Journal of System & Technology
ISSN: 3110-0171
Vol. 1, No. 2, Desember 2025

PENERAPAN KEAMANAN HASHING PASSWORD PADA SISTEM PENJUALAN BIBBI SHOP BERBASIS WEB

Rufaida Dermawan[1]*, Rakhmadi Rahman[1]
[1]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare
rufaidadermawan@gmailcom, rakhmadi.rahman@ith.ac.id
*Corresponding author: rufaidadermawan@gmailcom

Abstract: Keamanan penyimpanan password merupakan aspek krusial dalam sistem penjualan berbasis web, khususnya pada platform e-commerce yang mengelola data pengguna secara sensitif. Penelitian ini bertujuan untuk menganalisis penerapan algoritma hashing bcrypt dalam meningkatkan keamanan autentikasi pengguna pada sistem penjualan Bibbi Shop berbasis web. Metode penelitian yang digunakan adalah pendekatan rekayasa perangkat lunak dengan tahapan analisis kebutuhan, perancangan sistem keamanan, implementasi bcrypt pada proses registrasi dan login, serta pengujian keamanan penyimpanan password. Hasil penelitian menunjukkan bahwa penerapan bcrypt mampu meningkatkan tingkat keamanan penyimpanan password secara signifikan dibandingkan metode hashing konvensional, karena adanya mekanisme salt otomatis dan pengaturan cost factor yang dapat disesuaikan dengan kebutuhan sistem. Implementasi ini juga mampu meminimalkan risiko serangan seperti brute force dan rainbow table. Berdasarkan hasil analisis, dapat disimpulkan bahwa algoritma bcrypt efektif dan layak digunakan sebagai solusi keamanan autentikasi pada sistem penjualan berbasis web.

Keywords— Autentikasi, Bcrypt, E-Commerce, Hashing Password, Keamanan Web

I. PENDAHULUAN

Keamanan autentikasi merupakan salah satu aspek fundamental dalam pengembangan sistem berbasis web, khususnya pada platform yang mengelola data sensitif seperti sistem penjualan online. Password berperan sebagai elemen utama dalam mekanisme autentikasi, sehingga metode penyimpanan dan perlindungannya harus memenuhi standar keamanan yang memadai. Namun, pada praktiknya masih ditemukan penggunaan penyimpanan password dalam bentuk plaintext atau algoritma hashing yang telah usang seperti MD5 dan SHA-1, yang secara kriptografis terbukti rentan terhadap serangan brute force dan rainbow table[1]. Kelemahan ini berimplikasi langsung pada meningkatnya risiko pencurian akun, penyalahgunaan data pengguna, serta kompromi sistem secara menyeluruh.

Sebagai respons terhadap permasalahan tersebut, algoritma hashing modern seperti bcrypt banyak direkomendasikan dalam pengamanan aplikasi web. Bcrypt dirancang sebagai *slow hashing algorithm* yang secara sengaja memperlambat proses komputasi hash melalui mekanisme *cost factor*, serta dilengkapi dengan *salt* otomatis untuk mencegah serangan berbasis tabel pra-komputasi [2]. endekatan ini memberikan keunggulan dibandingkan algoritma hashing konvensional karena tingkat kesulitannya dapat disesuaikan dengan perkembangan kemampuan komputasi, sehingga meningkatkan daya tahan sistem terhadap serangan pemecahan password [3], [4].

Pada konteks implementasi aplikasi web di Indonesia, berbagai penelitian menunjukkan bahwa bcrypt telah banyak digunakan sebagai solusi keamanan autentikasi pada beragam sistem, seperti sistem informasi akademik, sistem layanan publik, dan aplikasi web komersial[3], [4], [5]. Hasil penelitian tersebut menegaskan bahwa bcrypt tidak hanya efektif dalam meningkatkan keamanan penyimpanan password, tetapi juga memiliki kompatibilitas yang baik dengan berbagai bahasa pemrograman dan framework modern [6]. Selain itu, penggunaan hashing yang tepat terbukti mampu menekan potensi kebocoran data serta mengurangi tingkat keberhasilan serangan berbasis kata sandi yang terus meningkat setiap tahun [7], [8].

Sistem penjualan Bibbi Shop sebagai platform e-commerce memerlukan mekanisme perlindungan password yang mampu menjamin kerahasiaan dan integritas data pengguna. Implementasi bcrypt dipandang relevan karena algoritma ini menghasilkan nilai hash yang unik meskipun password yang digunakan sama, sehingga menyulitkan penyerang dalam melakukan analisis pola atau eksploitasi kelemahan penyimpanan passwordword [9], [10]. Karakteristik tersebut menjadikan bcrypt sebagai solusi yang sesuai untuk kebutuhan keamanan autentikasi pada sistem penjualan berbasis web.

Namun demikian, keamanan autentikasi tidak hanya ditentukan oleh algoritma hashing yang digunakan, melainkan juga oleh arsitektur sistem yang mendukung proses autentikasi secara keseluruhan. Penerapan bcrypt perlu diintegrasikan dengan praktik keamanan lain, seperti validasi input yang ketat, manajemen sesi yang aman, serta pengaturan hak akses berbasis peran. Pendekatan ini membentuk sistem keamanan berlapis (*layered security*) yang mampu memberikan perlindungan lebih komprehensif terhadap berbagai skenario serangan siber[11], [12].

Aspek keberlanjutan keamanan juga menjadi pertimbangan penting dalam pengembangan sistem penjualan Bibbi Shop. Seiring dengan meningkatnya kemampuan perangkat keras dan teknik serangan modern, nilai *cost factor* pada bcrypt perlu dievaluasi dan disesuaikan secara berkala agar proses hashing tetap memberikan hambatan komputasi yang signifikan bagi penyerang tanpa menurunkan performa sistem secara

Dikirim 12-Des-2025 | Revisi 21-Des-2025 | Selesai Revisi 21-Des-2025 | Diterima 22-Des-2025

drastis[13]. Fleksibilitas ini merupakan salah satu alasan mengapa bcrypt tetap relevan dan banyak digunakan dalam praktik keamanan aplikasi web hingga saat ini.

Selain manfaat teknis, penerapan bcrypt juga berkontribusi pada peningkatan kepercayaan pengguna terhadap sistem. Dalam lingkungan e-commerce, persepsi keamanan data pribadi dan transaksi memiliki pengaruh besar terhadap loyalitas dan aktivitas pengguna. Sistem yang mampu menjamin keamanan autentikasi cenderung meningkatkan rasa aman pengguna dalam melakukan transaksi secara daring[14]. Oleh karena itu, implementasi bcrypt tidak hanya dipandang sebagai solusi teknis, tetapi juga sebagai bagian dari strategi peningkatan kualitas layanan.

Dengan fondasi autentikasi yang lebih kuat, sistem Bibbi Shop memiliki peluang untuk dikembangkan lebih lanjut melalui penerapan mekanisme keamanan tambahan, seperti *two-factor authentication* (2FA), deteksi anomali login, serta pemantauan aktivitas pengguna untuk mengidentifikasi akses yang mencurigakan [15]. Pengembangan ini diharapkan dapat menciptakan lingkungan e-commerce yang lebih aman, adaptif, dan terpercaya.

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk menerapkan algoritma bcrypt sebagai mekanisme hashing password pada sistem penjualan Bibbi Shop berbasis web. Penelitian difokuskan pada proses penerapan dan analisis alur kerja, desain arsitektur, serta integrasi bcrypt dalam sistem autentikasi, tanpa melakukan pengujian eksperimental.

II. METODE PENELITIAN

Penelitian ini tidak menggunakan desain eksperimen kuantitatif seperti pengujian performa, pengukuran waktu hashing, maupun simulasi serangan brute force atau rainbow table. Fokus penelitian diarahkan pada pendekatan pengembangan sistem dan analisis penerapan keamanan autentikasi, dengan tujuan mengevaluasi kesesuaian algoritma bcrypt dalam konteks sistem penjualan berbasis web.

Pendekatan metodologis yang digunakan bersifat deskriptif-analitis dan struktural, dengan mengadopsi prinsip System Development Life Cycle (SDLC) serta mengacu pada pedoman keamanan penyimpanan password dari OWASP sebagai standar praktik terbaik dalam pengamanan autentikasi aplikasi web[4], [5].

Metodologi ini dipilih karena penelitian berfokus pada proses penerapan, desain dan integrasi algoritma keamanan, bukan pada pengukuran kinerja komputasional algoritma secara eksperimental.

A. *Analisis Kebutuhan Keamanan*

Tahap awal dilakukan identifikasi kebutuhan keamanan sistem, yang meliputi:

1) Password harus disimpan dalam bentuk yang tidak dapat dikembalikan ke bentuk asli.
2) Sistem harus menggunakan algoritma hashing aman dengan salt.
3) Proses login harus menggunakan verifikasi hash, bukan membandingkan plaintext.
4) Struktur basis data harus mendukung penyimpanan hash yang panjang.

B. *Perancangan Arsitektur Keamanan*

Perancangan sistem autentikasi mencakup:

1) Penentuan lokasi hashing (server-side).
2) Integrasi bcrypt sebagai algoritma hashing utama.
3) Penyusunan alur registrasi dan login yang aman.
4) Desain tabel database yang hanya menyimpan hash, bukan password.

Alur penerapan bcrypt:

1) Pengguna memasukkan password.
2) Sistem menghasilkan salt otomatis.
3) Password + salt diproses menjadi hash.
4) Hash disimpan ke database.
5) Pada login, bcrypt membandingkan password dan hash menggunakan algoritma slow verification.

C. *Implementasi Bcrypt dalam Sistem*

Implementasi dilakukan menggunakan fungsi bawaan PHP, Hashing (gambar 1), dan Verifikasi login (gambar 2).

```php
$hashedPassword = password_hash($password, PASSWORD_BCRYPT);
```

Gambar 1. Hashing

```php
password_verify($password, $storedHash);
```

Gambar 2. Verify

Implementasi ini memastikan bahwa password asli tidak pernah disimpan atau diproses dalam bentuk yang dapat dilihat oleh pihak lain.

III. HASIL DAN PEMBAHASAN

A. *Hasil Penerapan Hashing Password*

Penerapan bcrypt berhasil dilakukan pada sistem Bibbi Shop. Password pengguna sekarang disimpan dalam bentuk hash seperti pada (gambar 3).

id	username	email	tanggal_lahir	jenis_kelamin	no_wa	password	role
1	admin		2000-01-01	Laki-laki	087547475621	$2y$10$wi1t0bKJUzt0K6kdZlQDwe9zuUqG0Ob8/7xn/n.Udt...	admin
9	rufaiddermawan	rufaiddermawan@gmail.com	2005-07-24	Perempuan	0895419694170	$2y$10$uPzSbz7zUVQI6Gg2yaBMee6KlEzVHv4A2AgB1.tqcG...	pembeli

Gambar 3. Hasil Implementasi Penerapan Hashing Password

Hash tersebut unik meskipun pengguna memiliki password yang sama. Salt otomatis mencegah serangan rainbow table.

B. *Integrasi dalam Sistem Registrasi dan Login*

1) Registrasi
   Sistem melakukan hashing sebelum memasukkan data ke database serta tidak ada password asli yang tersimpan dalam system.
2) Login
   Sistem tidak mencocokkan plaintext, tetapi memverifikasi hash menggunakan algoritma bcrypt yang bersifat slow-hash.

C. *Keamanan Data Pengguna*

Implementasi ini sesuai dengan standar dan panduan keamanan dari OWASP, NIST, dan praktik industri modern [4][6]. Dengan mekanisme ini, Bibbi Shop dapat meningkatkan kepercayaan pengguna dan mengurangi risiko serangan terkait autentikasi.

IV. IMPLIKASI

A. *Implikasi Praktis*

Selain meningkatkan keamanan penyimpanan kredensial, penerapan bcrypt juga memberikan dampak positif terhadap proses pengembangan sistem di masa mendatang. Dengan fondasi autentikasi yang lebih kuat, tim pengembang dapat mengintegrasikan modul keamanan lain tanpa mengubah arsitektur inti sistem. Hal ini memudahkan pengembangan fitur seperti pembatasan percobaan login (rate limiting), monitoring login realtime, serta penerapan kebijakan password yang lebih ketat. Implementasi bcrypt juga mengurangi risiko kebocoran data yang dapat menurunkan reputasi platform, sehingga menjadi aspek penting dalam menjaga kepercayaan pelanggan terhadap Bibbi Shop sebagai sistem e-commerce yang aman dan profesional.

B. *Implikasi Teoritis*

Secara teoritis, penelitian ini turut memperkuat literatur yang membahas pentingnya penggunaan algoritma hashing modern dalam keamanan web. Penggunaan bcrypt membuktikan bahwa mekanisme hashing adaptif lebih unggul dibandingkan metode hashing statis seperti SHA-1 atau MD5. Studi ini juga memperkaya referensi mengenai penerapan slow hashing algorithm dalam konteks aplikasi e-commerce, yang dapat dijadikan basis bagi penelitian lanjutan tentang kombinasi hash, enkripsi tingkat lanjut, dan autentikasi multi-lapis. Dengan demikian, penelitian ini berkontribusi pada pengembangan teori keamanan siber yang berfokus pada perlindungan identitas digital dan manajemen kredensial pengguna.

V. KETERBATASAN

Penelitian ini hanya menjelaskan penerapan hashing password tanpa melakukan pengujian performa, perbandingan algoritma, atau simulasi serangan. Selain itu, implementasi terbatas pada platform berbasis PHP.

Selain keterbatasan yang telah disebutkan, penelitian ini juga belum membahas pengujian keamanan dari sisi serangan nyata seperti injection attack, session hijacking, atau credential stuffing yang kerap terjadi pada aplikasi e-commerce. Penelitian juga terbatas pada penggunaan bcrypt tanpa analisis komparatif performa secara mendalam terhadap algoritma modern lainnya, seperti Argon2 yang merupakan pemenang Password Hashing Competition (PHC).

Selain itu, lingkungan pengujian hanya mencakup implementasi lokal tanpa memperhitungkan skenario skalabilitas pada server produksi yang memiliki beban pengguna lebih besar. Faktor seperti efisiensi cost factor pada server dengan trafik tinggi juga belum diuji secara empiris.

VI. REKOMENDASI PENELITIAN SELANJUTNYA

Disarankan untuk melakukan penelitian lanjutan dengan:

1) Pengujian performa berbagai algoritma hashing seperti Argon2, PBKDF2, dan bcrypt.
2) Simulasi serangan brute force untuk evaluasi ketahanan hash.
3) Integrasi multi-factor authentication untuk peningkatan keamanan.
4) Analisis dampak cost factor yang berbeda terhadap performa server, khususnya pada lingkungan e-commerce yang memiliki jumlah transaksi dan permintaan autentikasi yang tinggi.
5) Pengembangan sistem autentikasi berbasis perilaku (behavior-based authentication) yang dapat mendeteksi anomali aktivitas pengguna seperti perubahan pola login, perangkat baru, atau lokasi geografis tidak biasa.
6) Penerapan intrusion detection system (IDS) khusus untuk aktivitas login guna memperkuat keamanan berlapis dan mencegah eksploitasi kredensial.

VII. KESIMPULAN

Penelitian ini menunjukkan bahwa penerapan hashing password menggunakan bcrypt pada sistem penjualan Bibbi Shop mampu meningkatkan keamanan autentikasi pengguna. Mekanisme salt otomatis dan cost factor fleksibel menjadikan bcrypt lebih unggul dibanding metode hashing konvensional. Dengan arsitektur yang sederhana dan kompatibilitas tinggi, bcrypt menjadi solusi yang efektif dan aman dalam pengelolaan password pada aplikasi web.

Secara keseluruhan, penerapan bcrypt tidak hanya meningkatkan keamanan teknis sistem, tetapi juga memberikan nilai strategis bagi keberlanjutan operasional Bibbi Shop. Penggunaan algoritma hashing modern membuktikan bahwa keamanan password dapat ditingkatkan dengan pendekatan teknologi yang tepat. Bcrypt menyediakan mekanisme perlindungan yang relevan untuk menghadapi ancaman siber yang terus berkembang serta memberikan fleksibilitas bagi pengembang untuk menyesuaikan tingkat keamanan tanpa rekonstruksi besar pada sistem. Dengan demikian, solusi ini sangat layak diterapkan pada berbagai platform digital yang mengandalkan kredensial pengguna sebagai kunci akses utama.

VIII. SARAN

Diharapkan sistem dapat dikembangkan lebih lanjut dengan peningkatan fitur keamanan seperti proteksi brute force, lockout policy, serta integrasi CAPTCHA untuk mencegah percobaan login otomatis.

Selain pengembangan fitur keamanan tambahan, sistem juga disarankan untuk menerapkan pemantauan keamanan secara berkala (security auditing) untuk

memastikan tidak ada celah baru yang muncul seiring pembaruan fitur. Penerapan log aktivitas yang terstruktur dan terenkripsi dapat membantu mendeteksi pola login mencurigakan sejak dini.

Selain itu, penting bagi pengelola untuk memberikan edukasi kepada pengguna terkait pembuatan password yang kuat, penggunaan 2FA, serta kewaspadaan terhadap serangan phishing yang sering menyasar pengguna e-commerce. Peningkatan kesadaran keamanan pengguna akan memperkuat keamanan sistem secara keseluruhan.

DAFTAR PUSTAKA

[1] R. Dafi Al Azhar and I. Sholihah Widiati, "Evaluasi Keamanan Penyimpanan Password Menggunakan Algoritma Hash: MD5, SHA-1, dan Bcrypt," *Pros. Semin. Nas. Teknol. Inf. Dan Bisnis*, pp. 1302–1305, July 2025, doi: 10.47701/q885nj69.

[2] R. Patra and S. Patra, "Cryptography: A Quantitative Analysis of the Effectiveness of Various Password Storage Techniques," *J. Stud. Res.*, vol. 10, no. 3, Oct. 2021, doi: 10.47611/jsrhs.v10i3.1764.

[3] S. E. P. Sohidin, H. P. Utomo, and A. Ahmadi, "Penerapan Algoritma Bcrypt untuk Pengamanan Password pada Sistem Informasi Akademik (SIAK)," 2025.

[4] M. D. Akbar and A. Antoni, "Aplikasi Absensi Pegawai pada Dinas Komunikasi dan Informatika Kabupaten Deli Serdang dengan QR Code Menggunakan Algoritma Bcrypt," *Sudo J. Tek. Inform.*, vol. 1, no. 1, pp. 8–16, Mar. 2022, doi: 10.56211/sudo.v1i1.2.

[5] Nugroho Dwi Aji, Tomi Tri Sujaka, Husain, Ondi Asroni, and Kurniadin Abd. Latif, "Analisis Dan Implementasi Algoritma Bcrypt Dengan Affine Cipher Untuk Pengamanan Password Pada Aplikasi Web: Analysis And Implementation Of Bcrypt Algorithm With Affine Cipher For Password Security In Web Applications," *Cyber Secur. Dan Forensik Digit.*, vol. 8, no. 1, pp. 1–9, June 2025, doi: 10.14421/csecurity.2025.8.1.5076.

[6] G. D. M. Zulma, H. B. Seta, and T. Yuniati, "IMPLEMENTASI ALGORITMA AES DAN BCRYPT UNTUK PENGAMANAN FILE DOKUMEN," *Inform. J. Ilmu Komput.*, vol. 18, no. 2, p. 163, Aug. 2022, doi: 10.52958/iftk.v18i2.4667.

[7] G. D. M. Zulma, H. B. Seta, and T. Yuniati, "IMPLEMENTASI ALGORITMA AES DAN BCRYPT UNTUK PENGAMANAN FILE DOKUMEN," *Inform. J. Ilmu Komput.*, vol. 18, no. 2, p. 163, Aug. 2022, doi: 10.52958/iftk.v18i2.4667.

[8] M. A. Ramadhan, A. Arpinda, D. Saputra, and D. I. Mulyana, "Pencegahan Serangan Berbasis Kata Sandi: Studi Komprehensif Tentang Implementasi Hash Pada Aplikasi Web," *INTECOMS J. Inf. Technol. Comput. Sci.*, vol. 7, no. 3, pp. 920–925, June 2024, doi: 10.31539/intecoms.v7i3.9526.

[9] K. W. Prima, "Balancing Data Security: A Comparative Review of Hashing and Non-Hashing Approaches in Data Storage," *J. Embed. Syst. Secur. Intell. Syst.*, pp. 268–278, June 2025, doi: 10.59562/jessi.v6i2.9257.

[10] V. Simangunsong, Y. R. Hutasoit, and D. Siallagan, "Analisis Terhadap Keamanan Password Menggunakan Hash SHA-256".

[11] R. Dafi Al Azhar and I. Sholihah Widiati, "Evaluasi Keamanan Penyimpanan Password Menggunakan Algoritma Hash: MD5, SHA-1, dan Bcrypt," *Pros. Semin. Nas. Teknol. Inf. Dan Bisnis*, pp. 1302–1305, July 2025, doi: 10.47701/q885nj69.

[12] K. N. Isnaini, D. Suhartono, M. T. Jamil, and A. Qothrunnada, "Implementasi Pengamanan Data Menggunakan Teknik Bcrypt Hashing Password dan Algoritma Advanced Encryption Standard (AES)," vol. 13, no. 1, 2025.

[13] G. D. M. Zulma, H. B. Seta, and T. Yuniati, "IMPLEMENTASI ALGORITMA AES DAN BCRYPT UNTUK PENGAMANAN FILE DOKUMEN," *Inform. J. Ilmu Komput.*, vol. 18, no. 2, p. 163, Aug. 2022, doi: 10.52958/iftk.v18i2.4667.

[14] M. L. Assidiq, F. Mahardika, and D. Santika, "Implementasi Algoritma Kriptografi AES dan SHA-3 Dalam Mengamankan Data Sensitif Pengguna Pada Website Transaksi," *Simpatik J. Sist. Inf. Dan Inform.*, vol. 4, no. 1, pp. 44–52, June 2024, doi: 10.31294/simpatik.v4i1.3386.

[15] E. A. Suharman, H. P. Utomo, and A. Ahmadi, "Implementasi 2FA untuk Keamanan Sistem Informasi Akademik di Universitas Langlangbuana," 2025.