

**IMPLEMENTASI ALGORITMA HASHING & MULTI-
FACTOR AUTHENTICATION UNTUK
MENINGKATKAN KEAMANAN SISTEM LOGIN
PENGGUNA APLIKASI EVENTHINGS**

SKRIPSI

Oleh:

Ilham Maulana

202110715113



PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS BHAYANGKARA JAKARTA RAYA

2025

LEMBAR PERSETUJUAN PEMBIMBING

Judul Tugas Akhir : Implementasi Algoritma Hashing & Multi-Factor Authentication Untuk Meningkatkan Keamanan Sistem Login Pengguna Aplikasi Eventhings

Nama Mahasiswa : Ilham Maulana

Nomor Pokok Mahasiswa : 202110715113

Program Studi/Fakultas : Informatika/Ilmu Komputer

Jakarta, 04 Agustus 2025

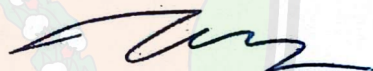
MENYETUJUI,

Pembimbing 1



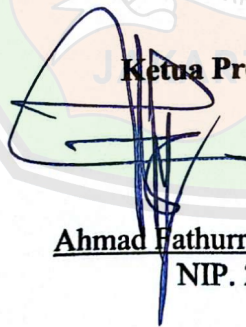
Aida Fitriyani, S.Kom., M.M.S.I.
NIDN. 0302078508

Pembimbing II



Hendarman Lubis, S.Kom., M.Kom.
NIDN. 0013077002

Ketua Program Studi



Ahmad Fathurrozi, S.E., M.M.SI.
NIP. 2012486

Program Studi Informatika
Fasilkom Ilmu Komputer
Universitas Bhayangkara Jakarta Raya
2025

LEMBAR PENGESAHAN

Judul Tugas Akhir : Implementasi Algoritma Hashing & Multi-Factor Authentication Untuk Meningkatkan Keamanan Sistem Login Pengguna Aplikasi Eventhings
Nama Mahasiswa : Ilham Maulana
Nomor Pokok Mahasiswa : 202110715113
Program Studi/Fakultas : Informatika / Ilmu Komputer
Tanggal Lulus Ujian Akhir : 28/07/2025

Jakarta, 4 Agustus 2025

MENGESAHKAN,

Ketua Tim Penguji : Ir. Muhammad Khaerudin., M.Kom.

NIDN: 0413066604

Penguji I : Ratna Salkiawati, S.T., M.Kom.

NIDN: 0310038006

Penguji II : Aida Fitriyani, S.Kom., M.M.S.I.

NIDN: 0302078508

MENGETAHUI,

Ketua

Program Studi Informatika

Ahmad Fathurrozi, S.E., M.M.S.I

NIP: 2012486

Dekan

Fakultas Ilmu Komputer

Dr. Robertus Suraji, SS., MA

NIP: 1904406



LEMBAR PERNYATAAN BUKAN PLAGIASI

Yang bertanda tangan dibawah ini :

Nama : Ilham Maulana
NPM : 202110715113
Program Studi : Informatika
Fakultas : Ilmu Komputer
Judul Tugas Akhir : Implementasi Algoritma Hashing & Multi-Factor
Authentication Untuk Meningkatkan Keamanan Sistem
Login Pengguna Aplikasi Eventhings

Dengan ini menyatakan bahwa hasil penulisan skripsi yang telah saya buat ini merupakan **hasil karya saya sendiri dan benar keasliannya**. Apabila dikemudian hari penulisan skripsi ini merupakan plagiat atau penjiplakan terhadap karya orang lain, maka saya bersedia mempertanggungjawabkan sekaligus bersedia menerima sanksi berdasarkan tata tertib di Universitas Bhayangkara Jakarta Raya.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan dari pihak manapun.

Bekasi, 16 Juli 2025

Penulis



Ilham Maulana

ABSTRAK

Ilham Maulana. 202110715113 . Implementasi Algoritma Hashing & Multi-Factor Authentication Untuk Meningkatkan Keamanan Sistem Login Pengguna Aplikasi Eventhings . Bekasi: Fakultas Ilmu Komputer . Universitas Bhayangkara Jakarta Raya. 2025

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 $\rightarrow$ 2,028 ms, Time Cost = 2 $\rightarrow$ 48,623 ms dan Time Cost = 3 $\rightarrow$ 71,219 ms. Semakin tinggi nilai parameter, waktu eksekusi meningkat, namun 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

Ilham Maulana . 202110715113 . *Implementation of Hashing Algorithm & Multi-Factor Authentication to Improve the Security of Event Application User Login System. Bekasi: Faculty of Computer Science . Bhayangkara University, Greater Jakarta. 2025*

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.

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIK

Sebagai sivitas akademik Universitas Bhayangkara Jakarta Raya, saya yang bertanda tangan di bawah ini :

Nama : Ilham Maulana
NPM : 202110715113
Program Studi : Informatika
Fakultas : Ilmu Komputer
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bhayangkara Jakarta Raya **Hak Bebas Royalti Non-Eksklusif (Non-Exclusive Royalty-Free Right)**, atas karya ilmiah saya yang berjudul :

Implementasi Algoritma Hashing & Multi-Factor Authentication Untuk Meningkatkan Keamanan Sistem Login Pengguna Aplikasi Eventhings

beserta perangkat yang ada (bila diperlukan). Dengan hak bebas royalti non-eksklusif ini, Universitas Bhayangkara Jakarta Raya berhak menyimpan, mengalihmediakan, mengelolanya dalam bentuk pangkalan data (*database*), mendistribusikannya dan mempublikasikannya di Internet atau media lain untuk kepentingan akademis tanpa perlu meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik hak cipta.

Segala bentuk tuntutan hukum yang timbul atas pelanggaran hak cipta dalam karya ilmiah ini menjadi tanggung jawab saya pribadi

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Bekasi
Pada tanggal : 17 Juli 2025
Yang Menyatakan



KATA PENGANTAR

Segala puji bagi Allah SWT, yang telah melimpahkan rahmat dan hidayah-Nya sehingga saya dapat menyelesaikan Tugas Akhir Skripsi yang berjudul **"Implementasi Algoritma Hashing & Multi-Factor Authentication Untuk Meningkatkan Keamanan Sistem Login Pengguna Aplikasi Eventhings"**. Skripsi ini disusun sebagai prasyarat untuk mencapai gelar Sarjana Strata Satu (S1) pada Program Studi Informatika Universitas Bhayangkara Jakarta Raya. Dengan adanya Penelitian Skripsi, saya mendapatkan banyak sekali wawasan, dan ilmu yang bermanfaat. Tugas Akhir ini saya kerjakan sebagai tanggung jawab dan bukti tertulis akan syarat untuk memperoleh gelar Sarjana pada Program Studi Informatika.

Dalam penyusunan proposal penelitian skripsi ini saya banyak sekali mendapatkan bantuan dari berbagai pihak, oleh sebab itu saya ingin mengungkapkan rasa terima kasih kepada:

1. Bapak Irjen Pol (Purn) Dr., Drs. Bambang Karsono, S.H., M.M., Ph.D., D.Crim., (Honoris Causa) Selaku Rektor Universitas Bhayangkara Jakarta Raya Bekasi.
2. Bapak Dr. Robertus Suraji, S.S, M.M. Selaku Dekan Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya Bekasi.
3. Bapak Ahmad Fathurrozi, S.E., M.M.S.I. selaku Ketua Program Studi Informatika Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.

4. Ibu Aida Fitriyani, S.Kom., M.M.S.I. selaku Dosen Pembimbing I dalam penyusunan Tugas Akhir skripsi Program Studi Informatika Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
5. Bapak Hendarman Lubis, S.Kom., M.Kom. selaku Dosen Pembimbing II dalam penyusunan Tugas Akhir skripsi Program Studi Informatika Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
6. Bapak Dani Yusuf S.Kom., M.Kom. selaku Dosen Pembimbing Akademik Raya Program Studi Informatika Fakultas Ilmu Komputer.
7. Kepada Orang Tua saya yang telah memberikan dukungan moral maupun material.
8. Kepada Teman – Teman perjuangan satu bimbingan skripsi, yang telah memberikan pemahaman dan bekerja sama dalam penyelesaian Tugas Akhir Skripsi ini.
9. Kepada Teman Group Eko, Taufik, Ray, Rifky, Rafi Lutfi, Naufal dan Reinanda yang memberi dukungan dan telah membantu dalam menyelesaikan Tugas Akhir Skripsi.

Bekasi, 14 Juli 2025

Hormat saya



Ilham Maulana
202110715113

DAFTAR ISI

LEMBAR PERSETUJUAN PEMBIMBING	i
LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN BUKAN PLAGIASI	iii
ABSTRAK	iv
<i>ABSTRACT</i>	v
LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI	ix
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN	xv
BAB I.....	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	4
1.3 Rumusan Masalah	4
1.4 Tujuan Penelitian.....	5
1.5 Manfaat Penelitian	5
1.6 Batasan Masalah.....	6
1.7 Sistematika Tugas Akhir.....	7
BAB II.....	9
2.1 Landasan Teori	9
2.2 Keamanan Sistem Login	18
2.3 Algoritma Hashing	19
2.3.1 Argon2	20

2.3.2 Tahap Perhitungan Argon2	23
2.4 Multi-Factor Authentication (MFA)	25
2.5 Ancaman Keamanan	27
2.5.1 Brute Force	28
2.6 Alat Pengembangan Sistem.....	29
2.6.1 UML (Unified Modeling Language)	29
2.6.2 Use Case Diagram.....	29
2.6.3 Sequence Diagram	31
2.6.4 Class Diagram.....	32
2.6.5 Activity Diagram.....	33
2.6.6 Android dan Android Studio	33
2.6.7 Kotlin	34
2.6.8 Firebase Analisis	35
2.7 Metode Pengembangan Sistem	35
2.7.1 Pengertian Waterfall.....	36
2.7.2 Tahapan Waterfall	36
2.8 Black Box Testing	38
BAB III	39
3.1 Kerangka Penelitian	39
3.1.1 Identifikasi Masalah.....	40
3.1.2 Rumusan Masalah.....	40
3.1.3 Metode Pengumpulan Data.....	40
3.1.4 Algoritma	40
3.1.5 Perancangan dan implementasi sistem	40
3.1.6 Pengujian Sistem.....	41
3.2 Tipe Penelitian.....	41

3.3 Pendekatan Penelitian.....	41
3.4 Objek Penelitian	41
3.5 Metode Pengumpulan Data	42
3.5.1 Studi Literatur	42
3.5.2 Eksperimen Sistem	42
3.6 Metode Analisis	43
3.6.1 Activity Diagram.....	43
3.6.2 Kebutuhan Penelitian.....	44
3.6.3 Analisis Pengujian (Blackbox Testing).....	45
3.7 Perancangan Antarmuka.....	48
3.7.1 Desain Antarmuka Login.....	48
3.7.2 Desain Antarmuka Register	50
BAB IV	52
4.1 Perhitungan Algoritma Argon2	52
4.1.1 Parameter Argon2	52
4.1.2 Format Output Hash.....	53
4.1.3 Analisis Keamanan	54
4.1.4 Waktu Hashing.....	56
4.2 Perancangan Sistem	56
4.2.1 <i>Use Case Diagram</i>	56
4.2.3 Analisis Sistem Usulan	58
4.2.4 <i>Sequence Diagram</i>	59
4.2.5 <i>Class Diagram</i>	61
4.2.6 UI Design (Jetpack Compose)	66
4.3 Perancangan Database	70
4.3.1 Struktur Koleksi Firestore.....	70

4.3.2 Tampilan Data Pengguna di Firebase Authentication	73
4.4 Implementasi Sistem	74
4.4.1 Implementasi Argon2	74
4.4.2 Impementasi MFA	75
4.6 Pengujian Sistem	76
4.6.1 Tujuan Pengujian	76
4.6.2 Data Uji Register	77
4.6.3 Metode Pengujian	85
4.6.4 Hasil Pengujian	85
BAB V	87
5.1 Kesimpulan	87
5.2 Saran	88
DAFTAR PUSTAKA	89
LAMPIRAN	93

DAFTAR TABEL

Tabel 2.1 Landasan Teori	9
Tabel 2.2 Simbol <i>Use Case Diagram</i>	30
Tabel 2.3 Simbol <i>Sequence Diagram</i>	31
Tabel 2.4 Simbol <i>Class Diagram</i>	32
Tabel 2.5 Activity Diagram	33
Table 3.1 Teknologi yang digunakan	44
Table 3.2 Skenario uji, input, output yang diharapkan, dan hasilnya.	47
Tabel 4.1 Parameter Algoritma Hashing Argon2	52
Tabel 4.2 Penjelasan Parameter dan Nilai Contoh pada Argon2.....	53
Tabel 4.3 Perbandingan Algoritma Hashing Berdasarkan Aspek Keamanan	54
Tabel 4.4 Keterangan Hubungan Antar <i>Class</i>	63
Tabel 4.5 Tabel User.....	64
Tabel 4.6 Tabel Argon2	65
Tabel 4.7 Tabel Multi-Factor.....	65
Tabel 4.8 Struktur Data pada <i>Firebase Firestore</i>	73
Tabel 4.9 Struktur Data <i>Firebase Authentication</i> Pengguna.....	73
Tabel 4.10 Data Pengguna 1.....	77
Tabel 4.11 Hasil Hashing <i>Password</i> Pengguna 1	77
Tabel 4.12 Data Hasil Registrasi Pengguna 1 pada <i>Firebase Authentication</i>	78
Tabel 4.13 Data Pengguna 2.....	79
Tabel 4.14 Hasil Hashing <i>Password</i> Pengguna 2.....	79
Tabel 4.15 Data Hasil Registrasi Pengguna 2 pada <i>Firebase Authentication</i>	80
Tabel 4.16 Data Pengguna 3.....	80
Tabel 4.17 Hasil Hashing <i>Password</i> Pengguna 3 percobaan 1	81
Tabel 4.18 Hasil Hashing <i>Password</i> Pengguna 3 percobaan 2.....	81
Tabel 4.19 Hasil Hashing <i>Password</i> Pengguna 3 percobaan 3.....	82
Tabel 4.20 Data Hasil Pengujian Waktu Eksekusi Algoritma Argon2 terhadap Variasi Time Cost	82
Tabel 4.21 Data Hasil Registrasi Pengguna 3 pada <i>Firebase Authentication</i>	85
Tabel 4.22 Hasil Pengujian Fitur Sistem Login dan OTP	85

DAFTAR GAMBAR

Gambar 2.1 Keamanan Informasi	19
Gambar 2.2 Parallesime	23
Gambar 2.3 Metode <i>Waterfall</i>	36
Gambar 3.1 Kerangka Penelitian	39
Gambar 3.2 Blackbox Testing	45
Gambar 3.3 Halaman Login	49
Gambar 3.4 Halaman Register	50
Gambar 4.1 Use Case Diagram	56
Gambar 4.2 Diagram Usulan	58
Gambar 4.3 <i>Sequence</i> Diagram	59
Gambar 4.4 <i>Class</i> Diagram	62
Gambar 4.6 Halaman Register	67
Gambar 4.7 Halaman OTP	68
Gambar 4.8 Halaman Login	69
Gambar 4.9 Halaman Utama	70
Gambar 4.10 Perancangan Database	71
Gambar 4.11 Kode Program Pengiriman OTP	76
Gambar 4.12 Analisis Kinerja Algoritma Argon2 Berdasarkan Variasi Time Cost	84

DAFTAR LAMPIRAN

Lampiran 1 Hasil Cek Plagiarisme	94
Lampiran 2 Biodata Mahasiswa.....	96
Lampiran 3 Kartu Konsultasi Bimbingan Skripsi (Tugas Akhir)	97
Lampiran 4 Kartu Bimbingan Skripsi (Pembimbing I)	98
Lampiran 5 Kartu Bimbingan Skripsi (Pembimbing II)	99
Lampiran 6 Tabel Kebocoran Data TokoPedia 2020[41].....	100
Lampiran 7 Tabel Konfigurasi Hashing Argon2	101
Lampiran 8 Kebocoran Data pada PDNS 2024	102

