Jurnal Sistem Komputer dan Informatika (JSON)
Volume 3, Nomor 4, Juni 2022
e-ISSN 2685-998X
DOI 10.30865/json.v3i4.4285

Implementasi Bcrypt dengan SHA-256 pada *Password* Pengguna Aplikasi Golek Kost

Rynaldy Shulton Giffary*, Erika Ramadhani

Fakultas Teknologi Industri, Program Studi Informatika, Universitas Islam Indonesia, Yogyakarta, Indonesia
Email: 1, *shulton.ghiffary23@gmail.com, 2erika@uii.ac.id
Email Penulis Korespondensi: shulton.ghiffary23@gmail.com
Submitted: **15/06/2022**; Accepted: **30/06/2022**; Published: **30/06/2022**

Abstrak–Brute force merupakan pemecahan password pada algoritma SHA-256, sehingga sistem yang menggunakan algoritma tersebut mudah untuk diambil data pentingnya. Selain itu ada MD5 yang dapat menyebabkan collusion. Akan tetapi, ada algoritma yang mampu bertahan dari serangan brute force, yaitu bcrypt. Keamanan data pribadi merupakan prioritas utama pada setiap sistem. Perbuatan brute force merupakan cyber crime yang perlu diwaspadai. Tujuan dari penelitian ini adalah mengkaji algoritma bcrypt yang digunakan sebagai password dengan tujuan agar mampu bertahan dari serangan brute force. Karena bcrypt memiliki nilai cost dan salt.

Kata Kunci: Hacker; Password; Kriptografi; Bcrypt; Hash

Abstract–Brute force is the breaking of passwords in the SHA¬-256 algorithm, so that systems using this algorithm are easy to retrieve important data. In addition there is MD5 which can cause collusion. However, there is an algorithm that can withstand brute force attacks, namely bcrypt. Personal data security is a top priority on every system. Brute force is a cyber crime that needs to be watched out for. The purpose of this study is to examine the bcrypt algorithm used as a password in order to be able to survive brute force attacks. Because bcrypt has a cost and a salt value.

Keywords: Hacker; Password; Kriptografi; Bcrypt; Hash

1. PENDAHULUAN

Perkembangan teknologi dan informasi memiliki dampak positif di masyarakat, yaitu kemudahan dalam mendapatkan data maupun informasi yang diinginkan [1]. Hal tersebut dapat menjadikannya sebagai tolak ukur dalam menentukan nasib seseorang. Adanya tolak ukur tersebut, dapat mengubah pola hidup dan pemicu di kalangan masyarakat yang berdampingan dengan teknologi. Hal tersebut menyebabkan masyarakat menjadi bergantung dengan adanya perkembangan teknologi, dan tentunya dibarengi dengan adanya kejahatan, yaitu "*cybercrime*" [2]. *Cyber crime* adalah kejahatan yang dilakukan di perangkat berbasis computer dan jaringan (*network*) [3]. Oleh karena itu, sistem membutuhkan pengamanan data dan informasi. Sistem pengamanan yang dapat dilakukan berupa otentikasi, enkripsi, akses kontrol, dan *data integrity* [4].

Golek kost merupakan aplikasi yang mendigitalkan aktivitas pencarian kost maupun kontrakan, jual beli barang, dan pencarian jasa angkut, khususnya daerah Yogyakarta. Dalam aplikasi tersebut memerlukan data pribadi, karena tingginya pengguna aplikasi yang bergerak di bidang teknologi. Bagaimanapun wujud data yang bersifat pribadi, dalam jumlah banyak ataupun sedikit dalam aplikasi harus tetap terjaga keamanannya dari pihak yang tidak bertanggung jawab. Hal tersebut merupakan konsep dari keamanan sistem informasi [5].

Hacker adalah individu ataupun sekelompok individu sebagai pelaku *cybercrime* yang memiliki rasa penasaran terhadap computer dan memiliki tingkat kecerdasan atau kemampuan yang tinggi, serta memiliki tiga klasifikasi, yaitu *black hats*, *white hats*, dan *grey hats* untuk membedakan perbuatan illegal ataupun legal mereka [6]. *Brute force* merupakan salah satu aktivitas yang dilakukan oleh *hacker*, yaitu dengan menyerang sistem keamanan komputer dengan berbagai percobaan kunci yang sesuai. Teknik yang digunakan *hacker* untuk melakukan *brute force* adalah *password cracker*. *Password cracker* adalah program yang digunakan untuk mengetahui *password* yang telah di enkripsi dengan algoritma tertentu [7]. Biasanya, *brute force* sering terjadi pada fungsi *hash SHA*-256. Kemudian ada MD5 yang apabila digunakan dapat menghasilkan nilai yang sama dengan nilai yang lain, makan akan terjadi *collision* atau bisa disebut tabrakan. Untuk menggantikan algoritma tersebut, menggunakan algoritma *bcrypt* yang sudah memiliki nilai *cost* dan *salt.*

Oleh karena itu, diperlukan adanya sistem untuk menjaga keamanan data pribadi pengguna aplikasi dari para pelaku kejahatan. Salah satu mekanisme yang diterapkan pada aplikasi ini adalah akses control. Mekanisme tersebut menggunakan kombinasi, antara *user id* dan *password*. *Password* yang disarankan menggunakan campuran berbagai jenis karakter, seperti huruf kecil, huruf kapital, angka, dan simbol [8]. Penggunaan *password* yang tidak bermacam-macam karakternya, akan dengan mudah dipecahkan oleh *hacker*, oleh karena itu diperlukannya ilmu kriptografi. Kriptografi adalah proses untuk menjaga keamanan pesan tersebut. Terdapat dua proses pada kriptografi, yaitu *plaintext* diubah menjadi *chipertext* disebut sebagai enkripsi dan proses *chipertext* diubah menjadi *plaintext* disebut dekripsi [9].

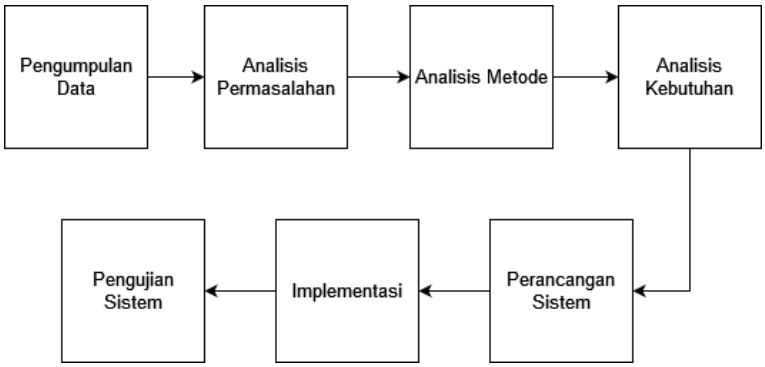
Jurnal Sistem Komputer dan Informatika (JSON)
Volume 3, Nomor 4, Juni 2022
e-ISSN 2685-998X
DOI 10.30865/json.v3i4.4285

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Metode yang digunakan dalam penelitian ini adalah menggunakan metode kualitatif. Menurut Meleong (2005:6), penelitian kualitatif adalah penelitian yang bermaksud untuk mengetahui kejadian yang di alami oleh subjek penelitian, yang kemudian menghasilkan data yang bersifat deskriptif [10].

Menggunakan metode kualitatif karena bagian-bagian yang digunakan dalam membangun sistem bersifat deskriptif, menggambarkan, dan mendiskripsikan. Berikut langkah-langkah penelitian kualitatif yang digambarkan dengan diagram ilmiah, seperti gambar berikut :



Gambar 1. Tahapan Penelitian

Pada pengumpulan data dilakukan studi literatur, karena yang dilakukan peneliti adalah mempelajari jurnal, artikel web, dan sumber internet lainnya. Dalam perancangan sistem atau aplikasi diperlukan adanya analisis kebutuhan pada sistem atau aplikasi Golek Kost menggunakan metode *Sprint*. Kemudian dalam implementasi terletak pada *user* akan register, dan memberikan *password* yang digunakan. *Password* pada aplikasi ini menggunakan fungsi *hash* dengan *Bcrypt.* Tahapan yang terakhir yaitu pengujian sistem, pengujian ini dilakukan untuk mengetahui sistem yang dibuat dapat berjalan sesuai dengan fungsionalitasnya.

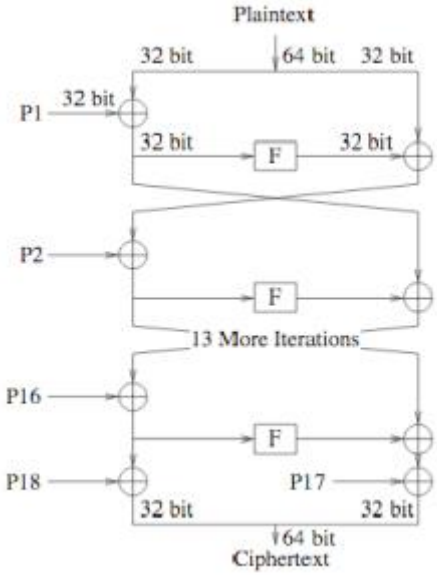
2.2 *BCRYPT*

Bcrypt adalah fungsi *hash* yang dibuat oleh Blowfish dan Crypt yang merupakan fungsi *hash* utama pada pemrograman *password* di UNIX. Blowfish melakukan penggabungan dengan fungsi *hash* Crypt agar pemecahan *password* memerlukan waktu yang lama. Pada *bcrypt* memiliki tahap inisialisasi kunci bernama "eksblowfish", yang memiliki makna *expensive key schedule blowfish*. *Bcrypt* memiliki ketahanan terhadap *rainbow table*, karena dalam pengkodeannya menggunakan 128-bit *salt* pada proses *hashing*-nya.

Bcrypt memiliki dua langkah, langkah pertama adalah menggunakan *eksblowfish* sebagai *set initial key*, *cost* sebagai parameternya, nilai *salt*, dan *text* yang akan dilakukan *hashing*. Setelah itu *bcrypt* akan melakukan penurunan kunci pada kunci utamanya, kemudian kunci utama tersebut diisi dengan *text* yang akan dilakukan *hashing*. Pada langkah yang kedua, *bcrypt* melakukan enkripsi pada *OrpheanBeholderScryDoubt* dengan ukuran 192-bit pada kunci yang sudah dibuat pada langkah pertama, kemudian dilakukan perulangan sebanyak 64 kali $(T_0, T_1, T_2, T_3, \dots, T_{63})$. Setelah melakukan perulangan sebanyak 64 kali, dilakukan enkripsi menggunakan ECB (*Electronic Code Book*) dan digabungkan dengan *cost* dan nilai *salt* dengan ukuran 128-bit. Berikut langka-langkah yang dilakukan untuk menghasilkan nilai *bcrypt* [11] :

a. Bentuk inisial array P sebanyak 18 buah masing-masing bernilai 32-bit. Array P terdiri dari delapan belas kunci 32-bit subkunci : (P1, P2, … , P18).
b. *Plaintext* yang akan di enkripsi diasumsikan sebagai masukan dan diambil sebanyak 64-bit dan apabila kurang dari 64-bit, maka akan dilakukan penambahan bit-nya, agar data yang dilakukan perhitungan sesuai.
c. Hasil pengambilan tadi dibagi menjadi dua, 32-bit pertama dibsebut XL dan 32-bit kedua disebut XR.
d. Selanjutnya melakukann operasi XL = XL xor Pi dan XR = F(XL) xor XR.
e. Hasil dari operasi diatas ditukar XL menjadi XR dan XR menjadi XL.
f. Lakukan sebanyak 16 kali, perulangan yang ke-16 dilakukan lagi proses penukaran XL dan XR.
g. Pada proses ke 17 lakukan operasi untuk XR = XR xor P17 dan XL = XL xor P18.
h. Proses terakhir yaitu menyatukan Kembali XL dan XR sehingga menjadi 64-bit kembali. Seperti gambar dibawah ini.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 3, Nomor 4, Juni 2022
e-ISSN 2685-998X
DOI 10.30865/json.v3i4.4285



Gambar 2. Proses Algoritma *bcrypt*

3. HASIL DAN PEMBAHASAN

3.1 Pengujian Sistem

Pengujian sistem aplikasi ini menggunakan pengujian *black box*, dilakukan untuk mengetahui fungsionalitas yang dibuat dapat berjalan dengan semestinya. *Black box* juga memungkinkan pengembang aplikasi untuk mengumpulkan data, yang nantinya bisa dijadikan sebagai bahan pengembangan aplikasi agar lebih baik.

1. Pengujian fungsionalitas *register* pada aplikasi Golek Kost

Tabel 1. Pengujian fungsionalitas registrasi

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Pengujian	Kesimpulan
1.	Registrasi yang digunakan oleh pengguna	Penguna dapat melakukan pendaftaran dengan menginputkan data diri (nama, nomor telfon, email, dan password).	Sukses	Fungsionalitas *registrasi* dapat dilakukan oleh pengguna.

2. Pengujian fungsionalitas *login* pada aplikasi Golek Kost

Tabel 2. Pengujian fungsionalitas *login*Hasil pengujian bcrypt

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Pengujian	Kesimpulan
1.	*Login* yang digunakan oleh pengguna	Pengguna dapat melakukan *login* di aplikasi Golek Kost, dengan meng-*input*-kan *e-mail* dan *password*.	Sukses	Fungsionalitas *login* dapat dilakukan oleh pengguna.

Dari hasil pengujian yang diperoleh terhadap fungsi *register* yang menggunakan fungsi *hash bcrypt* menghasilkan nilai *hash* terdiri dari 6 karakter desimal, 5 karakter symbol, 23 karakter huruf kecil, dan 21 karakter huruf besar. Walaupun masing-masing *plaintext* sama, nilai *hash* yang dihasilkan berbeda. Berikut hasil pengujian yang dilakukan :

Tabel 3. Hasil pengujian *bcrypt*

Email	*Text*	Nilai *Hash*
ujiBcrypt1@gmail.com	ujicoba	$2y$10$MXCi8XpigyUlcYzKyh6MJu4FO..K mJBMKaMZJ24BCG5eEc.m9Tiuq
ujiBcrypt2@gmail.com	ujicoba	$2y$10$mchbUtd7l0ihDqDEfFqo1OK/Xy1T uwT54fG2UqZV8hT2kA7KYyJii
ujiBcrypt3@gmail.com	ujicoba	$2y$10$SaE9kT6QmMcceX2EY4/zv.zVJ.0g gMOvhm1I/P3Y/qJ2/uO6KfHP2

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 3, Nomor 4, Juni 2022
e-ISSN 2685-998X
DOI 10.30865/json.v3i4.4285

4. KESIMPULAN

Berdasarkan penilitian yang telah dilakukan, untuk melakukan *login* pada aplikasi Golek Kost perlu melakukan registrasi di halam *register* agar data diri berada di *database*. Pada fungsi *hash* yang digunakan pada *password* yaitu *bcrypt*, sudah ada campuran nilai *cost* dan *salt* yang memiliki ukuran 128-bit. Pada *password* yang menggunakan algoritma *bcrypt* akan sulit terkena *brute force*, karena mendapatkan nilai *cost* dengan *default*-nya 10 dan memiliki jarak nilai antara 10-14. Selain itu juga dapat terhindar dari peristiwa *collision* atau bisa juga disebut tabrakan. Karena terdapat *salt* yang merupakan pengacakan pada nilai *hash* dan mendapatkan sejumlah 22 karakter unik. Kemudian dilakukan *hashing* kembali. Untuk aplikasi memerlukan pengujian, karena untuk mengukur sejauh mana aplikasi ini dapat bekerja seperti fungsionalitasnya. Dari hasil pengujian yang di dapat, diharapkan pengembang dapat melakukan pengembangan ataupun perbaikan aplikasi agar menjadi lebih baik lagi. Diharapkan juga nilai *hash* yang diuji memiliki akurasi yang tepat.

REFERENCES

[1] Afnesia, U., & Ayunda, R. (2022). Perlindungan Data Diri Peminjam Dalam Transaksi Pinjaman Online: Kajian Perspektif Perlindungan Konsumen Di Indonesia.Jurnal Komunitas Yustisia,4(3), 1035-1044.
[2] Anugerah, A. T.(2022). Pencurian Data Pribadi di Internet dalam Perspektif Kriminologi. Jurnal Komunikasi Hukum,8(1), https://ejournal.undiksha.ac.id/index.php/jkh/article/view/45434/21302, di akses pada 12 Juni 2022 pukul 13.57
[3] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
[4] D. C. Luminita, “Information security in E-learning Platforms,” Procedia - Social and Behavioral Sciences, vol. 15, pp. 2689–2693,2011
[5] A. Y. Husodo et al., “Sistem Keamanan Nilai Akademik Online Berbasis Kode Hash dengan Identitas Server Sebagai Parameter Validasi,” Jurnal Sains Teknologi dan Lingkungan vol. 1, no. 1, pp. 8–14, 2015
[6] Ginanjar, Y.(2019), “*Hacker* sebagai Aktor Non_negara: *Cyber Warfare* sebagai Dampak Penyadapan Pejabat Negara Indonesia oleh Intelijen Australia. https://www.researchgate.net/publication/338605144_HACKER_SEBAGAI_AKTOR_NON-NEGARA, di akses pada 12 Juni 2022 pukul 19.45
[7] Pramaditya, H.(2016).”*Brute Force Password Cracking* dengan menggunakan *Graphic Processing Power*. https://jurnal.unmer.ac.id/index.php/jtmi/article/view/615/308, di akses pada 13 Juni 2022 pukul 07.34
[8] Junaedi, D, I.(2018).”Peluang Keamanan dalam Transaksi Perbankan. https://media.neliti.com/media/publications/293479-peluang-keamanan-password-dalam-transaks-19645576.pdf, di akses pada 14 Juni 2022 pukul 14.40
[9] Febriana, I., Aji, G.(2017).”Penerapan Teknik Kriptografi pada Keamanan SMSANDROID”. https://jurnal.stkippgritulungagung.ac.id/index.php/joeict/article/download/103/53, di akses pada tanggal 14 Juni 2022 pukul 17.00
[10] P. S. Rahmat, “Penelitian Kualitatif,” Equilibrium, vol. 5, no. 9, pp. 1-8, Juni 2009.
[11] Yafie, H., N.(2021).”Analisis Penggunaan Fungsi *Hash Bcrypt* untuk Kemanan Kata Sandi”. https://docplayer.info/213803714-Analisis-penggunaan-fungsi-hash-bcrypt-untuk-keamanan-kata-sandi.html, di akses pada tanggal 15 Juni 2022 pukul 09.34.