2. Sistem telah dibangun dengan kemampuan mengamankan data kunci.
3. Sistem yang dibangun mempunyai tampilan yang sangat sederhana dan mudah digunakan oleh user.

Adapun kekurangan – kekurangan sistem yang dapat disimpulkan dari sistem keamanan data file menggunakan algoritma MD5 ini adalah :

1. Dalam menggunakan kata kunci pada sistem yang dibangun, tidak boleh ada huruf yang sama didalam kata kunci. Hal ini dapat menyebabkan saat pemilihan kata-kata kunci, user tidak bebas membuat kata kunci sesuai dengan keinginan user.
2. Hasil proses enkripsi dengan sistem yang dibuat masih menghasilkan data yang sama.
3. Gambar yang akan di enkripsi masih terbatas. Apabila melebihi karakter yang sesuai dengan dengan sistem, maka plaintext tidak bisa dikembalikan keaslinya.

Jurnal Widya
Volume 4, Nomor 1, April 2023: halaman 87-96
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id / editor.jurnalwidya@gmail.com
P-ISSN: 2746-5411
E-ISSN: 2807-5528

4. Kesimpulan.

Berdasarkan pembahasan dari bab-bab sebelumnya yang telah dilakukan maka dapat diambil beberapa kesimpulanm sebagai berikut :

1. Sistem berhasil mengamankan Data Agen Kapal Pada Kantor Distrik Navigasi Kelas I Belawan dengan menggunakan metode penguncian MD5, sehingga tidak dapat dibuka oleh siapapun.
2. Dengan menggunakan pemprograman *php* maka dapat menghasilkan Aplikasi Keamanan data *file* dengan menggunakan metode penguncian MD5 berbasis web.
3. Aplikasi yang dibangun dapat mengamankan data file.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Universitas Potensi Utama yang telah memberikan kesempatan pada penulis agar menyelesaikan karya ilmiah ini. Penulis berharap karya ilmiah dapat diambil ilmu dan manfaatnya.

Daftar Pustaka

[1] Sikumbang, A.H., Haryanto, E.V., & Saleh, A., 2020. Kombinasi antara stream cipher dan Caesar cipher dalam mengamankan data kredit pelanggan (Studi Kasus: PT. ACE HARDWARE). Koran FTIK. Penerbangan. 1, n° 1, hlm. 693-706.

[2] D. A. Pratama and H. Kurniawan, "Aplikasi Keamanan Teks SMS Menggunakan Metode Stream Cipher, ROT13, Dan Caesar Cipher Berbasis Android," *J. FTIK*, vol. 1, no. 1, pp. 274–282, 2020, [Online]. Available: http://e-journal.potensi-utama.ac.id/ojs/index.php/FTIK/article/view/864.

[3] M. Zulham, H. Kurniawan, and I. F. Rahmad, "Perancangan Aplikasi Keamanan Data Email Menggunakan Algoritma Enkripsi RC6 Berbasis Android," *Semin. Nas. Inform.*, pp. 96–101, 2014.

[4] Nugroho, A.Y., 2017. Membuat aplikasi kriptografi berbasis algoritma Base64 Menggunakan PHP untuk mengamankan data teks, Séminaire national sur l'informatique. halaman 134-139.

[5] Y. Yusfrizal, "Perancangan Aplikasi Kriptografi In-Text Menggunakan Metode Reverse Encryption dan Rsa Berbasis Android", J. Tek. informasi. Kapten, penerbangan. 3, tidak. 2, hal. 29-37 2019.

[6] Prasetio, Y., Triandi, B. dan Hardianto, 2018. Merancang aplikasi keamanan file teks dengan skema hybrid menggunakan algoritma Enigma dan algoritma RSA. Majalah komputer. Penerbangan. 6, Tidak. 1, hal. 46-55.

[7] R. N. Sari, I. Lazuly, and D. Daifiria, "Implementasi Algoritma Merkle Hellman Dalam Mengamankan Pesan Teks," *Infosys (Information Syst. J.*, vol. 6, no. 1, p. 93, 2021, doi: 10.22303/infosys.6.1.2021.93-102.

[8] Mashuri, "Implementasi Sistem Database Terdistribusi Dengan Metode Partial Replication," *Akad. Manaj. Inform. Komput. Selatpanjang*, vol. 3, 2020.

[9] M. Danny, "Perancangan Sistem Informasi LPPM pada STMIK Cikarang berbasis Web Menggunakan Database Mysql," *J. Chem. Inf. Model.*, vol. 12, no. 4, pp. 90–96, 2017.