e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.9 No.2 (December 2025)
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

KEAMANAN SISTEM LOGIN MENGGUNAKAN MULTIFACTOR AUTHENTICATION DAN ALGORITMA HASHING

Aida Fitriyani [1*], Hendarman Lubis[2], Yaddarabullah[3] , Rafika Sari[4]

Program Studi Informatika[1], Program Studi Informatika[2],
Program Studi Teknik Informatika[3],
Program Studi Desain Komunikasi Visual[4]
Fakultas Ilmu Komputer[1], Fakultas Ilmu Komputer[2],
Fakultas Teknik[3] , Fakultas Ilmu Komputer[4]
Universitas Bhayangkara Jakarta Raya[1],
Universitas Bhayangkara Jakarta Raya[2],
Universitas Trilogi[3] , Universitas Bhayangkara Jakarta Raya[4]

*Correspondent Author: aida.fitriyani@dsn.ubharajaya.ac.id

Author Email: aida.fitriyani@dsn.ubharajaya.ac.id[1],
hendarman.lubis@dsn.ubharajaya.ac.id[2],
yaddarabullah@trilogi.ac.id[3], rafika.sari@dsn.ubharajaya.ac.id.[4]

Received: October 18,2025**. Revised:** November 20,2025**. Accepted:** December 03, 2025**. Issue Period:** Vol.9 No.2 (2025), Pp. 263-276

Abstrak: Keamanan sistem login merupakan aspek krusial dalam pengembangan aplikasi digital untuk melindungi data pribadi pengguna. Penelitian ini bertujuan untuk mengimplementasikan algoritma hashing modern, yaitu Argon2, serta menambahkan lapisan keamanan melalui metode Multi-Factor Authentication (MFA) menggunakan kode OTP (One-Time Password). Algoritma Argon2 dipilih karena karakteristiknya yang memory-hard, dapat dikonfigurasi, serta lebih tahan terhadap serangan brute-force dan rainbow table. Metode pengembangan sistem yang digunakan adalah Waterfall, di mana sistem dikembangkan menggunakan bahasa pemrograman Kotlin dengan arsitektur Jetpack Compose, serta basis data Firebase Authentication dan Firestore. OTP dikirimkan kepada pengguna setelah proses registrasi berhasil sebagai verifikasi tambahan. Hasil implementasi menunjukkan bahwa parameter time cost pada Argon2id secara signifikan memengaruhi waktu eksekusi hashing, dimana nilai yang lebih tinggi meningkatkan keamanan namun tetap dalam batas toleransi performa. Kombinasi Argon2 dan MFA ini berhasil memberikan sistem login yang lebih aman dan tahan terhadap serangan siber dibandingkan metode otentikasi tradisional. Hasil pengujian menunjukkan bahwa parameter Time Cost pada Argon2id sangat memengaruhi waktu hashing. Dengan konfigurasi: Time Cost = 1 → 2,028 ms, Time Cost = 2 → 48,623 ms dan Time Cost = 3 → 71,219 ms. Semakin tinggi nilai parameter, waktu eksekusi meningkat, namun

DOI: 10.52362/jisicom.v9i2.2137

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.9 No.2 (December 2025)
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

juga memperkuat ketahanan terhadap serangan brute-force. Kombinasi algoritma Argon2 dan metode MFA menghasilkan sistem login yang lebih aman dan andal dibandingkan otentikasi tradisional, serta tetap responsif dalam performa aplikasi.

Kata kunci: Argon2, Hashing, MFA, OTP, Sistem Login, Keamanan

Abstract: *Login system security is a crucial aspect in digital application development to protect user personal data. This research aims to implement a modern hashing algorithm, Argon2, and add a security layer through Multi-Factor Authentication (MFA) using One-Time Password (OTP) codes. The Argon2 algorithm was chosen because it is memory-hard, configurable, and more resistant to brute-force attacks and rainbow table attacks. The system development method used is the Waterfall method, where the system is developed using the Kotlin programming language with the Jetpack Compose architecture, and the Firebase Authentication and Firestore databases. An OTP is sent to the user after successful registration as additional verification. Implementation results show that the time cost parameter in Argon2id significantly affects hashing execution time, with higher values improving security while remaining within performance tolerances. The combination of Argon2 and MFA successfully provides a more secure login system and is more resilient to cyberattacks than traditional authentication methods. Test results indicate that the Time Cost parameter in Argon2id significantly impacts hashing time. With the following configurations: Time Cost = 1 → 2.028 ms, Time Cost = 2 → 48.623 ms, and Time Cost = 3 → 71.219 ms. Higher parameter values increase execution time but also increase resistance to brute-force attacks. The combination of the Argon2 algorithm and MFA methods results in a more secure and reliable login system than traditional authentication, while remaining responsive in application performance.*

Keywords: *Argon2, Hashing, MFA, OTP, Login System, Security.*

I. PENDAHULUAN

1.1 Latar Belakang

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 Selekta Manajemen (Juli 2024), dua faktor utama penyebab kebocoran PDNS 2 di Surabaya adalah penggunaan sistem autentikasi yang tidak efektif dan kurangnya backup dan pemulihan sistem.

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. Dengan demikian, meskipun kata sandi pengguna berhasil dicuri, pihak yang tidak berwenang akan kesulitan untuk mengakses akun tersebut karena memerlukan faktor verifikasi tambahan.

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

DOI: 10.52362/jisicom.v9i2.2137

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.9 No.2 (December 2025)
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

mengirimkan kode OTP kepada pengguna. Oleh karena itu, diperlukan solusi OTP yang dapat memanfaatkan layanan gratis seperti WhatsApp, Telegram, atau e-mail.

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 Authetication Untuk Meningkatkan Keamanan Sistem Login Pengguna Aplikasi Eventhings".

1.2 Indentifikasi 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.

DOI: 10.52362/jisicom.v9i2.2137

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.9 No.2 (December 2025)
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

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 pembahasanya, 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.

DOI: 10.52362/jisicom.v9i2.2137

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.9 No.2 (December 2025)
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

II. METODE DAN MATERI

2.1 Keamanan Sistem Login

Sistem login (login, juga biasa disebut log in, log on, signon, sign on, signin, sign in) adalah proses untuk mengakses komputer dengan memasukkan identitas dari akun pengguna dan kata sandi untuk mendapatkan hak akses menggunakan sumber daya komputer tujuan. pada saat melakukan login untuk masuk kedalam sistem, user akan diminta untuk memasukkan identitas user seperti userid dan password sebagai antisipasi dalam hal pengamanan sistem. Password dapat diubah sesuai dengan kebutuhan sedangkan userid tidak pernah diubah karena berupa identitas unik yang merujuk ke user tertentu. Jika kedua pengamanan tersebut berhasil atau memenuhi maka user memiliki hak untuk mengakses sistem.

2.2 Algoritma Hashing

Algoritma hash merupakan salah satu komponen fundamental dalam arsitektur keamanan siber. Fungsi utamanya adalah mengkonversi data input dengan panjang bervariasi menjadi output dengan panjang tetap, yang dikenal sebagai nilai hash. Karakteristik unik dari algoritma hash mencakup beberapa prinsip dasar: determinisme, kecepatan komputasi, resistensi terhadap kolisi, dan sifat satu arah yang tidak memungkinkan rekonstruksi data asli dari nilai hash.

2.3 Multi-Factor Authentication (MFA)

Multi-Factor Authentication adalah autentikasi yang lebih aman dibandingkan dengan autentikasi satu faktor yaitu dengan nama pengguna atau email pengguna dan kata sandi. Metode Multi-Factor Authentication ini digunakan untuk mengecek identitas pengguna sebelum pengguna mengakses data sensitive dan rahasia. Multi-Factor Authentication akan menambahkan lapisan keamanan yang memungkinkan administrator sistem untuk menghubungkan dua atau lebih jenis autentikasi untuk memberikan cara yang lebih aman pada kredensial pengguna.

2.4 Ancaman Keamanan

Kemajuan teknologi membawa perubahan zaman yang membawa kemajuan manusia semakin modern. Dalam banyak hal, kemajuan teknologi telah memengaruhi kejahatan dunia maya. Pertama, penjahat dunia maya lebih mudah mendapatkan akses ke jaringan global karena kecepatan internet yang meningkat. Selain itu, aplikasi serangan yang lebih canggih telah dibuat berkat pengembangan perangkat lunak yang berkelanjutan.

2.5 Alat Pengembangan Sistem

2.5.1 UML (Unified Modeling Language)

UML (Unified Modeling Language) adalah bahasa standar yang berfungsi sebagai alat untuk mengidentifikasi, merancang, dan mendokumentasikan sistem informasi. UML adalah sebuah notasi yang digunakan untuk menggambarkan model suatu sistem, yang juga dikenal sebagai bahasa pemodelan perangkat lunak yang berorientasi objek.

2.5.2 Use Case Diagram

Use Case Diagram adalah rencana awal untuk desain sistem yang dapat digunakan oleh pengguna untuk mendiskusikan apa yang perlu ditambahkan dan dikurangi. Sedangkan pendapat lain tentang Use Case Diagram Menurut Satzinger, Jackson & Burd, Use Case Diagram adalah diagram yang menampilkan berbagai peran pengguna dan bagaimana peran ini berfungsi dalam sebuah sistem.

2.5.3 Sequence Diagram

Sequence diagram menggambarkan perilaku objek dalam sebuah use case dengan menunjukkan siklus hidup objek serta pesan yang dikirim dan diterima antar objek. Untuk membuat diagram sequence diagram, perlu diketahui objek-objek yang terlibat dalam use case tersebut. Diagram ini juga berguna untuk memvisualisasikan skenario yang terjadi dalam use case.

DOI: 10.52362/jisicom.v9i2.2137

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.9 No.2 (December 2025)
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

2.5.4 Class Diagram

Class diagram merepresentasikan struktur sistem yang fokus pada pendefinisian kelas-kelas yang akan digunakan dalam pembangunan sistem. Setiap kelas dalam diagram ini memiliki atribut, yaitu variabel-variabel yang menggambarkan karakteristik kelas tersebut, serta metode atau operasi, yaitu fungsi-fungsi yang dapat dijalankan oleh kelas tersebut.

2.5.5 Activity Diagram

Activity diagram menggambarkan alur kerja atau aktivitas dalam sebuah sistem, proses bisnis, atau menu perangkat lunak. Diagram ini fokus pada aktivitas yang dilakukan oleh sistem, bukan oleh aktor.

2.5.6 Android dan Android Studio

Android, yang pertama kali dikembangkan oleh Google dan dibeli oleh perusahan-perusahaan yang tergabung dalam Open Handset Alliance, memungkinkan penggunaan lebih lanjut untuk perangkat mobile dengan versi kustomisasi Bahasa Pemrograman Java. Android Studio adalah Integrated Development Environment (IDE) resmi untuk pengembangan aplikasi Android. Berbasis editor kode dan alat developer yang andal dari IntelliJ IDEA.

2.6 Metode Pengembangan Sistem

2.6.1 Pengertian Waterfall

Model Air Terjun digunakan secara sistematis dalam pembuatan perangkat lunak, sedangkan Model Air Terjun adalah model pengembangan berurutan, menurut Pressman.Analisis, desain, pengkodean, pengujian, dan pemeliharaan adalah semua bagian dari proses pembuatan.

2.6.2 Tahapan Waterfall

Adapun tahapan-tahapan dalam Waterfall Model yang diterapkan pada penelitian ini adalah sebagai berikut:

- Analisis Kebutuhan (Requirement Analysis).
- Perancangan Sistem.
- Pengujian.
- Pemeliharaan.

2.7 Black Box Testing

Blackbox testing merupakan metode pengujian perangkat lunak yang berfokus pada validasi fungsi sistem tanpa melihat struktur internal atau kode programnya. Tujuan pengujian ini adalah untuk memastikan bahwa perangkat lunak berjalan sesuai dengan spesifikasi dan menghasilkan output yang benar berdasarkan input yang diberikan.

III. PEMBAHASAN DAN HASIL

3.1 Kerangka Penelitian

DOI: 10.52362/jisicom.v9i2.2137

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.9 No.2 (December 2025)
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

Gambar 1 Kerangka Penelitian

3.2 Tipe Penelitian

Tipe penelitian yang digunakan dalam tugas akhir ini adalah pendekatan pengembangan (Research and Development). Penelitian ini bertujuan untuk mengembangkan sistem login dengan peningkatan keamanan, yaitu dengan implementasi algoritma hashing modern Argon2 untuk proses penyimpanan password, serta pengembangan fitur Multi-Factor Authentication (MFA) berbasis kode OTP. Sistem dikembangkan menggunakan bahasa pemrograman Kotlin dengan framework Jetpack Compose untuk platform Android.

3.3 Pendekatan Penelitian

Pendekatan yang digunakan dalam penelitian ini adalah pendekatan kuantitatif, karena melibatkan pengukuran kinerja hashing, waktu eksekusi, serta tingkat keberhasilan serangan terhadap sistem login.

3.4 Objek Penelitian

Objek penelitian dalam tugas akhir ini adalah aplikasi berbasis Android bernama Eventhings. Eventhings adalah aplikasi e-commerce yang menyediakan layanan penyediaan berbagai kebutuhan acara (event) seperti dekorasi, vendor makanan, hiburan, dan perlengkapan event lainnya. Fokus penelitian ini adalah mengembangkan dan menguji sistem login pengguna dalam aplikasi Eventhings, yang mengintegrasikan mekanisme keamanan password menggunakan Argon2 hashing dan verifikasi identitas melalui OTP (One-Time Password) untuk meningkatkan keamanan login.

3.5 Metode Pengumpulan Data

Metode pengumpulan data dalam penelitian ini dilakukan melalui dua pendekatan utama, yaitu studi literatur dan eksperimen sistem, yang dirancang untuk mendukung analisis dan validasi sistem login yang dibangun.

3.6 Metode Analisis

Analisis kebutuhan penelitian merupakan tahap dimana proses persiapan kebutuhan pelaksanaan penelitian agar dapat berjalan dengan baik, perlu dilakukan analisis kebutuhan penelitian sebelum melakukan analisis data yang mencakup:

- Activity Diagram.
- Kebutuhan Penelitian.
- Analisis Pengujian (Blackbox Testing).

3.7 Perancangan Antarmuka

Perancangan antarmuka (interface) merupakan tampilan dari suatu program aplikasi yang berperan sebagai media komunikasi yang digunakan sebagai sarana dialog antara program dengan user. Sistem yang akan dibangun diharapkan menyediakan interface yang sesuia dengan kebutuhan dan karakteristik user.

3.8 Perhitungan Algoritma Argon2

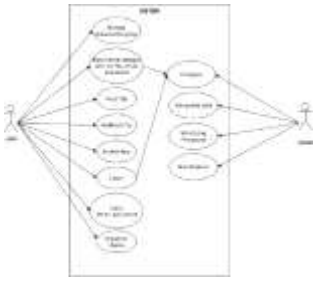
DOI: 10.52362/jisicom.v9i2.2137

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.9 No.2 (December 2025)
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 bagian ini dijelaskan bagaimana algoritma Argon2 bekerja secara matematis dan teknis untuk menghasilkan hash dari password yang dimasukkan pengguna. Dalam implementasi sistem login ini, digunakan algoritma Argon2id, yang merupakan varian gabungan dari Argon2i dan Argon2d, dengan keunggulan tahan terhadap serangan side-channel dan GPU cracking.

3.9 Perancangan Sistem

3.9.1 Use Case Diagram



Gambar 2 Use Case Diagram

Penjelasan:

1. Aktor: User

- Menuju Halaman Register, User yang belum memiliki akun dapat mengakses halaman untuk melakukan registrasi.
- Input name, tanggal lahir, no HP, email, password. User mengisi data pribadi sebagai syarat pembuatan akun baru. Data ini akan diproses oleh sistem dan disimpan didalam database.
- Input OTP, Setelah registrasi, user diminta memasukkan kode OTP yang dikirimkan melalui email sebagai bentuk verifikasi ganda (MFA).
- Verifikasi OTP, Sistem akan mencocokkan kode OTP yang dimasukkan dengan yang dikirim. Jika valid, proses registrasi berhasil.
- Login, User yang sudah terdaftar dapat masuk ke sistem menggunakan email dan password. Akan tersimpan didatabase saat login.
- Input email, password, User mengisikan data login untuk masuk ke dalam aplikasi.
- Access App, Setelah login berhasil, user diberi akses untuk menggunakan fitur-fitur aplikasi.
- Halaman Utama, Merupakan tampilan utama aplikasi yang diakses user setelah berhasil login.

2. Aktor: Admin

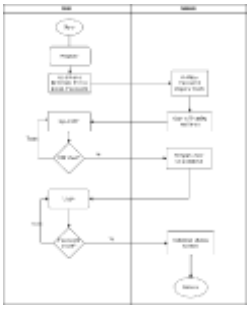
- Masuk ke firebase untuk mengelola akun pengguna.
- Mengelola Data, Admin memiliki otoritas untuk mengelola data dalam sistem, seperti memperbarui, menghapus, atau memeriksa informasi pengguna.
- Memonitoring pengguna untuk melihat kapan akun dibuat kapan terakhir aktif pada aplikasi.
- Maintenance ketika terjadi kesalahan.

3.9.2 Analisis Sistem Usulan

Sistem usulan ini dirancang sebagai solusi untuk meningkatkan keamanan proses autentikasi pengguna yang sebelumnya hanya mengandalkan email dan password. Dalam sistem yang diusulkan, ditambahkan proses hashing password menggunakan algoritma Argon2 serta verifikasi OTP (One-Time Password) berbasis email sebagai bentuk multi-factor authentication (MFA).

DOI: 10.52362/jisicom.v9i2.2137

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.9 No.2 (December 2025)
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

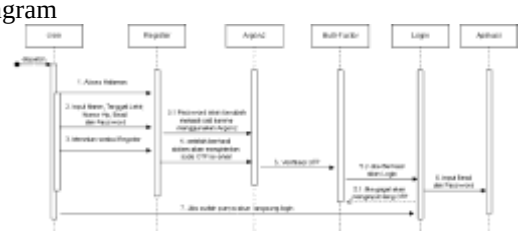


Gambar 3 Diagram Usulan

Keterangan:

1. Mulai.
2. User Membuka Aplikasi.
3. User pergi ke menu daftar.
4. Menginput kolom yang tersedia.
5. Sistem memverifikasi password (yang langsung di hash argon2).
6. Sistem mengirim Email.
7. User Input OTP.
8. Jika valid akan tersimpan di databse, jika tidak resend ulang kode atau masukan ulang kode.
9. Login (pastikan email dan password cocok pada saat register).
10. Menampilkan Halaman Utama.
11. Selesai.

3.9.3 Sequence Diagram



Gambar 4 Sequence Diagram

Penjelasan :

1. Alur Proses Registrasi Akun:

- Proses dimulai ketika Pengguna memilih opsi "Melakukan Registrasi" pada antarmuka Sistem.
- Sistem kemudian memanggil objek Akun untuk menjalankan operasi Create Akun.
- Objek Akun, yang bertanggung jawab atas manajemen data pengguna, akan mengirimkan pesan Save Data ke Database. Pada tahap ini, password yang diberikan oleh Pengguna akan terlebih dahulu di-hash menggunakan Algoritma Argon2 dengan parameter yang telah ditentukan (Time Cost, Memory Cost, Parallelism) untuk memastikan keamanan penyimpanan.
- setelah data berhasil disimpan ke Database, Database akan memberikan konfirmasi "Data Berhasil Disimpan" kembali ke objek Akun.
- Objek Akun lalu menginformasikan "Registrasi Berhasil" kepada Sistem.
- Terakhir, Sistem akan menampilkan "Tampilan Registrasi Berhasil" kepada Pengguna, menandakan bahwa pembuatan akun telah sukses.

2. Alur Proses Login Pengguna:

- Proses login dimulai ketika Pengguna memilih opsi "Melakukan Login" pada antarmuka Sistem dan memasukkan kredensialnya.

DOI: 10.52362/jisicom.v9i2.2137

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.9 No.2 (December 2025)
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

- Sistem mengirimkan pesan Authenticate kepada objek Akun untuk memverifikasi kredensial yang dimasukkan.
- Objek Akun kemudian memanggil Database untuk Ambil Data Akun pengguna berdasarkan username yang diberikan.
- Database merespons dengan mengembalikan "Data Akun" yang relevan (termasuk hashed password dan salt yang tersimpan) ke objek Akun.
- Objek Akun selanjutnya melakukan Verifikasi Data Akun. Pada tahap ini, password yang dimasukkan oleh Pengguna akan kembali di-hash menggunakan Algoritma Argon2 dan dibandingkan dengan hashed password yang tersimpan. Selain itu, jika fitur Multi-Factor Authentication (MFA) diaktifkan untuk akun pengguna tersebut, proses verifikasi tambahan (verifikasi kode OTP) juga akan dijalankan.
- Jika Verifikasi Data Akun Gagal: Objek Akun akan mengirimkan pesan "Gagal Login" ke Sistem, yang kemudian akan menampilkan "Tampilan Login Gagal" kepada Pengguna.
- Jika Verifikasi Data Akun Berhasil: Objek Akun akan mengirimkan pesan "Login Berhasil" ke Sistem, yang selanjutnya akan menampilkan "Tampilan Login Berhasil" (halaman utama) kepada Pengguna.

3.9.4 Class Diagram

Pada Class diagram ini dibuat untuk menggambarkan struktur internal sistem berdasarkan fungsi-fungsi utama dalam aplikasi Eventhings, khususnya pada modul login yang mengimplementasikan Argon2 dan Multi-Factor Authentication (MFA). Pembuatan setiap class didasarkan pada hasil analisis kebutuhan sistem (Bab 3) dan use case utama: register, login, hashing password, dan verifikasi OTP.

Gambar 5 Class Diagram

Penjelasan Kelas dan Hubungan:

1. User
- Atribut: Data-data yang dimiliki oleh setiap pengguna (nama pengguna, tanggal lahir, informasi kontak, email, password hashing, waktu register dan aktifitas terakhir).
- Metode: Aksi-aksi yang dapat dilakukan pengguna atau terkait dengan entitas pengguna (registrasi, login, buat pengguna baru dan update pengguna).

2. Aplikasi
- Merepresentasikan kelas utama atau entry point dari aplikasi Eventhings (Menu Utama).

3. Register
- Atribut: Pengguna memasukan data diri (nama, tanggal lahir, informasi kontak, email dan password).
- Metode: pada tahap ini pengguna membuat akun untuk bisa access aplikasi Eventhings.

4. Argon2
- Atribut: Berupa data-data yang akan dihasilkan oleh algoritma Argon2.
- Metode: Saat pengguna memasukan password setelah register, sistem akan membuat hashing dengan menggunakan Argon2.

5. Multi-Factor
- Atribut: Pengguna akan memasukan kode OTP untuk diverifikasi oleh sistem.

DOI: 10.52362/jisicom.v9i2.2137

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.9 No.2 (December 2025)
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: Sistem akan memverifikasi kode OTP.

3.9.5 UI Design (Jetpack Compose)

Berikut tampilan dari setiap halaman:

1. Halaman Register

Halaman ini digunakan untuk proses pendaftaran pengguna baru. Terdapat lima input field yang harus diisi pengguna, yaitu:

- Name
- Birth Date
- Phone Number
- Email
- Password.

Selain itu, terdapat tombol Continue di bagian bawah untuk melanjutkan ke proses verifikasi OTP. Desain ini dibuat minimalis dengan ilustrasi logo aplikasi Eventhings di bagian atas.

2. Halaman OTP

Halaman ini akan muncul setelah proses registrasi berhasil dilakukan. Sistem akan mengirimkan kode OTP ke alamat email yang telah didaftarkan. Pengguna diminta memasukkan 4 digit kode OTP sebagai validasi keamanan (Multi-Factor Authentication). Terdapat ilustrasi yang memperjelas fungsi halaman, serta tombol Continue untuk memverifikasi kode OTP.

3. Halaman Login

Halaman login digunakan bagi pengguna yang sudah memiliki akun. Field yang tersedia meliputi:

- Email
- Password

Selain tombol Login, terdapat juga tautan untuk Register dan Forgot Password. Halaman ini bersifat clean dan minimalis dengan tone warna ungu khas Eventhings.

4. Halaman Utama

Halaman utama ditampilkan setelah pengguna berhasil login. Fitur yang ditampilkan meliputi:

- Pencarian event.
- Rekomendasi event terpopuler.
- Navigasi tab bar (Home, Booking, Profile).
- Informasi rating dan harga event.

Tampilan ini dirancang agar responsif dan memudahkan pengguna dalam menelusuri berbagai kebutuhan acara.

3.10 Perancangan Database

Dalam sistem ini, penyimpanan data pengguna dan kode OTP dilakukan menggunakan Firebase Firestore sebagai basis data berbasis cloud yang disediakan oleh Google. Firestore dipilih karena bersifat realtime, mudah diintegrasikan dengan aplikasi Android berbasis Kotlin, serta mendukung struktur data fleksibel yang cocok untuk pengembangan sistem login modern dengan autentikasi ganda.

3.10.1 Struktur Koleksi Firestore

Firestore menyimpan data dalam bentuk koleksi dan dokumen. Dalam sistem ini, terdapat koleksi utama yaitu users, Digunakan untuk menyimpan data pengguna.

3.10.2 Tampilan Data Pengguna di Firebase Authentication

Setelah proses registrasi berhasil, sistem menyimpan data pengguna ke dalam layanan Firebase Authentication. Firebase Authentication berfungsi sebagai penyedia layanan identitas (identity provider) yang mencatat informasi autentikasi dasar seperti alamat email, waktu pembuatan akun, dan ID unik pengguna (UID).

3.11 Implementasi Sistem

Implementasi sistem dilakukan menggunakan bahasa pemrograman Kotlin dengan framework Jetpack Compose untuk antarmuka pengguna, Room untuk penyimpanan lokal (sementara), serta Firebase Authentication &

DOI: 10.52362/jisicom.v9i2.2137

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.9 No.2 (December 2025)
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

Firestore sebagai backend utama. Algoritma hashing yang digunakan adalah Argon2 dan sistem otentikasi ganda (Multi-Factor Authentication) dilakukan dengan pengiriman OTP setelah registrasi berhasil.

IV. KESIMPULAN

Berdasarkan hasil penelitian dan implementasi yang telah dilakukan, dapat disimpulkan beberapa hal sebagai berikut:

1. Penggunaan algoritma Argon2 terbukti mampu meningkatkan keamanan dalam proses penyimpanan password. Argon2 merupakan algoritma yang telah diakui secara luas memiliki ketahanan terhadap serangan seperti brute-force dan rainbow table attack, karena bersifat memory-hard dan menghasilkan output hash yang unik untuk setiap input berbeda (berkat penggunaan salt). Penerapan Multi-Factor Authentication (MFA) melalui pengiriman kode OTP ke email pengguna memberikan lapisan keamanan tambahan dalam sistem login. Dengan metode ini, hanya pengguna yang dapat mengakses email terdaftar yang dapat menyelesaikan proses registrasi.
2. Integrasi antara Argon2 dan MFA menghasilkan sistem login yang lebih kuat dan tahan terhadap serangan siber seperti credential stuffing dan phishing. Kombinasi ini menurunkan risiko akses tidak sah secara signifikan.
3. Pengujian pada sistem menunjukkan bahwa konfigurasi parameter hashing (terutama time cost) mempengaruhi waktu eksekusi hashing secara signifikan. Semakin tinggi nilai time cost, maka semakin lama waktu hashing, namun semakin tinggi pula tingkat keamanannya.
4. Hasil pengujian parameter Argon2 menunjukkan pengaruh signifikan terhadap waktu hashing: Time Cost = 1 menghasilkan waktu 2,028 ms, Time Cost = 2 menghasilkan waktu 48,623 ms dan Time Cost = 3 menghasilkan waktu 71,219 ms. Artinya, semakin tinggi nilai time cost, semakin tinggi pula keamanan hashing, namun harus tetap memperhatikan performa sistem.
5. Firebase Authentication dan Firestore terbukti efektif untuk menyimpan data autentikasi dan informasi pengguna secara realtime dan aman, serta mendukung sistem login modern yang terintegrasi dengan layanan cloud.

REFERENSI

[1] A. Fitriyani, R. Sari, and S. Faiz, “Sistem Informasi Pengelolaan Zakat Dan Infaq Menggunakan Metode RAD,” J. Inf. Inf. Secur., vol. 2, no. 2, pp. 197–210, 2021, [Online]. Available: http://ejurnal.ubharajaya.ac.id/index.php/jiforty.

[2] A. Fitriani, Sfenrianto, G. Wang, and A. Susanto, “Examining the security issues of automated teller machine based on revised technical acceptance model,” Telkomnika (Telecommunication Comput. Electron. Control., vol. 14, no. 4, pp. 1521–1526, 2016, doi: 10.12928/TELKOMNIKA.v14i4.2920..

[3] B. O. ALSaleem and A. I. Alshoshan, “Multi-Factor Authentication to Systems Login,” Natl. Comput. Coll. Conf.,2021,[Online].Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9428806&isnumber=9428786.

[4] D. D. and D. K. A. Biryukov, “Argon2: New Generation of Memory-Hard Functions for Password Hashing and Other Applications,” IEEE Eur. Symp. Secur. Priv., pp. 292–302, 2016, doi: 10.1109/EuroSP.2016.31.

[5] J. Informatika, F. Teknik, U. P. Semarang, G. P. Lantai, K. Jl, and S. Timur, “IMPLEMENTASI MULTI-FACTOR AUTHENTICATION (MFA) DENGAN METODE HASHING (SHA-256) UNTUK MENINGKATKAN KEAMANAN PENGGUNA E-COMMERCE Tahap terakhir adalah Implementasi , di mana sistem MFA dikembangkan menggunakan dengan implementasi algoritma SHA-256 , sem,” vol. 9, no. Sens 9, pp. 624–630, 2024.

[6] Suendri, “Hashing Argon2 Untuk Keamanan Password Pada Sistem Berbasis Web,” J. Islam. Sci. Technol., vol. 4, no. 1, pp. 46–56, 2019.

DOI: 10.52362/jisicom.v9i2.2137

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.9 No.2 (December 2025)
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

[7] Lucas Lee, Hash Power: Cryptographic Hash Functions and Their Applications. Norwegia: Publifye AS, 2025.
[8] R. Renaldy and J. Informatika, "PENERAPAN MULTI-FACTOR AUTHENTICATION MENGGUNAKAN," vol. 9, no. Sens 9, pp. 638–650, 2024.
[9] S. Eum, H. Kim, M. Song, and H. Seo, "Optimized Implementation of Argon2 Utilizing the Graphics Processing Unit," Appl. Sci., vol. 13, no. 16, 2023, doi: 10.3390/app13169295.
[10] P. A. Johnston, "Login System," Manchester, 2005.
[11] D. Marisa Khairina, "Analisis Keamanan Sistem Login," J. Inform. Mulawarman, vol. Vol. 6 No., no. 2, pp. 64–67, 2011.
[12] R. Sofana, Iwan & Primarthe, Network Security Dan Cyber Security. Bandung: Informatika, 2019.
[13] A. W. Samsico, "Desain Algoritma Randomisasi pada persoalan Hashing: Studi Kasus SPOJ 40643 AHASHREV - The Revenge Of Anti Hash," 2024.
[14] I. Malviya and T. Chetty, "International Journal on Recent and Innovation Trends in Computing and Communication: Performance and Limitation Review of Secure Hash Function Algorithm," Int. J. Recent Innov. Trends Comput. Commun., vol. 7, no. 6, pp. 48–51, 2019, [Online]. Available: http://www.ijritcc.org.
[15] K. Phan, "Implementing Resiliency of Adaptive Multi-Factor Authentication Systems," vol. 65, pp. 1–96, 2018,[Online].Available:https://repository.stcloudstate.edu/msia_etdshttps://repository.stcloudstate.edu/msia_etds/65.
[16] T. Suleski, M. Ahmed, W. Yang, and E. Wang, "A review of multi-factor authentication in the Internet of Healthcare Things," Digit. Heal., vol. 9, 2023, doi: 10.1177/20552076231177144.
[17] M. Fanti, Implementing Multifactor Authentication: Protect Your Applications from Cyberattacks with the Help of MFA. Packt Publishing, 2023. [Online]. Available: https://www.google.co.id/books/edition/Implementing_Multifactor_Authentication/r-zDEAAAQBAJ?hl=id&gbpv=1.
[18] I. Yurita, M. Kevin Ramadhan, M. Candra, and U. Muhammadiyah Kotabumi, "Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana Cybercrime," J. Huk. Leg., pp. 144–155, 2023, [Online]. Available: https://jurnal.umko.ac.id/index.php/legalita/article/view/995.
[19] K. Mubarok and M. A. Romli, "Implementation of Rule Based Method in Detecting Brute Force Attacks on Owncloud Implementasi Metode Rule Based dalam Mendeteksi Serangan Brute Force pada Owncloud," vol. 5, no. January, pp. 159–167, 2025.
[20] M. C. Sinaga, Kriptografi Python. Tarutung, 2017. [Online]. Available: https://books.google.co.id/books?id=HCroDwAAQBAJ&printsec=frontcover&hl=id&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.
[21] Y. Mulyanto and A. Algi Fari, "ANALISIS KEAMANAN LOGIN ROUTER MIKROTIK DARI SERANGAN BRUTEFORCE MENGGUNAKAN METODE PENETRATION TESTING (Studi Kasus: SMK NEGERI 2 SUMBAWA)," J. Inform. Teknol. dan Sains, vol. 4, no. 3, pp. 145–155, 2022, doi: 10.51401/jinteks.v4i3.1897.
[22] A. R. Naufal, D. A. Nawangnugraeni, and A. T. Suseno, "Rancang Bangun Sistem Informasi Point of Sale Multi Outlet Dengan Menggunakan Framework Laravel Di Koperasi Itsnu Pekalongan," J. Tek. Inf. dan Komput., vol. 5, no. 2, p. 280, 2022, doi: 10.37600/tekinkom.v5i2.591.
[23] R. Permana, A. Abdilah, Fuad Nur Hasan, and Mahmud Syarif, "Estimation Effort Pengembangan Software Inventory PT. Infinity Global Mandiri Menggunakan Metode Use Case Point," J. RESTIKOM Ris. Tek. Inform. dan Komput., vol. 5, no. 2, pp. 73–84, 2023, doi: 10.52005/restikom.v5i2.144.

DOI: 10.52362/jisicom.v9i2.2137

e-ISSN : 2597-3673 (Online) , p-ISSN : 2579-5201 (Printed)
Vol.9 No.2 (December 2025)
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

[24] M. Shalahuddin and R. A. Sukamto, "Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek Edisi Revisi," pp. 25–41, 2018.

[25] "Mengenal Android Studio," Developers.Android. [Online]. Available: https://developer.android.com/studio/intro?hl=id.

[26] Fauzan M, Rinandi A, and Maulid H, "Jago Menabung Aplikasi Untuk Mengelola Uang Saku Bebasis Mobile," e-Proceeding Appl. Sci., vol. 10, no. 1, pp. 419–425, 2024, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/22496/21647.

[27] R. Risqi and A. Herlambang, "Penggunaan Firebase Analytics pada Pengembangan Aplikasi Mobile I ' m UII dengan Framework Flutter," Automata, vol. 4, 2023, [Online]. Available: https://jurnal.uii.ac.id/AUTOMATA/article/view/28841.

[28] N. Telaumbanua, M. Yusuf, and A. Saifudin, "Implementasi Aplikasi Stock Opname Dengan Metode Waterfal," Jubitek J. BIG DATA DAN Teknol. Inf., vol. 1, pp. 61–83, 2023.

[29] Y. F. and C. Taurusta, Buku ajar rekayasa perangkat lunak terstruktur dan berorientasi objek. Umsida Press, 2021. doi: https://doi.org/10.21070/2018/978-602-5914-09-6.

[30] W. Setiyaningsih, KONSEP SISTEM PENDUKUNG KEPUTUSAN, vol. 1. 2015.

DOI: 10.52362/jisicom.v9i2.2137