INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer
Vol. 01, No. 03, Tahun 2026, Hal. 237-242, ISSN: 3123-5573 (Online)

Evaluasi Keamanan Sistem *Login* Menggunakan *Hashing* dan *Salting Password*

Rakhmadi Rahman[1], Saripa Citra[2], Hikmah Julia Andini[3]
[1.2]Sistem Informasi Institut Teknologi Bacharuddin Jusuf Habibie Parepare, Indonesia
rakhmadi.rahman@ith.ac.id[1], ctraasyh@gmail.com[2] , andinihikmahjulia@gmail.com[3]

Article Info

Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Keywords:

login system, information security, hashing, salting, password.

ABSTRACT

Login security is essential to protect user authentication data in web-based systems. Passwords remain the most common authentication mechanism and are frequently targeted by brute-force, dictionary attacks, and precomputed-table attacks. This study evaluates password hashing and salting in a login system to assess how effectively stored credentials are protected. A descriptive-evaluative approach was applied through a literature review, observation of the authentication flow, and documentation analysis of source code and database structures. The findings indicate that hashing with a unique per-user salt prevents plaintext storage, mitigates rainbow table attacks, and increases the attacker's computational cost. However, optimal protection also requires additional controls such as login attempt limiting, strong password policies, and secure transport (HTTPS). This paper provides technical recommendations to strengthen authentication, including the use of password-specific hashing algorithms and complementary security mechanisms.

Article Info

Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Kata Kunci:
sistem login, keamanan informasi, hashing, salting, password.

ABSTRAK

Keamanan sistem login menentukan perlindungan data autentikasi pengguna pada aplikasi berbasis web. Password sebagai metode autentikasi paling umum sering menjadi sasaran serangan seperti brute force, dictionary attack, dan pemanfaatan tabel pra-hitung. Penelitian ini mengevaluasi penerapan hashing dan salting pada sistem login untuk menilai efektivitas perlindungan password di basis data. Metode yang digunakan adalah deskriptif-evaluatif melalui studi literatur, observasi alur autentikasi, serta analisis dokumentasi kode dan struktur basis data. Hasil evaluasi menunjukkan bahwa penerapan hashing dengan salt unik per pengguna mencegah penyimpanan password dalam bentuk plaintext, mengurangi risiko serangan rainbow table, dan memperbesar biaya komputasi penyerang saat mencoba menebak password. Meski demikian, keamanan belum optimal apabila tidak diimbangi pembatasan percobaan login, kebijakan password yang kuat, serta pengamanan transmisi (HTTPS). Penelitian ini menghasilkan rekomendasi teknis untuk memperkuat autentikasi, termasuk pemilihan algoritma hashing khusus password dan kontrol keamanan tambahan pada proses login.

Corresponding Author:
Rakhmadi Rahman
Institut Teknologi Bacharuddin Jusuf Habibie
Email: rakhmadi.rahman@ith.ac.id

PENDAHULUAN

Pemanfaatan sistem informasi berbasis internet semakin luas pada sektor pendidikan, pemerintahan, bisnis, dan layanan publik. Hampir seluruh sistem tersebut menerapkan autentikasi untuk membatasi akses pengguna. Komponen login berperan sebagai gerbang utama; kelemahan pada bagian ini dapat memicu pengambilalihan akun, kebocoran data, hingga gangguan layanan.

Permasalahan yang sering muncul adalah pengelolaan password. Praktik penyimpanan password dalam bentuk teks asli (plaintext) sangat berisiko apabila basis data bocor. Teknik hashing digunakan untuk menyamarkan password menjadi nilai satu arah. Namun, hashing tanpa penguatan dapat tetap rentan terhadap tabel pra-hitung (rainbow table), khususnya ketika banyak pengguna memakai password yang sama.

Salting memperkuat hashing dengan menambahkan nilai acak unik pada password sebelum di-hash. Dengan salt unik per pengguna, dua password identik menghasilkan hash yang berbeda sehingga serangan berbasis tabel menjadi tidak efektif. Penelitian ini mengevaluasi implementasi hashing dan salting pada sistem login berbasis web serta merumuskan rekomendasi perbaikan agar mendekati praktik terbaik keamanan.

METODOLOGI PENELITIAN

Penelitian ini menggunakan metode deskriptif-evaluatif. Pendekatan deskriptif menggambarkan alur autentikasi dan mekanisme penyimpanan password, sedangkan pendekatan evaluatif menilai kekuatan implementasi berdasarkan kriteria keamanan (kerahasiaan password, ketahanan terhadap serangan umum, dan kesesuaian praktik terbaik).

Pengumpulan data dilakukan melalui:

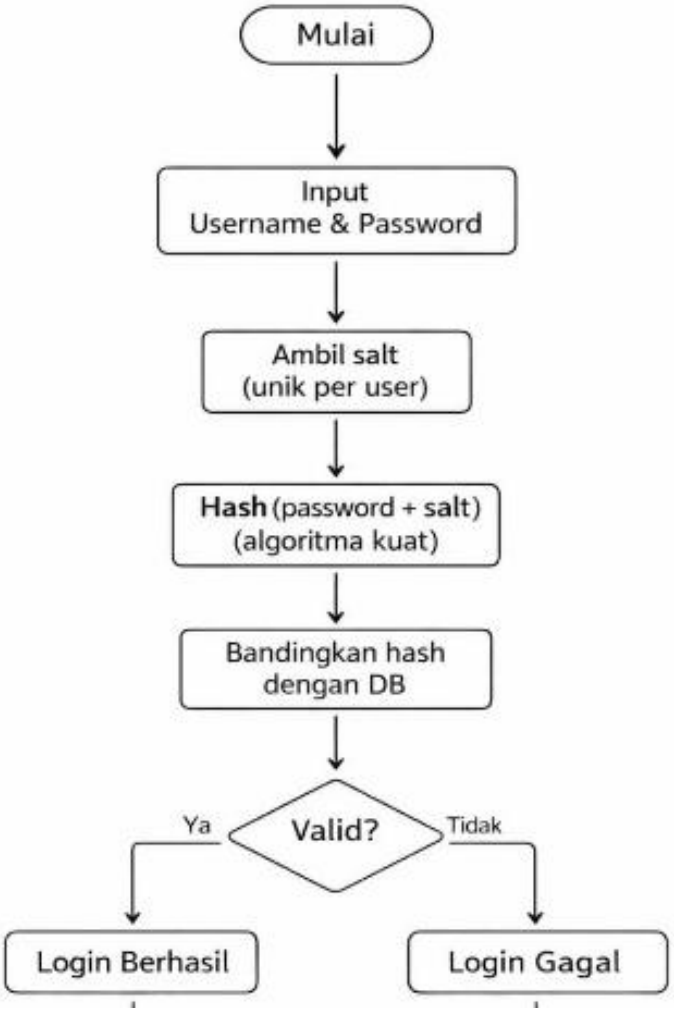
1) studi literatur terkait keamanan autentikasi, hashing, dan salting;
2) observasi alur login dari input kredensial hingga keputusan akses;
3) analisis dokumentasi berupa struktur tabel basis data serta komponen kode yang mengatur hashing, pengelolaan salt, dan verifikasi password.

Analisis kualitatif dilakukan dengan mengidentifikasi mekanisme penyimpanan password, mengevaluasi algoritma hashing, menilai penerapan salt (keunikan, keacakan, dan penyimpanan), menganalisis potensi ancaman (brute force/dictionary/rainbow table), serta menyusun rekomendasi perbaikan (kontrol login, kebijakan password, dan keamanan koneksi).

HASIL DAN PEMBAHASAN

a. Alur Sistem Login dan Titik Kontrol Keamanan

Observasi menunjukkan alur autentikasi dimulai dari input username dan password pada halaman login. Sistem kemudian mengambil salt yang sesuai, melakukan hashing terhadap gabungan password dan salt, lalu membandingkannya dengan hash yang tersimpan di basis data. Dengan cara ini, sistem tidak perlu menyimpan maupun membandingkan password dalam bentuk asli.

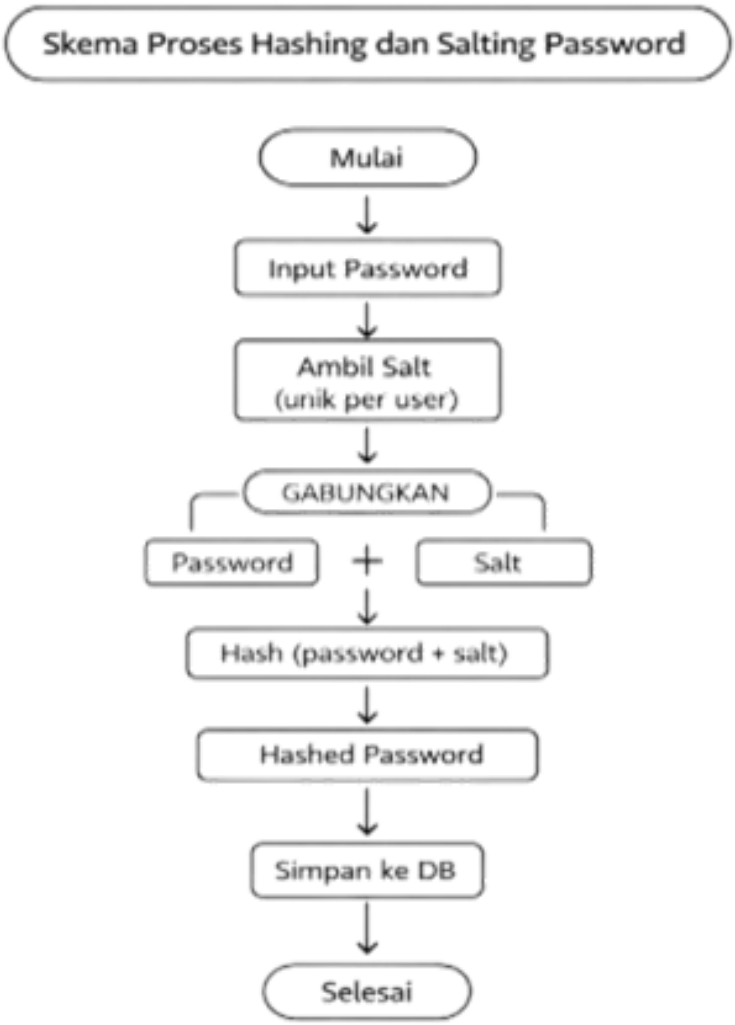


Gambar 1. Flowchart Sistem Login Menggunakan Hashing dan Salting Password

Flowchart pada Gambar 1 menampilkan percabangan keputusan (valid/tidak valid). Pada implementasi yang baik, percabangan ini perlu ditopang pembatasan percobaan login dan jeda (delay) agar serangan brute force menjadi tidak efisien.

b. Implementasi Hashing dan Salting Password

Dari analisis dokumentasi, password tidak disimpan sebagai plaintext. Sebelum disimpan, password diproses melalui hashing dan dikombinasikan dengan salt. Salt bersifat unik per pengguna sehingga walaupun dua pengguna memilih password yang sama, nilai hash di basis data tetap berbeda.



Gambar 2. Skema Proses Hashing dan Salting Password

Skema pada Gambar 2 menegaskan bahwa salt ditambahkan sebelum hashing. Praktik ini menurunkan risiko pemanfaatan rainbow table dan menghambat penyerang untuk melakukan pencocokan hash secara massal.

c. Evaluasi Ketahanan terhadap Ancaman

Kombinasi hashing dan salting meningkatkan ketahanan sistem terhadap beberapa ancaman. Pertama, brute force dan dictionary attack menjadi lebih mahal secara komputasi, terutama bila algoritma hashing khusus password digunakan. Kedua, rainbow table attack menjadi tidak efektif karena salt unik menghasilkan hash berbeda.

Ketiga, ketika basis data bocor, penyerang tidak memperoleh password mentah sehingga peluang pengambilalihan akun berkurang.

No	ASPEK	PLAINTEXT	HASH	HASH + SALT
1	Kerahasiaan password	Sangat rendah	sedang	Tinggi
2	Resiko Rainbow table	Sangat tinggi	Tinggi	Rendah
3	Dampak kebocoran DB	Akun mudah diambil	Tergantung kekuatan Hash	Jauh lebih sulit diekspolitasi
4	Pola password sama	Terlihat Sama	Hash bisa sama	Hash berbeda (Salt unik)

Gambar 3. Perbandingan Risiko Keamanan Berdasarkan Metode Penyimpanan Password

Ringkasan pada Gambar 3 menunjukkan bahwa penyimpanan plaintext merupakan kondisi paling berisiko. Hashing tanpa salt masih dapat meninggalkan peluang analisis pola dan serangan tabel pra-hitung. Hashing dengan salt unik memberikan tingkat perlindungan yang lebih baik.

d. Temuan Kelemahan dan Rekomendasi Teknis

Walaupun hashing dan salting sudah diterapkan, terdapat area yang perlu diperkuat agar keamanan lebih optimal: (1) gunakan algoritma hashing khusus password seperti bcrypt/Argon2/PBKDF2; (2) terapkan pembatasan percobaan login (rate limiting) dan/atau CAPTCHA; (3) buat kebijakan password kuat (panjang minimum, kombinasi karakter, larangan password umum); (4) gunakan HTTPS untuk mencegah penyadapan saat transmisi; (5) lakukan evaluasi keamanan berkala dan pembaruan konfigurasi.

KESIMPULAN

Penerapan hashing dan salting pada sistem login berbasis web meningkatkan keamanan penyimpanan password dengan mencegah plaintext dan menurunkan efektivitas serangan rainbow table. Evaluasi juga menunjukkan bahwa perlindungan autentikasi perlu didukung kontrol lain seperti rate limiting, kebijakan password yang kuat, dan koneksi aman (HTTPS). Rekomendasi utama penelitian ini adalah menggunakan algoritma hashing khusus password, mengelola salt secara unik per pengguna, serta menambahkan mekanisme penguatan proses login untuk menekan risiko serangan.

DAFTAR PUSTAKA

Kurniawan, A. (2018). Keamanan Sistem Informasi. Yogyakarta: Andi Offset.

Munir, R. (2019). Kriptografi. Bandung: Informatika.

Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Boston: Pearson Education.

OWASP Foundation. (2023). OWASP Top 10 Web Application Security Risks. Diakses dari https://owasp.org