e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed) Vol.7 No.2 (December 2023)
**JISICOM (Journal of Information System, Informatics and Computing)**
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

# IMPLEMENTATION OF BCRYPT ALGORITHM ON WEBSITE-BASED HASHING GENERATOR USING LARAVEL FRAMEWORK

*Implementasi Algoritma Bcrypt Pada Hashing Generator Berbasis Website Menggunakan Framework Laravel*

**Dio Febrian[1], Yoel Christian[2], Alifan Widad Sutisna[3], Gunawan Budiarto[4], Muhammad Syukur[5], Xena Hadi Ramadhan[6], Antonius Yadi K[7], Riza Pahlapi[8]**

Program Studi Teknologi Informasi[1,2,3,4,5,6,7]
Program Studi Teknologi Informasi[7]
Fakultas Teknik Informatika[1,2,3,4,5,6,7]
Universitas Bina Sarana Informatika[1,2,3,4,5,6,7],
Universitas NusaMandiri, Jaarta6

17200485@bsi.ac.id[1], 17200176@bsi.ac.id[2], 17200415@bsi.ac.id[3], 17200005@bsi.ac.id[4], 17200564@bsi.ac.id[5], 17200565@bsi.ac.id[6], antonius.aio@nusamandiri.ac.id[7] , riza.rzf@bsi.ac.id

**Received:** June 29, 2023. **Revised:** July 29, 2023. **Accepted:** August 9, 2023 **Issue Period:** Vol.7 No.2 (2023), Pages 199-212

**Abstrak:** Implementasi algoritma Bcrypt pada hashing generator berbasis website menggunakan framework Laravel telah dilakukan dalam penelitian ini. Latar belakang penelitian ini di dasarkan pada perkembangan teknologi informasi yang telah mempengaruhi banyak aspek kehidupan manusia, di mana data dan informasi menjadi sangat penting dan perlu dilindungi. Sistem informasi yang berbasis web rentan terhadap ancaman keamanan, seperti penyadapan dan penyusupan oleh pihak yang tidak berkepentingan. Oleh karena itu, penerapan keamanan informasi bertujuan untuk mengatasi masalah tersebut dan memberikan solusi baik secara teknis maupun non-teknis. Penelitian ini menggunakan framework Laravel, sebuah framework PHP open-source yang memungkinkan pengembangan aplikasi web dengan modul-modul yang dapat mengoptimalkan kinerja PHP. Algoritma Bcrypt dan salt digunakan dalam proses hashing untuk melindungi data pengguna. Hasil penelitian menunjukkan bahwa penggunaan Laravel sebagai framework yang tepat untuk pembuatan hashing generator. Hasil dari proses hashing menghasilkan nilai yang konstan sebanyak 60 karakter, bahkan jika teks yang diinput lebih dari 60 karakter dengan teks acak. Cost factor, yang merupakan faktor pengaturan kekuatan hashing, berpengaruh terhadap waktu yang dibutuhkan dalam proses hashing dan verifikasi hash. Penggunaan alat Bcrypt generator ini berguna dalam pengujian lintas browser, terutama dalam pengujian yang melibatkan kata sandi ter-hash. Dengan alat ini, dapat dibuat banyak hash kata sandi bcrypt yang valid untuk pengujian. Penelitian ini

**DOI:** 10.52362/jisicom.v7i2.1130

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed) Vol.7 No.2 (December 2023)
**JISICOM (Journal of Information System, Informatics and Computing)**
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

memberikan kontribusi penting dalam meningkatkan keamanan sistem informasi berbasis web dengan menerapkan algoritma Bcrypt pada proses hashing. Implementasi ini dapat memberikan perlindungan data yang lebih baik bagi pengguna dan meningkatkan kinerja sistem secara keseluruhan.

**Kata kunci:** Keamanan Informasi, Hashing Generator, Framework Laravel.

***Abstract:*** *Implementation of the Bcrypt algorithm on a website-based hashing generator using the Laravel framework has been carried out in this study. The background of this research is based on the development of information technology which has affected many aspects of human life, where data and information are very important and need to be protected. Web-based information systems are vulnerable to security threats, such as wiretapping and intrusion by unauthorized parties. Therefore, the implementation of information security aims to overcome these problems and provide solutions both technically and non-technically. This research uses the Laravel framework, an open-source PHP framework that enables the development of web applications with modules that optimize PHP performance. Bcrypt and salt algorithms are used in the hashing process to protect user data. The results of the research show that using Laravel as the right framework for making hashing generators. The result of the hashing process produces a constant value of 60 characters, even if the input text is more than 60 characters with random text. The cost factor, which is a factor that regulates hashing power, affects the time required for the hashing process and hash verification. Using the Bcrypt generator tool is useful in cross-browser testing, especially in tests involving hashed passwords. With this tool, many valid bcrypt password hashes can be generated for testing. This research makes an important contribution in improving the security of web-based information systems by applying the Bcrypt algorithm to the hashing process. This implementation can provide better data protection for users and improve overall system performance.*

***Keywords:*** *Information Security, Hashing Generator, Laravel framework.*

## I. PENDAHULUAN

Perkembangan Teknologi Informasi berpengaruh signifikan dalam kehidupan sehari-hari. Keamanan sistem informasi berbasis web menjadi perhatian penting karena rentan terhadap penyadapan dan penyusupan (Santoso, 2013). Penerapan keamanan informasi bertujuan untuk melindungi data pengguna dan mengatasi masalah teknis maupun non-teknis seperti faktor ketersediaan, kerahasiaan, dan kesatuan(Umar et al., 2019). Mekanisme login dengan tahapan identifikasi, otentikasi, dan otorisasi diperlukan untuk melindungi data dari pengguna yang tidak berhak (Marisa Khairina, 2011).

Penelitian ini fokus pada pembuatan website Hashing berbasis web dengan menggunakan framework Laravel. Laravel adalah framework PHP open-source yang mudah dimengerti dan menyediakan modul untuk pengembangan aplikasi web (Suendri, 2017). Penelitian ini mengimplementasikan algoritma Bcrypt pada proses hashing untuk meningkatkan keamanan data.

Rumusan masalah penelitian ini mencakup pembuatan keamanan hashing berbasis web, cara kerja sistem tersebut, dan apakah sistem tersebut berfungsi dengan baik. Maksud dan tujuan penelitian ini adalah membuat sistem pengamanan data yang mudah, mengembangkan sistem hash berbasis web, dan memenuhi syarat Tugas Akhir.

**DOI:** 10.52362/jisicom.v7i2.1130

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed) Vol.7 No.2 (December 2023)
**JISICOM (Journal of Information System, Informatics and Computing)**
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

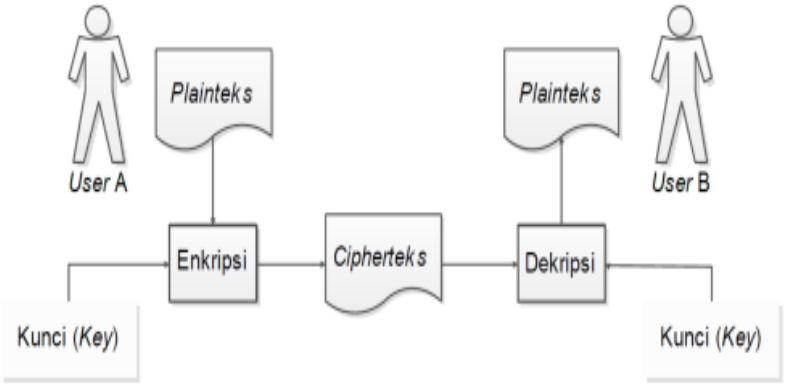
Metode penelitian yang digunakan adalah Library Research, dengan mengumpulkan teori-teori terkait enkripsi dan hashing, serta menganalisis dan membahas implementasi hash pada sistem berbasis web yang menggunakan bahasa pemrograman PHP.

## II. METODE DAN MATERI

### 2.1 Kriptografi

2.1.1 Definisi Kriptografi

Menurut Ariyus (2008), kriptografi adalah ilmu dan seni dalam melindungi informasi dengan mengubahnya menjadi karakter acak yang tidak dapat dibaca. Secara umum, kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan saat dikirim dari satu tempat ke tempat lain (Munir, 2006).




Gambar 2.1. Konsep Kriptografi

2.1.2 Enkripsi dan Dekripsi

Enkripsi adalah proses mengubah pesan yang dapat dimengerti (plaintext) menjadi kode yang tidak dapat dimengerti (ciphertext), sedangkan dekripsi adalah proses kebalikan untuk mengubah ciphertext menjadi plaintext (Sanger, 2015).

2.1.3 Komponen Utama Kriptografi

Berdasarkan Budi Rahardjo (2017), terdapat tiga komponen utama dalam kriptografi, yaitu:

- Plain text: Data asli yang belum diproses, bisa berupa teks atau berkas biner.
- Ciphertext: Data hasil enkripsi yang dihasilkan. Perlu diasumsikan bahwa penyerang dapat mengakses ciphertext.
- Algoritma dan kunci: Algoritma dan kunci yang digunakan untuk mengubah plaintext menjadi ciphertext. Algoritma diasumsikan diketahui oleh penyerang, tetapi kunci tidak diketahui.

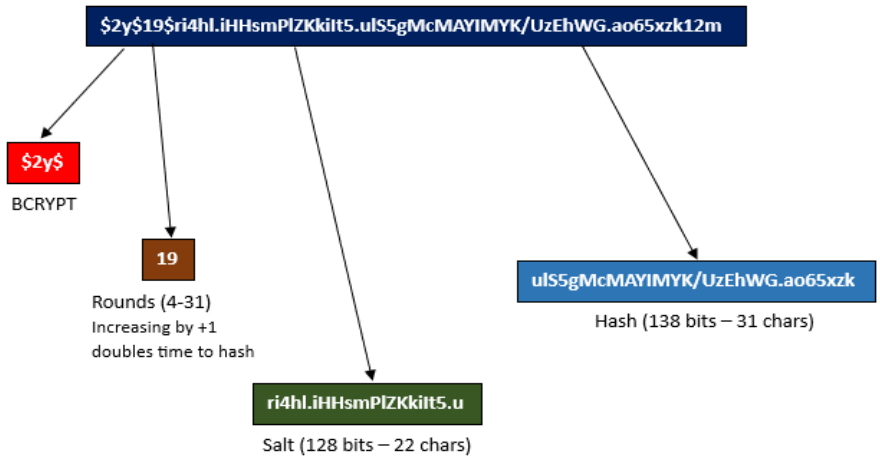
### 2.2 Hash

2.2.1 Definisi Fungsi Hash

**DOI:** 10.52362/jisicom.v7i2.1130

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed) Vol.7 No.2 (December 2023)
**JISICOM (Journal of Information System, Informatics and Computing)**
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

Menurut Yahya (2018), fungsi hash adalah fungsi matematika yang menerima input berupa string dan menghasilkan output berupa string dengan panjang tetap. Output hash tidak tergantung pada ukuran input awal.




Gambar 2.2. Struktur Bcrypt

2.2.2 Algoritma Hash yang Berkembang

Beberapa algoritma hashing yang telah berkembang, antara lain (Li et al., 2013):

- MD4 (Message-Dig est Algorithm 4)
- MD5 (Message-Dige st Algorithm 5)
- MD5 ($pass.$salt)
- MD5 ($salt.$pass)
- SHA-1 (Secure Hash Algorithm),
- SHA-256 (Secure Hash Algorithm)
- SHA-512 (Secure Hash Algorithm)
- Base64

## 2.3 Bcrypt

2.3.1 Definisi Bcrypt

Bcrypt adalah algoritma hashing yang menggunakan banyak iterasi untuk memperlambat dan melindungi dari serangan brute force. Algoritma ini juga menggunakan salt untuk melindungi data dari serangan rainbow table(Zulma et al., 2022).

2.3.2 Tahapan Enkripsi Bcrypt

Menurut Zulma, tahapan enkripsi Bcrypt meliputi:,

- Inisiasi array P dengan 18 iterasi.
- Proses enkripsi plaintext
- Dalam proses pengambilan data, hasilnya dibagi menjadi dua bagian, yaitu XL yang terdiri dari 32-bit pertama dan XR yang terdiri dari 32-bit kedua.
- Setelah menyelesaikan langkah 1-3, dilakukan operasi XL = XL xor Pi dan XR = F(XL) xor XR.
- Hasil dari operasi di atas kemudian ditukar, dengan XL menjadi XR dan XR menjadi XL.
- Setelah melakukan operasi sebanyak 16 kali, terjadi operasi penukaran antara XL dan XR pada iterasi ke-16.

**DOI:** 10.52362/jisicom.v7i2.1130

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed) Vol.7 No.2 (December 2023)
**JISICOM (Journal of Information System, Informatics and Computing)**
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

- Pada proses ke-17, dilakukan operasi XR = XR xor P17 dan XL = XL xor P18.
- XL dan XR kemudian digabungkan agar jumlah bitnya kembali menjadi 64 bit.

### 2.4 Laravel

Laravel merupakan sebuah framework PHP open-source yang menyediakan modul dasar untuk meningkatkan kinerja PHP dalam pengembangan aplikasi web. Diluncurkan pada tanggal 9 Juni 2011 oleh Taylor Otwell, Laravel awalnya dikembangkan sebagai alternatif untuk framework CodeIgniter. Tujuan utama Laravel adalah menyediakan fitur-fitur yang belum tersedia dalam CodeIgniter, seperti dukungan otentikasi dan otorisasi pengguna. Dengan berbagai pembaruan dan penambahan fitur, Laravel telah mencapai versi 9 dengan berbagai keunggulan.

Laravel berfokus pada sisi back-end (server-side) dan menyediakan kekuatan serta kemudahan penggunaan. Menggunakan pola arsitektur model-view-controller (MVC), Laravel mempercepat proses pengembangan aplikasi web dengan memisahkan tugas-tugas ke dalam model (pengelolaan database), view (tampilan pengguna), dan controller (penghubung antara model dan view).

Framework Laravel menggabungkan fitur-fitur dasar dari beberapa framework PHP populer seperti CodeIgniter, Yii, dan Ruby on Rails. Bagi pengembang yang sudah mengenal Core PHP atau Advance PHP, Laravel dapat meningkatkan efektivitas dan efisiensi dalam pengembangan aplikasi web. Selain itu, keamanan Laravel juga lebih baik dalam menghadapi berbagai ancaman siber.

Kelebihan Laravel meliputi percepatan waktu pengembangan aplikasi, kemudahan pengelolaan resource, performa aplikasi yang lebih baik, keamanan bawaan yang kuat terhadap serangan CSRF, script, dan SQL injection, penggunaan kode yang lebih sedikit melalui fungsi built-in Laravel, serta dukungan komunitas yang luas.

Beberapa fitur kunci dalam Laravel antara lain Eloquent ORM yang memungkinkan interaksi tanpa batas antara model data dan database, Artisan CLI yang merupakan antarmuka baris perintah untuk memodifikasi Laravel, penggunaan pola arsitektur MVC yang umum digunakan dalam pengembangan aplikasi web, serta paginasi otomatis yang membatasi tampilan data menjadi halaman-halaman terpisah untuk memudahkan navigasi.

## III. PEMBAHASAN DAN HASIL

### 3.1 Analisa Kebutuhan

Analisis kebutuhan sistem adalah tahap awal dalam pengembangan sistem yang bertujuan untuk menemukan masalah yang akan dihadapi dan kebutuhan yang harus dipenuhi.

Kebutuhan sistem terdiri dari kebutuhan perangkat keras, perangkat lunak, input, dan output.

1. Analisis Kebutuhan Perangkat Keras:
   Laptop Lenovo Ideapad V14 dengan spesifikasi:
   a. Processor AMD RYZEN 3 (2,6 GHz)
   b. RAM 8 GB
   c. SSD 250 GB
2. Analisis Kebutuhan Perangkat Lunak:
   Perangkat lunak yang digunakan:
   a. Sistem Operasi Windows 10 64-bit
   b. Microsoft Visual Studio Code versi 1.78.2
   c. Laravel 9.52.4
   d. PHP 8.0
   e. Browser Google Chrome
3. Analisis Kebutuhan Input:
   Data masukan yang dibutuhkan:
   Teks dalam bentuk huruf dengan minimal 1 huruf.
   Pilihan jumlah cost factor yang diinginkan.
4. Analisis Kebutuhan Proses:
   - Pengguna memasukkan teks pada form input.

**DOI:** 10.52362/jisicom.v7i2.1130

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed) Vol.7 No.2 (December 2023)
**JISICOM (Journal of Information System, Informatics and Computing)**
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

- Teks tersebut diubah menggunakan fungsi hashing di dalam controller setelah tombol generate diklik.
- Hasil hashing ditampilkan pada output sebagai huruf, simbol, dan angka acak.
- Pengguna dapat menekan tombol "Copy To Verify Hash" untuk menyalin hasil hashing dan teks biasa ke form verifikasi hashing.
- Data tersebut diproses oleh fungsi verifikasi hashing di dalam controller.
- Jika kedua data sesuai, muncul modal dialog di tengah halaman dengan tulisan "Match". Jika tidak sesuai, tulisan yang muncul adalah "Not Match".

5. Analisis Kebutuhan Output:
   - Bycrypt (hasil hashing)
   - Hasil verifikasi (verification result)

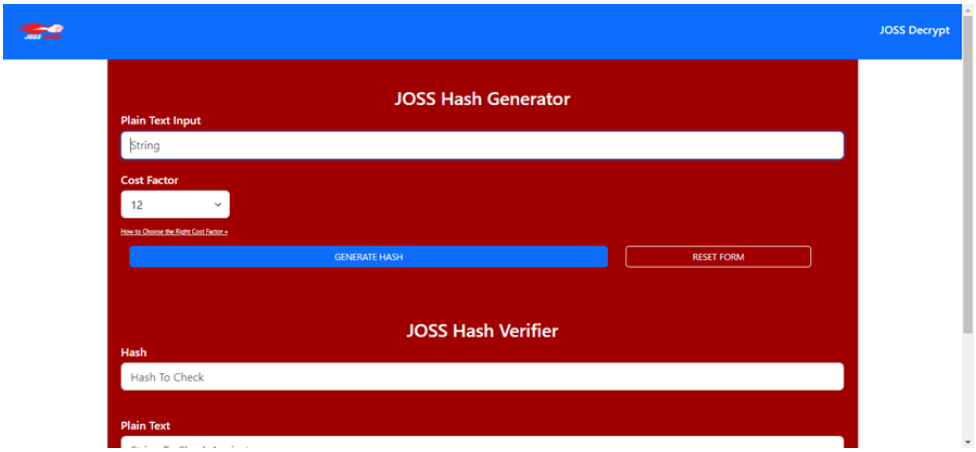
### 3.2 Perancangan Objek

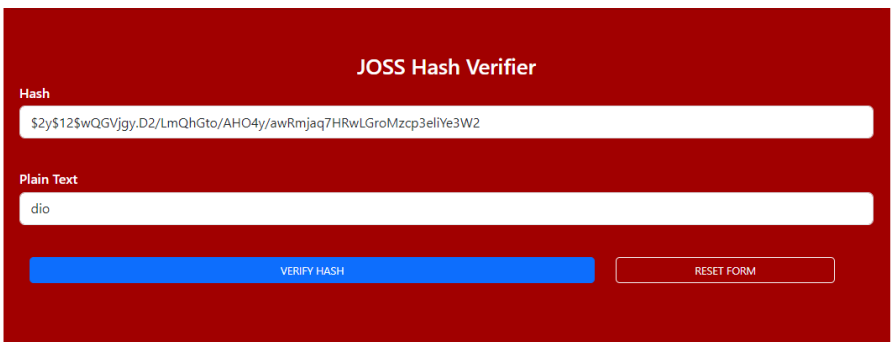
Perancangan awal meliputi:

1. Kode tampilan untuk fungsi hashing.
2. Kode tampilan untuk fungsi verifikasi hashing.
3. Fungsi JavaScript untuk tombol "Copy To Verify Hash" dan tombol verifikasi hashing.
4. Kode rute di dalam file routes yang mengarahkan ke fungsi di dalam controller.
5. Kode dalam controller untuk fungsi hashing, termasuk membuka halaman dan menghasilkan hashing.
6. Kode dalam controller untuk fungsi verifikasi hashing.

### 3.3 Tampilan Hasil

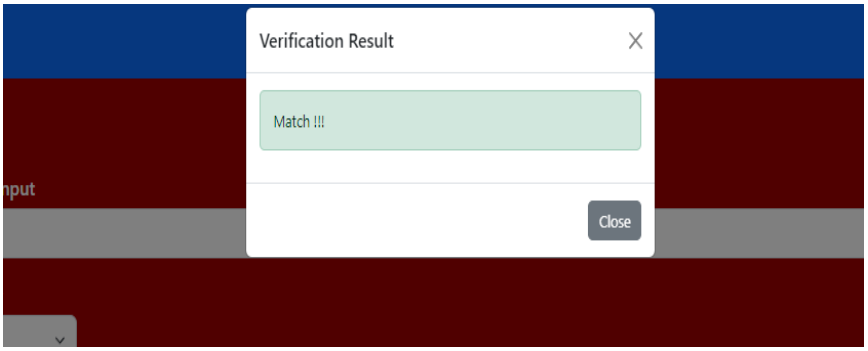
Tampilan Hasil meliputi:



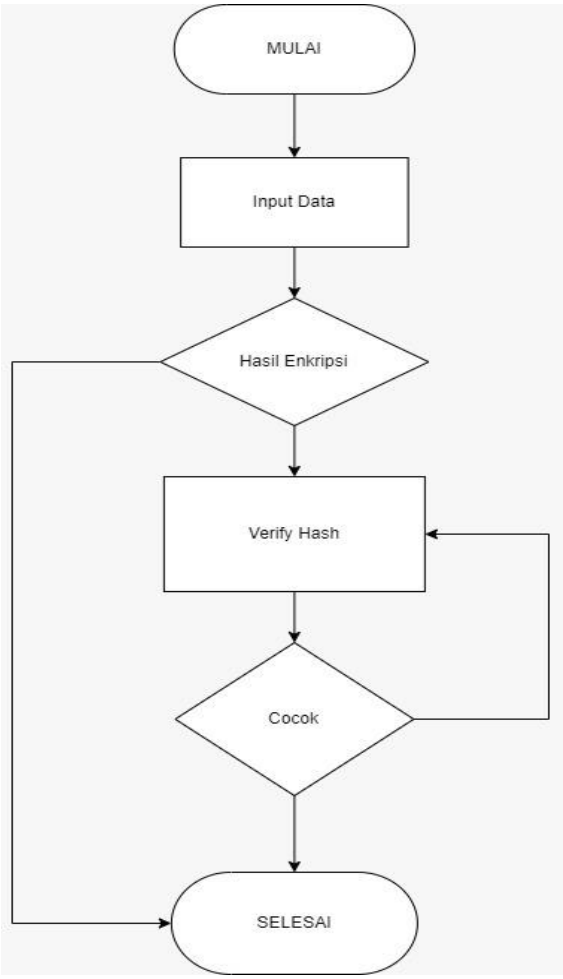

**DOI:** 10.52362/jisicom.v7i2.1130

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed) Vol.7 No.2 (December 2023)
**JISICOM (Journal of Information System, Informatics and Computing)**
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com




### 3.4 Cara Kerja Aplikasi

Cara kerja aplikasi dijelaskan melalui flowchart yang disediakan.




Demikianlah ringkasan dari analisis kebutuhan, perancangan objek, tampilan hasil, dan cara kerja aplikasi.

**DOI:** 10.52362/jisicom.v7i2.1130

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed) Vol.7 No.2 (December 2023)
**JISICOM (Journal of Information System, Informatics and Computing)**
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

### 3.5 Hasil Penelitian

1. Pengujian Pertama Hasil Jumlah karakter berdasarkan Panjang *plain text*

| Plain text | Hasil hash | Cost factor | Jumlah karakter |
|---|---|---|---|
| Bsi | $2y$12$SW1R9GEO2JJE.X91PLWEKubcblxUxp3T0le4l3jI7uy.ShIs1dXRm | 12 | 60 |
| Kramat 98 | $2y$12$LiBGRHH6530GJLQaLzxzQO2AJOq9vnZGVf.hmFSLuGD66v4kdtk/W | 12 | 60 |
| BinaSaranaInformatikaKramat98 | $2y$12$obWXWJ5yQo9kkir3XSUmgO.49HMj4BdSQ99ou1wED/xFQvvr.Xst. | 12 | 60 |
| BinaSaranaInformatikaKramat98 | $2y$15$eUV9AQvDf..PJPcDMf8BKOSKvV91exlpUgzGfrUz2UW/TrZY8ooxS | 15 | 60 |

Jumlah *plain text* dan *cost factor* tidak akan mempengaruhi jumlah karakter pada hasil *hash*nya.

2. Pengujian kedua menggunakan *plain text* BinaSaranaInformatikaKramat98 untuk menguji waktu hasil perulangannya yang disesuai kan berdasarkan cost factor yang dipilih menggunakan laptop Lenovo V14

| Cost Factor | Waktu ( Detik ) |
|---|---|
| 4 | 00.00.01.40 |
| 5 | 00.00.01.45 |
| 6 | 00.00.01.50 |
| 7 | 00.00.01.50 |
| 8 | 00.00.01.53 |
| 9 | 00.00.01.55 |
| 10 | 00.00.01.58 |
| 11 | 00.00.01.60 |
| 12 | 00.00.01.62 |
| 13 | 00.00.01.70 |
| 14 | 00.00.02.10 |
| 15 | 00.00.04.10 |

**DOI:** 10.52362/jisicom.v7i2.1130

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed) Vol.7 No.2 (December 2023)
**JISICOM (Journal of Information System, Informatics and Computing)**
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

| | |
|---|---|
| 16 | 00.00.07.25 |
| 17 | 00.00.12.54 |
| 18 | 00.00.24.60 |
| 19 | 00.00.48.10 |

Dari hasil pengujiannya untuk cost factor dibawah 12 waktu perulangan yang dibutuhkan sangat cepat bahkan kurang dari 2 detik, sedangkan semakin tinggi cost factor terutama diatas 13 maka waktu yang dibutuhkan untuk perulangan akan semakin lama terutama di cost factor 19.

3. Pengujian ketiga hanya menggunakan *cost factor* 12 sampai 19 19 saja karena data pengujian sebelumnya untuk cost factor dibawah 12 membutuhkan waktu yang sangat cepat dan kurang dari 1 detik. Teks yang digunakan adalah @BinaSaranaInformatikaKramat98.

| *Cost Factor* | *Bcrypt* atau *Hash* | Waktu yang dibutuhkan (Detik) |
|---|---|---|
| 12 | $2y$12$8sNMQW/2vtwqBQKqcTTcyOUyY8jvcTySELukECRdlyYLZzR.OHp.u | 00.00.01.10 |
| 13 | $2y$13$TwXw1X4KteYBTdf6PdOF9un7rvX7zOeBATmT.a7HT8YntWY7/F5Gu | 00.00.01.22 |
| 14 | $2y$14$Lmu4eRU0ttnBeXgEyUJsxOR6w5E7tFNSlMssd0puWbrfgirVfUrkS | 00.00.01.65 |
| 15 | $2y$15$110Fo06CGYCOIMWU2Zhav.6uCzoNOKg3vIxIYFXfP1ZJXfu/T5hji | 00.00.03.85 |
| 16 | $2y$16$.AnEMT0uif/EKxpelWoTpuQK6eEBeuWgOUd5wLLUxTRb9obo.4Qgu | 00.00.05.19 |
| 17 | $2y$17$9FAyyFg6/5iWcHm.28l45.MmY6G4dZR/ltFQf8Vc0QUPddKrtBAsG | 00.00.10.38 |
| 18 | $2y$18$4a.sULTNDMoWJlVRKRxYv.pKHHUK5KBzWX1I00rewDypsE.cNt.h. | 00.00.19.87 |
| 19 | $2y$19$ri4hl.iHHsmPlZKkiIt5.ulS5gMcMAYIMYK/UzEhWG.ao65xzk12m | 00.00.38.31 |

Hasil pengujian verify hashnya menunjukan semakin tinggi cost factor yang digunakan maka semakin lama juga waktu yang dibutuhkan untuk verify hash nya

## 4. KESIMPULAN DAN SARAN

### 4.1 Kesimpulan

1. Setelah dilakukan pendalaman ilmu dengan menggunakan framework yang tersedia, Laravel merupakan framework yang tepat untuk pembuatan hashing karena menggunakan algoritma bcrypt dan salt;
2. Hasil dari hashing cukup konstan sebanyak 60 karakter sekalipun teks yang di input lebih dari 60 karakter yang berisikan random teks;
3. Jumlah cost factor sangat berpengaruh terhadap waktu hashing dilakukan makin tinggi cost factor nya semakin lama waktu yang dibutuhkan untuk melakukan hashingnya;
4. Hasil pengujian verify hashnya menunjukan semakin tinggi cost factor yang digunakan maka semakin lama juga waktu yang dibutuhkan untuk verify hash nya;
5. Bcrpt generator ini dapat berguna jika Anda melakukan pengujian lintas browser. Sebagai contoh, jika anda sedang menulis pengujian yang melibatkan kata sandi ter-hash, maka anda dapat

**DOI:** 10.52362/jisicom.v7i2.1130

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed) Vol.7 No.2 (December 2023)
**JISICOM (Journal of Information System, Informatics and Computing)**
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

menggunakan utilitas ini untuk membuat banyak hash kata sandi bcrypt yang valid untuk pengujian anda**.**

**4.2 Saran**

1. Design UI masih terlihat statik maka perlu dikembangkan lagi untuk UI nya;
2. Saat pengguna melakukan hash verify masih membutuhkan reload page terlebih dahulu sebelum menunjukan hasilnya;
3. Memilih algoritma hashing lainnya untuk penelitian terkait seperti SHA-3, Argon2, SHA2-384 dan Scrypt;
4. Cost factor yang digunakan hanya 4 sampai 19, harusnya dapat menggunakan 20 sampai 31.

**REFERENSI**

Marisa Khairina, D. (2011). Analisis Keamanan Sistem Login. *Jurnal Informatika Mulawarman, Vol. 6 No.*(2), 64–67.

Umar, R., Riadi, I., & Handoyo, E. (2019). Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI). *Jurnal Sistem Informasi Bisnis*, *9*(1), 47. https://doi.org/10.21456/vol9iss1pp47-54

Zulma, G. D. M., Seta, H. B., & Yuniati, T. (2022). Implementasi Algoritma Aes Dan Bcrypt Untuk Pengamanan File Dokumen. *Informatik : Jurnal Ilmu Komputer*, *18*(2), 163. https://doi.org/10.52958/iftk.v18i2.4667

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi*: Teori, Analisa, dan Implementasi. Yogyakarta: Andi.

Komarudin, Asep Ririh Riswaya. (2013). "Sistem Keamanan Web Dengan Menggunakan Kriptografi Message Digest 5/Md5 Pada Koperasi Mitra Sejahtera Bandung". Jurnal Computech & Bisnis, Vol. 7, No. 1, Juni 2013, 30-41 ISSN: 2442-4943

https://sim.ubaya.ac.id/bahasa-pemrograman-populer-php/. Diakses 8 Juni 2023

https://www.biznetgio.com/news/apa-itu-laravel. Diakses 15 Juni 2023

**DOI:** 10.52362/jisicom.v7i2.1130

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed) Vol.7 No.2 (December 2023)
**JISICOM (Journal of Information System, Informatics and Computing)**
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

## LAMPIRAN

**Tampilan Hash**

a. Coding tampilan hashing

hashing.blade.php

```
<form id="generate_form" method="POST" action="/home/hashing">
                        @csrf
                        <h2 class="pt-5 text-center text-white">JOSS Hash Generator</h2>
                        <div class="container-fluid">
                            <div class="row mb-3">
                                <div class="col-12">
                                    <label for="plain_text" class="h5 mb-2 text-white">Plain Text Input</label>
                                    <input type="text" id="plain_text" name="plain_text" class="mb-2 form-control form-control-lg"
                                    placeholder="String" @if(isset($password))value="{{ $password }}"@endif autofocus required />
                                </div>
                            </div>
```

snappify.com

```
<div class="row mb-2">
    <div class="col-sm-2">
        <label for="cost_factor" class="h5 mb-2 text-white">Cost Factor</label>
        <div class="input-select">
            <select id="cost_factor" name="cost_factor" class="form-select form-select-lg">
                <option value="4">4</option>
                <option value="5">5</option>
                <option value="6">6</option>
                <option value="7">7</option>
                <option value="8">8</option>
                <option value="9">9</option>
                <option value="10">10</option>
                <option value="11">11</option>
                <option value="12" selected>12</option>
                <option value="13">13</option>
                <option value="14">14</option>
                <option value="15">15</option>
                <option value="16">16</option>
                <option value="17">17</option>
                <option value="18">18</option>
                <option value="19">19</option>
            </select>
        </div>
    </div>
</div>
<div class="row mb-3">
    <div class="col-sm-6">
        <a href="https://security.stackexchange.com/a/17238" target="_blank" rel="noopener noreferrer"
            title="How to Choose the Right Cost for Bcrypt" class="learn-more-lnk text-white"
            style="font-size:11px">How to Choose the Right Cost Factor »
        </a>
    </div>
```

**DOI:** 10.52362/jisicom.v7i2.1130

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed) Vol.7 No.2 (December 2023)
**JISICOM (Journal of Information System, Informatics and Computing)**
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

```
            <div class="row">
                <div class="col-sm-8">
                    <input type="submit" class="mb-2 ms-3  btn btn-primary btn-md btn-block" style="width: 100%" value="GENERATE HASH">
                </div>
                <div class="col-sm-4">
                    <a href="/home" type="button" class="ms-4 btn btn-outline-light " style="width: 80%">RESET FORM</a>
                </div>
            </div>
            @if(isset($hashedPassword))
            <div class="row">
                <div class="col">
                    <div class="row">
                        <div class="col-12 mb-5">
                            <p class="h5 mb-2 text-white">Output</p>
                            <div class="form-control alert alert-success mt-3" role="alert">
                                <input type="text" id="hashed_password" name="hashed_password" value="{{ $hashedPassword }}" hidden>
                                {{ $hashedPassword }}
                            </div>
                            <button type="button" class="btn btn-md btn-primary copy-button" onclick="copyData()">
                            <i class="fas fa-copy"></i> Copy To Verify Hash</button>
                        </div>
                    </div>
                </div>
            </div>
            @endif
        </div>
    </form>
```

b. Coding tampilan verify hashing

```
<div class="boxed boxed--border pt-5" style="height:30em">
    <h2 class="text-center text-white">JOSS Hash Verifier</h2>
    <form id="verifier_form" method="POST" action="/home/verify">
        @csrf
        <div class="container-fluid">
            <div class="row mb-5">
                <div class="col">
                    <label for="verify_hash" class="text-white h5 mb-2">Hash</label>
                    <input type="text" id="verify_hash" name="verify_hash" class="form-control form-control-lg"
                    placeholder="Hash To Check" @if(isset($verify_hash))value="{{ $verify_hash }}"@endif autofocus required />
                </div>
            </div>
            <div class="row mb-5">
                <div class="col">
                    <label for="verify_plain_text" class="text-white h5 mb-2">Plain Text</label>
                    <input type="text" id="verify_plain_text" name="verify_plain_text" class="form-control form-control-lg"
                    placeholder="String To Check Against" @if(isset($verify_plain_text))value="{{ $verify_plain_text }}"@endif required />
                </div>
            </div>
    @if(isset($verification))
        <div class="modal fade" id="verificationModal" tabindex="-1" aria-labelledby="verificationModalLabel" aria-hidden="true">
            <div class="modal-dialog">
                <div class="modal-content">
                    <div class="modal-header">
                        <h5 class="modal-title" id="verificationModalLabel">Verification Result</h5>
                        <button type="button" class="btn-close" data-bs-dismiss="modal" aria-label="Close"></button>
                    </div>
                    <div class="modal-body">
                        @if($verification === 'valid')
                            <div class="alert alert-success" role="alert">
                                Match !!!
                            </div>
                        @else
                            <div class="alert alert-danger" role="alert">
                                Not a match !!!!!!
                            </div>
                        @endif
                    </div>
                    <div class="modal-footer">
                        <button type="button" class="btn btn-secondary" data-bs-dismiss="modal">Close</button>
                    </div>
                </div>
            </div>
        </div>
    @endif
```

**DOI:** 10.52362/jisicom.v7i2.1130

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed) Vol.7 No.2 (December 2023)
**JISICOM (Journal of Information System, Informatics and Computing)**
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

```
            <div class="row">
                <div class="col-sm-8">
                    <input type="submit" class="mb-2 ms-3  btn btn-primary btn-md" style="width: 100%" value="VERIFY HASH">
                </div>
                <div class="col-sm-4">
                    <a href="/home" type="button" class="ms-4 btn btn-outline-light" style="width: 80%">RESET FORM</a>
                </div>
            </div>
        </div>
    </form>
</div>
<script>
    function copyData() {
        var plaintText = document.getElementById("plain_text").value;
        var hashedPassword = document.getElementById("hashed_password").value;

        document.getElementById("verify_plain_text").value = plaintText;
        document.getElementById("verify_hash").value = hashedPassword;
    }
</script>
<script>
    window.addEventListener('DOMContentLoaded', function () {
        var verificationModal = new bootstrap.Modal(document.getElementById('verificationModal'));
        verificationModal.show();
    });
</script>
```

c. Javascript function yang di gunakan untuk tombol *Copy To Verify* Hash dan tombol verifier hash

```
<script>
    function copyData() {
        var plaintText = document.getElementById("plain_text").value;
        var hashedPassword = document.getElementById("hashed_password").value;

        document.getElementById("verify_plain_text").value = plaintText;
        document.getElementById("verify_hash").value = hashedPassword;
    }
</script>
<script>
    window.addEventListener('DOMContentLoaded', function () {
        var verificationModal = new bootstrap.Modal(document.getElementById('verificationModal'));
        verificationModal.show();
    });
</script>
```

d. Berikut adalah Code untuk routes mengarah kan ke function di controller

web.php

```
Route::get('/', function () {
    return view('hashing');
});
Route::get('/home', [App\Http\Controllers\HashingController::class, 'index'])->name('home');
Route::post('/home/hashing', [App\Http\Controllers\HashingController::class, 'generate'])->name('hashing');
Route::post('/home/verify', [App\Http\Controllers\HashingController::class, 'verify'])->name('verify');
```

snappify.com

**DOI:** 10.52362/jisicom.v7i2.1130

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed) Vol.7 No.2 (December 2023)
**JISICOM (Journal of Information System, Informatics and Computing)**
Website/URL: http://journal.stmikjayakarta.ac.id/index.php/jisicom
Email: jisicom@stmikjayakarta.ac.id , jisicom2017@gmail.com

e. Berikut adalah code untuk controller function hashing. Code untuk membuka halamannya, dan code untuk melakukan generate hashing.

HashingController.php

```php
class HashingController extends Controller
{
    public function index()
    {
        return view('hashing');
    }

    public function generate(Request $request)
    {

        $config = config('hashing.bcrypt');
        $config['rounds'] = $request->input('cost_factor');

        // Set konfigurasi cost factor
        config(['hashing.bcrypt' => $config]);

        // Hashing kata sandi dengan cost factor yang ditentukan
        $password = $request->input('plain_text');
        $hashedPassword = Hash::make($password);
        return view('hashing', ['password' => $password, 'hashedPassword' => $hashedPassword]);
    }
```

snappify.com

f. Berikut adalah code untuk controller function verify hashing

HashingController.php

```php
public function verify(Request $request)
    {
        // contoh hash yang disimpan di database
        $passwordVerify = $request->input('verify_plain_text');

        // contoh plaintext password yang akan divalidasi
        $hashVerify = $request->input('verify_hash');

        if (Hash::check($passwordVerify, $hashVerify)) {
            return view('hashing', [
                'verify_plain_text' => $passwordVerify,
                'verify_hash' => $hashVerify,
                'verification' => 'valid'
            ]);
        } else {
            return view('hashing', [
                'verify_plain_text' => $passwordVerify,
                'verify_hash' => $hashVerify,
                'verification' => 'invalid'
            ]);
        }
    }
}
```

snappify.com

**DOI:** 10.52362/jisicom.v7i2.1130