JURNAL ILMU KOMPUTER
KHARISMA .TECH

Jurnal KHARISMA Tech | ISSN:1907-2317 | e-ISSN: 2810-0344
https://jurnal.kharisma.ac.id/kharismatech
published by: Pusat Penelitian STMIK KHARISMA Makassar

Volume: 20 no. 01 – Maret 2025- hlm. 57-71

IMPLEMENTASI ALGORITMA AES DAN BCRYPT UNTUK PENGAMANAN DATA PENGGUNA PADA WEBSITE JAHITKU

Oleh:

Richie Mulyo Liauren[1], Baizul Zaman[2*], Syamsul Bahri[3]
[1,2,3]Teknik Informatika, STMIK Kharisma Makassar
e-mail: [1]richiemulyo_21@kharisma.ac.id, [2]baizul@kharisma.ac.id,
[3]syamsulbahri@kharisma.ac.id

Abstrak: *Keamanan data pengguna merupakan aspek yang sangat penting dalam sistem informasi berbasis website. Penelitian ini bertujuan untuk melakukan implementasi algoritma AES dan Bcrypt guna melindungi data pengguna yang disimpan di database MySQL pada website Jahitku, sebuah startup yang baru dibangun dalam waktu yang relatif singkat dan belum memiliki sistem keamanan yang memadai. Metode yang digunakan mengikuti alur pengembangan perangkat lunak, dimulai dengan studi literatur, analisis kebutuhan sistem, dan perancangan arsitektur sistem. Data yang digunakan untuk evaluasi adalah data kualitatif berupa data pengguna yang dihasilkan dari 30 data dummy. Dalam implementasi ini, algoritma AES 256 CBC dan Bcrypt diterapkan untuk mengenkripsi dan menghashing data pengguna. Hasil evaluasi menunjukkan bahwa AES dapat melakukan enkripsi dengan rata-rata waktu 0,378 ms dan dekripsi 0,260 ms, serta memiliki tingkat keacakan yang baik dibandingkan algoritma simetris lainnya seperti DES dan Blowfish, dengan Avalanche Effect sebesar 50,27%. Sementara itu, Bcrypt membutuhkan waktu hashing rata-rata 369,045 ms dan waktu verify 145,569 ms. Meskipun Avalanche Effect Bcrypt hanya mencapai 36,65%, Bcrypt tetap dapat menghasilkan hash yang unik untuk input yang sama dan menunjukkan ketahanan yang baik terhadap Brute Force Attack dibandingkan algoritma hashing lainnya seperti MD5, SHA1, dan SHA256. Implementasi ini berhasil meningkatkan keamanan data pengguna pada website Jahitku, memberikan kontribusi positif terhadap pengembangan startup, dan meningkatkan kepercayaan pengguna terhadap layanan yang diberikan.*

Kata kunci: *AES 256 CBC, Bcrypt, Website Jahitku, Enkripsi, Dekripsi, Hash, Verify*

Abstract: *User data security is a very important aspect in web-based information systems. This research aims to implement the AES and Bcrypt algorithms to protect user data stored in the MySQL database on the Jahitku website, a startup that has only been built in a relatively short time and does not yet have an adequate security system. The method used follows the flow of software development, starting with a literature study, analyzing system requirements, and designing system architecture. The data used for evaluation is qualitative data in the form of user data generated from 30 dummy data. In this implementation, AES 256 CBC and Bcrypt algorithms are applied to encrypt and hash user data. The evaluation results show that AES can perform encryption with an average time of 0.378 ms and decryption of 0.260 ms, and has a good level of randomness compared to other symmetric algorithms such as DES and Blowfish, with an Avalanche Effect of 50.27%. Meanwhile, Bcrypt requires an average hashing time of 369.045 ms and verify time of 145.569 ms. Although Bcrypt's Avalanche Effect only reaches 36.65%, Bcrypt can still produce unique hashes for the same input and shows good resistance to Brute Force Attacks compared to other hashing algorithms such as MD5, SHA1, and SHA256. This implementation succeeded in increasing the security of user data on the Jahitku website, making a positive contribution to startup development, and increasing user confidence in the services provided.*

Keywords: *AES 256 CBC, Bcrypt, Jahitku Website, Encryption, Decryption, Hash, Verify*

[*] Corresponding author : Baizul Zaman (baizul@kharisma.ac.id)

Diterima : *September, 2024* ***Disetujui :*** *November, 2024* ***Dipublikasikan :*** *April, 2025*

1. PENDAHULUAN

Keamanan data pengguna merupakan aspek yang sangat penting dalam sistem informasi berbasis *website*. Data yang tidak dienkripsi dengan baik dapat disalahgunakan oleh pihak yang tidak bertanggung jawab [1]. Di era digital ini, kerahasiaan dan keamanan data pengguna menjadi hal yang harus dijaga [2]. Dengan kemajuan teknologi informasi yang terus berkembang, kebutuhan akan keamanan yang kuat dan memadai juga meningkat [3]. Pertumbuhan teknologi digital turut membawa ancaman terhadap keamanan data [4], [5], [6], [7], [8], yang menegaskan pentingnya pengamanan data digital [9], [10]. Namun, masalah keamanan siber dan potensi kebocoran data pengguna tetap menjadi ancaman serius yang dapat merusak kepercayaan [11].

Website Jahitku merupakan sebuah *platform* penyedia jasa jahit *online* yang dapat diakses melalui *url* https://jahitku.my.id/. Website Jahitku merupakan sebuah *startup* yang baru dibangun dalam waktu yang relatif singkat dan pada tahap awal ini, belum ada sistem keamanan yang memadai. Website ini menggunakan *database MySQL* yang diakses melalui *PhpMyAdmin*, *platform* yang dikenal rentan terhadap akses tidak sah. *Database* tersebut dapat dengan mudah diakses oleh pihak luar atau bahkan terekspos, hal ini menimbulkan risiko keamanan yang signifikan. Oleh karena itu, diperlukan sistem keamanan yang dapat melindungi data pengguna dari potensi ancaman seperti pencurian data atau serangan siber [12]. Salah satu solusi untuk mengatasi masalah ini adalah dengan mengimplementasikan algoritma kriptografi seperti AES dan Bcrypt [13], [14].

Algoritma AES (*Advanced Encryption Standard*) adalah salah satu algoritma kriptografi simetris yang paling populer digunakan untuk proses enkripsi dan dekripsi data. Keunggulan utama dari AES adalah kecepatan proses enkripsi dan dekripsinya yang relatif lebih cepat dibandingkan dengan algoritma kriptografi simetris lainnya seperti DES, IDEA dan Blowfish [15]. Bcrypt adalah algoritma *hashing* yang dirancang khusus untuk mengamankan kata sandi dan memiliki beberapa keunggulan signifikan dibandingkan algoritma *hashing* lainnya seperti MD5, SHA-1, dan SHA-256 [16], [17], [18]. Kunggulan utama dari Bcrypt adalah penggunaan *salt* unik untuk setiap *hash*, sehingga dua kata sandi yang sama menghasilkan *hash* yang berbeda. Ini membuat Bcrypt tahan terhadap *Rainbow Table Attack*. Selain itu, Bcrypt memiliki *cost factor* yang dapat disesuaikan, sehingga memungkinkan peningkatan keamanan seiring bertambahnya kekuatan komputasi. Semakin tinggi *cost factor*, semakin banyak waktu yang diperlukan untuk menghasilkan *hash*, sehingga *Brute Force Attack* sulit dilakukan [19], [20], [21].

Penelitian ini bertujuan untuk melakukan implementasi algoritma AES dan Bcrypt untuk pengamanan data pengguna yang disimpan di *database MySQL* pada website Jahitku, serta mengevaluasi performa website Jahitku yang menggunakan kedua algoritma tersebut. Dengan demikian, penelitian ini tidak hanya berfokus pada peningkatan keamanan sistem secara keseluruhan, tetapi juga bertujuan untuk menambah kepercayaan pengguna terhadap layanan yang diberikan oleh Website Jahitku. Implementasi ini diharapkan dapat mengatasi masalah

potensial terkait pencurian data oleh pihak yang tidak bertanggung jawab, serta memberikan kontribusi positif terhadap pengembangan *startup* Jahitku.

2. METODE PENELITIAN

Penelitian ini mengikuti alur pengembangan perangkat lunak yang dimulai dari studi literatur, mengacu pada penelitian sebelumnya untuk memperoleh informasi tentang penggunaan dan kinerja algoritma AES dan Bcrypt. Langkah selanjutnya adalah analisis kebutuhan sistem untuk enkripsi, *hashing*, dekripsi dan *verify*, diikuti dengan perancangan arsitektur sistem. Pada penelitian ini, jenis data yang digunakan adalah data kualitatif berupa data pengguna seperti *name, email, password, phone number,* dan *gender*. Sumber data yang digunakan adalah data primer yang terdapat pada *database MySQL PhpMyAdmin* Website Jahitku. Penelitian ini menggunakan 30 data *dummy* dengan format yang sama dengan data pengguna pada website Jahitku. Pemilihan data *dummy* bertujuan untuk menghindari risiko kerusakan atau manipulasi data pengguna yang asli. Metode pengumpulan data yang digunakan adalah observasi, di mana peneliti membuat dan mengamati data *dummy* tersebut. Gambar 1 menunjukkan proses penelitian ini.

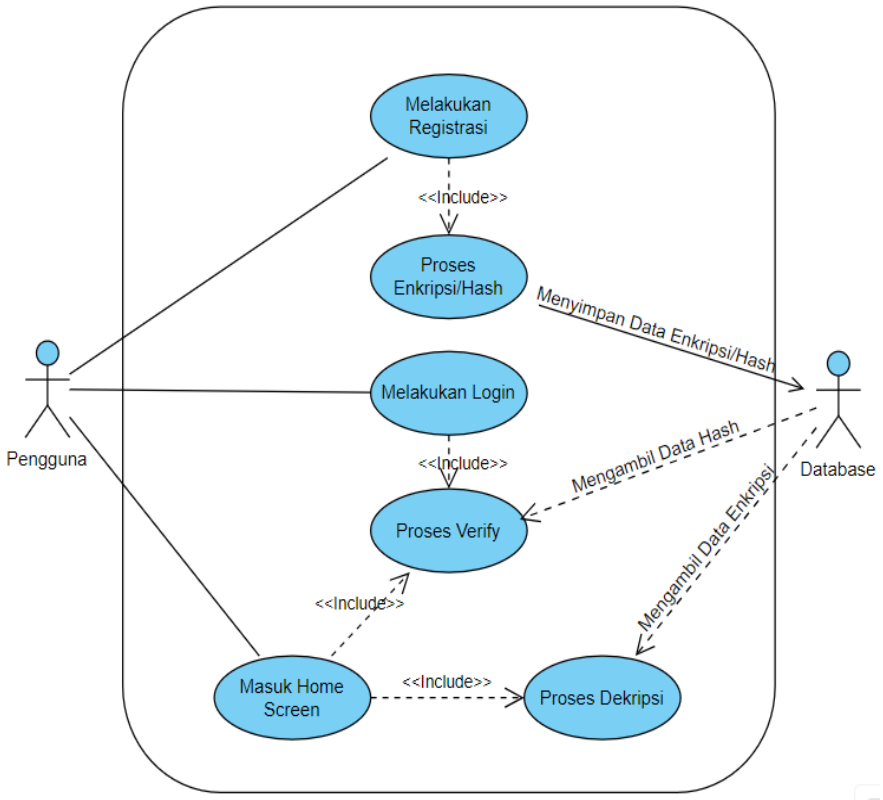
Gambar 1. Tahapan Penelitian

Tahap implementasi dimulai dengan menerapkan desain sistem ke dalam *platform* target menggunakan bahasa pemrograman *PHP*. Dalam implementasi ini, algoritma AES 256 CBC digunakan untuk mengenkripsi data pengguna seperti *name, phone number*, dan *gender*, sementara algoritma Bcrypt dengan *cost factor* 10 digunakan untuk melakukan *hashing* terhadap *email* dan *password*. Evaluasi sistem dilakukan melalui beberapa tahap, yang meliputi evaluasi proses enkripsi, *hashing*, dekripsi, dan *verify*. Selain itu, waktu yang diperlukan untuk setiap proses, evaluasi tingkat keacakan hasil enkripsi dilakukan dengan menghitung *Avalanche Effect*, dan evaluasi ketahanan hasil *hashing* terhadap *Brute Force Attack*. Evaluasi proses enkripsi, *hashing*, dekripsi, dan *verify* dilakukan untuk memastikan bahwa website Jahitku berhasil melakukan proses enkripsi dan *hashing* serta menyimpan hasilnya di *database MySQL*. Evaluasi ini juga mencakup pengujian proses dekripsi untuk memastikan data asli dapat ditampilkan kembali setelah dienkripsi. Selain itu, evaluasi *verify* dilakukan untuk memastikan bahwa *hash* yang disimpan di *database* dapat diverifikasi dalam proses autentikasi. Evaluasi waktu proses dilakukan dengan menyisipkan penghitung waktu ke dalam kode implementasi. Evaluasi *Avalanche Effect* menggunakan *CrypTools* dan juga dilakukan pada algoritma simetris lainnya seperti DES dan Blowfish sebagai perbandingan. Evaluasi ketahanan terhadap *Brute Force Attack* dilakukan pada Bcrypt dan juga pada algoritma *hashing* lainnya seperti MD5, SHA1, dan SHA256 sebagai perbandingan. Hasil dari seluruh evaluasi digunakan sebagai dasar untuk menyusun kesimpulan penelitian, yang mencakup keberhasilan implementasi, kinerja algoritma, serta tingkat keamanan yang diperoleh.

3. HASIL DAN PEMBAHASAN

3.1. Analisis Sistem

Pada tahap awal pengembangan, website Jahitku sudah memiliki fitur registrasi, *login*, dan halaman *home screen*. Enkripsi ditambahkan saat Melakukan Registrasi, di mana data pengguna seperti *name*, *phone number*, dan *gender* dienkripsi, sementara *email* dan *password* di-*hash* sebelum disimpan ke *database MySQL*. Saat pengguna Melakukan *Login*, sistem melakukan proses *verify* dengan mencocokkan *hash* dari *email* dan *password*. Setelah *login* berhasil, data yang terenkripsi didekripsi dan ditampilkan di halaman *Home Screen*, memastikan keamanan data pengguna selama proses autentikasi dan penggunaan *website*. Gambar 1 memperlihatkan bagian dari spesifikasi kebutuhan fungsional dari proses enkripsi, *hashing*, dekripsi, dan *verify* data pengguna dalam bentuk diagram *use case* pada website Jahitku.

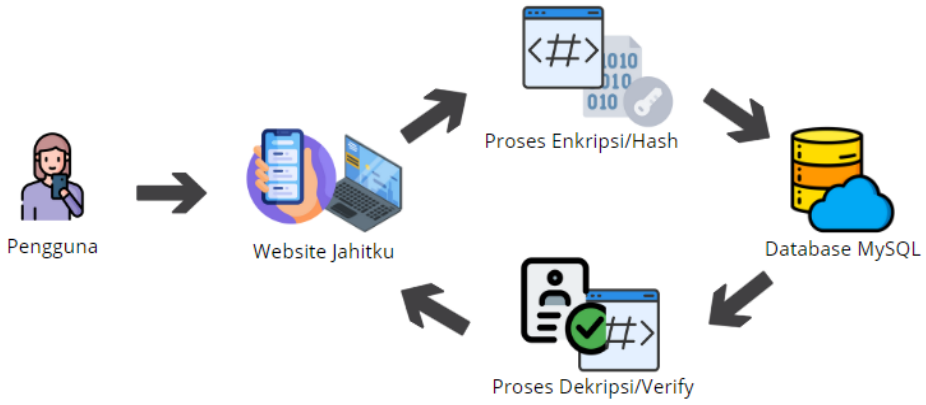


Gambar 2. Diagram *Usecase* Website Jahitku

3.2. Arsitektur Sistem

Arsitektur sistem website Jahitku dirancang untuk menggambarkan komponen utama dalam proses enkripsi, *hashing*, dekripsi, dan *verify* data pengguna. Secara umum, komponen sistem terdiri dari pengguna, perangkat laptop maupun *smartphone*, website Jahitku, proses enkripsi, *hashing*, dekripsi, dan *verify*, serta *database MySQL*. Pengguna berinteraksi dengan website Jahitku, seperti melakukan registrasi, di mana data pengguna dienkripsi menggunakan algoritma AES 256 CBC dan di-*hash* menggunakan Bcrypt. Setelah proses enkripsi dan *hashing* selesai, data dalam bentuk terenkripsi disimpan di *database MySQL*. Ketika diperlukan, data yang sudah tersimpan akan melalui proses *verify* saat pengguna melakukan

login, dan melalui proses dekripsi saat pengguna berada di antarmuka *home screen* website Jahitku. Gambar 3 menunjukkan arsitektur sistem pada website Jahitku.



Gambar 3. Arsitektur Sistem Website Jahitku

3.3. Implementasi

Dalam penelitian ini, mekanisme enkripsi dan dekripsi data pengguna menggunakan algoritma AES 256 CBC serta *hashing* dan *verify* dengan Bcrypt memanfaatkan *package* dan *class* bawaan dari *framework* Laravel, yaitu *'Illuminate\Support\Facades\Crypt'* dan *'Illuminate\Support\Facades\Hash'*. Proses enkripsi dilakukan menggunakan metode *'Crypt::encrypt'*, sedangkan dekripsi dilakukan dengan metode *'Crypt::decrypt'*. Untuk *hashing*, metode yang digunakan adalah *'Hash::make'*, sementara *verify* hasil *hashing* dilakukan melalui *'Hash::check'*. Berikut kode untuk enkripsi, dekripsi, *hashing* dan *verify*.

3.3.1 Kode Enkripsi :

```php
public function encrypt($value, $serialize = true)
{
    $iv = random_bytes(openssl_cipher_iv_length(strtolower($this->cipher)));

    $tag = '';

    $value = self::$supportedCiphers[strtolower($this->cipher)]['aead']
        ? \openssl_encrypt(
            $serialize ? serialize($value) : $value,
            strtolower($this->cipher), $this->key, 0, $iv, $tag
        )
        : \openssl_encrypt(
            $serialize ? serialize($value) : $value,
            strtolower($this->cipher), $this->key, 0, $iv
        );

    if ($value === false) {
        throw new EncryptException('Could not encrypt the data.');
    }

    $iv = base64_encode($iv);
    $tag = base64_encode($tag);

    $mac = self::$supportedCiphers[strtolower($this->cipher)]['aead']
        ? '' // For AEAD-algoritms, the tag / MAC is returned by openssl_encrypt...
        : $this->hash($iv, $value);

    $json = json_encode(compact('iv', 'value', 'mac', 'tag'), JSON_UNESCAPED_SLASHES);

    if (json_last_error() !== JSON_ERROR_NONE) {
        throw new EncryptException('Could not encrypt the data.');
    }

    return base64_encode($json);
}
```

3.3.2 Kode Dekripsi :

```php
public function decrypt($payload, $unserialize = true)
{
    $payload = $this->getJsonPayload($payload);

    $iv = base64_decode($payload['iv']);

    $this->ensureTagIsValid(
        $tag = empty($payload['tag']) ? null : base64_decode($payload['tag'])
    );

    $decrypted = \openssl_decrypt(
        $payload['value'], strtolower($this->cipher), $this->key, 0, $iv, $tag ?? ''
    );

    if ($decrypted === false) {
        throw new DecryptException('Could not decrypt the data.');
    }

    return $unserialize ? unserialize($decrypted) : $decrypted;
}
```

3.3.3 Kode *Hashing* :

```php
public function make($value, array $options = [])
{
    $hash = password_hash($value, PASSWORD_BCRYPT, [
        'cost' => $this->cost($options),
    ]);

    if ($hash === false) {
        throw new RuntimeException('Bcrypt hashing not supported.');
    }

    return $hash;
}
```

3.3.4 Kode *Verify* :

```php
public function check($value, $hashedValue, array $options = [])
{
    if ($this->verifyAlgorithm && $this->info($hashedValue)['algoName'] !== 'bcrypt') {
        throw new RuntimeException('This password does not use the Bcrypt algorithm.');
    }

    return parent::check($value, $hashedValue, $options);
}
```

3.4. Evaluasi

3.4.1 Enkripsi, *Hash*, Dekripsi dan *Verify*

Evaluasi ini bertujuan menguji proses enkripsi, *hashing*, dekripsi, dan *verify* pada website Jahitku. Saat registrasi, data pengguna seperti *name*, *phone number*, dan *gender* dienkripsi, sementara *email* dan *password* di-*hash* sebelum disimpan di *database MySQL*. Saat *login*, *verify* dilakukan, dan setelah berhasil, data terenkripsi didekripsi dan ditampilkan di *home screen*. Tabel 1 memperlihatkan 5 contoh data *dummy* pengguna dalam bentuk *plaintext*. Tabel 2 menunjukkan data yang tersimpan di *database MySQL* sebagai hasil enkripsi (*ciphertext*), dan Tabel 3 menyajikan data yang di-*hash* dan disimpan di *database MySQL* serta *verify* yang berhasil dilakukan.

Tabel 1: Data *Dummy* Pengguna

No	Data *Dummy*				
	Nama	***Email***	***Password***	**No_Telp**	***Gender***
1	Andi Pratama	andi.pratama@example.com	peserta1	081234567890	Male
2	Budi Santoso	budi.santoso@example.com	peserta2	081234567891	Male
3	Citra Dewi	citra.dewi@example.com	peserta3	081234567892	Female
4	Dedi Suhendra	dedi.suhendra@example.com	peserta4	081234567893	Male
5	Evi Lestari	evi.lestari@example.com	peserta5	081234567894	Female

Tabel 2: Data Hasil Enkripsi

No	Data *Dummy*		
	Nama	**No_Telp**	***Gender***
1	eyJpdiI6IklFVGwrb0ZhUEVlUFFUNUg4RzJOWFE9PSIsInZhbHVlIjoiZVZwQWZvN1c5a1VrYXJHdUZYVzAybW1LUjJnWDFwUGtSazQ1MmFSUTY0QT0iLCJtYWMiOiJjNmVhMzgwMGU1N2NmMzFhOTAwMzQ2YzQwMTBhZmNmODZkYzlkMTc0YjlmNTAxMWM0YzZhYWNkMmMwMzNiMGI1IiwidGFnIjoiIn0=	eyJpdiI6IkZJVDVkZU42UWJuWmFtTGx5a0YrV3c9PSIsInZhbHVlIjoiRThLM3FUcVlXZU9MSDNackRoTzQ4QVZpL1gwbnhIdnRkN1JEY3A2R2FNRT0iLCJtYWMiOiI3YzdhOTlmYzYzZDI5YzQ0ZDBkYTY1YjIzYTVmYTc2OTYxYzk3Yzk3NDc4MDk5YzJiYTc4MzM5MDc3ZDE0M2E3IiwidGFnIjoiIn0=	eyJpdiI6InNjaEFFb0duSnlPZE40ZDRrUW9WdUE9PSIsInZhbHVlIjoiQWtUZzFIKzEyWjIzVmlKNTl6N0ZLUT09IiwibWFjIjoiZTA3NmRiNWQyZTAwMzQ5NzAyOGZkNTI2ZTA0YTNhYzM2ZGQ1NGIxYTYxZDM3ODJiZTRkNzYwMGJiYjBmOWZmMCIsInRhZyI6IiJ9
2	eyJpdiI6ImdlZEZKNUpacHgrZXkvbldycVR3VUE9PSIsInZhbHVlIjoiTnZOWm9sUzhIb1RjS0I4OHRyNUlYTzc1bWwxcGJzdXlBbDF0bGt1QjhtUT0iLCJtYWMiOiJjNzU3NDBlMTQ4OTgzZjA4MmU4NzE3M2MyMzdmOWFkMTU1MzQ3NWQzOTAyZTU5MzcyZTE3Y2I2MjJiMDkyNmU0IiwidGFnIjoiIn0=	eyJpdiI6ImRyRk9oUms0Y0tNSDhCamg5dXBUTVE9PSIsInZhbHVlIjoiekYyZDZTTUZacWpublRvZW5Kc0xLd2dNU24vQzBtVisra3p2cDVrTDNpVT0iLCJtYWMiOiI0Y2M3ZTYzMzIwYzY5NmRlMWU2NWFmOTA5ZjIyMzNjOGFiYzdhNDQwOTYyZWQzODlkZTU2NGYyMWM3MzEyMTAwIiwidGFnIjoiIn0=	eyJpdiI6IjRyM1FlRThkcHFTQ3E5OU1KbkhwY0E9PSIsInZhbHVlIjoicHlXTjQ4NHR5aGx2MStxT0Yyek83dz09IiwibWFjIjoiOTc5M2Y0OTM3OWQ2ZDRiZmJmMjdkYWFjNDc1NDkxZDI3ZTBjNzlhZDE4NTk5NjdiYTZmNGE3ZjM5NzhiNmRiOSIsInRhZyI6IiJ9
3	eyJpdiI6IjBHbXdQUHJYUEFsbUlrMDVVWEJCSUE9PSIsInZhbHVlIjoiVngxRk9xcmgwTXZlRTBHUGZxQjRiaXQyM3RueHZEblliRncrS1BncTk0Yz0iLCJtYWMiOiI4M2E2NjQyYTg4N2M3NTYyYjBlNDc4YWQ3YWE3NWEyMWFmZDljNjJiMGZhNjEyMWUxZjVmYTU3ZjI1OTk0YmIyIiwidGFnIjoiIn0=	eyJpdiI6IjdOMUV1NGFIMWduUEdZV0NGK0Fwd3c9PSIsInZhbHVlIjoiclc5Sm1ta0lyS0ZvaG9jWFc5U3F5WlRnZHJqZnVIYTNhVUMwUXBERFd0bz0iLCJtYWMiOiIzNzVjYTZkMjVmYTA4NjhiM2EyMjc0NjliYzIyZWRkNWFmOWIyY2U0OGZjODRhYjcyZTFjZjM3MTU4ZjkwMjhlIiwidGFnIjoiIn0=	eyJpdiI6InYzOWN6RkQxb0pCUDZzWVBkSWNlUWc9PSIsInZhbHVlIjoic1dQMkp5aWNLbTFVY0F1RFRNQzh2Zz09IiwibWFjIjoiMjBhNTA0M2I0ZGQxOTZkYjNkOWE1YTZjNjczNzEzZWZjNWFmMzg4ZTU4OTEwYTc1NDI5NDdhZGJhZDFmNGVkYSIsInRhZyI6IiJ9
4	eyJpdiI6IjN6N2p6NW9jMThqdzg4R29LRkswNkE9PSIsInZhbHVlIjoiQjF6U3Vi	eyJpdiI6InJUNTdLUWp3VytjZFBOcy8xaXpIMXc9PSIsInZhbHVlIjoiT09ucW1vYldLT	eyJpdiI6InpKTkhUWGNIK0I0RFdjc1BGOFJidnc9PSIsInZhbHVlIjoiT0JZUjJ

	MzdFNVFoTUtndDdrWnZRRGR0OTVVbFdsUkxkVnAycXRwOWZkaz0iLCJtYWMiOiIwMDYwZDJhMjhmMGFmNjk2NWMzMzQxNWYxNmE3MjU3N2ExNjczZDgxNzc1ODFiZDM2MTYyMDg4ZjQ5NjU4MTJhIiwidGFnIjoiIn0=	RFgySEJ6U3ZPOW91eXM3Qjh1bnk0N0FDUlBBUE1BazJTOD0iLCJtYWMiOiJhZGUwYTNhM2EzMGQzNzE1ZTQ2ZWVhM2M4YTQzMzFhYTg2MTA5OGViYzQ0YTdlNDEzNjg0MjNmZGNhYzIwYWU2IiwidGFnIjoiIn0=	PSmI4eTJsbHBQRzZhdWp2QT09IiwibWFjIjoiODViYjE5MjA3NWJmNWVkOTE5MzU1YTg2MmY5MDdmMWViMzhmNTY5N2U2NWVkZWRhYTU3MTJiYjQ2MWU0ZmFlMSIsInRhZyI6IiJ9
5	eyJpdiI6Im9pczhmci9mbzYzb01UOGFJSzNRUUE9PSIsInZhbHVlIjoiY1lFd2FVUk8raFFJTXpORzd2YWRySzdKa3g3ZXUyUjFWcFU2QXJmZm5QUT0iLCJtYWMiOiIwNzRhZDAyMmY1NmY0Y2E2ZDI2NTg0OGQwODQ0MDEwM2M5MzZjNDY4OTczOGIxYjViYmVlMmNkYTNkYzIxYTAxIiwidGFnIjoiIn0=	eyJpdiI6ImJkZlJTdk9TOWU2ci96ODBEc2VRMkE9PSIsInZhbHVlIjoidlBBcnAxOE4vOCsrQ3Q3SlhBNkFKZDh2azIzbC9YUGZNMDhCdnJuNTJhND0iLCJtYWMiOiI1YjQwYjU4ZDdiYmYwMWM3MDFhNWI1ZTYxZDEzNDNiMTMzNzE5MTJlOWY1MGZjMGRhMWNkYmIxYzcyYzIxMTYxIiwidGFnIjoiIn0=	eyJpdiI6IlJTcGlBS3J2VFBZdUNRV0xSZm9pZWc9PSIsInZhbHVlIjoib2pubUVTNGhTSFlsWjNwVWFKelpqQT09IiwibWFjIjoiOTExMWM4YWU0YmU1YWNjNzgzZjE5ODgzODI1Y2ZmNTBkNjAwNTZjNGM0OWE4OGY3ZjMxMDhiY2U2MTRlYWU4OSIsInRhZyI6IiJ9

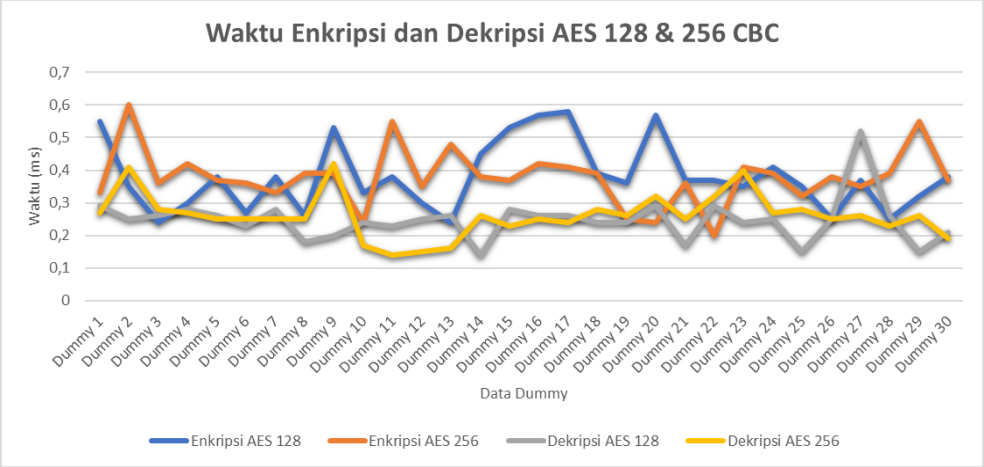
Tabel 3: Data Hasil *Hash* dan *Verify*

No	Data *Dummy*		
	Email	***Password***	***Verify***
1	$2y$10$IRDJ17Oe7tEUcc/z9sRg6eG2oaSxes/S7I7LUhxOa.hufKe4RJ7Gm	$2y$10$wvfvH8C33VHlO/Ac6BdH8.vXtXdkO5XYJXOsTVUsk7G.Qb90LZ3n.	Berhasil
2	$2y$10$CTs0.OGx0E6Pz.mgO5wEWeX/Sh5/x7qF2d5HI5Lh/FUalOas7LS1i	$2y$10$7DEHr6wBX1dP6Ciw3nOZ/eOKzFqIFSopLGo3y4J1Zip4WutMMbMfC	Berhasil
3	$2y$10$0ypMnsAwuK9l/DA.Ps9e9ugp6BBuI6OfaWMkAcaz.pomC5g3aR7dy	$2y$10$JkALYOqAxsO4SUgVqb6dD.FZ4wL6JlgDBd0YcLQ3LSuEt4xg18y52	Berhasil
4	$2y$10$gpbPMSvN8F7i8FmHGNOexeeWIObt/xPtc4kd3/nHp6MyghM2NFx7q	$2y$10$HiGT.g75Gs5kTgVXG4Hs5enFCBtz3jWPbu.iz0CGPpyi.4JfoD/KW	Berhasil
5	$2y$10$EuT7s086T0izV/R/42QfFuAi.7z6tUNo8zs7MVMOAH9FtKrjN3aGO	$2y$10$xIXOVZlpJ1rsJfeJMtojyuGI8NOWEOAU04SWr4PdMRzdebKkLOZn.	Berhasil

3.4.2 Evaluasi Waktu Proses

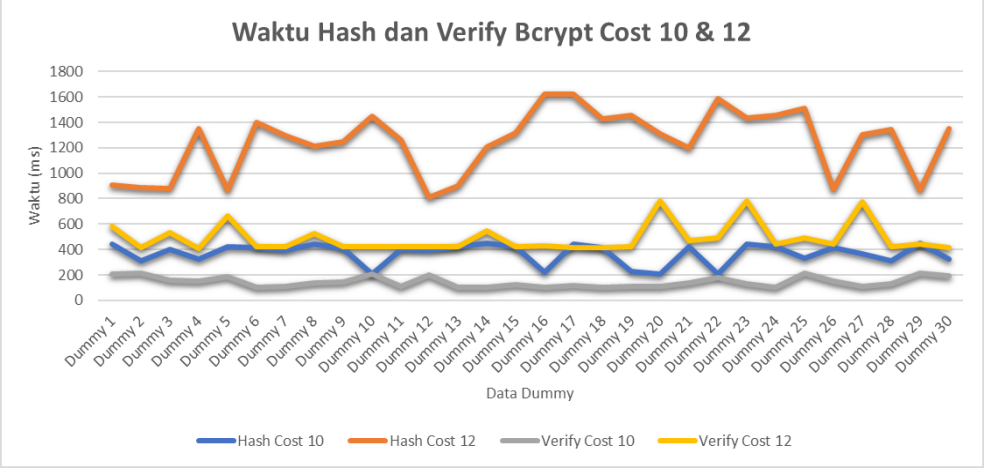
Evaluasi waktu proses dilakukan untuk mengukur kecepatan enkripsi dan dekripsi pada website Jahitku yang menggunakan algoritma AES 256 CBC dan AES 128 CBC sebagai perbandingan. Evaluasi ini dilakukan dengan menggunakan 1 perangkat secara bergantian untuk 30 data *dummy* pengguna. Hasil menunjukkan bahwa waktu proses enkripsi AES 256 CBC rata-rata adalah 0,378 ms, sedangkan dekripsinya 0,260 ms. Untuk AES 128 CBC, waktu enkripsi rata-rata 0,379 ms dan dekripsi 0,247 ms. Meskipun AES 256 CBC memiliki lebih banyak putaran (14 putaran) dibandingkan AES 128 CBC (10 Putaran), kecepatan keduanya hampir sama, namun AES 256 CBC lebih aman karena lapisan kompleksitas tambahan. Penelitian lain juga menunjukkan bahwa AES memiliki kecepatan yang lebih tinggi

dibandingkan algoritma simetris lainnya. Dalam penelitian tersebut, AES terbukti lebih cepat daripada Twofish, dengan waktu rata-rata 3,94 detik untuk enkripsi dan 3,99 detik untuk dekripsi. Sebaliknya, Twofish memerlukan 8,67 detik untuk enkripsi dan 9,02 detik untuk dekripsi [22]. Hasil pengukuran waktu proses dapat dilihat pada Gambar 4.



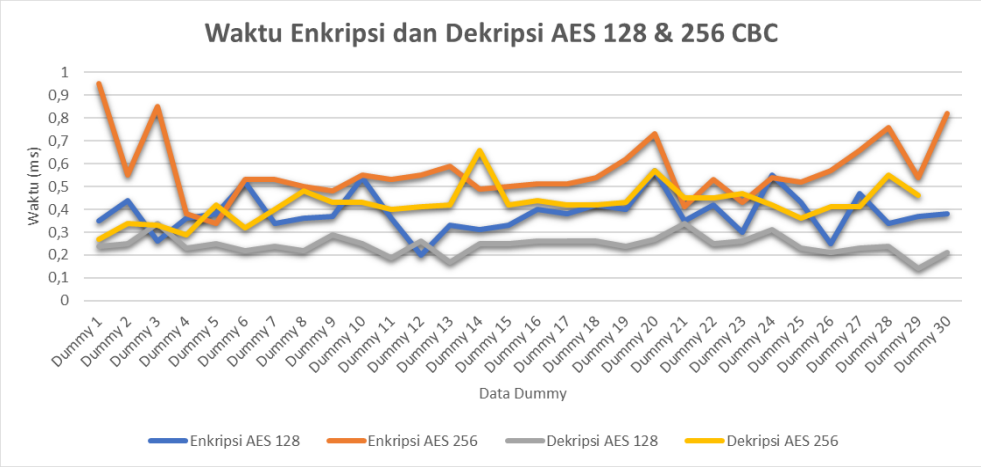
Gambar 4. Diagram Waktu Proses Enkripsi dan Dekripsi

Evaluasi waktu proses juga dilakukan untuk algoritma Bcrypt pada website Jahitku dengan *cost* 10 dan 12. Hasil menunjukkan bahwa *cost* 10 lebih efisien dengan waktu *hash* rata-rata 369,045 ms dan *verify* 145,569 ms, dibandingkan *cost* 12 yang membutuhkan 1244,924 ms untuk *hash* dan 489,596 ms untuk *verify*. *Cost* 10 dipilih karena memberikan keseimbangan antara keamanan dan kecepatan. Hasil pengukuran waktu proses dapat dilihat pada gambar 5.



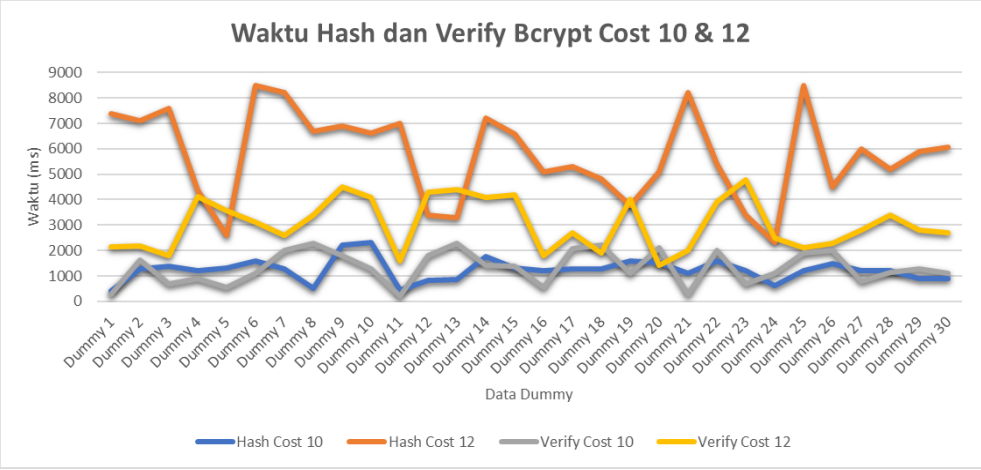
Gambar 5. Diagram Waktu Proses *Hash* dan *Verify*

Proses evaluasi yang sama juga dilakukan dengan skenario berbeda, di mana website Jahitku diakses secara bersamaan menggunakan 5 perangkat untuk menilai dampaknya terhadap performa enkripsi, *hashing,* dekripsi, dan *verify*. Hasil menunjukkan bahwa algoritma AES 256 CBC memiliki waktu enkripsi rata-rata 0,567 ms dan dekripsi 0,419 ms, sementara AES 128 CBC mencatat waktu rata-rata 0,382 ms untuk enkripsi dan 0,245 ms untuk dekripsi. Hasil pengukuran waktu proses dapat dilihat pada gambar 6.



Gambar 6. Diagram Waktu Proses Enkripsi dan Dekripsi

Pada algoritma Bcrypt, *cost* 10 menghasilkan waktu *hash* rata-rata 1231,809 ms dan *verify* 1333,262 ms, sedangkan *cost* 12 memerlukan 5765,525 ms untuk *hash* dan 3040,296 ms untuk *verify*. Pengujian ini memperlihatkan bahwa penggunaan banyak perangkat secara bersamaan berdampak signifikan terhadap performa algoritma, terutama pada Bcrypt dengan *cost* yang lebih tinggi, yang menunjukkan peningkatan waktu proses yang cukup besar. Hasil pengukuran waktu proses dapat dilihat pada gambar 7.



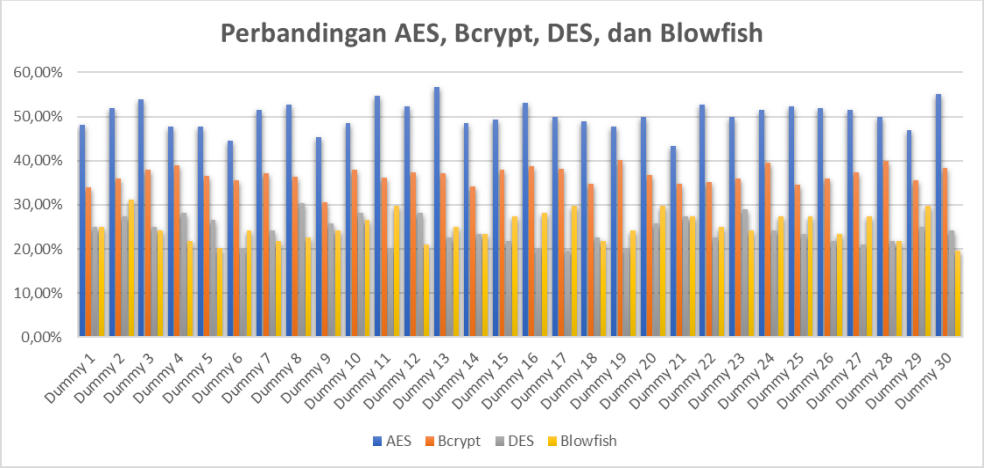
Gambar 7. Diagram Waktu Proses *Hash* dan *Verify*

3.4.3 Evaluasi *Avalanche Effect*

Avalanche Effect adalah metode evaluasi yang digunakan untuk mengukur tingkat keacakan hasil enkripsi. Proses ini melibatkan enkripsi data pengguna, kemudian melakukan perubahan pada 1 karakter dalam data tersebut sebelum mengenkripsinya kembali. Perbedaan antara kedua hasil enkripsi ini dibandingkan menggunakan rumus *Avalanche Effect*.

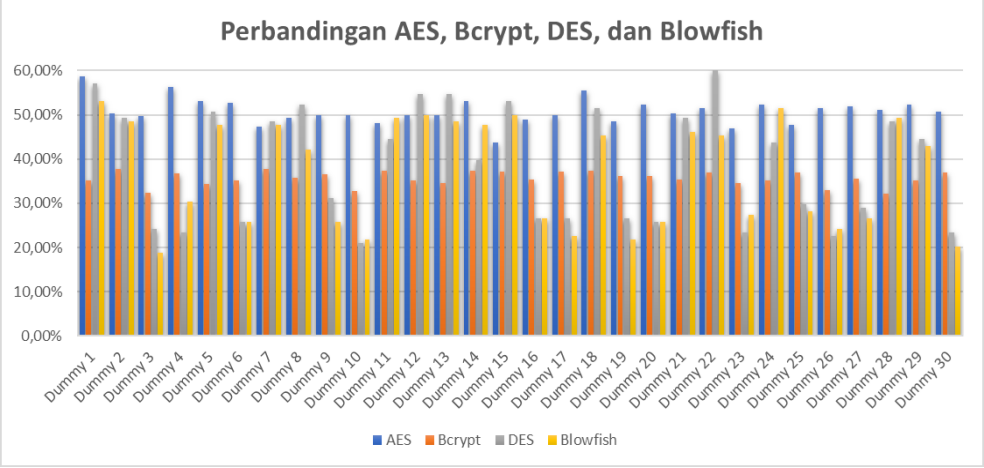
$$AE = \frac{Number\ of\ changed\ bits\ in\ ciphertext}{Total\ number\ of\ bits\ in\ ciphertext} \times 100\%$$

Algoritma yang baik berdasarkan AE sebaiknya memiliki nilai minimum 45%-50%. Semakin tinggi persentase AE, semakin baik tingkat keacakannya, sehingga meningkatkan kesulitan dalam memecahkan *ciphertext* melalui metode *statistical analysis* atau *cryptanalysis* [23], [24], [25]. Dalam evaluasi ini, AES 256 CBC menggunakan *field name* dari data pengguna dan menghasilkan rata-rata AE sebesar 50,27%, yang dinilai baik. Sebaliknya, algoritma simetris lainnya seperti DES dan Blowfish hanya mencapai AE masing-masing sebesar 24,22% dan 25,18%, yang dianggap kurang memadai. Sementara itu, algoritma Bcrypt dengan *cost* 10 menghasilkan rata-rata AE sebesar 36,65%. Walaupun lebih rendah dari standar AE yang baik, Bcrypt unggul dalam menghasilkan *hash* yang berbeda meskipun teks yang di *input* tetap sama. Hasil pengukuran tingkat keacakan dapat dilihat pada Gambar 8.



Gambar 8. Diagram Hasil Evaluasi *Avalanche Effect*

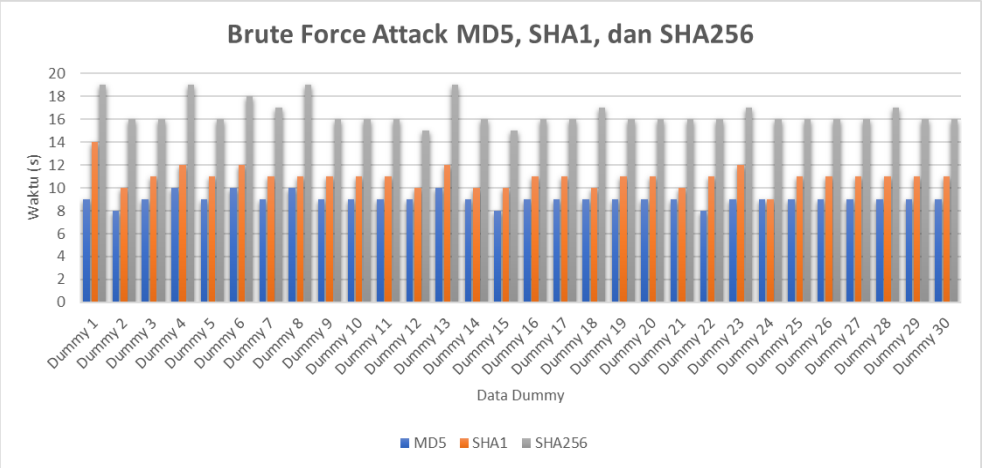
Proses evaluasi yang sama juga dilakukan dengan skenario berbeda, yaitu mengubah 5 karakter pada data pengguna. Hasilnya, AES mencapai AE sebesar 50,79%, Bcrypt 35,69%, DES 38,72%, dan Blowfish 37,03%. Pada skenario ini, tidak ada perubahan signifikan untuk AES dan Bcrypt, sedangkan DES dan Blowfish menunjukkan peningkatan AE yang cukup signifikan dibandingkan evaluasi sebelumnya dengan perubahan 1 karakter. Hasil pengukuran tingkat keacakan dapat dilihat pada Gambar 9.



Gambar 9. Diagram Hasil Evaluasi *Avalanche Effect*

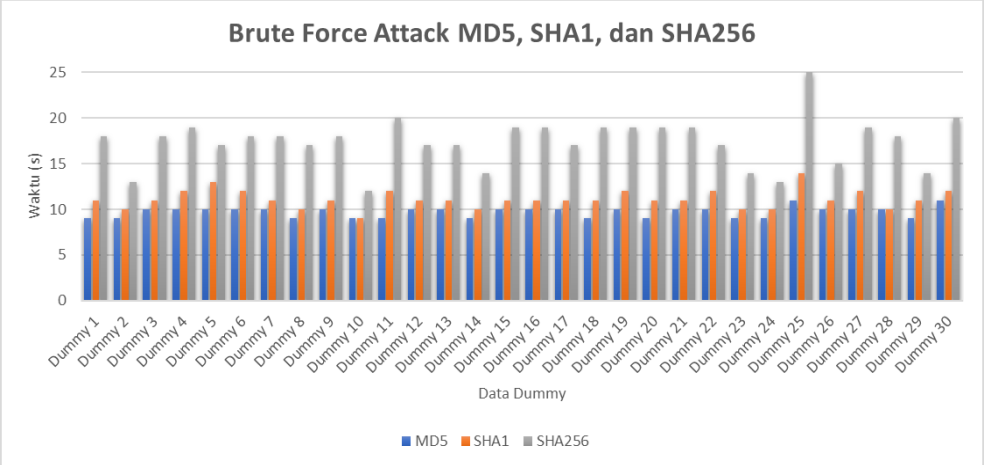
3.4.4 Evaluasi *Brute Force Attack*

Brute Force Attack merupakan salah satu evaluasi yang dilakukan untuk mengukur kualitas keamanan dari hasil *hash*. Evaluasi ini menggunakan data pengguna berupa *plaintext name*, di mana hanya 7 karakter awal yang diambil dan seluruhnya berupa huruf kecil, untuk mempermudah proses penyerangan. *Hashcat* digunakan sebagai *tools* untuk melakukan pengujian *Brute Force Attack*, sementara *Cryptools* dan *Hashing Online Genetor* digunakan untuk mensimulasikan proses *hashing* dari algoritma Bcrypt. Selain itu, evaluasi juga dilakukan pada algoritma MD5, SHA1, dan SHA256 sebagai perbandingannya. Hasil evaluasi menunjukkan bahwa *hash* dari algoritma MD5, SHA1, dan SHA256 dapat dipecahkan dengan cepat menggunakan *Brute Force Attack*, dengan rata-rata waktu 9,03 detik untuk MD5, 10,96 detik untuk SHA1, dan 16,53 detik untuk SHA256. Namun, *hash* yang dihasilkan oleh algoritma Bcrypt tidak dapat dipecahkan atau sangat sulit dipecahkan menggunakan metode yang sama. Penelitian lain juga mendukung hasil ini, menunjukkan bahwa *Brute Force Attack* terhadap Bcrypt dengan *plaintext* 7 karakter sederhana membutuhkan waktu sekitar 8-10 jam untuk dipecahkan [21]. Hasil pengukuran kualitas keamanan dapat dilihat pada Gambar 10.



Gambar 10. Diagram Hasil Evaluasi *Brute Force Attack*

Proses evaluasi yang sama juga dilakukan dengan skenario berbeda, yaitu menggunakan 30 *plaintext* yang terdiri dari 7 karakter lebih rumit, yang dihasilkan menggunakan *strong password generator*. Karakter tersebut merupakan kombinasi huruf kecil, huruf besar, angka, dan simbol. Hasilnya menunjukkan bahwa waktu yang dibutuhkan untuk memecahkan *hash* adalah 9,7 detik untuk MD5, 11,13 detik untuk SHA1, dan 17,4 detik untuk SHA256. Sementara itu, untuk algoritma Bcrypt, hasilnya tetap sama, yaitu tidak dapat dipecahkan. Penelitian lain juga mendukung hasil ini, di mana *plaintext* 7 karakter yang lebih rumit tidak dapat dipecahkan meskipun telah dilakukan *Brute Force Attack* selama 5 hari [21]. Hasil pengukuran kualitas keamanan dapat dilihat pada Gambar 11.



Gambar 11. Diagram Hasil Evaluasi *Brute Force Attack*

4. KESIMPULAN

Berdasarkan evaluasi yang telah dilakukan, dapat dilihat bahwa website Jahitku yang telah melakukan implementasi algoritma AES dan Bcrypt dapat menjalankan proses enkripsi dan dekripsi serta *hashing* dan *verify* data pengguna yang tersimpan pada *database MySQL PhpMyAdmin*. Hasil evaluasi menunjukkan bahwa AES 256 CBC membutuhkan rata-rata waktu 0,378 ms untuk enkripsi dan 0,260 ms untuk dekripsi. Pada skenario yang berbeda, waktu enkripsi meningkat menjadi 0,567 ms dan waktu dekripsi menjadi 0,245 ms. Algoritma AES unggul dalam tingkat keacakan (*Avalanche Effect*) dengan persentase sebesar 50,27%, yang menunjukkan tingkat keacakan dipandang baik dibandingkan dengan algoritma simetris lainnya seperti DES dengan 24,22% dan Blowfish dengan 25,18%. Dalam skenario yang berbeda, AES mencapai 50,79%, sedangkan DES 38,72%, dan Blowfish 37,03%. Di sisi lain, Bcrypt membutuhkan rata-rata waktu 369,045 ms untuk *hashing* dan 145,569 ms untuk *verifiy*. Pada skenario berbeda, waktu *hashing* meningkat menjadi 1231,809 ms dan waktu *verify* menjadi 1333,262 ms. Meskipun *Avalanche Effect* hanya mencapai 36,65%, yang menunjukkan tingkat keacakan dipandang kurang baik, tetapi Bcrypt tetap dapat menghasilkan *hash* yang unik untuk *input* yang sama. Dalam hal keamanan, menunjukkan bahwa hasil *hash* dari *plaintext* 7 karakter sederhana dan skenario berbeda dengan *plaintext* 7 karakter lebih rumit, Bcrypt sulit dipecahkan menggunakan *Brute Force Attack* dibandingkan algoritma *hashing* lainnya seperti MD5, SHA1, dan SHA256 terbukti rentan terhadap *Brute Force Attack*. Adapun saran untuk penelitian selanjutnya adalah menguji kombinasi algoritma simetris lainnya seperti ChaCha20 atau Serpent, serta algoritma *hashing* lainnya seperti Argon2 atau Scrypt, untuk membandingkan kinerja dan keamanannya dengan AES dan Bcrypt. Selain itu, algoritma asimetris seperti RSA atau ECC dapat diteliti lebih lanjut untuk membandingkan penggunaannya dalam skenario tertentu. Penelitian juga dapat dilakukan pada skala data yang lebih besar untuk mengevaluasi performa dan skalabilitas dalam skenario yang lebih kompleks. Penelitian lebih lanjut juga perlu menguji ketahanan algoritma terhadap serangan lainnya, seperti *Dictionary Attack* atau *Timing Attack*.

DAFTAR PUSTAKA

[1] W. Stallings, *Cryptography and network security : principles and practice*. 2017.

[2] T. S. Alasi, R. Wanto, and V. H. Sitanggang, "IMPLEMENTASI KRIPTOGRAFI ALGORITMA IDEA PADA KEAMANAN DATA TEKS BERBASIS ANDROID," vol. 2, no. 1, 2021.

[3] E. Dwi Hastri, "Cyber Espionage Sebagai Ancaman Terhadap Pertahanan Dan Keamanan Negara Indonesia," *Law & Justice Review Journal*, vol. 1, no. 1, pp. 12–25, Jun. 2021, doi: 10.11594/lrjj.01.01.03.

[4] Raodia, "PENGARUH PERKEMBANGAN TEKNOLOGI TERHADAP TERJADINYA KEJAHATAN MAYANTARA (CYBERCRIME) Raodia," 2019.

[5] I. Juan Alfreda, R. Ratna Permata, and T. Safiranita Ramli, "Pelindungan Dan Tanggung Jawab Kebocoran Informasi Pada Penyedia Platform Digital Berdasarkan Perspektif Rahasia Dagang," *Jurnal Sains Sosio Humaniora P-ISSN*, vol. 5, pp. 2580–1244, 2021.

[6] M. R. Ramadhani and A. Raf'ie Pratama, "Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia," 2020.

[7]) Magister, M. Bencana, and K. Nasional, "NUSANTARA: Jurnal Ilmu Pengetahuan Sosial DEGRADASI MORAL SEBAGAI DAMPAK KEJAHATAN SIBER PADA GENERASI MILLENIAL DI INDONESIA 1 Nurbaiti Ma'rufah 1) , Hayatul Khairul Rahmat 2) , I Dewa Ketut Kerta Widana," *Tahun*, vol. 7, no. 1, pp. 191–201, 2020, doi: 10.31604/jips.v7i1.2020.191-201.

[8] E. F. Pakpahan, K. Chandra, and A. Tanjaya, "Urgensi Pengaturan Financial Technology Di Indonesia," 2020.

[9] F. Prasetyo Nugroho, R. Wariyanto Abdullah, and S. Wulandari, "KEAMANAN BIG DATA DI ERA DIGITAL DI INDONESIA," 2019.

[10] M. Fadlan, S. Sinawati, A. Indriani, and E. D. Bintari, "PENGAMANAN DATA TEKS MELALUI PERPADUAN ALGORITMA BEAUFORT DAN CAESAR CIPHER," *JURNAL TEKNIK INFORMATIKA*, vol. 12, no. 2, pp. 149–158, Nov. 2019, doi: 10.15408/jti.v12i2.12262.

[11] L. Loqman, A. Rahman, P. Studi, D. Pertahanan, and S. Pertahanan, "Implikasi Diplomasi Pertahanan terhadap Keamanan Siber dalam Konteks Politik Keamanan Implications of Defense Diplomacy on Cybersecurity in Context Security Politics," 2020.

[12] A. Widarma, H. F. Siregar, and M. Dedi Irawan, "Teknik Keamanan Data Menggunakan Vigenere Cipher Dan Electronic Code Book (ECB)," 2019. [Online]. Available: http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

[13] C. Ntantogian, S. Malliaros, and C. Xenakis, "Evaluation of password hashing schemes in open source web platforms," *Comput Secur*, vol. 84, pp. 206–224, Jul. 2019, doi: 10.1016/j.cose.2019.03.011.

[14] G. Divva, M. Zulma, H. B. Seta, and T. Yuniati, "Implementasi Algoritma AES Dan Bcrypt untuk Pengamanan File Dokumen," *JURNAL INFORMATIK*, 2022.

[15] D. A. Meko, "Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data," *Jurnal Teknologi Terpadu*, vol. 4, no. 1, 2018.

[16] S. Gupta, S. K. Yadav, A. P. Singh, and K. C. Maurya, "A comparative study of secure hash algorithms," in *Smart Innovation, Systems and Technologies*, Springer Science

and Business Media Deutschland GmbH, 2016, pp. 125–133. doi: 10.1007/978-3-319-30927-9_13.

[17] D. Aipina and H. Witriyono, "PEMANFAATAN FRAMEWORK LARAVEL DAN FRAMEWORK BOOTSTRAP PADA PEMBANGUNAN APLIKASI PENJUALAN HIJAB BERBASIS WEB," *Jurnal Media Infotama*, vol. 18, no. 1, pp. 36–42, 2022.

[18] D. S. R. S. K. D. Neha Yadav, "LARAVEL: A PHP Framework for E-Commerce Website," pp. 503–508, 2019.

[19] F. Wiemer and R. Zimmermann, *High-Speed Implementation of bcrypt Password Search using Special-Purpose Hardware*. IEEE, 2014.

[20] B. S. and B. S. P. C. Skanda, "Secure Hashing using BCrypt for Cryptographic Applications," *2022 IEEE North Karnataka Subsection Flagship International Conference (NKCon)*, pp. 1–5, 2022.

[21] T. P. Batubara, S. Efendi, and E. B. Nababan, "Analysis Performance BCRYPT Algorithm to Improve Password Security from Brute Force," in *Journal of Physics: Conference Series*, IOP Publishing Ltd, 2021. doi: 10.1088/1742-6596/1811/1/012129.

[22] E. Awal, E. H. Nurkifli, and T. Padilah, "ANALISIS PERBANDINGAN HASIL ENKRIPSI DAN DEKRIPSI ALGORITMA KRIPTOGRAFI RIJNDAEL DAN TWOFISH UNTUK PENYANDIAN DATA," *Jurnal Mahasiswa Ilmu Komputer (JMIK)*, Mar. 2022.

[23] I. Fitriani and A. Baskoro Utomo, "Implementasi Algoritma Advanced Encryption Standard (AES) pada Layanan SMS Desa," 2020.

[24] R. R. Fauzi and W. Theophilus, "Perancangan Kriptografi Block Cipher berbasis Pola Dribbling Practice," *AITI: Jurnal Teknologi Informasi*, vol. 18, no. Agustus, pp. 158–172, 2021.

[25] A. Prajuhana Putra, S. Maryana, A. Setiawan, and P. Teknik Informatika Universitas Pakuan Bogor, "Implementasi Algoritma AES (Advance Encryption Standard) Rijndael Pada Aplikasi Keamanan Data," 2020.