Jurnal Sistem Cerdas dan Rekayasa (JSCR)
Volume 8 , Nomor 1, Juni 2026
Website Jurnal : ojs.widyakartika.ac.id/index.php/jscr

Implementasi *Cryptography Based Multilayer Authentication* pada Sistem Login Berbasis Web Menggunakan *Bcrypt Hashing* dan *One Time Password (OTP)*

Nurul Jannah[1], Lailatul Istianah[2], Muhlis Tahir[3]

[1]Pendidikan Informatika, Universitas Trunodjoyo Madura, Bangkalan, Indonesia, 230631100114@student.trunojoyo.ac.id
[2]Pendidikan Informatika, Universitas Trunodjoyo Madura, Bangkalan, Indonesia, 230631100116@student.trunojoyo.ac.id
[3]Pendidikan Informatika, Universitas Trunodjoyo Madura, Bangkalan, Indonesia, muhlis.tahir@trunojoyo.ac.id

STATUS ARTIKEL

Dikirim 26 April 2026
Direvisi 29 April 2026
Diterima 09 Juni 2026

Kata Kunci:
Autentikasi, Bcrypt, Keamanan Sistem, OTP, Web

A B S T R A K

Meningkatnya penggunaan layanan berbasis internet menuntut sistem login web memiliki tingkat keamanan yang lebih baik. Autentikasi yang hanya menggunakan email dan password masih menyimpan risiko, terutama terhadap percobaan brute force dan kebocoran data pengguna. Untuk mengatasi hal tersebut, penelitian ini mengembangkan sistem login berbasis web dengan menerapkan dua lapisan keamanan, yaitu bcrypt hashing dan OTP. Metode pengembangan yang digunakan adalah SDLC dengan model Waterfall, mencakup tahap kebutuhan, perancangan, pembuatan, dan pengujian sistem. Aplikasi dibuat menggunakan Flask berbasis Python, database SQLite, bcrypt untuk enkripsi password, serta SMTP sebagai media pengiriman OTP. Hasil pengujian membuktikan bahwa sistem lebih aman karena password tidak disimpan dalam bentuk asli dan login harus melewati verifikasi OTP.

1. PENDAHULUAN

Kemajuan teknologi informasi yang semakin dinamis menjadikan internet sebagai kebutuhan utama dalam berbagai aktivitas masyarakat modern (Pamungkas and Zulaiman Zaney 2021). Website kini tidak hanya berperan sebagai sumber informasi, melainkan juga sebagai media interaksi, transaksi jual beli, dan layanan keuangan berbasis online (Faqih et al. 2023).

Seiring meningkatnya pemanfaatan teknologi tersebut, keamanan jaringan menjadi perhatian penting, khususnya pada sistem yang melibatkan banyak pengguna dan perangkat (Wahyusesa, Hidayanto, and Ramdayani 2023). Jumlah perangkat yang saling terhubung dapat memperbesar kemungkinan terjadinya ancaman terhadap data. Oleh karena itu, setiap proses identifikasi pengguna dalam sistem perlu didukung oleh metode yang dapat memverifikasi keaslian identitas pengguna secara tepat (Azhar, Arkarni, and Atthariq 2020).

Login menjadi komponen penting karena berperan sebagai akses awal menuju sistem. Sayangnya, banyak sistem masih menerapkan autentikasi dasar berupa email dan password. Cara ini memiliki risiko tinggi terhadap serangan brute force, dictionary attack, maupun kebocoran kredensial. Selain itu, kebiasaan pengguna yang membuat password sederhana atau menggunakan password yang sama di berbagai layanan turut memperbesar potensi kebocoran data. Kondisi ini menunjukkan pentingnya penerapan sistem keamanan login yang lebih kuat.

Salah satu strategi yang dapat diterapkan untuk memperkuat keamanan sistem adalah penggunaan kriptografi. Kriptografi merupakan bidang ilmu yang berfungsi melindungi informasi dengan cara menyamarkan data agar tidak dapat dipahami oleh pihak yang tidak memiliki hak akses. Istilah kriptografi berasal dari bahasa Yunani, yaitu *kripto* yang berarti menyembunyikan dan *graphia* yang berarti tulisan, sehingga secara harfiah dapat dimaknai sebagai tulisan tersembunyi (Hidayat et al., 2023). Dalam keamanan transaksi digital, hashing menjadi salah satu teknik kriptografi yang berperan penting dalam menjaga keutuhan data (Iqbal & Sari Harahap, 2026). Pada proses autentikasi, hashing digunakan untuk menyimpan kata sandi dalam bentuk hash agar lebih aman. Namun, hashing sederhana masih memiliki risiko terhadap serangan *brute force* dan *rainbow table*. Oleh karena itu, algoritma bcrypt digunakan karena memiliki mekanisme *salt* dan *cost factor* yang membuat proses peretasan menjadi lebih sulit. Saputra dan Kurniati (2026) menyatakan bahwa penerapan bcrypt pada sistem autentikasi mampu meningkatkan perlindungan data login dan menekan risiko penyalahgunaan password.

Upaya peningkatan keamanan sistem login dapat dilakukan tidak hanya dengan menerapkan hashing pada password, tetapi juga dengan menambahkan lapisan autentikasi tambahan berupa One Time Password (OTP). OTP merupakan kode verifikasi yang digunakan secara terbatas, yaitu hanya satu kali dalam satu sesi autentikasi pengguna. Kode ini bersifat acak, sementara, dan tidak dapat digunakan ulang, sehingga memberikan perlindungan tambahan terhadap ancaman keamanan sistem (Maulana et al., 2025). Studi terdahulu mengungkapkan bahwa penerapan OTP dalam sistem login mampu memperkuat proses autentikasi karena dilengkapi dengan mekanisme kedaluwarsa. Artinya, kode OTP hanya dapat digunakan dalam rentang waktu tertentu dan harus merupakan kode terbaru yang diterbitkan oleh sistem, sehingga dapat mengurangi kemungkinan penyalahgunaan akun oleh pihak yang tidak berwenang (Azhar et al., 2020).

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada perancangan dan pembangunan sistem login berbasis web yang lebih aman melalui penerapan autentikasi ganda menggunakan bcrypt hashing dan One Time Password (OTP). Integrasi kedua metode tersebut diharapkan dapat meningkatkan keamanan informasi pengguna serta memperkecil risiko masuknya pihak yang tidak memiliki hak akses ke dalam sistem.

2. METODE PENELITIAN

Dalam penelitian ini, proses pengembangan sistem dilakukan menggunakan metode System Development Life Cycle (SDLC) dengan pendekatan Waterfall. Pendekatan tersebut memungkinkan pengembangan berjalan secara runtut, mulai dari tahap analisis kebutuhan sampai pada proses pengujian. Setiap tahapan menghasilkan output yang jelas sebagai dasar untuk melanjutkan ke tahap berikutnya, sehingga proses pengembangan sistem dapat berlangsung lebih terarah dan minim kesalahan (Steven et al. 2018).

2.1 Analisis Kebutuhan

Pada tahap ini dilakukan identifikasi kebutuhan sistem yang akan dibuat. Meliputi:

- Sistem memfasilitasi pengguna dalam melakukan registrasi akun.

- Sistem menerapkan bcrypt untuk menyimpan kata sandi dalam format hash yang lebih aman.
- Sistem memungkinkan pengguna melakukan proses masuk ke dalam akun.
- Sistem dapat membuat kode OTP untuk mendukung keamanan autentikasi.
- Sistem mengirimkan kode OTP secara otomatis ke email pengguna.
- Sistem memastikan OTP yang dimasukkan valid sebelum pengguna memperoleh akses login

2.2 Perancangan Sistem

Pada fase perancangan, alur sistem dirancang untuk menggambarkan tahapan login dari awal hingga akhir. Pengguna memasukkan email dan kata sandi, lalu sistem memverifikasi kata sandi dengan metode bcrypt. Setelah proses tersebut, pengguna diminta mengisi kode OTP yang sebelumnya telah dikirimkan ke email pengguna.

2.3 Implementasi sistem

Pada tahap ini, sistem mulai dibuat sesuai rancangan. Sistem dikembangkan menggunakan:

- *Python* sebagai bahasa pemrograman
- *Flask* sebagai framework web
- *SQLite* sebagai database
- Bcrypt untuk hashing password
- SMTP untuk mengirim OTP

2.4 Pengujian Sistem

Setelah sistem selesai dibuat, dilakukan pengujian untuk memastikan semua fitur berjalan dengan baik.

Pengujian dilakukan pada beberapa bagian, seperti:

- Registrasi pengguna
- Login dengan password benar dan salah
- Pengiriman OTP
- Verifikasi OTP
- Akses dashboard setelah login

3. HASIL DAN PEMBAHASAN

3.1 Hasil Implementasi Sistem

Sistem berbasis web ini dibangun untuk mendukung keamanan akses pengguna, khususnya pada tahap login. Di dalamnya terdapat fitur registrasi, autentikasi login, verifikasi kode OTP, dan halaman dashboard

Pada gambar 3.1 Pengguna diminta untuk input email password agar dapat mengakses sistem. Setelah itu sistem akan memverifikasi data yang dimasukkan.

Gambar 3.1 Halaman Login

Kemudian, sistem memeriksa kecocokan password menggunakan bcrypt. Jika autentikasi berhasil, sistem akan melanjutkan ke proses selanjutnya.

Setelah itu, sistem akan menerbitkan kode OTP dan mengirimkannya ke email pengguna sebagai bentuk autentikasi lanjutan.

Gambar 3.2 Halaman Verifikasi OTP

Setelah menerima kode OTP, pengguna diminta untuk memasukkannya ke dalam sistem. Jika OTP yang diinput sesuai dan masih dalam masa berlaku, maka login berhasil dilakukan. Pengguna kemudian diarahkan ke halaman dashboard sebagai halaman awal setelah masuk. Dashboard tersebut menjadi bukti bahwa pengguna telah lolos dari proses autentikasi dua tahap, yaitu pengecekan password dan verifikasi OTP.

3.2 Pembahasan

Implementasi sistem menunjukkan adanya peningkatan keamanan dibandingkan metode login konvensional. Bcrypt digunakan untuk melindungi password agar tidak tersimpan dalam bentuk asli, sedangkan OTP berfungsi sebagai verifikasi tambahan. Dengan demikian, sistem memiliki mekanisme autentikasi yang lebih aman dan berlapis.

4. KESIMPULAN

Hasil penelitian menunjukkan bahwa sistem login berbasis web yang memanfaatkan autentikasi ganda melalui bcrypt dan OTP dapat berjalan secara efektif. Bcrypt memberikan kontribusi penting dalam menjaga keamanan password dengan cara mengubah data asli menjadi bentuk hash, sehingga informasi sensitif tidak mudah dibaca maupun dimanfaatkan oleh pihak yang tidak berwenang. Sementara itu, OTP berfungsi sebagai tahapan verifikasi tambahan yang memperketat proses autentikasi pengguna. Adanya masa berlaku pada kode OTP juga menjadi langkah preventif untuk menghindari penggunaan kode secara tidak sah. Oleh karena itu, integrasi bcrypt dan OTP mampu menghasilkan sistem login yang lebih aman dan kuat dibandingkan sistem login biasa yang hanya menggunakan kata sandi.

5. UCAPAN TERIMA KASIH

Dengan penuh rasa syukur, penulis mengucapkan terima kasih kepada Tuhan Yang Maha Esa atas segala karunia-Nya sehingga penelitian ini dapat diselesaikan dengan lancar. Penghargaan dan terima kasih juga penulis sampaikan kepada dosen pengampu mata kuliah Sistem Keamanan Jaringan atas bimbingan, masukan, dan arahan yang diberikan selama proses penelitian. Selain itu, penulis turut berterima kasih kepada seluruh pihak yang telah mendukung pengembangan sistem hingga penelitian ini dapat tersusun dengan baik

6. DAFTAR PUSTAKA

Azhar, Wais Arkarni, and Atthariq. 2020. “Sistem Keamanan Pada Halaman Login Menggunakan One Time Password 1.” 01(November):106–13.

Faqih, Fauziah Nur, Muhlis Tahir, Zarwanda Ashfarina, and Robby Irsyad. 2023. “Efektivitas Peningkatan Keamanan Login Pada Website Menggunakan Enkripsi Caesar Chipper

Pendahuluan Peningkatan Teknologi Informasi Dan Internet Telah Membuat Banyak Orang Bergantung." 01(02):354–62.

Hidayat, Maulid, Muhlis Tahir, Achmad Sukriyadi, Amir Sulton, and Article History. 2023. "Penerapan Kriptografi Caesar Chiper Dalam Pengamanan Data." 2(3):35–41.

Iqbal, Muhammad, and Nurlina Sari Harahap. 2026. "METODE PEMBAYARAN ELEKTRONIK BERDASARKAN PADA KRIPTOGRAFI." *JATI (Jurnal Mahasiswa Teknik Informatika)* 10(2):2167–73.

Liauren, Richie Mulyo, Baizul Zaman, and Syamsul Bahri. 2025. "IMPLEMENTASI ALGORITMA AES DAN BCRYPT UNTUK PENGAMANAN." 20(01):57–71.

Maulana, Fajar, Yomei Hendra, Putri Sakinah, Yofhanda Septi Eirlangga, and Aisyah Qurrata Ayun. 2025. "Efektivitas Dan Kelemahan Autentikasi Berbasis Web Menggunakan One-Time Password (OTP) Dalam Mencegah Akses Tidak Sah." 12(3).

Pamungkas, Ridho, and Ferdinand Wahyu Zulaiman Zaney. 2021. "Penerapan Hashing SHA1 Dan Algoritma Asimetris RSA Untuk Keamanan Data Pada Sistem Informasi Berbasis Web." *Journal of Computer, Information System, & Technology Management* 4(1):84–89.

Saputra, Aryan, and Rezki Kurniati. 2026. "APLIKASI PENJUALAN UDANG PEPAI BERBASIS WEB DENGAN." *Jurnal Mahasiswa Teknik Informatika* 10(1):726–33.

Steven, Weiskhy, Wahyu Nugraha, Muhamad Syarif, and Weiskhy Steven Dharmawan. 2018. "PENERAPAN METODE SDLC WATERFALL DALAM SISTEM INFORMASI." 03(01):23–29.

Wahyusesa, Anggriawan Sifa, Pradana Wahyu Hidayanto, and Enen Arienda Ramdayani. 2023. "Solusi Cerdas : Meningkatkan Keamanan Dan Kinerja Jaringan Pada Warnet Dengan Mengatasi Kelemahan Sistem Dike : Jurnal Ilmu Multidisiplin." 1:62–66.