jurnalteknik.unisla.ac.id/index.php/informatika
JOUTICA Volume 7 No.2 Tahun 2022

ISSN: 2503-071X
E-ISSN: 2621-511X

PENERAPAN ALGORITMA MESSAGE DIGGEST ALGORITHM 5 PADA LOGIN SISTEM INFORMASI MANAGEMEN RUMAH SAKIT

Amir Ali[1], Eka Wilda Faida[2]
Stikes Yayasan Rumah Sakit Dr.Soetomo
Kalidami 12-14 Surabaya
(031) 59181757
Email: amir_ali@stikes-yrsds.ac.id[1], eka-wilda@stikes_yrsds.ac.id[2]

ABSTRAKS

Aplikasi SIMRS (Sistem Informasi Managemen Informasi Rumah Sakit) belum menerapkan proses enkripsi akun untuk masing-masing pengguna di masing-masing unit kerja. Hal ini terjadi karena aplikasi SIMRS belum difasilitasi dengan kemampuan enkripsi akun untuk tiap pengguna. Hal ini didukung dengan hasil survey awal dengan survey kuesioner kepada petugas kesehatan pengguna SIMRS di Rumah Sakit Surabaya Medical Service dimana sebanyak 66,7 % mengatakan belum ada metode khusus dalam login ke aplikasi SIMRS dan sebanyak 77,8 % mengatakan perlu diberikan metode khusus terhadap penggunaan *username* dan *password*nya. Tujuan dari penelitian ini adalah mengenkripsi password pada modul login pengguna dengan menggunakan algoritma MD5. Metode yang digunakan yaitu Algoritma MD5. Hasil dari penelitian ini adalah melakukan pengubahan pada tabel login pengguna untuk kolom password dengan function MD5 di databasenya dan penambahan pembacaan function MD5 pada codingan querynya. Kesimpulan dari penelitian ini adalah proses enkripsi menggunakan algoritma MD5 dapat diterapkan dalam pengamanan password pada aplikasi SIMRS

Kata Kunci: Algoritma MD, Enkripsi, Function MD5, Query, SIMRS

ABSTRACT

The SIMRS (Hospital Information Management Information System) application has not implemented an account encryption process for each user in each work unit. This happens because the SIMRS application has not been facilitated with account encryption capabilities for each user. This is supported by the results of the initial survey with a questionnaire survey to health workers using SIMRS at the Surabaya Medical Service Hospital where as many as 66.7% said there was no special method for logging into the SIMRS application and as many as 77.8% said it was necessary to provide a special method for the use of SIMRS. username and password. The purpose of this study is to encrypt the password on the user login module using the MD5 algorithm. The method used is the MD5 Algorithm. The result of this research is to make changes to the user login table for the password column with the MD5 function in the database and add the MD5 function reading to the query coding. The conclusion of this study is that the encryption process using the MD5 algorithm can be applied to password security in the SIMRS application

Keywords: MD Algorithm, Encryption, MD5 Function, Query, SIMRS

1. PENDAHULUAN

1.1 Latar Belakang

Sistem Komputer yang terhubung dalam jaringan komputer perlu untuk dilindungi. Terutama untuk melindungi data maupun informasi yang dimiliki dari target serangan oleh pihak-pihak yang tidak bertanggungjawab. Data dan informasi yang ada dalam aplikasi berbasis web perlu mekanisme tersendiri dalam melindunginya dari pengguna yang tidak berhak. Mekanisme ini dapat diwujudkan dalam bentuk sebuah proses login pengguna yang biasanya terdiri dari tiga buah pendekatan yaitu identifikasi, otentikasi dan otorisasi(Khairina, 2011).

Proses melindungi data pada sistem serta untuk memastikan bahwa seseorang yang mengakses sistem adalah autentik atau asli adalah dengan autentikasi, yaitu proses memverifikasi identitas dari seorang anggota yang memberikan suatu data dan integritas dari data tersebut. Autentikasi adalah program pengamanan untuk mencegah pihak-pihak yang tidak memiliki otoritas dalam mengakses sistem. Salah satu cara untuk melakukan autentikasi adalah dengan menggunakan password. Untuk menjaga agar password tidak mudah dibaca oleh sniffer atau pengendus diperlukan proses pengamanan dengan melakukan enkripsi dan dekripsi (Khairina, 2011)

Rumah Sakit Surabaya Medical Services (RS SMS) telah memiliki aplikasi Sistem Informasi Manajemen Rumah Sakit (SIMRS) dengan nama Medical Management System (MMS). Aplikasi SIMRS ini telah terintegrasi mulai dari loket

ISSN: 2503-071X
E-ISSN: 2621-511X

pembayaran sampai pada kasir. Tetapi aplikasi SIMRS ini belum menerapkan proses enkripsi akun untuk masing-masing pengguna di masing-masing unit kerja. Hal ini terjadi karena aplikasi SIMRS belum difasilitasi dengan kemampuan enkripsi akun untuk tiap pengguna pada modul loginnya. Hal ini didukung dengan hasil survey awal dengan survey kuesioner kepada petugas kesehatan pengguna SIMRS MMS di RS SMS dimana sebanyak 66,7 % mengatakan belum ada metode khusus dalam login ke aplikasi SIMRS MMS dan sebanyak 77,8 % mengatakan perlu diberikan metode khusus terhadap penggunaan username dan passwordnya. Oleh karena itu, peneliti tertarik untuk mengembangkan aplikasi SIMRS dengan memfasilitasi sistem login untuk pengguna di masing-masing unit kerja dengan menerapkan penggunaan algoritma MD5 (Message-Diggest Algorithm 5). Algoritma MD5 saat ini banyak digunakan mengenkripsi data guna mengamankan data pada basis data. Dimana informasi username dan password tersimpan dalam database aplikasi SIMRS SMS.

1.2 Rumusan Masalah

Dalam penelitian ini rumusan masalahnya adalah Bagaimana melakukan pengamanan akun pengguna untuk tiap modul dengan menggunakan teknik enkripsi akun pada modul login di aplikasi SIMRS *unit* kerja Rumah Sakit Surabaya Medical Service untuk modul pendaftaran, modul rawat jalan, modul rawat inap, modul pembayaran, modul farmasi, dan modul laboratorium

1.3 Tujuan Penelitian

Tujuan penelitian yaitu mengenkripsi password akun pengguna untuk tiap modul login pada aplikasi SIMRS RS SMS untuk modul pendaftaran, modul rawat jalan, modul rawat inap, modul pembayaran, modul farmasi, dan modul laboratorium

1.4 Referensi

1.4.1 Kriptografi

Kata kriptografi berasal dari bahasa yunani yaitu krupto (hidden atau secret) dan grafh (writing) sehingga berarti secret writing. Secara istilah kriptografi didefinisikan sebagai ilmu sekaligus seni untuk menjaga kerahasiaan pesan (data atau informasi) yang mempunyai pengertian, dengan cara menyamarkannya (mengacak) menjadi bentuk yang tidak dapat dimengerti menggunakan suatu algoritma tertentu. Secara umum kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau informasi tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga (Kadri, 2020).

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data serta autentikasi data (Khairina, 2011). Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga (Stalling, 1998)

Terminologi dalam kriptografi diantaranya enkripsi yang merupakan mekanisme untuk merubah plaintext menjadi chipertext. Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Fungsi hash merupakan fungsi yang secara efisien mengubah string masukan dengan panjang berhingga menjadi string keluararn dengan panjang tetap yang disebut nilai hash. MD5 adalah salah satu dari serangkaian algoritma message-digest yang dirancang oleh Profesor Ronald Rivest dari Massachusetts Institute of Technology (MIT). Ketika kerja analitis menunjukkan bahwa pendahulu MD5 yaitu MD4 mulai tidak aman, maka MD5 kemudian dirancang pada tahun 1991 sebagai pengganti dari MD4. Hash MD5 sepanjang 128-bit (16-byte), yang dikenal juga sebagai intisari pesan, message digest secara tipikal ditampilkan dalam bilangan heksadesimal 32- digit. MD5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan dan MD5 juga umum digunakan untuk melakukan pengujian integritas data.(Khairina, 2011)

1.4.2 Autentikasi

Autentikasi merupakan proses validasi pengguna saat masuk ke dalam sistem. Setelah admin melakukan setting hak user baik userid dan username ketika sesuai dengan entrian yang telah dimasukkan dalam database, maka pengguna bisa masuk ke sistem. Proses pengecekan tersebut akan dilakukan oleh sistem. Autorisasi ini disetting oleh administrator, webmaster atau pemilik situs pada userid dan password. Proses autentikasi terhadap sebuah objek adalah melakukan konfirmasi terhadap kebenaran objeknya. Sedangkan melakukan autentikasi terhadap pengguna adalah untuk memverifikasi identitasnya baik userid dan passwordnya dalam sistem. Proses autentikasi ini memberi kesempatan pengguna dan pemberi layanan dalam proses pengaksesan sistemnya. Pengguna harus mampu memberikan informasi yang dibutuhkan untuk berhak masuk ke sistem. Sedangkan sistem akan memberikan feedback bahwasannya menjamin bahwa pihak yang tidak berhak tidak akan dapat mengakses sistem ini.(Khairina, 2011)

Autentikasi bertujuan untuk membuktikan identitas pengguna sebenarnya. Ada banyak cara untuk membuktikan pengguna sebenarnya. Ada empat kategori metode autentikasi (Khairina, 2011):

1. Something You Know

Merupakan metode autentikasi yang paling umum. Kerahasiaan informasi penting dalam hal ini.

ISSN: 2503-071X
E-ISSN: 2621-511X

Kerahasiaan informasi identik dengan password, userid atau PIN. Metode ini berasumsi bahwa tidak ada seorangpun yang mengetahui rahasia itu kecuali dirinya.

2. Something You Have

Merupakan faktor tambahan untuk membuat autentikasi menjadi lebih aman. Metode ini menggunakan kepemilikan hardware seperti kartu magnetic/smartcard, hardware token, USB token dan sebagainya. Metode menyatakan bahwa tidak ada seorangpun yang memiliki barang tersebut kecuali miliknya sendiri

3. Something You Are

Penggunaan bagian tubuh tertentu yang dimiliki oleh manusia merupakan ciri khas metode ini. Metode ini mengandalkan keunikan bagian-bagian tubuh yang tidak mungkin ada pada orang lain seperti sidik jari, suara atau sidik retina mata Karena setiap manusia mempunyai perbedaan terkait ciri khas tersebut seperti sidik jari, suara atau sidik retina

4. Something You Do

Merupakan metode yang melibatkan bahwa setiap pengguna dalam melakukan sesuatu dengan cara berbeda, contohnya penggunaan pengenalan suara (voice recognation) dan analisis tulisan tangan

1.4.3 Sistem Login

Pada saat melakukan login kedalam sistem, pengguna diminta untuk menginputkan identitas user seperti userid dan password sebagai antisipasi dalam hal pengamanan sistem. Password dapat diubah sesuai dengan kebutuhan sedangkan userid tidak pernah diubah karena berupa identitas unik yang merujuk ke pengguna tertentu. Jika userid dan password yang diinputkan cocok maka pengguna memiliki hak untuk mengakses sistem. Proses login memiliki mekanisme yang terdiri dari tiga tahap, yaitu (Khairina, 2011):

1. Identifikasi. Tahap dimana pengguna memberitahukan identitas dirinya.
2. Otentikasi. Tahap dimana pengguna memverifikasi pengguna menggunakan sesuatu yang diketahui, seperti kode PIN atau password; juga sesuatu yang dimiliki, seperti kartu magnetik; dan sesuatu yang menjadi ciri khas dari dirinya, seperti sidik jari
3. Otorisasi. Tahap terakhir dimana jika identifikasi pengguna telah sukses atau benar, maka sistem akan menyelesaikan proses loginnya dan mengasosiasikan identitas pengguna serta informasi kontrol akses ke sistem dengan sesi pengguna

1.4.4 Keamanan Komputer

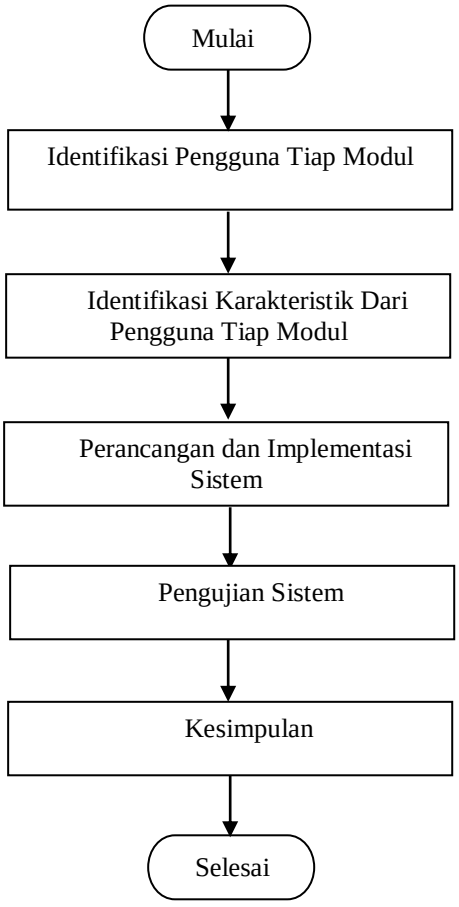
Keamanan komputer meliputi beberapa aspek diantaranya (Santoso, 2013):

a. Authentication: agar penerima informasi memastikan bahwa pesan yang disampaikan memang berasal dari orang yang dimintai informasi
b. Integrity: memastikan pesan atau informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak.
c. Nonrepudiation: hal ini merupakan hal yang bersangkutan dengan si pengirim. Pengirim tidak mengelak bahwa pesan itu memang berasal dari dirinya.
d. Authority: Informasi yang dikirim tidak dimodifikasi oleh pihak yang tidak berhak mengakses informasi tersebut.
e. Confidentiality: merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses informasi tersebut

2. HASIL DAN PEMBAHASAN

Penelitian ini dimulai dari identifikasi akun pengguna aplikasi SIMRS SMS, validasi username dan password, melakukan enkripsi dan deskripsi password pengguna sampai terbaca oleh system. Jika cocok maka pengguna dapat melakukan login dan menggunakan pada aplikasi SIMRS SMS, jika tidak cocok maka pengguna tidak dapat melakukan login dan menggunakan aplikasi SIMRS SMS

2.1 Kerangka Penelitian



Gambar 1. Kerangka Penelitian

ISSN: 2503-071X
E-ISSN: 2621-511X

2.2 Identifikasi Pengguna tiap modul

Data yang digunakan dalam penelitian ini adalah data pengguna baik itu pengguna di unit pendaftaran, pembayaran, rawat jalan, rawat inap, farmasi dan laboratorium. Mencatat jumlah petugas yang mengoperasikan aplikasi SIMRS yang meliputi unit loket pendaftaran pembayaran, rawat jalan, rawat inap, farmasi, dan laboratorium

Tabel 1. Identifikasi data pengguna aplikasi simrs sms

No	*Nama Modul*	*Jumlah Petugas*	*Unit/ Instalasi*
1.	Modul Pendaftaran Pasien	1	Rekam Medik
2.	Modul Pembayaran	1	Keuangan
3.	Modul Rawat Jalan	6	Poli Dalam, Kamar Operasi, Poli Anak, Poli Bedah, Poli Gigi, IGD
4.	Modul Farmasi	1	Farmasi
5.	Modul Rawat Inap	1	Rawat Inap
6.	Modul Laboratorium	1	Laborat

Dari hasil identifikasi didapatkan data sebanyak 1 orang pengguna dengan nama endang agustin bertugas di unit loket pendaftaran, 1 orang pengguna dengan nama alfi nurul warda bertugas di unit rawat inap, 6 orang pengguna dengan lukmanul hakim, alfi nurul warda, laili yusholikha, siti nur jannah, deffi okta, farida yatim bertugas di unit rawat jalan. 1 orang pengguna dengan nama marini septi bertugas di unit farmasi. 1 orang pengguna dengan nama choiril yuniansyah yang bertugas di unit pembayaran. 1 orang pengguna dengan nama widyaningsih yang betugas di unit laboratorium. Masing-masing pengguna aplikasi simrs yang telah ditentukan untuk unit masing-masing akan memberikan ketegasan tanggungjawab dalam melakukan pekerjaanya. Selain itu Pembagian tugas dalam bekerja yang jelas dapat membantu pegawai dalam meningkatkan kinerja pegawai karena pegawai memiliki arah terhadap apa yang menjadi tugas pokok dan fungsinya dalam bekerja. Hal ini seperti dijelaskan dalam penelitian (Syelviani, 2017)

2.3 Identifikasi Karakteristik Dari Pengguna Tiap Modul

Dilakukan pengumpulan data karakteristik dari petugas yang bertugas pada modul di unit pendaftaran, unit pembayaran, unit rawat jalan, unit rawat inap, unit farmasi dan unit laboratorium. Data ini digunakan untuk mengetahui usia dan tingkat pendidikan dari petugas yang bertugas di unit pendaftaran, unit pembayaran, unit rawat jalan, unit rawat inap, unit farmasi dan unit laboratorium. Data pengumpulan data tersebut, diketahui bahwasannya pengguna dari modul tersebut rata-rata berusia 33 tahun dan rata-rata riwayat pendidikannya minimal adalah D3 (Diploma).

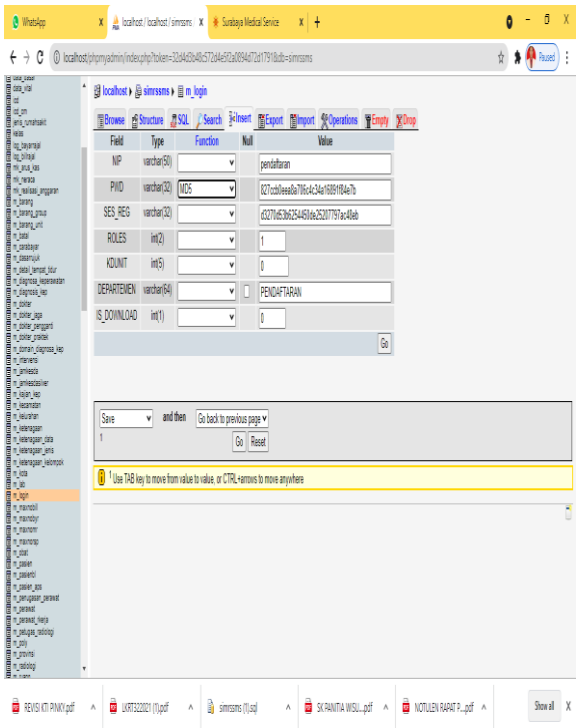
Dengan usia yang matang dan tingkat pendidikan yang baik maka akan berpengaruh pada kinerja seseorang dalam menjalankan pekerjaan dan tentunya akan meningkatkan pendapatannya. Hal ini seperti pada penelitian (Putri Utami dkk, 2021)

2.4 Perancangan dan Implementasi Sistem

Pada proses perancangan dan implementasi sistem ini akan dilakukan proses enkripsi password pada modul login pengguna dengan menggunakan algoritma MD5. Selain akan dilakukan validasi terhadap username dan password dalam database aplikasi SIMRS SMS.

2.4.1 Enkripsi password pada modul login Pengguna dengan Algoritma MD5

Proses enkripsi password dengan menggunakan teknik kriptografi yaitu menggunakan algoritma MD5. Proses ini melibatkan pengubahan function MD5 pada settingan databasenya. Tabel dalam database aplikasi SIMRS yang akan di modifikasi dengan algoritma MD5 yaitu tabel m_login dimana pengubahan dilakukan untuk kolom PWD akan diberikan function MD5.



Gambar 2. Setting Function MD5 Untuk Unit Pendaftaran

ISSN: 2503-071X
E-ISSN: 2621-511X

Pada proses pengubahan function MD5 ini, akan dilakukan proses pengubahan function Null ke Function MD5, setelah di proses maka tampilan dari kolom PWD yang memanfaatkan function MD5 akan tampak seperti diatas. Hal ini teori penggunaan algoritma MD5 pada penelitian(Kadri, 2020).

2.4.2 Validasi terhadap username dan password Dalam database aplikasi SIMRS SMS

Untuk melakukan proses validasi username dan password pada modul login, dilakukan proses pengubahan koding dalam pemrograman simrs sms.

Berikut pengubahan coding pada bagian user_level.php untuk menambahkan koding dengan algoritma MD5.

$sql ="SELECT * FROM m_login WHERE NIP = '".$NIP1."' AND PWD = '".md5($_REQUEST['PWD'])."'";

Peneliti menggunakan kolom PWD sebagai variabel yang dibutuhkan dalam proses penerapan algoritma MD5 pada modul login untuk masuk ke modul masing-masing unit.

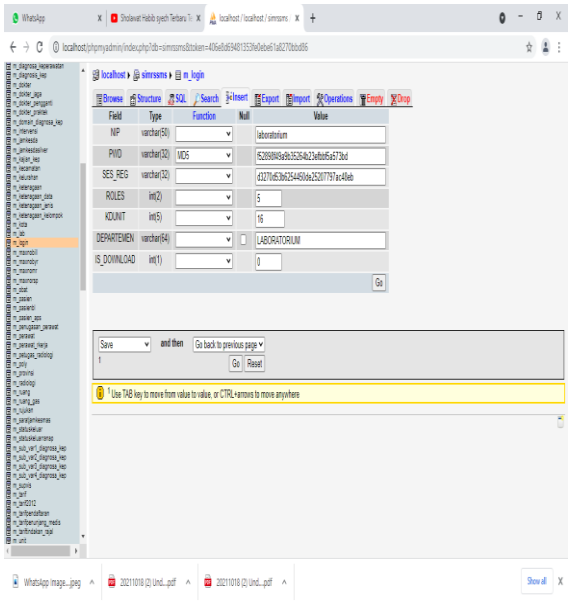
Hasil dari validasi username dan password yang di baca dalam database dengan kodingan program diatas, ketika sesuai maka form aplikasi akan terbuka dan bisa dinputkan data, tetapi sebaliknya jika hasil validasi username dan password tidak sama dengan yang ada dalam database maka form aplikasi tidak akan terbuka. Hal ini sesuai dengan teori dari penelitian (Khairina, 2011) bahwasannya terdapat tiga tahapan dalam proses login yaitu identifikasi, otentikasi dan otorisasi 3 tahapan tersebut terpenuhi dalam melakukan proses validasi terhadap username dan password dari masing-masing modul yaitu modul unit pendaftaran, unit pembayaran, unit rawat jalan, unit rawat inap, unit farmasi dan unit laboratorium.

2.5 Pengujian Sistem

Pengujian sistem dilakukan pada proses pengubahan function MD5 di kolom PWD pada database aplikasi SIMRS SMS dan validasi username dan password untuk akun pengguna.

2.5.1 Pengubahan Function MD5

Hasil dari pengubahan function MD5 di kolom PWD akan menghasilkan kombinasi sejumlah karakter dan huruf yang mana ini adalah password yang dienkripsi menggunakan algoritma MD5.

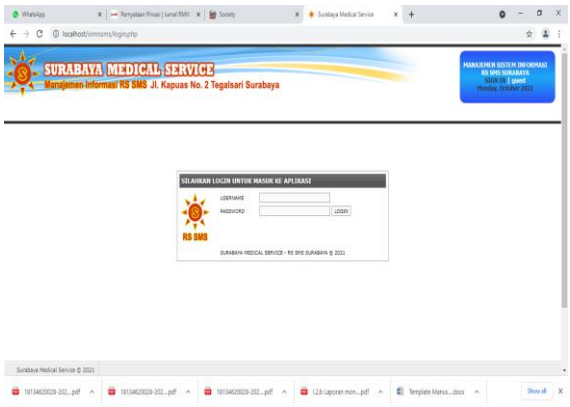


Gambar 3. Setting Function MD5 Untuk Unit Laboratorium

Pada contoh diatas user dengan NIP: laboratorium dengan password PWD awal yaitu 12345, setelah dilakukan penerapan algoritma MD5 maka kolom PWD dalam hal ini password akan berubah menjadi kombinasi huruf dan angka sebagai berikut f52898f49a9b35264b23efbbf5a573bd

2.5.2 Validasi Username dan Password Akun Pengguna

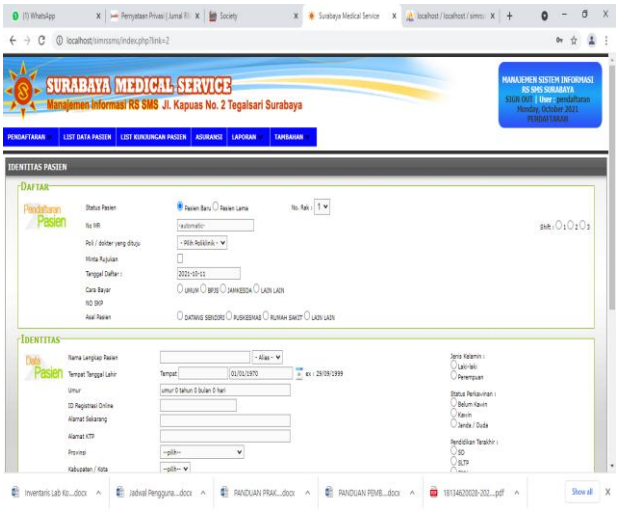
Untuk melakukan proses validasi username dan password pada modul login, dilakukan proses pengubahan koding dalam pemrograman simrs sms. Hasil programnya dapat dilihat sebagai berikut:



Gambar 4. Modul Login Aplikasi SIMRS SMS

Hasil dari validasi username dan password yang di baca dalam database dengan kodingan program yang telah dibuat, ketika sesuai maka form aplikasi akan terbuka dan bisa dinputkan datanya, tetapi sebaliknya jika hasil validasi username dan password tidak sama dengan yang ada dalam database maka form aplikasi tidak akan terbuka

ISSN: 2503-071X
E-ISSN: 2621-511X



Gambar 5. Hasil Login Pada Modul Pendaftaran Aplikasi SIMRS SMS

3. KESIMPULAN

Dari hasil penelitian ini, dapat disimpulkan bahwa :

1. Peneliti dapat mengidentifikasi terdapat 6 orang pengguna untuk modul pendaftaran, pembayaran, rawat jalan, rawat inap, farmasi dan laboratorium yang ada diaplikasi SIMR SMS
2. Peneliti dapat mengidentifikasi usia rata-rata usia pengguna SIMRS SMS adalah 33 tahun dengan tingkat pendidikan rata-rata minimal D3 (Diploma)
3. Peneliti dapat menerapkan proses enkripsi pada kolom password dalam database dengan menggunakan algoritma MD5 dengan menerapkan function MD5 pada kolom PWD di database SIMRS SMS
4. Peneliti menghasilkan kodingan terhadap pembacaan username dan password yang ada di database. Hasil dari validasi username dan password yang di baca dalam database, ketika sesuai maka form aplikasi akan terbuka dan bisa dinputkan data, tetapi sebaliknya jika hasil validasi username dan password tidak sama dengan yang ada dalam database maka form aplikasi tidak akan terbuka

Pada penelitian selanjutnya perlu dikembangkan teknik lain dalam melakukan enkripsi password pada aplikasi SIMRS, agar lebih aman.

PUSTAKA

Kadri, y. (2020). Penerapan algoritma md5 sebagai pengaman akun pada aplikasi web emusrenbang kota binjai. jurnal teknik informatika kaputama (jtik), 4.

Khairina, d. m. (2011). Analisis keamanan sistem login. jurnal informatika mulawarman, 6, 64

Putri Utami, Gusti Ayu Putu Yulina. Yuliarmi, N. N. (2021). Pengaruh tingkat pendidikan, umur dan pengalaman kerja terhadap pendapatan para pekerja di kawasan objek wisata tanah lot. Ekonomi Pembangunan Unud, 10 No.7.

Santoso, K. I. (2013). Studi Pengamanan Login Pada Sistem Informasi Akademik Menggunakan Otentifikasi One Time Password Berbasisis SMS dengan Hash MD5. Jurnal Sistem Informasi Bisnis,3(1).https://doi.org/10.21456/vol3iss1pp07-12

Stalling, W. (1998). Cryptography and Network Security, Principle and Practice 2 nd Edition. Pearson Education, Inc.

Syelviani, M. (2017). Pengaruh deskripsi pekerjaan terhadap kinerja pegawai negeri sipil pada kantor camat tembilahan. Economy, Business and Accounting (COSTING), 1 No.1.