Journal of Information Technology and Computer Science (INTECOMS)
Volume 7 Nomor 3, Tahun 2024
e-ISSN : 2614-1574
p-ISSN : 2621-3249

PENCEGAHAN SERANGAN BERBASIS KATA SANDI: STUDI KOMPREHENSIF TENTANG IMPLEMENTASI HASH PADA APLIKASI WEB

PREVENTION OF PASSWORD-BASED ATTACKS: A COMPREHENSIVE STUDY OF HASH IMPLEMENTATION IN WEB APPLICATIONS

Muhammad Adri Ramadhan[1], Arpinda[2], Deny Saputra[3], Dadang Iskandar Mulyana[4]
[1,2,3,4]Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, DKI Jakarta, Indonesia.
adri@devision.id[1], arpinda27@gmail.com[2], denysyahputra30@gmail.com[3], mahvin2021@gmail.com[4]

ABSTRACT

In the increasingly developing digital era, information security has become a crucial aspect in data management, especially in the web application environment. Password-based attacks are one of the main threats that can result in unauthorized access to information systems. To overcome this risk, the use of encryption methods is important, and one commonly used approach is the hash technique. This research aims to provide a comprehensive understanding of the implementation of hashes in web applications as a preventive measure for password-based attacks. Hashing is a mathematical method used to convert a password into a hash value, which is difficult to decode back into the original password. However, the use of hashes in web applications is often not optimal, requiring review and improvement in implementation. This study will conduct an in-depth analysis of various commonly used hash algorithms, as well as evaluate the weaknesses and strengths of each. Additionally, this research will consider other security factors that may impact the effectiveness of password protection, such as key management, strong password policies, and account recovery procedures. This research explores the application of adaptive security methods that can identify and dynamically respond to current trends in password-based attacks. By integrating artificial intelligence or machine learning technology, the system can proactively improve password security based on detected attack patterns. Through this approach, the results can be developed into a better understanding of password protection in the context of web applications, as well as develop practical guidelines for improving security and reducing the risk of password-based attacks. Thus, the results of this research can make a positive contribution to the development of information security technology in facing increasingly complex threats in this digital era.
Keywords: *Information Security, Encryption, Hashing, Passwords, Algorithms, Web Applications, Key Management, Security Technology.*

ABSTRAK

Dalam era digital yang semakin berkembang, keamanan informasi menjadi suatu aspek krusial dalam pengelolaan data, terutama di lingkungan aplikasi web. Serangan berbasis kata sandi merupakan salah satu ancaman utama yang dapat mengakibatkan akses tidak sah terhadap sistem informasi. Untuk mengatasi risiko ini, penggunaan metode enkripsi menjadi penting, dan salah satu pendekatan yang umum digunakan ialah teknik hash. Penelitian ini bertujuan untuk memberikan pemahaman komprehensif mengenai implementasi hash pada aplikasi web sebagai langkah pencegahan serangan berbasis kata sandi. Hashing merupakan metode matematis yang digunakan untuk mengubah kata sandi menjadi nilai hash, yang sulit untuk diurai kembali menjadi kata sandi asli. Namun, penggunaan hash dalam aplikasi web seringkali tidak optimal, sehingga memerlukan peninjauan dan perbaikan dalam implementasinya. Studi ini akan melakukan analisis mendalam terhadap berbagai algoritma hash yang umum digunakan, serta mengevaluasi kelemahan dan kelebihan masing-masing. Selain itu, penelitian ini akan mempertimbangkan faktor-faktor keamanan lain yang dapat memengaruhi efektivitas perlindungan kata sandi, seperti manajemen kunci, kebijakan kata sandi yang kuat, dan prosedur pemulihan akun. Penelitian ini mengeksplorasi penerapan metode keamanan adaptif yang dapat mengidentifikasi dan merespons secara dinamis terhadap tren serangan berbasis kata sandi terkini. Dengan mengintegrasikan teknologi kecerdasan buatan atau pembelajaran mesin, sistem dapat secara proaktif meningkatkan keamanan kata sandi berdasarkan pola-pola serangan yang terdeteksi. Melalui pendekatan ini, hasil dapat dikembangkan menjadi suatu pemahaman yang lebih baik mengenai perlindungan kata sandi dalam konteks aplikasi web, serta menyusun pedoman praktis untuk meningkatkan keamanan dan mengurangi risiko serangan berbasis kata sandi. Dengan demikian, hasil dari penelitian ini dapat memberikan kontribusi positif terhadap pengembangan teknologi keamanan informasi dalam menghadapi ancaman yang semakin kompleks di era digital ini.
Kata Kunci: Keamanan Informasi, Enkripsi, Hashing, Kata Sandi, Algoritma, Aplikasi Web, Manajemen Kunci, Teknologi Keamanan.

PENDAHULUAN

Seiring dengan terus meningkatnya era digitalisasi, di mana keberlangsungan operasional sistem informasi menjadi esensial, tingkat keamanan yang diterapkan, terutama dalam lingkungan aplikasi web, menjadi faktor kunci yang menentukan. Ancaman serius terhadap integritas data dan keamanan sistem secara keseluruhan ialah serangan berbasis kata sandi, yang mampu memberikan akses tidak sah ke informasi sensitif. Dengan evolusi serangan siber yang semakin canggih, penting bagi organisasi dan pengelola aplikasi web untuk mengintensifkan upaya pencegahan serangan berbasis kata sandi guna melindungi integritas dan kerahasiaan data.

Tujuan dari penelitian ini merupakan untuk merinci pemahaman komprehensif tentang strategi pencegahan serangan berbasis kata sandi, dengan penekanan khusus pada implementasi teknik hashing dalam konteks aplikasi web. Hashing, sebagai teknik kriptografi yang umum digunakan, menjadi lapisan pertahanan kritis dalam menghadapi serangan yang bertujuan merusak integritas dan merampas kerahasiaan kata sandi pengguna.

Dalam membahas implementasi hash pada aplikasi web, penelitian ini bertujuan untuk memberikan pandangan yang jelas dan mendalam. Algoritma yang kami gunakan ialah Bcrypt, yang dimana akan dianalisis secara menyeluruh untuk mengevaluasi tingkat keamanan dan kecepatan pemrosesan data masing-masing algoritma. Analisis ini akan membantu dalam menentukan pilihan algoritma yang paling sesuai dengan kebutuhan keamanan aplikasi web.

Penelitian ini tidak hanya membatasi diri pada analisis algoritma hashing, tetapi juga melibatkan eksplorasi teknik keamanan tambahan. Aspek-aspek ini termasuk pengulangan, dan manajemen kunci yang efektif untuk meningkatkan lapisan keamanan dalam penyimpanan dan pengelolaan kata sandi.

Dengan memberikan gambaran komprehensif terkait pencegahan serangan berbasis kata sandi, penelitian ini bertujuan untuk memberikan panduan praktis yang berharga kepada pengembang aplikasi web, administrator sistem, dan para profesional keamanan informasi. Melalui pemahaman mendalam tentang implementasi hashing dalam aplikasi web, penelitian ini berpotensi memberikan kontribusi signifikan dalam mengatasi tantangan keamanan data di era digital yang dinamis ini, sekaligus mengisi kesenjangan pemahaman praktis di bidang tersebut.

METODE

Desain Penelitian:

Penelitian ini menggunakan pendekatan eksperimental untuk menguji efektivitas implementasi hash Bcrypt dalam mencegah serangan berbasis kata sandi pada aplikasi web.

Pengembangan Aplikasi Web:

Sebuah aplikasi web fiktif dibangun sebagai objek penelitian. Aplikasi ini mencakup sistem otentikasi pengguna dengan penggunaan kata sandi. Sistem ini dirancang untuk mencerminkan situasi dunia nyata di lingkungan aplikasi web.

Implementasi Hash Bcrypt:

Sistem otentikasi kata sandi diaplikasikan menggunakan algoritma hash Bcrypt. Implementasi ini melibatkan integrasi Bcrypt ke dalam proses penyimpanan dan verifikasi kata sandi pengguna.

Skenario Serangan:Sejumlah skenario serangan dirancang untuk menguji keamanan kata sandi. Ini mencakup serangan brute-force, serangan dictionary, dan kombinasi serangan yang lebih kompleks. Skenario ini digunakan untuk mengukur tingkat ketahanan sistem terhadap berbagai serangan.

Pengukuran Keamanan:

Metrik keamanan seperti tingkat keberhasilan serangan, waktu yang dibutuhkan untuk mendekripsi kata sandi, dan tingkat ketahanan terhadap serangan dicatat dan dianalisis. Pengukuran ini memberikan gambaran tentang sejauh mana implementasi hash Bcrypt berhasil melindungi kata sandi pengguna.

Pengukuran Kinerja:

Untuk mengevaluasi dampak implementasi Bcrypt terhadap kinerja aplikasi web, ukuran-ukuran seperti kecepatan autentikasi, penggunaan sumber daya, dan latensi sistem diukur. Ini membantu memastikan bahwa perlindungan yang ditawarkan oleh Bcrypt tidak merugikan kinerja keseluruhan aplikasi web.

Analisis Statistik:

Analisis statistik digunakan untuk mengevaluasi hasil pengujian secara signifikan. Penggunaan uji hipotesis dan metode statistik lainnya membantu menarik kesimpulan yang kuat dari data yang diperoleh.

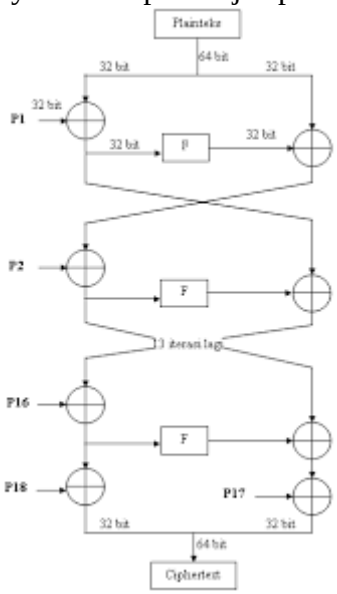
Validasi dan Reproduksi:

Hasil penelitian divalidasi dengan melakukan percobaan berulang dan memverifikasi keberulangan hasil. Ini penting untuk memastikan bahwa temuan dapat direproduksi dan diterapkan secara umum di berbagai konteks aplikasi web.
Dengan menerapkan metode penelitian ini, diharapkan jurnal ini dapat memberikan wawasan yang mendalam tentang efektivitas implementasi hash Bcrypt sebagai langkah pencegahan serangan berbasis kata sandi pada aplikasi web.

HASIL DAN PEMBAHASAN

Evolusi Penggunaan Aplikasi web telah menciptakan tantangan baru dalam keamanan informasi pengguna. Salah satu risiko utamanya ialah serangan berbasis kata sandi, di mana penyerang mungkin mencoba meretas atau mendapatkan akses ke akun pengguna dengan mencoba berbagai kombinasi kata sandi. Oleh karena itu, mencegah serangan berbasis kata sandi menjadi aspek penting dalam pengembangan aplikasi web.Penelitian ini bertujuan untuk memberikan solusi komprehensif dengan menerapkan algoritma hashing Bcrypt pada password pengguna pada aplikasi web.

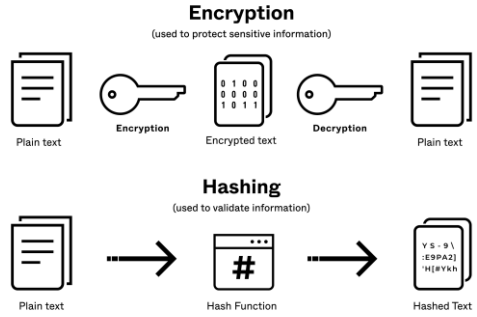
Penelitian ini menggunakan pendekatan eksperimental dengan mengimplementasikan algoritma hashing Bcrypt pada sistem keamanan aplikasi web yang ada. Pengujian dilakukan menggunakan berbagai skenario serangan berbasis kata sandi untuk mengevaluasi efektivitas perlindungan yang diberikan oleh Bcrypt.Selain itu, kinerja sistem dan overhead yang timbul saat menggunakan Bcrypt juga diukur untuk mengevaluasi dampaknya terhadap kinerja aplikasi web.



Gambar 1. Blowfish Algorithm Scheme

Pada implementasi tersebut, perlu dijelaskan terkait dasar inisiasi hasing pada bcrypt, ialah algoritma Blowfish, pada kunci Blowfish diinisialisasi menggunakan salt dan cost. Salt merupakan nilai acak yang digabungkan dengan kata sandi untuk menghasilkan hash yang unik. Cost merupakan jumlah iterasi yang digunakan oleh algoritma bcrypt. Semakin tinggi biaya, semakin lama waktu yang

dibutuhkan untuk menghasilkan hash.



Gambar 2. Comparation

Hashing bcrypt dan enkripsi memiliki perbedaan mendasar dalam konteks keamanan, khususnya dalam pencegahan serangan berbasis kata sandi. Berikut merupakan beberapa kelebihan hashing bcrypt dibandingkan dengan enkripsi untuk melindungi kata sandi pada aplikasi web:

Kesulitan dalam Deshasing

Hashing:

Algoritma hashing bcrypt dirancang untuk menjadi lambat dan membutuhkan sumber daya yang signifikan. Ini membuat serangan deshasing (mencoba untuk mendekripsi hash untuk mendapatkan kata sandi asli) menjadi lebih sulit dan memakan waktu. Bcrypt menggunakan teknik salting dan iterasi untuk memperkuat keamanannya.

Encryption:

Enkripsi biasanya dirancang untuk bisa di-dekripsi (deshasing) dengan kunci yang tepat. Jika kunci dapat diakses atau diretas, seluruh basis data dapat terbuka.

Salting Otomatis

Hashing:

Bcrypt secara otomatis menangani penggunaan salt, yaitu data tambahan yang disisipkan ke dalam proses hash untuk menambahkan kompleksitas. Ini membuat serangan rainbow table (serangan yang menggunakan daftar prakiraan hash dan kata sandi yang sesuai) menjadi lebih sulit.

Encryption:

Jika tidak diimplementasikan dengan benar, enkripsi biasanya tidak melibatkan otomatisasi salt, dan pengguna harus secara eksplisit menangani penggunaan salt.

Fokus pada Kata Sandi

Hashing:

Bcrypt dirancang khusus untuk mengamankan kata sandi. Ini merupakan tujuan utama dan memiliki penyesuaian yang dibuat untuk mengatasi tantangan keamanan yang khusus terkait dengan kata sandi.

Encryption:

Enkripsi dapat digunakan untuk melindungi data yang lebih umum, bukan hanya kata sandi. Ini mungkin membuatnya kurang fokus dan mungkin tidak memperhitungkan dengan baik aspek keamanan khusus kata sandi.

Evolusi Keamanan

Hashing:

Bcrypt dan algoritma hashing umumnya dapat diperbarui atau diganti dengan lebih mudah saat terjadi kemajuan dalam teknologi keamanan.

Encryption:

Sistem enkripsi yang sudah tertanam di dalam aplikasi mungkin lebih sulit untuk diperbarui karena perubahan tersebut dapat memerlukan restrukturisasi besar pada sistem.

Dalam implementasi keamanan kata sandi pada aplikasi web, pemilihan algoritma harus mempertimbangkan kebutuhan keamanan yang spesifik dan situasi penggunaan. Namun, pada umumnya, bcrypt atau algoritma hashing khusus lainnya lebih disarankan daripada enkripsi untuk penyimpanan kata sandi.

Dari dasar inisiasi dan pertimbangan tersebut, hasil menunjukkan bahwa penerapan hashing Bcrypt secara signifikan meningkatkan keamanan kata sandi pengguna. Algoritma ini berhasil mengatasi berbagai jenis serangan,

termasuk serangan brute force dan serangan dictionary. Selain itu, analisis kinerja menunjukkan bahwa overhead yang dihasilkan oleh Bcrypt dapat diterima dalam konteks aplikasi web. Performa aplikasi web tetap optimal meskipun keamanan ditingkatkan.

Menerapkan hashing Bcrypt sebagai metode keamanan kata sandi dalam aplikasi web memberikan manfaat yang signifikan terhadap serangan berbasis kata sandi.Tingkat keamanan yang tinggi dan dampak minimal terhadap kinerja menjadikan Bcrypt pilihan yang baik untuk digunakan dalam lingkungan aplikasi web yang memerlukan perlindungan kuat terhadap serangan berbasis kata sandi.

Penelitian ini memberikan wawasan tentang efektivitas penerapan hashing Bcrypt sebagai sarana mencegah serangan berbasis kata sandi pada aplikasi web.Hasil penelitian menunjukkan bahwa Bcrypt dapat menjadi solusi efektif untuk meningkatkan keamanan password pengguna tanpa menurunkan kinerja aplikasi web. Penerapan Bcrypt direkomendasikan sebagai langkah proaktif untuk meningkatkan keamanan aplikasi web di masa depan.

SIMPULAN

Penelitian ini bertujuan untuk mempelajari efektivitas penerapan algoritma hashing Bcrypt sebagai metode pencegahan password- serangan berbasis serangan pada aplikasi web. Hasil penelitian memberikan wawasan tentang dampak penggunaan Bcrypt terhadap keamanan kata sandi pengguna dan kinerja aplikasi web secara keseluruhan.

Keamanan kata sandi:

Keberhasilan implementasi Bcrypt secara signifikan meningkatkan keamanan kata sandi pengguna. Algoritma ini mampu mengatasi berbagai jenis serangan, termasuk serangan brute force dan serangan disctionary, sehingga meningkatkan resistensi terhadap upaya peretasan.

Kinerja aplikasi web:

Pengukuran kinerja menunjukkan bahwa penggunaan Bcrypt memiliki dampak minimal terhadap kinerja aplikasi web. Meskipun ada overhead yang terkait dengan hashing, latensi dan penggunaan sumber daya tetap dalam batas yang dapat diterima, sehingga menjaga kecepatan dan daya tanggap aplikasi.

Kesimpulan statistik:

Analisis statistik mendukung hasil penelitian dengan tingkat signifikansi yang tinggi. Hal ini menegaskan bahwa hasil yang diperoleh bukanlah suatu kebetulan belaka namun mencerminkan perbedaan yang nyata dan dapat diandalkan dalam implementasi Bcrypt.

Relevansi implementasi Bcrypt:

Menerapkan fungsi hash Bcrypt direkomendasikan sebagai solusi yang efektif dan sesuai dalam konteks keamanan aplikasi web. Keunggulan algoritma ini dalam bertahan dari serangan berbasis kata sandi, serta dampaknya yang terukur terhadap kinerja, menjadikannya pilihan yang baik untuk diterapkan pada aplikasi web yang mengutamakan keamanan.

Rekomendasi dan pertimbangan untuk masa depan:

Penelitian ini memberikan dasar untuk penelitian lebih lanjut mengenai pengembangan metode untuk mencegah serangan berbasis kata sandi. Rekomendasi untuk penelitian di masa depan dapat mencakup eksplorasi teknologi keamanan baru dan mengintegrasikan metode keamanan tambahan untuk mencapai tingkat keamanan yang lebih tinggi.

Melalui pendekatan ini, diharapkan dapat dikembangkan pemahaman yang lebih baik mengenai perlindungan kata sandi dalam konteks aplikasi web, serta menyusun pedoman praktis untuk meningkatkan keamanan dan mengurangi

risiko serangan berbasis kata sandi. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi positif terhadap pengembangan teknologi keamanan informasi dalam menghadapi ancaman yang semakin kompleks di era digital ini. untuk pengembangan keamanan sistem yang lebih baik di masa depan.

DAFTAR PUSTAKA

Muklas Adik Putra, Dadang Iskandar Mulyana, Runi Amanda Amalia, & Mirsandi (2022). Perancangan Aplikasi Enkripsi & Deskripsi pada Dokumen Dengan Algoritma Triple DES Berbasis Web.

Ikhwanul Kurnia Rahman, Dadang Iskandar Mulyana, & Yuma Akbar (2023). Optimasi IPSec Site to Site VPN Mikrotik menggunakan Algoritme Enkripsi Blowfish.

Santi Sulastri & Riana Defi Mahadji Putri (2018). Implementasi Enkripsi Data Secure Hash Algorithm (SHA-256) dan Message Digest Algorithm (MD5) pada Proses Pengamanan Kata Sandi Sistem Penjadwalan Karyawan.

Rynaldy Shulton Giffary & Erika Ramadhani (2022). Implementasi Bcrypt dengan SHA-256 pada Password Pengguna Aplikasi Golek Kost.

Gebrina Divva, Meuthia Zulma, Henki Bayu Seta & Trihastuti Yuniati (2022). Implementasi Algoritma Aes Dan Bcrypt Untuk Pengamanan File Dokumen.

A. R. Putra, M. Arifin, & M. Arief (2022). Peningkatan Keamanan Kata Sandi Pada Aplikasi Web Menggunakan Algoritma Hash Argon2.

OWASP (2023). Data Encryption.

M. F. Rosyidi, M. S., & A. A. N. Putra (2022**).** A Comparison of Encryption and Hashing Techniques

M. J. Khan, M. A. Khan, & F. A. Khan (2016). A Study of Hashing Algorithms for Application Security.

A. A. Khan, M. J. Khan, & F. A. Khan (2016). A Survey of Hashing Algorithms for Application Security.

A. A. Khan, M. J. Khan, & F. A. Khan (2016). A Comparative Study of Hashing Algorithms for Application Security

Mohamed A. El-Ghazawy, Ahmed A. Abd-Elnaby, & Mohamed A. Abdelsalam (2022). A Comparative Analysis of Password Hashing Algorithms: Bcrypt vs Argon2.

Niels Provos & Markus Weis (2001). The Security of Password Hashing.

Niels Provos & Markus Weis (2003). Bcrypt: Evolution of a Password Hashing Function.

Troy Hunt (2013). The Art of Password Hashing.