# IMPLEMENTASI *ALGORITMA BLOWFISH* UNTUK KEAMANAN DATA *LOGIN* PADA *WEBSITE*

**Irfan Sazali, Rezki Kurniati, Muhammad Ikhsan Wibowo**
Teknik Informatika, Politeknik Negeri Bengkalis
Jalan Bathin Alam Desa Sungai Alam, Kab. Bengkalis, Indonesia
*irfansazali822@gmail.com*

**ABSTRAK**

Keamanan data login merupakan aspek penting dalam sistem informasi berbasis web, khususnya pada website akademik yang menyimpan data sensitif dan memiliki akun dengan hak akses tinggi. Website Teknik Informatika Politeknik Negeri Bengkalis masih memiliki potensi kerentanan pada sistem login akibat penggunaan metode pengamanan kata sandi yang kurang optimal, sehingga berisiko terhadap serangan siber seperti *brute force attack* dan pencurian kredensial. Penelitian ini bertujuan untuk meningkatkan keamanan data autentikasi dengan mengimplementasikan algoritma Blowfish pada sistem login website. Metode penelitian yang digunakan adalah metode pengembangan sistem yang meliputi tahap identifikasi masalah, analisis kebutuhan sistem, perancangan sistem, implementasi, dan pengujian. Algoritma Blowfish diterapkan untuk mengenkripsi password sebelum disimpan ke dalam basis data, serta dikombinasikan dengan mekanisme autentikasi dua faktor berbasis OTP dan pembatasan percobaan login. Hasil penelitian menunjukkan bahwa password berhasil disimpan dalam bentuk *ciphertext* dan tidak dapat dibaca secara langsung, sistem login berjalan sesuai fungsionalitas yang diharapkan, serta mekanisme OTP efektif dalam mencegah percobaan login berulang dan serangan *brute force*. Dengan demikian, penerapan algoritma Blowfish terbukti mampu meningkatkan keamanan data login pada website akademik.

***Kata kunci :*** *Keamanan Data, Sistem Login, Algoritma Blowfish, OTP, Brute Force Attack*

## 1. PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat telah mendorong pemanfaatan website sebagai media utama dalam penyediaan layanan dan pengelolaan data pada berbagai sektor, termasuk sektor pendidikan. Website tidak hanya berfungsi sebagai sarana penyampaian informasi, tetapi juga sebagai sistem penyimpanan data yang bersifat sensitif, seperti data akademik dan data autentikasi pengguna. Sistem login menjadi komponen krusial karena berperan sebagai gerbang awal dalam mengendalikan hak akses pengguna terhadap sistem informasi, sehingga kelemahan pada mekanisme login dapat berdampak langsung pada kebocoran data dan penyalahgunaan akses [1].

Seiring meningkatnya penggunaan sistem berbasis web, ancaman keamanan siber juga mengalami peningkatan yang signifikan. Serangan seperti *brute force attack* kerap memanfaatkan lemahnya sistem autentikasi untuk memperoleh akses tidak sah dengan mencoba berbagai kombinasi kata sandi secara berulang. Apabila data login dikirim dan disimpan tanpa perlindungan kriptografi yang memadai, maka risiko pencurian identitas dan peretasan sistem akan semakin besar [2].

Website Teknik Informatika Politeknik Negeri Bengkalis merupakan sistem informasi akademik yang berfungsi sebagai pusat layanan digital bagi mahasiswa, dosen, dan pengelola jurusan. Website ini menyimpan data penting, termasuk akun administrator yang memiliki hak akses penuh terhadap sistem. Berdasarkan dokumentasi dan pengamatan, dalam kurun waktu satu tahun terakhir website tersebut beberapa kali mengalami gangguan keamanan yang mengindikasikan adanya kerentanan pada sistem login, khususnya pada pengamanan data username dan password [3].

Salah satu penyebab utama kerentanan tersebut adalah masih digunakannya algoritma hashing lama seperti Message Digest Algorithm 5 (MD5). MD5 merupakan algoritma hash kriptografi yang menghasilkan nilai hash 128-bit dan telah lama digunakan dalam pengamanan kata sandi. Namun, sejak ditemukannya berbagai celah keamanan dan serangan kolisi, MD5 dinilai tidak lagi aman untuk melindungi data sensitif, terutama terhadap serangan *brute force* dan *dictionary attack* [4].

Kriptografi modern menawarkan solusi yang lebih andal untuk mengatasi permasalahan keamanan data login. Algoritma Blowfish merupakan salah satu algoritma kriptografi simetris yang dirancang untuk memberikan tingkat keamanan tinggi dengan performa yang efisien. Blowfish menggunakan blok data 64-bit dengan panjang kunci yang bervariasi antara 32 hingga 448 bit, sehingga memberikan fleksibilitas dan ketahanan yang baik terhadap berbagai jenis serangan kriptografi [5].

Keunggulan algoritma Blowfish terletak pada struktur *Feistel network* yang terdiri dari 16 ronde enkripsi dengan operasi sederhana seperti XOR, penambahan modulo, dan substitusi menggunakan S-box. Struktur ini menjadikan Blowfish sulit untuk diretas tanpa kunci yang sah, sekaligus memiliki kecepatan proses yang tinggi, sehingga cocok diterapkan pada sistem login berbasis web yang membutuhkan respons cepat [6].

Berbagai penelitian terdahulu menunjukkan bahwa penerapan algoritma Blowfish efektif dalam meningkatkan keamanan data pada sistem berbasis web. Blowfish telah berhasil diterapkan pada sistem e-commerce, manajemen surat digital, pengamanan file multimedia, hingga sistem autentikasi website, dengan hasil yang menunjukkan peningkatan perlindungan data serta ketahanan terhadap serangan *brute force* dan manipulasi basis data [7], [8].

Selain penerapan algoritma enkripsi yang kuat, keamanan sistem login juga dapat ditingkatkan dengan mekanisme tambahan seperti pembatasan jumlah percobaan login dan autentikasi dua faktor (*Two-Factor Authentication*). Penggunaan kode OTP sebagai lapisan keamanan tambahan terbukti mampu mengurangi risiko akses ilegal meskipun kredensial utama berhasil diketahui oleh pihak tidak berwenang [9].

Berdasarkan permasalahan tersebut, diperlukan penerapan metode pengamanan yang lebih andal dan relevan dengan perkembangan ancaman siber saat ini. Oleh karena itu, penelitian ini berfokus pada implementasi algoritma Blowfish untuk mengamankan data login pada website Teknik Informatika Politeknik Negeri Bengkalis. Implementasi ini diharapkan mampu meningkatkan kerahasiaan dan keamanan data autentikasi, serta meminimalkan risiko kebocoran data akibat serangan siber [10].

Keamanan data login merupakan aspek krusial dalam pengelolaan sistem informasi berbasis web, khususnya pada website akademik yang menyimpan data sensitif dan memiliki akun dengan hak akses tinggi. Sistem login berfungsi sebagai pintu utama autentikasi pengguna, sehingga setiap kelemahan pada mekanisme ini dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk memperoleh akses ilegal ke dalam sistem.

Permasalahan utama yang dihadapi pada website Teknik Informatika Politeknik Negeri Bengkalis adalah masih lemahnya sistem pengamanan data login. Website tersebut masih menggunakan metode pengamanan kata sandi yang tidak lagi relevan dengan perkembangan ancaman siber, seperti algoritma hashing lama yang rentan terhadap serangan *brute force* dan *dictionary attack*. Kondisi ini diperparah dengan meningkatnya frekuensi serangan siber yang menargetkan sistem autentikasi, sehingga berpotensi menyebabkan kebocoran data login, pengambilalihan akun administrator, dan gangguan terhadap layanan akademik.

Selain itu, sistem login yang ada belum dilengkapi dengan mekanisme pengamanan tambahan seperti pembatasan percobaan login dan autentikasi berlapis. Akibatnya, sistem menjadi lebih mudah dieksploitasi oleh penyerang yang mencoba berbagai kombinasi kata sandi secara berulang tanpa adanya perlindungan yang memadai. Permasalahan-permasalahan tersebut menunjukkan perlunya penerapan metode pengamanan yang lebih kuat, modern, dan sesuai dengan karakteristik sistem berbasis web.

Penelitian ini bertujuan untuk mengimplementasikan algoritma Blowfish sebagai metode pengamanan data login pada website Teknik Informatika Politeknik Negeri Bengkalis. Penerapan algoritma Blowfish diharapkan mampu meningkatkan tingkat keamanan data autentikasi, khususnya *username* dan *password*, agar tidak tersimpan dalam bentuk yang mudah dibaca atau disalahgunakan oleh pihak tidak berwenang. Selain itu, penelitian ini bertujuan untuk mengurangi risiko serangan siber seperti *brute force attack* dan pencurian kredensial dengan memanfaatkan karakteristik Blowfish yang memiliki tingkat keamanan tinggi dan performa enkripsi yang efisien. Melalui penerapan sistem login yang lebih aman dan andal, penelitian ini juga diharapkan dapat memberikan kontribusi akademik dalam pengembangan sistem keamanan berbasis kriptografi pada aplikasi web, khususnya di lingkungan akademik.

Rencana penyelesaian masalah dalam penelitian ini dilakukan melalui pendekatan sistematis yang dimulai dengan analisis terhadap sistem login yang berjalan untuk mengidentifikasi kelemahan pada mekanisme autentikasi dan metode pengamanan data login. Setelah itu, dilakukan perancangan sistem keamanan login dengan mengintegrasikan algoritma Blowfish sebagai metode enkripsi password sebelum data disimpan atau diverifikasi di dalam basis data. Implementasi algoritma Blowfish dilakukan pada proses login sehingga data autentikasi tidak pernah berada dalam bentuk *plaintext*. Untuk meningkatkan perlindungan sistem, ditambahkan mekanisme keamanan pendukung berupa pembatasan jumlah percobaan login dan autentikasi tambahan menggunakan kode OTP sebagai lapisan keamanan kedua. Tahap akhir dari penyelesaian masalah adalah melakukan pengujian dan evaluasi sistem untuk memastikan bahwa proses enkripsi berjalan dengan benar serta sistem mampu meminimalkan risiko serangan siber, khususnya serangan *brute force* terhadap akun administrator.

## 2. TINJAUAN PUSTAKA

### 2.1. Keamanan Data

Keamanan data merupakan upaya untuk melindungi informasi dari akses, penggunaan, pengungkapan, perubahan, maupun perusakan oleh pihak yang tidak berwenang. Dalam sistem informasi berbasis web, keamanan data menjadi aspek yang sangat penting karena data disimpan dan diakses melalui jaringan terbuka. Tujuan utama dari keamanan data adalah menjaga kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi agar tetap dapat digunakan sesuai dengan fungsinya dan terhindar dari ancaman siber [1].

### 2.2. Sistem Login dan Autentikasi

Login adalah proses autentikasi pengguna untuk memperoleh akses ke dalam suatu sistem dengan cara memasukkan identitas berupa *username* dan *password*. Sistem login berfungsi sebagai mekanisme kontrol akses untuk memastikan bahwa hanya pengguna yang berwenang yang dapat menggunakan layanan sistem. Lemahnya sistem login dapat menyebabkan penyalahgunaan hak akses, pencurian data, dan pengambilalihan akun, sehingga diperlukan mekanisme autentikasi yang aman dan andal [2].

### 2.3. Algoritma Blowfish

Blowfish merupakan algoritma kriptografi simetris yang dikembangkan oleh Bruce Schneier pada tahun 1993. Algoritma ini menggunakan blok data 64-bit dengan panjang kunci variatif antara 32 hingga 448 bit. Blowfish dikenal memiliki tingkat keamanan yang tinggi, performa enkripsi yang cepat, serta bersifat *open source*, sehingga dapat digunakan secara bebas tanpa lisensi. Karakteristik tersebut menjadikan Blowfish cocok untuk diterapkan pada sistem login berbasis web [5].

### 2.4. Brute Force Attack

*Brute force attack* merupakan metode serangan yang dilakukan dengan mencoba berbagai kombinasi kata sandi secara berulang hingga menemukan kombinasi yang benar. Serangan ini sering menargetkan sistem login yang tidak memiliki perlindungan memadai, seperti enkripsi yang lemah atau tanpa pembatasan jumlah percobaan login. Oleh karena itu, penggunaan algoritma enkripsi yang kuat dan mekanisme pembatasan login sangat diperlukan untuk mencegah jenis serangan ini [7].

### 2.5. Penelitian Terdahulu

Berbagai penelitian terdahulu telah dilakukan untuk mengkaji penerapan algoritma kriptografi dalam meningkatkan keamanan data pada sistem berbasis web. Penelitian-penelitian tersebut menunjukkan bahwa penggunaan algoritma enkripsi yang tepat dapat memberikan perlindungan yang signifikan terhadap data sensitif, khususnya pada sistem autentikasi dan penyimpanan kata sandi.

Penelitian yang membahas perbandingan algoritma RSA dan Blowfish dalam perancangan aplikasi keamanan data menunjukkan bahwa algoritma Blowfish memiliki keunggulan dari sisi kecepatan proses enkripsi dan efisiensi penyimpanan *ciphertext*. Hasil penelitian tersebut menyimpulkan bahwa Blowfish lebih sesuai digunakan pada aplikasi berbasis web yang membutuhkan proses autentikasi cepat namun tetap aman dibandingkan algoritma kriptografi asimetris seperti RSA [1].

Penelitian lain yang mengimplementasikan algoritma Blowfish pada sistem manajemen surat digital membuktikan bahwa Blowfish mampu menjaga kerahasiaan data dokumen dan mencegah akses ilegal. Penggunaan Blowfish pada sistem ini juga dinilai tidak memberikan beban komputasi yang signifikan, sehingga tetap mendukung kinerja sistem secara optimal dalam lingkungan organisasi [9].

Selain itu, penelitian mengenai penerapan algoritma Blowfish pada aplikasi e-commerce berbasis web menunjukkan bahwa Blowfish efektif dalam mengamankan data login dan transaksi pengguna. Hasil pengujian memperlihatkan bahwa data yang telah dienkripsi tidak dapat dibaca maupun dimanipulasi tanpa kunci yang sah, serta mampu meningkatkan kepercayaan pengguna terhadap keamanan sistem [3].

Penelitian lainnya yang mengkaji penggunaan Blowfish untuk pengamanan file digital menyimpulkan bahwa algoritma ini memiliki tingkat ketahanan yang tinggi terhadap serangan *brute force*. Blowfish mampu mengenkripsi berbagai jenis data dengan hasil yang konsisten dan aman, sehingga layak digunakan sebagai solusi pengamanan data pada berbagai aplikasi berbasis teknologi informasi [4].

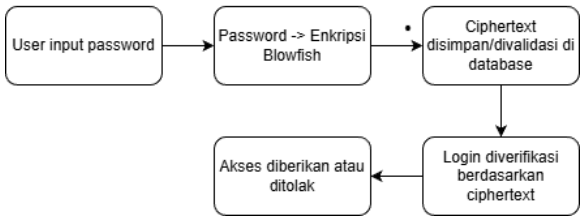
Berdasarkan hasil penelitian-penelitian terdahulu tersebut, dapat disimpulkan bahwa algoritma Blowfish terbukti efektif dalam meningkatkan keamanan data pada berbagai sistem berbasis web. Oleh karena itu, penelitian ini mengadopsi algoritma Blowfish untuk mengamankan data login pada website Teknik Informatika Politeknik Negeri Bengkalis dengan fokus pada perlindungan akun administrator dan pencegahan akses tidak sah.

## 3. METODE PENELITIAN

Bab ini membahas metode penelitian yang digunakan dalam pelaksanaan penelitian, meliputi pendekatan penelitian, tahapan perancangan sistem, serta teknik yang diterapkan untuk mencapai tujuan penelitian. Metode yang digunakan berfokus pada penerapan algoritma kriptografi Blowfish sebagai mekanisme utama dalam pengamanan data login pada website Program Studi Teknik Informatika Politeknik Negeri Bengkalis. Selain itu, bab ini juga menjelaskan proses enkripsi dan dekripsi password, serta integrasi algoritma Blowfish dengan mekanisme keamanan tambahan berupa pembatasan percobaan login dan autentikasi dua faktor berbasis *One Time Password* (OTP).

### 3.1. Metode Blowfish

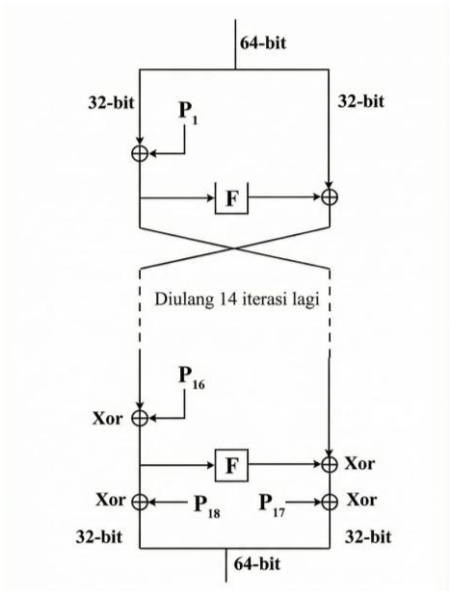
Metode yang digunakan dalam penelitian ini adalah implementasi algoritma kriptografi simetris Blowfish untuk mengamankan data login admin pada website Teknik Informatika Politeknik Negeri Bengkalis. Algoritma Blowfish diterapkan untuk mengenkripsi password sebelum disimpan dan diverifikasi pada basis data, sehingga data autentikasi tidak berada dalam bentuk plaintext.




Gambar 1. Alur Blowfish

Gambar 1 menunjukkan alur umum penerapan algoritma Blowfish pada proses login aplikasi web. Proses dimulai ketika pengguna memasukkan password melalui halaman login (*user input password*). Password yang diinput tidak diproses secara langsung, melainkan terlebih dahulu dienkripsi menggunakan algoritma Blowfish. Hasil dari proses enkripsi berupa ciphertext kemudian disimpan atau divalidasi di dalam basis data. Pada tahap selanjutnya, sistem melakukan proses verifikasi login berdasarkan ciphertext dengan membandingkan hasil enkripsi password yang dimasukkan pengguna dengan data terenkripsi yang tersimpan di database. Apabila hasil verifikasi sesuai, sistem memberikan akses kepada pengguna, sedangkan jika tidak sesuai maka akses ditolak. Alur ini bertujuan untuk memastikan bahwa password tidak pernah disimpan dalam bentuk plaintext sehingga dapat meningkatkan keamanan sistem login berbasis web.

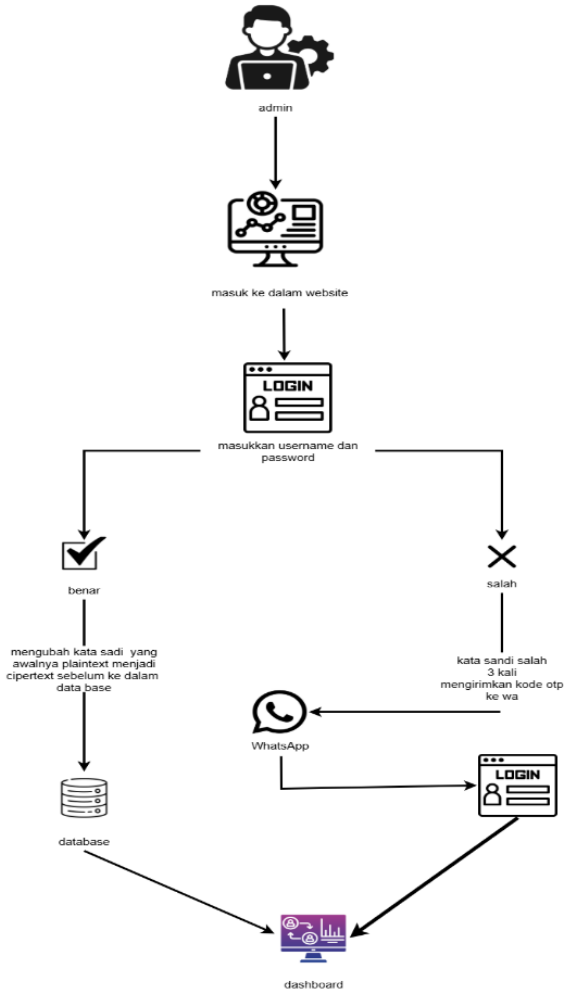
### 3.2. Proses Enkripsi Password Menggunakan Blowfish




Gambar 2. Proses Enkripsi Blowfish

Gambar 2 menjelaskan proses enkripsi algoritma Blowfish diawali dengan masukan berupa plaintext berukuran 64-bit yang dibagi menjadi dua bagian, yaitu 32-bit bagian kiri (XL) dan 32-bit bagian kanan (XR). Selanjutnya, data diproses menggunakan struktur Feistel Network melalui 16 putaran, di mana pada setiap putaran bagian kiri dioperasikan dengan subkunci P menggunakan operasi XOR, kemudian hasilnya diproses oleh fungsi F sebagai fungsi non-linear dan di-XOR dengan bagian kanan, setelah itu kedua bagian dipertukarkan. Proses tersebut diulang secara berurutan menggunakan subkunci $P_1$ hingga $P_{16}$. Setelah putaran ke-16 selesai, dilakukan pertukaran terakhir, kemudian masing-masing bagian di-XOR dengan subkunci $P_{17}$ dan $P_{18}$ tanpa pertukaran blok. Tahap akhir ini menghasilkan ciphertext berukuran 64-bit yang merupakan hasil enkripsi dan hanya dapat dikembalikan ke bentuk semula melalui proses dekripsi menggunakan kunci yang sama.

### 3.3. Perancangan Sistem




Gambar 3. Alur Sistem Login

Gambar 3 menggambarkan alur proses autentikasi sistem login yang dilengkapi dengan mekanisme enkripsi Blowfish dan autentikasi dua faktor berbasis OTP. Proses dimulai ketika admin mengakses website dan memasukkan *username* serta *password* pada halaman login, kemudian sistem melakukan validasi terhadap data yang dimasukkan dengan mencocokkannya ke basis data yang menyimpan password dalam bentuk terenkripsi menggunakan algoritma Blowfish. Apabila data yang dimasukkan benar, pengguna akan diarahkan ke halaman dashboard, sedangkan jika data login salah

maka sistem akan menolak akses. Setelah terjadi tiga kali percobaan login yang gagal, sistem secara otomatis mengirimkan kode OTP melalui aplikasi WhatsApp ke nomor yang terdaftar sebagai langkah keamanan tambahan, di mana pengguna harus memasukkan kode OTP yang valid untuk dapat melanjutkan proses login, sehingga sistem lebih tahan terhadap upaya akses tidak sah dan serangan *brute force*.

```
parent::__construct();
$this->key = (string) $this->config->item('encryption_key_blowfish');

if (empty($this->key)) {
    log_message(level: 'error',
    message: 'encryption_key_blowfish KOSONG. Login/enkripsi akan gagal.');
    // lempar key dummy tapi aman: paksa semua operasi gagal supaya ketahuan
    $this->key = '';
    $this->iv  = '';
    return;
```

Gambar 4. Penentuan Algoritma Blowfish

Gambar 4 menunjukkan proses penentuan algoritma Blowfish sebagai metode pengamanan data login. Algoritma Blowfish dipilih karena memiliki tingkat keamanan tinggi, panjang kunci yang fleksibel, serta performa enkripsi yang efisien sehingga sesuai untuk diterapkan pada sistem login berbasis web.

```
private function encrypt_password($plaintext)
{
 $raw = openssl_encrypt(
   $plaintext,
   $this->method_password,
   $this->key,
   OPENSSL_RAW_DATA,
   $this->iv
 );
 return base64_encode($raw);
}
```

Gambar 5. Proses Enkripsi Password

Gambar 5 memperlihatkan alur proses enkripsi password menggunakan algoritma Blowfish. Password yang dimasukkan oleh pengguna akan diproses melalui algoritma Blowfish sebelum disimpan ke dalam basis data, sehingga data autentikasi tidak tersimpan dalam bentuk plaintext.

```
private function decrypt_password($cipher_base64)
{
 $raw = base64_decode($cipher_base64, true);
 return openssl_decrypt(
   $raw,
   $this->method_password,
   $this->key,
   OPENSSL_RAW_DATA,
   $this->iv
 );
}
```

Gambar 6. Proses Dekripsi Password

Gambar 6 menunjukkan proses dekripsi password terenkripsi menggunakan algoritma Blowfish. Proses ini dilakukan saat verifikasi login, di mana password yang tersimpan dalam basis data didekripsi terlebih dahulu untuk dicocokkan dengan input pengguna.

```
public function verify_password($password_plain, $password_enc)
{
 $dec = $this->decrypt_password($password_enc);
 return hash_equals($dec, $password_plain);
}
```

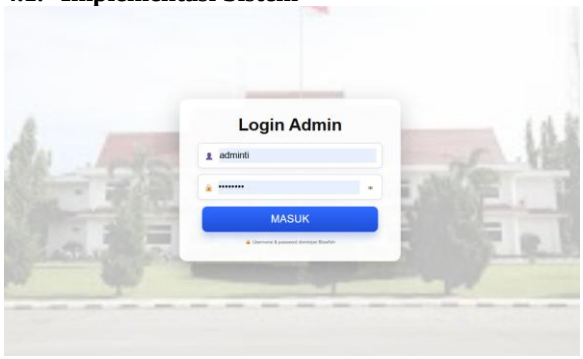
Gambar 7. Verifikasi Password

Gambar 7 menggambarkan proses verifikasi password pada sistem login. Setelah proses dekripsi dilakukan, sistem membandingkan hasil dekripsi dengan password yang dimasukkan pengguna untuk menentukan apakah proses autentikasi berhasil atau gagal.

## 4. HASIL DAN PEMBAHASAN

Bagian hasil dan pembahasan menjelaskan hasil dari perancangan dan implementasi sistem yang telah dibangun serta pembahasan terhadap fungsi-fungsi yang dihasilkan. Pembahasan dilakukan untuk mengetahui sejauh mana sistem mampu memenuhi kebutuhan pengguna dan menyelesaikan permasalahan yang telah diidentifikasi pada tahap sebelumnya.

### 4.1. Implementasi Sistem




Gambar 8. Halaman Login

Gambar 8 menunjukkan tampilan halaman login pada sistem yang telah dikembangkan. Halaman ini berfungsi sebagai antarmuka awal autentikasi pengguna sebelum mengakses sistem, dengan mekanisme keamanan yang telah diperkuat menggunakan algoritma Blowfish.

Hasil implementasi menunjukkan bahwa algoritma Blowfish berhasil diterapkan pada sistem login website untuk mengamankan data autentikasi pengguna. Implementasi dilakukan pada sisi model dengan memanfaatkan pustaka OpenSSL menggunakan algoritma Blowfish mode CBC (*Cipher Block Chaining*) untuk enkripsi password. Setiap password yang dimasukkan oleh pengguna akan dienkripsi terlebih dahulu sebelum disimpan ke dalam

basis data, sehingga data autentikasi tidak pernah tersimpan dalam bentuk *plaintext*. Dengan mekanisme ini, meskipun basis data berhasil diakses oleh pihak tidak berwenang, informasi password tetap tidak dapat dibaca secara langsung.

| id_user | username | password | email |
|---|---|---|---|
| 51 | /I8BO0aobWLtx2vGbGDEfA== | 9estHHi6d8N4x7KNu721HA== | admin@example.com |
| 52 | /I8BO0aobWLtx2vGbGDEfA== | 9estHHi6d8N4x7KNu721HA== | admin@example.com |
| 55 | OeFeFosz5svfrjS++sHNHg== | 9HoBWBUQtx35rU+6kspmAA== | nasxbwi@gmail.com |

Gambar 9. Hasil Enkripsi

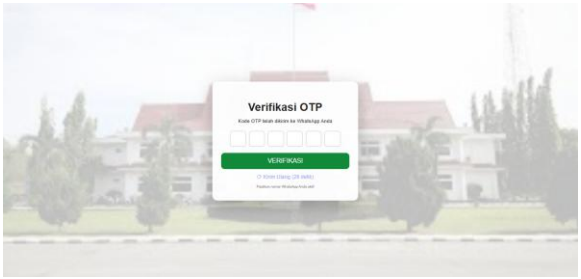
Gambar 9 menampilkan hasil enkripsi password menggunakan algoritma Blowfish. Password yang telah dienkripsi ditampilkan dalam bentuk ciphertext yang tidak dapat dibaca secara langsung, sehingga meningkatkan keamanan data apabila terjadi kebocoran basis data.

Setelah implementasi Blowfish, struktur penyimpanan password pada basis data mengalami perubahan signifikan. Password yang sebelumnya berpotensi disimpan dalam bentuk yang mudah ditebak kini disimpan dalam bentuk *ciphertext* hasil enkripsi Blowfish. Untuk memudahkan penyimpanan dan transmisi data, hasil enkripsi dikodekan menggunakan Base64.

Tabel 1. Perbandingan Password Sebelum dan Sesudah Enkripsi Blowfish

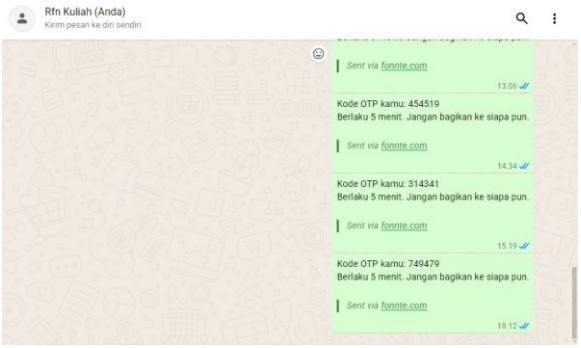
| Kondisi Data | Password asli | Password enkrpsi |
|---|---|---|
| Password | adminti | EZRAYIW48 OU6JVYZTEFF0A= |
| Bentuk Data | Teks biasa | Ciphertext |
| Keterbacaan oleh Manusia | Dapat di baca | Tidak dapat dibaca |

Berdasarkan Tabel 1, dapat dilihat bahwa hasil enkripsi Blowfish menghasilkan data yang tidak memiliki pola yang dapat dikenali secara visual, sehingga menyulitkan upaya pencurian password melalui kebocoran basis data.




Gambar 10. Halaman Verifikasi OTP

Gambar 10 menampilkan proses verifikasi autentikasi dua faktor (OTP) pada sistem login yang dikembangkan. Pada bagian atas gambar ditunjukkan tampilan halaman verifikasi OTP, di mana pengguna diminta untuk memasukkan kode OTP yang dikirimkan ke nomor WhatsApp terdaftar sebelum dapat melanjutkan proses login. Halaman ini berfungsi sebagai lapisan keamanan tambahan setelah terjadi beberapa kali percobaan login yang gagal.




Gambar 11. Kode OTP

Gambar 11 memperlihatkan contoh pengiriman kode OTP melalui aplikasi WhatsApp. Kode OTP dikirim secara otomatis oleh sistem dan bersifat sementara dengan batas waktu penggunaan tertentu. Mekanisme ini bertujuan untuk memastikan bahwa hanya pengguna yang memiliki akses ke nomor WhatsApp terdaftar yang dapat melanjutkan autentikasi, sehingga dapat meminimalkan risiko akses tidak sah dan serangan *brute force* terhadap akun pengguna.

### 4.2. Pengujian Sistem

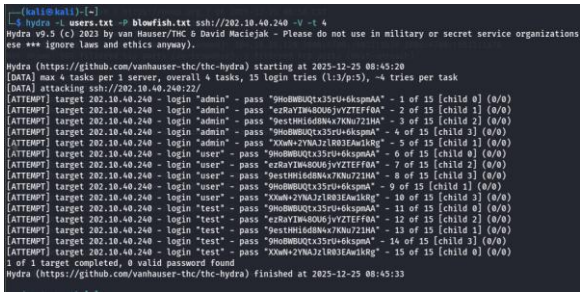
Pengujian sistem dilakukan untuk memastikan bahwa sistem login yang telah dikembangkan berjalan sesuai dengan kebutuhan fungsional dan nonfungsional yang telah ditetapkan pada tahap perancangan. Pengujian ini bertujuan untuk mengevaluasi kinerja sistem dalam melakukan autentikasi pengguna secara aman serta menilai efektivitas penerapan algoritma Blowfish dalam melindungi data *username* dan *password*. Selain itu, pengujian juga dilakukan untuk memastikan bahwa proses enkripsi dan dekripsi password dapat berjalan dengan benar tanpa mengganggu fungsionalitas sistem login.

Pengujian difokuskan pada beberapa skenario utama, yaitu proses login dengan data yang valid dan tidak valid, penyimpanan password dalam bentuk terenkripsi pada basis data, serta proses verifikasi password saat autentikasi berlangsung. Selain itu, pengujian juga mencakup penerapan mekanisme keamanan tambahan berupa autentikasi dua faktor berbasis OTP yang diaktifkan setelah terjadinya percobaan login gagal secara berulang. Mekanisme ini diuji untuk memastikan bahwa sistem mampu membatasi akses tidak sah dan memberikan perlindungan tambahan terhadap akun pengguna.

Selanjutnya, pengujian dilakukan untuk menilai ketahanan sistem terhadap percobaan serangan *brute force*, yaitu dengan melakukan login menggunakan kombinasi password yang salah secara berulang. Hasil

pengujian ini digunakan untuk mengetahui sejauh mana sistem mampu menolak akses ilegal, mengaktifkan mekanisme pengamanan tambahan, serta menjaga kerahasiaan data autentikasi pengguna. Dengan demikian, pengujian sistem ini diharapkan dapat memberikan gambaran menyeluruh mengenai tingkat keamanan dan keandalan sistem login yang telah dikembangkan

Gambar 12 menampilkan pengujian serangan brute force dilakukan menggunakan tools Hydra dengan mencoba berbagai kombinasi username dan password secara otomatis. Berdasarkan hasil pengujian, tidak ditemukan kredensial yang valid meskipun dilakukan percobaan login berulang dalam jumlah banyak. Kondisi ini menunjukkan bahwa sistem login telah dilengkapi dengan pembatasan percobaan login serta mekanisme keamanan tambahan, sehingga serangan brute force tidak dapat berjalan secara efektif dan akses tidak sah dapat dicegah.




Gambar 12. Pengujian serangan brute force

Tabel 2. Hasil Pengujian Sistem

| No | Jenis Pengujian | Skenario Pengujian | Data Uji | Hasil yang Diharapkan | Hasil Pengujian |
|---|---|---|---|---|---|
| 1 | Login Normal | Login dengan username dan password benar | Username: adminti Password: admin123 | Sistem menerima login dan mengarahkan ke halaman utama | Berhasil |
| 2 | Berhasil | Login dengan password salah | Username: adminweb17 Password: admin123 | Sistem menolak login dan menampilkan pesan kesalahan | Berhasil |
| 3 | Login Kosong | Login tanpa mengisi field password | Username: adminweb17 Password: (kosong) | Sistem menolak login dan menampilkan peringatan | Berhasil |
| 4 | Enkripsi Password | Penyimpanan password ke database | Password: adminti | Password tersimpan dalam bentuk ciphertext | Berhasil |
| 5 | Verifikasi Password | Pencocokan password saat login | Password input ≠ password DB | Login ditolak | Berhasil |
| 6 | Validasi OTP | Input kode OTP yang benar | OTP valid | Login berhasil | Berhasil |
| 7 | Keamanan Database | Membaca password langsung dari database | Data terenkripsi | Password tidak dapat dibaca | Berhasil |
| 8 | Brute Force | Percobaan login berulang menggunakan tools Hydra | Kombinasi username dan password secara otomatis | Sistem membatasi percobaan login dan menolak akses tidak sah | Kredensial tidak ditemukan, login gagal |

Berdasarkan hasil pengujian pada Tabel 2, sistem login yang dikembangkan mampu berjalan sesuai dengan fungsionalitas yang diharapkan. Sistem berhasil melakukan autentikasi pengguna dengan data yang valid serta menolak akses ketika data yang dimasukkan tidak sesuai. Password yang disimpan dalam basis data telah terenkripsi menggunakan algoritma Blowfish sehingga tidak dapat dibaca secara langsung. Selain itu, penerapan pembatasan percobaan login dan autentikasi dua faktor berupa OTP terbukti efektif dalam mencegah percobaan login berulang atau serangan *brute force* terhadap sistem.

## 5. KESIMPULAN DAN SARAN

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dilakukan, dapat disimpulkan bahwa penerapan algoritma Blowfish pada sistem login website Teknik Informatika Politeknik Negeri Bengkalis berhasil meningkatkan keamanan data autentikasi pengguna. Password tidak lagi disimpan dalam bentuk *plaintext*, melainkan dalam bentuk *ciphertext* hasil enkripsi Blowfish sehingga tidak dapat dibaca secara langsung meskipun terjadi kebocoran basis data. Integrasi mekanisme autentikasi tambahan berbasis OTP serta pembatasan percobaan login terbukti mampu meningkatkan ketahanan sistem terhadap percobaan akses tidak sah dan serangan *brute force*. Dengan demikian, sistem login yang dikembangkan mampu memenuhi kebutuhan fungsional dan memberikan perlindungan yang lebih optimal terhadap data pengguna. Adapun saran untuk penelitian selanjutnya adalah pengembangan sistem keamanan dengan menerapkan algoritma kriptografi yang lebih modern atau kombinasi dengan metode *hashing* adaptif, integrasi layanan OTP menggunakan API resmi, serta pengujian performa sistem pada skala pengguna yang lebih besar untuk memperoleh hasil evaluasi yang lebih komprehensif.

**DAFTAR PUSTAKA**

[1] A. Rahayu, A. P. Ardana, C. Pramudhita, D. Syafitri, and R. Z. Sirega, "Perbandingan Algoritma RSA dengan Algoritma Blowfish Pada Perancangan Aplikasi Keamanan Data," *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI*, vol. 7, no. 1, pp. 203–207, 2024.

[2] S. Muryanah and D. Rahmawati, "Implementasi Hidden Text dengan Algoritma Blowfish dan Kompresi Huffman dalam Security Dokumen," 2023.

[3] H. A1, C. Rai, A. Pramartha, I. A. Gde, S. Putra, and A. Di, "Aplikasi Keamanan E-Commerce Berbasis Web Menggunakan Metode Algoritma Blowfish," 2022.

[4] N. M. Sitinjak, R. Oktari Batubara, and F. Ikorasaki, "PERANCANGAN DAN IMPLEMENTASI ALGORITMA BLOWFISH UNTUK KEAMANAN DATA FILE CITRA DIGITAL Design And Implementation Of Blowfish Algorithms For Security Of Digital Image File Data," vol. 5, no. 1, pp. 468–481, 2024, [Online]. Available: https://jurnal.amikwidyaloka.ac.id/index.php/awl

[5] T. Pamuji, "Pembahasan Serangan Kolisi (Collision Attack) Dan Variasinya Pada Algoritma Hash MD5," 2022.

[6] A. Gunawan, "Studi dan Implementasi Kolisi pada Fungsi Hash MD5," 2022. [Online]. Available: www.wikipedia.org

[7] R. Gunawan, "IMPLEMENTASI ALGORITMA BLOWFISH UNTUK PENGAMANAN TRANSAKSI DALAM APLIKASI BERBASIS WEBSITE," 2025.

[8] D. Yudi Priyanggodo, "Implementation of the Blowfish Cryptographic Algorithm with Android ID Combination in Android-Based Applications," vol. 14, pp. 45–52, 2025, [Online]. Available: http://jurnal.umt.ac.id/index.php/jt/index

[9] Filan Firmansyah, Saputra Dwi Nurchaya, and Zuhana Realita Alfy, "IMPLEMENTASI ALGORITMA BLOWFISH PADA SISTEM MANAJEMEN SURAT DENGAN PENDEKATAN RATIONAL UNIFIED PROCESS YANG RAMAH LINGKUNGAN," *JSiI (Jurnal Sistem Informasi)*, vol. 11, no. 2, pp. 1–6, Sep. 2024, doi: 10.30656/jsii.v11i2.9065.

[10] M. Romzi and B. Kurniawan, "Implementasi Pemrograman Python Menggunakan Visual Studio Code," 2020. [Online]. Available: www.python.org