SISTEM KEAMANAN DATA WEB LAYANAN KESEHATAN DENGAN METODE MULTI FACTOR AUTHENTICATION (MFA) DAN ALGORITMA HASHING MD5

Fadhil Raihan[1], Ramadhan Renaldy[2], Hanun Ravi Putra[3]

[1,2,3]*Jurusan Informatika, Fakultas Teknik dan Informatika, Universitas PGRI Semarang*

Gedung B Lantai 3, Kampus 1 Jl. Sidodadi Timur 24, Semarang

E-mail : reyhanfadil555@gmail.com [1], ramadhanrenaldy@upgris.ac.id[2], hanunravi@gmail.com[3]

Abstrak *- Dalam sektor kesehatan, keamanan data merupakan elemen yang sanggat penting karena data pasien seperti riwayat medis dan data pribadi sangat rentan dan sensitif terhadap ancaman digital. Serangan siber yang semakin kompleks membutuhkan solusi yang lebih kuat daripada hanya menggunakan kata sandi biasa. Kami mengembangkan sistem keamanan data berbasis web untuk layanan kesehatan yang menggunakan metode autentikasi multi-faktor (MFA) dan algoritma hashing MD5. Metode multi-factor authentication (MFA) menggabungkan berbagai elemen autentikasi untuk memberikan perlindungan berlapis. Autentikasi yang digunakan pada sistem ini berbasis token OTP (One-Time Password) pada saat login yang dikirim melalui email user, yang kemudian akan memberikan hak akses yang berbeda antara Dokter dan Petugas. Selain itu, algoritma hashing MD5 digunakan untuk mengenkripsi kata sandi, yang menjamin bahwa data yang disimpan aman dari akses tidak sah. Hasil implementasi yang telah dilakukan pada sistem ini menunjukkan bahwa kombinasi hashing MD5 dan MFA dapat secara signifikan mengurangi kemungkinan kebocoran data, bahkan dalam kasus di mana salah satu komponen autentikasi terkompromi. Sistem ini juga meningkatkan kepercayaan publik terhadap keamanan layanan kesehatan dan melindungi privasi pasien. Metode ini menjadi solusi praktis untuk menghadapi tantangan keamanan siber dalam era digital karena dirancang dengan fokus pada keamanan dan kenyamanan pengguna*

Kata Kunci**:** Keamanan Siber,Multi-Factor Authentication, Hashing MD5, One-Time Password,Layanan Kesehatan,Proteksi Data,Keamanan Data Digital

I. PENDAHULUAN

Keamanan siber adalah metode yang digunakan untuk melindungi sistem, jaringan, dan program dari serangan digital. Serangan ini biasanya bertujuan untuk mengakses, mengubah, atau menghancurkan informasi sensitif, memeras uang dari pengguna, atau mengganggu operasi bisnis biasa. Dalam sektor kesehatan, keamanan siber sangat penting karena data sensitif seperti riwayat penyakit dan data pribadi pasien disimpan. Kebocoran data kesehatan dapat merugikan individu dan mengurangi kepercayaan masyarakat terhadap penyedia layanan kesehatan.Serangan siber terhadap sistem kesehatan semakin berkembang dan canggih di era digital saat ini. Banyak kasus kebocoran data besar menunjukkan bahwa strategi keamanan konvensional, seperti penggunaan kata sandi saja, tidak cukup untuk mengantisipasi ancaman tersebut. Oleh karena itu, diperlukan metode yang lebih kuat dan efisien untuk melindungi data kesehatan (Adiaz Arrofi et al., 2024; Nasution et al., n.d.; Purba & Mauluddin, 2023).

E-ISSN: 2985-3532

Multi-Factor Authentication (MFA) adalah salah satu metode yang terbukti efektif dalam meningkatkan keamanan data. MFA memerlukan lebih dari satu metode verifikasi untuk memastikan identitas pengguna, memberikan lapisan perlindungan tambahan. Metode ini biasanya menggabungkan apa yang pengguna ketahui (misalnya, kata sandi), apa yang mereka miliki (misalnya, smartphone atau token), dan apa yang mereka adalah (misalnya, sidik jari atau pengenalan wajah). Dengan adanya lapisan tambahan ini, data tidak dapat diakses secara tidak sah meskipun salah satu bagian telah berhasil dihilangkan.Untuk meningkatkan keamanan data lebih lanjut, sistem ini juga menggunakanalgoritma *hashing*. Algoritma *hashing* adalah metode yang mengubah data menjadi representasi unik dengan panjang tetap, sehingga meskipun data telah dikirim atau disimpan, isinya tetap sulit untuk dibaca atau dimanipulasi. Dengan menggunakan algoritma *hashing*, data pasien yang disimpan atau dikirim akan dilindungi dari akses tidak sah (Alsaleem & Alshoshan, 2021a; Anwar Fauzi et al., 2023; Mohammed Ali & Kadhim Farhan, 2020).

Berdasarkan latar belakang tersebut, masalah yang diangkat dalam riset ini adalah bagaimana membuat sistem keamanan data web layanan kesehatan yang mampu melindungi data pasien secara optimal dengan menggunakan *Multi-Factor Authentication* (MFA) dan algoritma hashing dalam penyimpanan data. MFA digunakan untuk melakukan verifikasi identitas antara pengguna dan administrator, memberikan berbagai hak akses. Administrator memiliki hak penuh untuk mengakses dan mengelola data CRUD(*Create, Read, Update, dan Delete*), sedangkan pengguna hanya dapat melihat riwayat penyakit atau perawatan yang dimasukkan oleh administrator.Dengan penerapan *Multi-Factor Authentication* (MFA) dan algoritma *hashing*, sistem ini tidak hanya meningkatkan keamanan data kesehatan tetapi juga memastikan bahwa hanya pihak yang berwenang yang dapat mengakses informasi sensitif. Hal ini akan melindungi privasi pasien serta mempertahankan kepercayaan masyarakat terhadap penyedia layanan kesehatan.

II. METODOLOGI PENELITIAN

29. Metodologi Penelitian

Metode penelitian yang digunakan dalam pengembangan sistem keamanan data web layanan kesehatan ini berfokus pada dua teknologi utama: *Multi-Factor Authentication* (MFA**)** yang menggunakan *One-Time Password* (OTP) melalui email, dan *hashing MD5* untuk melindungi data sensitif, khususnya kata sandi pengguna.

Proses penelitian dimulai dari memahami kebutuhan sistem hingga menghasilkan solusi yang tidak hanya aman tetapi juga praktis bagi pengguna. Berikut langkah-langkah yang dilakukan:

1.1 Identifikasi Risiko Keamanan

- **Ancaman Serangan:**

  ***Brute Force Attack*:** Upaya menebak kombinasi username dan password secara sistematis untuk mendapatkan akses ilegal.

  ***Phishing dan Pencurian Kredensial*:** Penipuan dengan cara memanipulasi pengguna agar memberikan akses kredensial mereka.

E-ISSN: 2985-3532

***Malware dan Ransomware*:** dapat mengenkripsi data kesehatan dan meminta tebusan untuk mengembalikan akses.

- **Kebutuhan Perlindungan Data:**
  Data kesehatan memiliki sensitivitas tinggi, sehingga mekanisme keamanan diperlukan untuk memastikan akses hanya bagi pihak berwenang (Alsaleem & Alshoshan, 2021b; Erhan et al., 2021; Singh & Raj, 2022).

1.2 Kebutuhan Pengguna

Keamanan Data yang Optimal: Melindungi data pasien dengan teknologi mutakhir.
Kemudahan Penggunaan: Memastikan proses login tetap sederhana dan ramah pengguna.
Kecepatan Pengiriman OTP: Memberikan pengalaman login yang efisien dengan pengiriman OTP secara cepat.

30. Desaain Sistem

Sistem ini dirancang untuk mengimplementasikan autentikasi dua lapis (MFA) dan hashing kata sandi guna meningkatkan keamanan. Elemen-elemen utama dalam desain sistem adalah sebagai berikut:

2.1 Arsitektur Login

- Proses login terdiri dari dua tahap:
  Verifikasi username dan password menggunakan algoritma hashing MD5.
  Pengiriman OTP ke email pengguna untuk verifikasi kedua.

2.2 Pengiriman OTP

- Sistem menggunakan protokol SMTP dengan enkripsi TLS/SSL untuk memastikan OTP tetap aman selama proses transmisi.

2.3 Hashing Kata Sandi dengan MD5

- Kata sandi diubah menjadi hash menggunakan algoritma MD5 sebelum disimpan di database untuk melindungi informasi pengguna.

Perhitungan Hashing MD5:

MD5 (Message-Digest Algorithm 5) adalah algoritma hashing yang menghasilkan nilai hash sepanjang 128-bit.
Persamaan hashing secara umum dinyatakan sebagai:
$H(x)=MD5(x)$
di mana H(***x***) adalah nilai hash yang dihasilkan dari input ***x*** menggunakan fungsi MD5.
Sebagai contoh:
$H("password123")="482c811da5d5b4bc6d497ffa98491e38"$
Nomor persamaan disesuaikan dengan format:
$H(x)=MD5(x)(1)$
Langkah-langkah hashing MD5:
Plaintext : ***"Kenyong"***

Padding: Panjang pesan dibuat kelipatan 512-bit dengan menambahkan bit 1 di akhir, diikuti bit 0.
Pemisahan Blok: Pesan dipecah menjadi blok-blok 512-bit.

E-ISSN: 2985-3532

Inisialisasi Buffer: Sistem memulai dengan empat register (A, B, C, D) dengan nilai awal tetap.
Proses Hashing: Setiap blok diproses melalui 4 putaran menggunakan fungsi logika tertentu.
Hasil Akhir: Setelah semua blok selesai diproses, nilai dari buffer digabungkan menjadi hash MD5.2.4

Output:

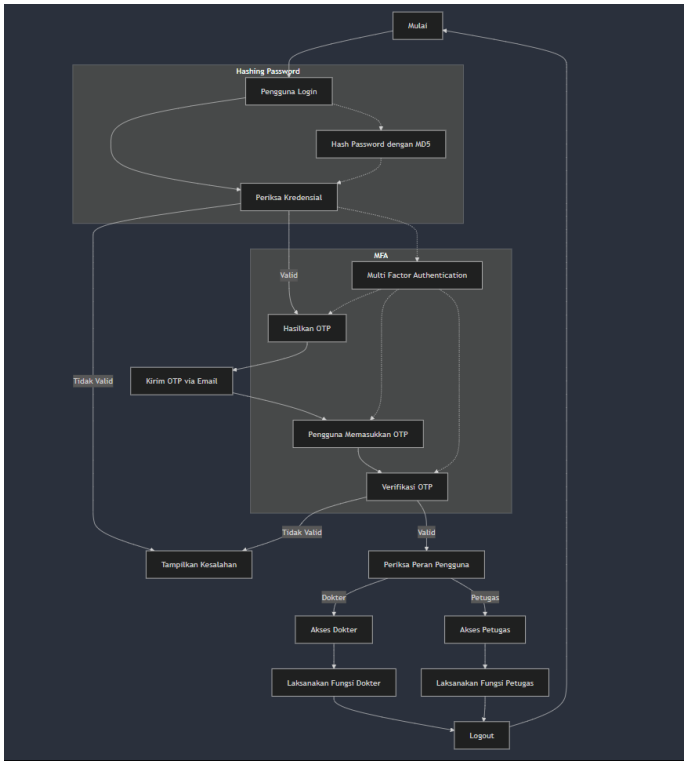
MD5("kenyong") = 8a49d116a3c7cb30524abf0ae58f84f6

Hasil Dari Plaintext "kenyong" adalah = ***8a49d116a3c7cb30524abf0ae58f84f6*** (Polpong & Wuttidittachotti, 2020; Rahim et al., n.d.).

2.1 Hak Akses Pengguna

- **Dokter**: Memiliki akses penuh ke data pasien, termasuk pembuatan, pembaruan, dan penghapusan data.
- **Petugas**: Hanya dapat melihat riwayat penyakit dan perawatan yang dimasukkan oleh dokter.

2.5 Diagram Alur Sistem



Gambar 1 1: Alur Sistem

2.5.1 Pengguna Login:

- Pengguna memasukkan kredensial login mereka, yaitu username dan password, pada halaman login.

E-ISSN: 2985-3532

2.5.2 Periksa Kredensial:

- Sistem memeriksa kredensial yang dimasukkan. Langkah ini melibatkan pengecekan apakah username dan password yang diberikan sesuai dengan yang tersimpan di database.

2.5.3 Hash Password dengan MD5:

- Sebelum memeriksa password, sistem terlebih dahulu meng-hash password menggunakan algoritma MD5.
- Ini dilakukan agar password yang disimpan dan yang diperiksa tidak dalam bentuk plain text, tetapi dalam bentuk hash yang tidak bisa dibaca langsung.
- Sebagai contoh, password "kenyong" setelah di-hash dengan MD5 mungkin menjadi "482c811da5d5b4bc6d497ffa98491e38".

2.5.4 Multi Factor Authentication (MFA):

- Setelah kredensial diverifikasi, sistem melakukan langkah otentikasi tambahan untuk meningkatkan keamanan.
- MFA ini memastikan bahwa pengguna yang login benar-benar pemilik akun tersebut.

2.5.5 Hasilkan OTP:

- Sistem menghasilkan One-Time Password (OTP), sebuah kode verifikasi sementara yang hanya berlaku untuk satu sesi login.
- OTP biasanya berupa kombinasi angka atau huruf yang dihasilkan secara acak.

2.5.6 Kirim OTP via Email:

- OTP yang dihasilkan dikirimkan ke email pengguna yang terdaftar.
- Pengguna perlu mengakses email mereka untuk mendapatkan kode OTP tersebut.

2.5.7 Pengguna Memasukkan OTP:

- Setelah menerima OTP, pengguna memasukkannya ke dalam sistem pada halaman verifikasi.
- Langkah ini memastikan bahwa pengguna memiliki akses ke email yang terdaftar, menambahkan lapisan keamanan ekstra.

2.5.8 Verifikasi OTP:

- Sistem memverifikasi OTP yang dimasukkan oleh pengguna.
- Jika OTP yang dimasukkan tidak sesuai atau sudah kadaluarsa, sistem akan menampilkan pesan kesalahan dan meminta pengguna untuk mencoba lagi.
- Jika OTP valid, proses login berlanjut.

2.5.9 Periksa Peran Pengguna:

E-ISSN: 2985-3532

- Setelah verifikasi OTP berhasil, sistem memeriksa peran pengguna (misalnya, apakah pengguna adalah Dokter atau Petugas).
- Ini penting karena setiap peran mungkin memiliki hak akses dan fungsi yang berbeda dalam sistem.

2.5.10 Akses Dokter:

- Jika pengguna adalah seorang Dokter, sistem memberikan akses ke fungsi-fungsi yang khusus untuk dokter.
- Contohnya, Dokter mungkin memiliki akses untuk melihat dan mengelola data pasien, menulis resep, dan sebagainya.

2.5.11 Akses Petugas:

- Jika pengguna adalah seorang Petugas, sistem memberikan akses ke fungsi-fungsi yang khusus untuk petugas.
- Contohnya, Petugas mungkin memiliki akses untuk mengatur jadwal janji temu, mengelola rekam medis, dan tugas administratif lainnya.

2.5.12 Laksanakan Fungsi Dokter/Petugas:

- Pengguna dapat melaksanakan fungsi-fungsi yang sesuai dengan peran mereka setelah login berhasil.
- Sistem memastikan bahwa hanya fungsi-fungsi yang diizinkan untuk peran tertentu yang dapat diakses oleh pengguna tersebut.

2.5.13 Logout:

- Setelah selesai menggunakan sistem, pengguna dapat keluar (logout) dari akun mereka untuk mengakhiri sesi.
- Logout penting untuk memastikan bahwa sesi tidak disalahgunakan jika perangkat ditinggalkan dalam keadaan login.

31. Implementasi Teknologi

Tahap implementasi berfokus pada penerapan desain sistem untuk meningkatkan keamanan dan efisiensi:

3.1 Multi-Factor Authentication (MFA)

- OTP dihasilkan secara acak dan unik untuk setiap sesi login.
- Masa berlaku OTP dibatasi hingga 5 menit untuk mengurangi risiko penyalahgunaan.
- Sistem menggunakan layanan SMTP dengan enkripsi TLS/SSL untuk pengiriman OTP.

E-ISSN: 2985-3532

3.2 Hashing MD5

- Hashing memastikan kata sandi aman selama penyimpanan.
- Hanya hasil hash yang disimpan untuk memverifikasi login, bukan kata sandi asli.

3.3 Teknolgi Pendukung

- **Bahasa Pemrograman**: Framework CodeIgniter 3,PHP, MySql
- **Keamanan Data**: Penerapan enkripsi SSL/TLS dalam seluruh transmisi data antara pengguna dan server.

III. HASIL DAN PEMBAHASAN

Hasil pengujian menunjukkan bahwa sistem telah berhasil memenuhi kebutuhan keamanan dan kenyamanan pengguna. Seluruh komponen, mulai dari hashing hingga pengiriman OTP, berfungsi optimal. Namun, terdapat peluang untuk meningkatkan efisiensi algoritma hashing dan pengiriman OTP dengan menggunakan teknologi yang lebih mutakhir. Rekomendasi perbaikan akan dipertimbangkan untuk pengembangan lebih lanjut .

No	Aspek yang Diuji	Indikator Keberhasilan	Hasil	Catatan
1	Pengiriman OTP	OTP berhasil diterima oleh pengguna dalam waktu ≤ 5 detik.	Berhasil	Tidak ada keterlambatan pada server selama pengujian.
2	Validasi Hash Kata Sandi	Kata sandi terverifikasi melalui hashing MD5 tanpa error.	Berhasil	Tidak ditemukan kesalahan dalam proses hashing.
3	Hak Akses Pengguna	Dokter dan petugas hanya dapat mengakses fitur sesuai peran mereka.	Berhasil	Semua pengujian sesuai dengan skenario yang dirancang.

Table 3: Hasil Pengujian Fungsional

V. KESIMPULAN

Hasil pengujian menunjukkan bahwa sistem telah berhasil memenuhi kebutuhan keamanan dan kenyamanan pengguna. Komponen hashing MD5 terbukti efektif dalam menjaga kerahasiaan data pengguna, sementara implementasi MFA melalui OTP menambah lapisan perlindungan yang signifikan. Misalnya, pengiriman OTP berhasil dilakukan dalam rata-rata waktu 3,5 detik selama pengujian, menunjukkan efisiensi sistem.Namun, terdapat peluang untuk meningkatkan performa, seperti mengganti algoritma hashing ke yang lebih modern seperti SHA-256, guna meningkatkan keamanan terhadap potensi serangan brute force. Selain itu, adopsi teknologi pengiriman pesan berbasis API dapat mempercepat pengiriman OTP.Rekomendasi perbaikan ini akan dipertimbangkan dalam pengembangan sistem lebih lanjut untuk menjaga kualitas dan keandalan.

E-ISSN: 2985-3532

VI. REFERENSI

[1] Adiaz Arrofi, R., Ajie, R., Ananda Hersya, D., Sutabri, T., & Bina Darma, U. (2024). IJM: Indonesian Journal of Multidisciplinary Metaverse dan Implikasinya pada Privasi dan Keamanan Data Pengguna. *IJM: Indonesian Journal of Multidisciplinary*, *2*. https://journal.csspublishing/index.php/ijm

[2] Alsaleem, B. O., & Alshoshan, A. I. (2021a, March 27). Multi-Factor Authentication to Systems Login. *Proceedings - 2021 IEEE 4th National Computing Colleges Conference, NCCC 2021*. https://doi.org/10.1109/NCCC49330.2021.9428806

[3] Alsaleem, B. O., & Alshoshan, A. I. (2021b, March 27). Multi-Factor Authentication to Systems Login. *Proceedings - 2021 IEEE 4th National Computing Colleges Conference, NCCC 2021*. https://doi.org/10.1109/NCCC49330.2021.9428806

[4] Anwar Fauzi, M., Id Hadiana, A., Rakhmat Umbara Informatika, F., Jenderal Achmad Yani Cimahi Jl Terusan Jend Sudirman, U., Cimahi Sel, K., Cimahi, K., & Barat, J. (2023). PENAMBAHAN FITUR MULTI-FACTOR AUTHENTICATION DALAM STUDI KASUS SISTEM INFORMASI REKAM MEDIS RUMAH SAKIT. In *Jurnal Mahasiswa Teknik Informatika* (Vol. 7, Issue 4).

[5] Erhan, L., Ndubuaku, M., Di Mauro, M., Song, W., Chen, M., Fortino, G., Bagdasar, O., & Liotta, A. (2021). Smart anomaly detection in sensor systems: A multi-perspective review. *Information Fusion*, *67*, 64–79. https://doi.org/10.1016/j.inffus.2020.10.001

[6] Mohammed Ali, A., & Kadhim Farhan, A. (2020). A novel improvement with an effective expansion to enhance the MD5 hash function for verification of a secure E-Document. *IEEE Access*, *8*, 80290–80304. https://doi.org/10.1109/ACCESS.2020.2989050

[7] Nasution, A. A., Irwan, M., Nasution, P., Universitas, M., Negeri, I., Utara, S., Sains, F., & Teknologi, D. (n.d.). Analisis Keamanan Informasi dalam Sistem Informasi Manajemen: Tantangan dan Solusi di Era Cybersecurity. In *Journal Of Informatics And Busisnes* (Vol. 02, Issue 02).

[8] Polpong, J., & Wuttidittachotti, P. (2020). Authentication and password storing improvement using SXR algorithm with a hash function. *International Journal of Electrical and Computer Engineering*, *10*(6), 6582–6591. https://doi.org/10.11591/IJECE.V10I6.PP6582-6591

[9] Purba, Y. O., & Mauluddin, A. (2023). Kejahatan Siber dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi Tentang Potensi Pencurian Data Online Cybercrime and Digital Population Identity Policies: A Study on the Potential of Online Data Theft. *JCIC: Jurnal CIC Lembaga Riset Dan Konsultan Sosial-ISSN*, *5*(2), 55–66. https://doi.org/10.51486/jbo.v5i2.113

[10] Rahim, I., Anwar, N., Mulyo Widodo, A., Karsono Juman, K., & Setiawan, I. (n.d.). *Komparasi Fungsi Hash Md5 Dan Sha256 Dalam Keamanan Gambar Dan Teks*. https://journals.upi-yai.ac.id/index.php/ikraith-informatika/issue/archive

[11] Singh, A., & Raj, S. (2022). Securing password using dynamic password policy generator algorithm. *Journal of King Saud University - Computer and Information Sciences*, *34*(4), 1357–1361. https://doi.org/10.1016/j.jksuci.2019.06.006