

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam era digital, sistem login menjadi gerbang utama bagi pengguna untuk mengakses layanan online seperti e-commerce, media sosial, dan perbankan. Masalah utama yang dihadapi untuk mengakses platform layanan online adalah tingginya angka peretasan pada akun pengguna. Kasus kebocoran data yang dialami platform Tokopedia pada April 2020 menjadi salah satu contoh nyata resiko keamanan sistem digital. Hacker dengan nama samaran “Why So Dank” berhasil mencuri data pribadi hingga 91 juta pengguna dan 7 juta merchant, yang menyangkut informasi sensitif seperti email, password dan nama pengguna. [1].

Pada Juli 2024, kasus kebocoran data Pusat Data Nasional Sementara (PDNS) 2 menjadi perhatian publik setelah lebih dari 8 juta data penduduk dilaporkan terakses secara ilegal oleh pihak tak bertanggung jawab. Serangan ini diduga dilakukan melalui ransomware LockBit 3.0, yang mengeksploitasi sistem autentikasi yang lemah dan tidak dilengkapi Multi-Factor Authentication (MFA). Terlepas dari kenyataan bahwa informasi teknis tentang penyimpanan kata sandi tidak tersedia untuk publik, insiden ini menunjukkan bahwa kegagalan sistem login, termasuk penyimpanan kata sandi yang tidak aman, terus menjadi faktor utama dalam kebocoran data nasional. Menurut analisis Selektamanajemen (Juli 2024), dua faktor utama penyebab kebocoran PDNS 2 di Surabaya adalah penggunaan sistem autentikasi yang tidak efektif dan kurangnya backup dan pemulihan sistem[2].

Untuk mengatasi permasalahan tersebut, diperlukan suatu mekanisme keamanan yang lebih kuat untuk melindungi akun pengguna. Salah satu solusi yang dapat diimplementasikan adalah Multi-Factor Authentication (MFA). MFA adalah metode autentikasi elektronik yang mengharuskan pengguna memasukkan dua atau lebih faktor keamanan untuk mengakses aplikasi atau situs web[3]. Dengan demikian, meskipun kata sandi pengguna berhasil dicuri, pihak yang tidak berwenang akan kesulitan untuk mengakses akun tersebut karena memerlukan faktor verifikasi tambahan.

Banyak sistem masih menggunakan metode penyimpanan password yang lemah, seperti plaintext atau hashing yang sudah usang (MD5, SHA-1), sehingga rentan terhadap serangan. Salah satu metode yang dapat meningkatkan keamanan sistem login adalah penggunaan algoritma hashing modern seperti Argon2, yang dirancang untuk menghambat serangan brute-force dengan meningkatkan waktu komputasi. Selain itu, penerapan Multi-Factor Authentication (MFA) dapat memberikan lapisan keamanan tambahan dengan memastikan bahwa hanya pemilik akun yang dapat mengakses layanan[4].

Beberapa penelitian terkait telah dilakukan. Penelitian sebelumnya mengembangkan sistem OTP (*One Time Password*) sebagai proses otentikasi ganda melalui SMS (*Short Message Service*). Namun, sistem ini memiliki kelemahan karena jika nomor handphone pengguna telah disalahgunakan, proses OTP menjadi tidak efektif. Selain itu, penelitian sebelumnya berhasil membangun mekanisme 2FA menggunakan OTP yang dikirimkan melalui SMS, namun ia juga menjelaskan bahwa SMS memerlukan biaya berupa pulsa untuk mengirimkan kode OTP kepada

pengguna. Oleh karena itu, diperlukan solusi OTP yang dapat memanfaatkan layanan gratis seperti WhatsApp, Telegram, atau e-mail[5].

Fenomena ini menunjukkan bahwa sistem otentikasi yang hanya mengandalkan username dan password dengan metode hashing konvensional tidak lagi memadai. Metode hashing yang usang rentan diretas, sementara ketiadaan otentikasi ganda membuat akun mudah dibobol jika password pengguna bocor. Melihat potensi risiko yang ada, aplikasi Eventhings sebagai platform yang mengelola data pengguna memiliki tanggung jawab untuk membangun fondasi keamanan yang kokoh sejak awal. Meskipun aplikasi Eventhings belum pernah mengalami insiden kebocoran data, langkah-langkah pencegahan sangat diperlukan untuk memastikan kepercayaan dan perlindungan data pengguna jangka panjang.

Penelitian ini bertujuan untuk memperkuat sistem otentikasi pada aplikasi Eventhings dengan mengimplementasikan dua teknologi keamanan. Kedua teknologi tersebut adalah Algoritma Hashing Argon2, yang dikenal memiliki karakteristik memory-hard dan tahan terhadap serangan brute-force; serta Multi-Factor Authentication (MFA) sebagai lapisan verifikasi kedua untuk memastikan hanya pengguna yang sah yang bisa mengakses akun, meskipun password mereka tercuri. Dengan adanya implementasi ini, diharapkan sistem login dapat menjadi lebih tahan terhadap serangan siber dan memberikan perlindungan yang lebih baik bagi data pengguna.

Berdasarkan penjelasan latar belakang yang telah disampaikan sebelumnya, penulis berminat untuk melakukan penelitian dengan judul “Implementasi Algoritma Hashing & Multi-Factor Authentication Untuk Meningkatkan Keamanan Sistem Login Pengguna Aplikasi Eventhings”.

1.2 Identifikasi Masalah

Berdasarkan latar belakang di atas, terdapat beberapa masalah yang dapat diidentifikasi, antara lain:

1. Sistem otentikasi pada aplikasi Eventhings rentan terhadap serangan siber seperti *brute-force*, yaitu serangan yang dilakukan dengan mencoba semua kemungkinan kombinasi password secara berulang-ulang hingga menemukan yang benar berpotensi membahayakan data pengguna di masa mendatang.
2. Kebutuhan akan metode *hashing password* yang lebih kuat dan modern (Argon2) untuk menggantikan metode lama yang lebih rentan terhadap serangan siber.
3. Belum adanya lapisan keamanan tambahan seperti Multi-Factor Authentication (MFA) yang dapat melindungi akun pengguna, meskipun *password* utama telah terkompromi.
4. Diperlukan sebuah perancangan dan implementasi sistem keamanan yang tidak hanya robust, tetapi juga memberikan pengalaman pengguna yang baik dan terintegrasi dengan alur *login* yang sudah ada.

1.3 Rumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah yang diangkat dalam penelitian ini dirumuskan secara objektif adalah sebagai berikut.

1. Bagaimana merancang dan mengimplementasikan algoritma hashing modern Argon2 untuk meningkatkan keamanan penyimpanan password pada sistem login pengguna, serta bagaimana pengaruhnya dapat diukur secara teknis?

2. Seberapa efektif algoritma Argon2id dalam mencegah serangan brute-force dan sejauh mana Multi-Factor Authentication (MFA) dapat meningkatkan tingkat keberhasilan autentikasi, berdasarkan hasil pengujian sistem?
3. Bagaimana dampak implementasi metode keamanan berbasis Argon2id dan MFA terhadap performa sistem login (misalnya waktu respons atau waktu hashing), dan bagaimana hal ini diukur melalui eksperimen?

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka yang menjadi tujuan penelitian ini adalah sebagai berikut.

1. Menganalisis dan mengimplementasikan metode hashing password yang lebih aman (Argon2) untuk melindungi data pengguna.
2. Mengintegrasikan Hashing dan Multi-Factor Authentication (MFA) sebagai lapisan keamanan tambahan untuk mencegah akses tidak sah.
3. Menguji dan membandingkan performa sistem login sebelum dan sesudah penerapan metode keamanan baru.
4. Melakukan simulasi serangan untuk menguji ketahanan sistem terhadap brute-force attack dan credential stuffing.

1.5 Manfaat Penelitian

Terdapat beberapa manfaat yang diharapkan dari penelitian ini yang dapat berguna bagi pihak-pihak terkait, di antaranya:

1. Bagi Pengguna, Menyediakan sistem login yang lebih aman dan tahan terhadap serangan siber seperti **Brute Force**, yaitu serangan yang dilakukan dengan

mencoba semua kemungkinan kombinasi password secara berulang-ulang hingga menemukan yang benar, dan **Credential Stuffing**, yaitu serangan yang menggunakan kombinasi username dan password hasil kebocoran data dari situs lain untuk mencoba login ke sistem secara otomatis. Sistem ini mengatasi serangan tersebut melalui penggunaan algoritma hashing yang kuat (Argon2) untuk melindungi password, serta penerapan Multi-Factor Authentication (MFA) yang mempersulit akses meskipun kredensial berhasil ditebak atau bocor.

2. Bagi Pengembang, Memberikan wawasan mengenai metode terbaik dalam implementasi keamanan login.
3. Bagi Akademisi, Menambah referensi dalam studi keamanan siber, khususnya dalam implementasi Hashing dan MFA.

1.6 Batasan Masalah

Untuk menjaga fokus dan ruang lingkup penelitian, maka penelitian ini dibatasi pada:

1. Sistem login yang dikembangkan hanya mencakup proses autentikasi pengguna menggunakan username dan password. Sistem dikembangkan menggunakan bahasa pemrograman Kotlin dengan framework Jetpack Compose untuk platform Android.
2. Algoritma Hashing yang diuji menggunakan Argon2.
3. MFA yang diterapkan hanya berupa OTP (*One-Time Password*) melalui email pada saat registrasi.

4. Penelitian ini tidak mencakup aspek keamanan jaringan seperti SSL/TLS atau firewall, melainkan hanya fokus pada proses autentikasi pengguna melalui simulasi localhost/server pengujian.

1.7 Sistematika Tugas Akhir

Sistematika penulisan ini disusun secara runtut untuk memudahkan pemahaman alur penelitian. Bagian ini menjelaskan rangkaian bab beserta cakupan materinya. Berikut adalah sistematika penulisan tiap bab beserta fokus pembahasannya.

BAB I PENDAHULUAN

Bab I yaitu terdiri dari latar belakang masalah dari penelitian ini, rumusan masalah, tujuan penelitian, dan manfaat, dan sistematika pembahasan.

BAB II TINJAUAN PUSTAKA

Bab II yaitu terdiri teori-teori yang berkaitan dengan penelitian ini. Bab ini juga akan menjelaskan penelitian sebelumnya yang terkait, bentuk kerangka pemikiran, dan hipotesis penelitian.

BAB III METODOLOGI PENELITIAN

Bab III yaitu terdiri dari pendekatan dan jenis penelitian, kerangka penelitian dan sampel, teknik pengumpulan data, dan teknik analisis data.

BAB IV HASIL DAN PEMBAHASAN

Bab IV yaitu berisi hasil dan pembahasannya, terdiri dari penyajian data, analisis data dan pembahasan.

BAB V PENUTUP

Bab V yaitu merangkum hasil penelitian, kesimpulan dan saran.

Merangkum jawaban atas rumusan masalah berdasarkan hasil penelitian dan memberikan rekomendasi berdasarkan temuan penelitian.

