VOL. 19. NO. 1 AGUSTUS 2024
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Universitas Nusa Mandiri

INTI NUSA MANDIRI
DOI: https://doi.org/10.33480/inti.v19i1.5263

PERANCANGAN AUTENTIKASI MULTI FAKTOR DENGAN PENGENALAN WAJAH DAN FIDO (*FAST IDENTITY ONLINE*)

Rizky Atmawijaya[1*]; Ummu Radiyah[2]

Program Studi Informatika[1,2]
Universitas Nusa Mandiri[1,2]
www.nusamandiri.ac.id[1,2]
rizky.atmawijaya.traspac@gmail.com[1*]; ummu.urd@nusamandiri.ac.id[2]
(*) Corresponding Author

Abstract*—Digital services based online are assets that need to be safeguarded, especially if the application still uses single-factor authentication vulnerable to cyberattacks and potential data leaks and identity theft. The proposed solution is to implement multi-factor authentication (MFA) utilizing facial recognition, particularly through FaceNet technology. Although facial recognition can provide an additional layer of security, the main challenge is to maintain user privacy even if biometric information might leak. This research aims to create a secure, reliable MFA model that protects the privacy of employees at PT Traspac Makmur Sejahtera. The proposed method involves an MFA system with four factors: knowledge factor (password), biometric factor (facial measurements), ownership factor (OTP) and location factor (optional if facial accuracy is insufficient). The implementation of this MFA model enhances security, reliability, and protects employee privacy. Considering the specific needs of the company, this research can assist the company in monitoring the locations of employees working from home (WFH).*

Keywords*: FaceNet, face recognition, multi-factor authentication, privacy preserving.*

Abstrak—Layanan digital berbasis *online* merupakan aset yang perlu dijaga keamanannya, terutama jika aplikasi masih menggunakan autentikasi satu-faktor yang rentan terhadap serangan siber dan dapat menyebabkan kebocoran data dan pencurian identitas. Solusi yang diusulkan adalah menerapkan autentikasi multi-faktor (MFA) dengan memanfaatkan pengenalan wajah, terutama melalui teknologi FaceNet. Walaupun pengenalan wajah dapat memberikan lapisan keamanan tambahan, tantangan utamanya adalah tetap menjaga privasi pengguna meskipun informasi biometrik mungkin bocor. Penelitian ini bertujuan untuk menciptakan model MFA yang aman, andal dan melindungi privasi karyawan PT. Traspac Makmur Sejahtera. Metode yang diusulkan melibatkan sistem MFA dengan empat faktor, yaitu faktor pengetahuan (*password*), faktor biometrik (pengukuran wajah), faktor kepemilikan (OTP), dan faktor lokasi (opsional jika akurasi wajah tidak memadai). Implementasi model MFA ini meningkatkan tingkat keamanan, keandalan, dan melindungi privasi karyawan. Dengan mempertimbangkan kebutuhan khusus perusahaan, penelitian ini dapat membantu perusahaan dalam memonitor lokasi karyawan yang sedang bekerja dari rumah (WFH).

Kata kunci: *FaceNet*, pengenalan wajah, autentikasi multi faktor, melindungi privasi.

PENDAHULUAN

Pandemi COVID-19 memicu transformasi signifikan dalam model kerja perusahaan, mengarah pada adopsi kerja hibrida dan digitalisasi operasional berbasis *cloud*. PT. Traspac Makmur Sejahtera terpengaruh oleh perubahan ini dan melakukan adaptasi layanan aplikasi dari jaringan lokal ke daring. Perubahan ini meningkatkan risiko keamanan (Otta et al., 2023), terutama jika aplikasi masih menggunakan autentikasi satu-faktor yang rentan terhadap berbagai serangan seperti *brute-force*, taktik rekayasa sosial, dan serangan malware (Xin et al., 2021). Disisi lain, skema otentikasi berbasis satu faktor rentan untuk aplikasi yang memerlukan tingkat keamanan tinggi, sehingga perlu menggabungkan dua atau lebih faktor autentikasi untuk meningkatkan keamanan system

VOL. 19. NO. 1 AGUSTUS 2024
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Universitas Nusa Mandiri

(Wang & Wang, 2023). Oleh karena itu, autentikasi multi-faktor (MFA) menjadi solusi yang paling handal untuk melindungi akun daring dari serangan (Otta et al., 2023), dengan pengenalan wajah sebagai aspek penting.

Pengenalan wajah merupakan salah satu metode *nonintrusive* (tidak mengganggu) yang menjadi pilihan di banyak aplikasi keamanan (Taskiran et al., 2020). Penelitian tentang pengenalan wajah menunjukkan kemajuan yang signifikan mencapai tingkat akurasi 92.86% untuk dataset LFW menggunakan model FaceNet (Jin et al., 2021). FaceNet menggunakan *Deep Convolutional Neural Network* (DCNN) untuk melakukan pemetaan wajah seseorang ke dalam *Euclidean space*, yang merupakan kumpulan titik geometris. Titik geometris ini kemudian digunakan untuk menentukan nilai *embedding*, yang merupakan ukuran untuk mengukur tingkat kemiripan wajah (Cahyono, 2020). Pada Gambar 1 dijelaskan dengan detail arsitektur *Facenet*.

Sumber: (Maheswari et al., 2020)
Gambar 1. Ekstraksi fitur FaceNet

Meskipun teknologi pengenalan wajah memiliki tingkat kecanggihan yang mencukupi untuk menjadi elemen kunci dalam autentikasi MFA, namun ketidakamanan dalam privasi pengguna, terutama ketika informasi biometrik yang digunakan dalam sistem autentikasi bocor, menjadi kerentanan yang signifikan. Privasi biometrik seperti wajah mudah terungkap di media sosial. Dalam lingkungan praktis, sidik jari dan rekaman suara bisa bocor di tempat umum, sementara dalam jaringan, informasi biometrik rentan dicuri atau dimanipulasi selama penyimpanan dan transmisi (Meden et al., 2021). Data biometrik yang ditransmisikan melalui jaringan dapat rentan terhadap serangan yang mengakibatkan intersepsi atau manipulasi data (Arman et al., 2024).

Untuk mencegah kerentanan ini, *anti-spoofing* diperlukan untuk menangkal serangan dari biometrik wajah yang dicuri agar bisa membedakan wajah asli atau foto hasil curian (Anthony et al., 2021). Walaupun metode-metode canggih untuk mengatasi serangan *spoof* pada sistem pengenalan wajah terus dikembangkan, penyerang terus menciptakan jenis serangan palsu baru, yang menjadi ancaman serius bagi keamanan sistem tersebut. Sebagai respons terhadap hal ini, *Zero-Shot Face Anti-spoofing* (ZSFA) muncul sebagai konsep deteksi serangan palsu yang tidak diketahui (Ming et al., 2020).

Sementara itu untuk mengamankan privasi pada lapisan transmisi jaringan dibutuhkan FIDO sebagai *protocol* autentikasi *biometric* untuk melindungi privasi (Ali, 2023). FIDO menggunakan kriptografi asimetris untuk saluran komunikasi aman, memastikan autentikasi yang aman dan perlindungan privasi (Kim et al., 2020). Kelebihan FIDO meliputi keunikan, kenyamanan, skalabilitas, dan peningkatan pengalaman pengguna . FIDO juga tahan terhadap berbagai serangan, termasuk *phising*, *sniffing*, pencurian identitas, serangan replay (*replay attack*), dan serangan MITM (*Man-in-the-Middle Attack*) (Klieme et al., 2020; Feng et al., 2021).

Otentikasi dapat berbasis pengetahuan (PIN, kata sandi), kepemilikan (perangkat, kartu pintar), fisiologis (sidik jari, wajah), perilaku (dinamika pengetikan) dan konteks (lokasi, alamat IP). Faktor-faktor ini meningkatkan keamanan dan kesesuaian otentikasi dengan pengguna (Baig & Eskeland, 2021). Penelitian terkait dengan autentikasi multi-faktor (MFA) menggunakan pengenalan wajah atau biometrik telah dilakukan oleh (Xin et al., 2021) dalam konteks *smart home* dan (Ali, 2023) dalam aplikasi *mobile* keuangan. (Xin et al., 2021) mengusulkan sistem MFA dengan pengenalan wajah dan kode OTP (*One-Time Password*) untuk *smart home*. *Server* mengirimkan kode OTP ke aplikasi mobile setelah autentikasi wajah berhasil, dan pengguna memiliki tiga kesempatan untuk memasukkan kode tersebut. Akan tetapi pada penelitian tersebut minim pembahasan terkait bagaimana implementasi MFA yang aman dan melindungi *privacy* pengguna. Sementara itu, Guma Ali merancang desain algoritma MFA untuk aplikasi *mobile* keuangan yang berfokus pada keamanan dan *privacy* pengguna menggunakan *protocol* FIDO yang melibatkan kombinasi informasi pribadi, nomor telepon, PIN, sidik jari dan OTP. Kedua penelitian tersebut menjadi bahan dasar untuk merancang MFA dengan teknologi pengenalan wajah yang aman, melindungi privasi, dan dapat diintegrasikan pada aplikasi web di PT. Traspac Makmur Sejahtera.

BAHAN DAN METODE

Teknik Pengumpulan Data

A. Observasi

Pada penelitian ini observasi dilakukan dengan identifikasi bisnis proses aplikasi dan melakukan pengukuran akurasi pengenalan wajah dengan enam responden dari karyawan PT. Traspac serta meminta masukannya untuk perbaikan ke depan.

B. Wawancara

Wawancara dilakukan dengan HRD (*Human Resource Development*) untuk analisis kebutuhan perancangan *mobile* MFA dan Kepala Departemen Teknologi untuk mendapatkan perspektif langsung mengenai kebutuhan, harapan, dan tantangan terkait implementasi autentikasi multi-faktor dan pengenalan wajah.

C. Studi Pustaka

Pada penelitian ini sumber pustaka diambil dari jurnal-jurnal terbaru dan tesis tentang MFA, *Face Recognition, Anti-Spoofing,* menjaga *privacy* dalam biometrik wajah dan protokol FIDO.

Teknik Pengembangan Aplikasi

Pendekatan pengembangan sistem yang digunakan adalah model *waterfall*. *Waterfall* adalah model pengembangan perangkat lunak sekuensial yang bersifat sistematis dan berurutan. Berikut adalah tahapan-tahapan secara lebih rinci.

A. Analisa Kebutuhan

Studi kebutuhan fungsional sistem autentikasi multi-faktor dengan fokus pada pengenalan wajah.

B. Desain

Peneliti merancang *database*, termasuk ERD (*Entity Relational Database*). *Software Architecture*: *Pseudocode* algoritma dan pemodelan UML (*Unified Modelling Language*). *User Interface*: Rancangan antarmuka sistem dengan *Mobile Application*.

C. Implementasi

Tampilan aplikasi Mobile MFA dan Web Pelayanan Kepegawaian di PT. Traspac Makmur Sejahtera.

D. Pengujian

Pengujian *black-box* dan UAT (*User Acceptance Testing*) untuk kehandalan dan keamanan MFA.

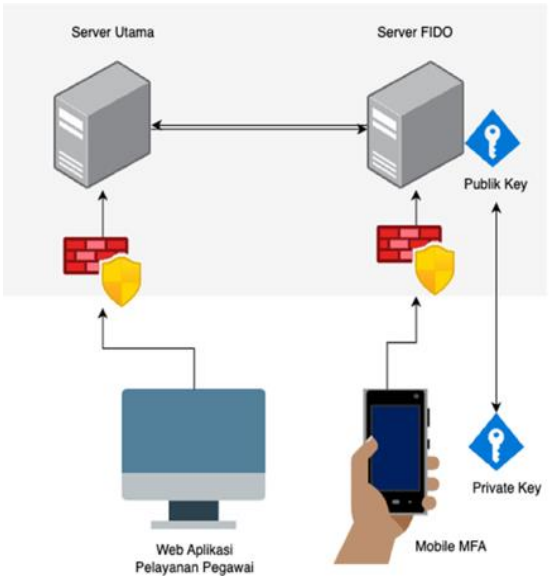
HASIL DAN PEMBAHASAN

A. Analisa Kebutuhan

Penulis telah membuat hasil kompilasi kebutuhan yang ditemukan di PT. Traspac Makmur Sejahtera. Pertama, pengguna memerlukan *reminder* atau informasi yang jelas mengenai batasan waktu laporan pekerjaan agar dapat menghindari potongan gaji. Kedua, bagian SDM (Sumber Daya Manusia) mengambil langkah memastikan transparansi lokasi kerja karyawan yang melakukan izin *Work From Home* (WFH) dengan mengawasi informasi dan memastikan konfirmasi lokasi-lokasi WFH.

B. Desain Aplikasi

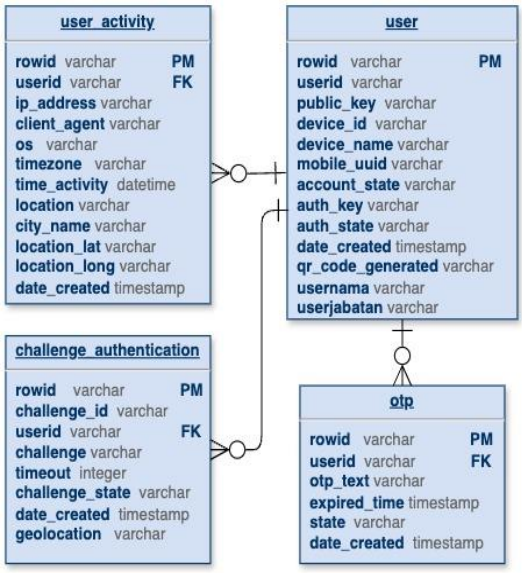
Rancangan solusi MFA mengusulkan peran utama perangkat *mobile* dalam pengenalan wajah menggunakan model FaceNet untuk autentikasi yang akurat. FIDO diimplementasikan sebagai protokol autentikasi untuk menjaga privasi biometrik wajah, dan enkripsi RSA digunakan untuk melindungi kunci publik atau privat, meningkatkan keamanan autentikasi. Rancangan infrastruktur pada Gambar 2 bertujuan untuk meningkatkan keamanan aplikasi secara signifikan dengan memisahkan Server Utama dan Server FIDO sebagai Autentikasi.



Sumber: (Hasil Penelitian, 2024)

Gambar 2. Infrastruktur MFA Sistem Usulan

Desain database yang digunakan pada aplikasi mobile MFA ini menggunakan ERD yang ditampilkan pada Gambar 3.



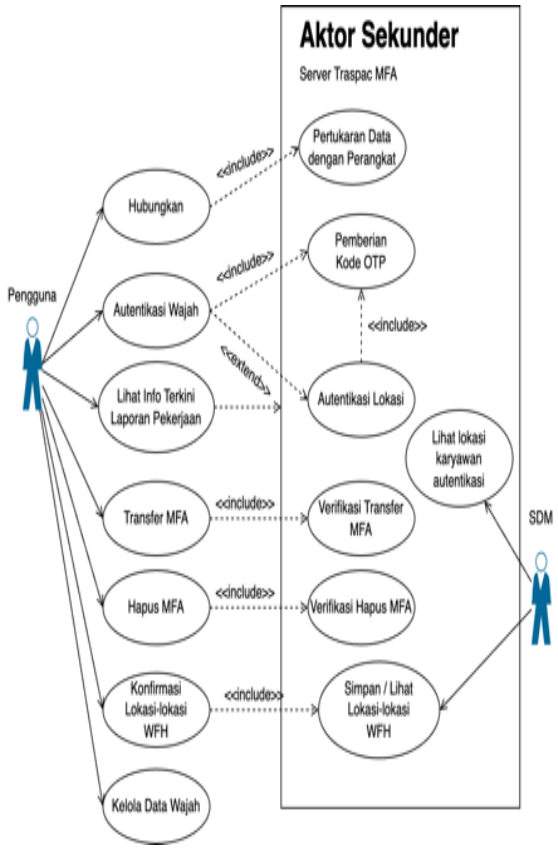
Sumber: (Hasil Penelitian, 2024)

Gambar 3. ERD Database FIDO

VOL. 19. NO. 1 AGUSTUS 2024
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Universitas Nusa Mandiri

Sistem keamanan berbasis *One Time Password* (OTP) pada Gambar 3 menggunakan 4 (empat) entitas utama: User, OTP, *Challenge Authentication*, dan *Location*. Hubungan antara entitas ini melibatkan pengguna yang memiliki banyak kode OTP, tetapi hanya menggunakan yang terbaru untuk verifikasi. Pengguna juga memiliki banyak tantangan autentikasi, tetapi hanya tantangan yang masih aktif. Selain itu, setiap pengguna memiliki banyak lokasi untuk verifikasi geolokasi. Sistem ini menggunakan dua jenis tantangan autentikasi, yaitu OTP yang dikirimkan melalui Aplikasi MFA dan *Challenge* yang diberikan melalui permintaan tanda tangan digital. Location digunakan untuk mencatat GPS untuk audit trail.

Sementara itu, struktur sistem yang diterapkan untuk konstruksi aplikasi melibatkan penerapan UML, dengan diagram yang terdiri dari Use Case Diagram dan Sequence Diagram. Use Case Diagram, seperti yang terlihat pada Gambar 4 memberikan penjelasan mengenai interaksi antara pengguna dan sistem MFA.



Sumber: (Hasil Penelitian, 2024)
Gambar 4. Use Case Diagram Sistem MFA

Selain itu, *pseudocode* algoritma pada saat registrasi perangkat MFA ditampilkan pada Gambar 5.

ALGORITMA : REGISTRASI PERANGKAT MFA

```
    Input: User_i, Pass_i
    START
1   k_i ← Ambil input {Username_i, Password_i}
2   if ( isLoginValid ( k_i ) AND HPBelumDaftar ()) then
3     QRCode_p = GenerateQRCode( String(64) )
4
5     TampilkanQRCodeWeb( QRCode_p )
6     if ( ScanQRCode( QRCode_p ) == "Berhasil" ) then
7         P_i, F_i = GenerateKeyPair() //private key
      disimpan di Perangkat Mobile
8         B_i  = ProsesPerekamanDataWajah() // simpan di
      perangkat mobile
9         BF_i = InputFace()
10        if ( bandingkanWajah ( BF_i, B_i ) ) then
11            OTP_server = GenerateOTPfromFIDO()
12            h(OTP_server) hash OTP disimpan di DB_fido
13            KirimOTPkePerangkat( E_encrypt( OTP_server ) )
14            showOTPdiPerangkat( D_crypt (OTP_server) )
15            OTP_input = InputKodeOTPdiWeb()
16            if ( hash (OTP_input) = OTP_database ) then
17                SelesaiRegistrasi()
18            Else
19                Ulangi input OTP_input di langkah 15
                  sampai 3 kali
20            end if
21        else
22            Ulangi retake wajah di line 9
              sampai 3 kali
23            end if
24      else
25          PesanError("Scan QR Code gagal.")
26    end if
27  else if ( isLoginValid ( k_i ) AND
              PerangkatSudahTerdaftar {} ) then
28    OTP_i = WebMenampilkanInputanKodeOTP()
29  else
30    PesanError("Verifikasi gagal")
31  end if
32  Return
33  STOP
```

Sumber: (Hasil Penelitian, 2024)
Gambar 5. *Pseudocode* Algoritma Perangkat MFA

Pseudocode yang ditampilkan pada Gambar 5 menjelaskan fase pendaftaran perangkat di mana perangkat seluler didaftarkan untuk digunakan sebagai langkah autentikasi tambahan dalam MFA.

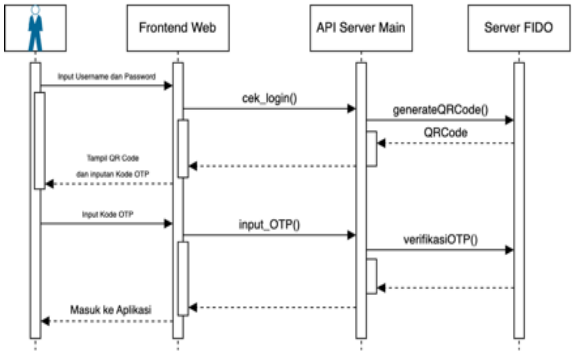
Langkah 1: Pengguna memasukkan nama pengguna dan kata sandi di situs web. Validasi login dilakukan untuk memastikan bahwa informasi login valid dan perangkat belum terdaftar.
Langkah 2: Jika login valid dan perangkat belum terdaftar, hasilkan QR Code unik dan simpan informasinya bersama UserID di database FIDO. QR Code tersebut ditampilkan pada halaman web.
Langkah 3: Pengguna menggunakan perangkat untuk memindai QR Code yang ditampilkan melalui Aplikasi Traspac MFA. Jika berhasil, lanjut ke langkah berikutnya.
Langkah 4: Setelah berhasil memindai QR Code, lakukan registrasi perangkat dengan menghasilkan kunci publik dan privat. Simpan informasi registrasi

seperti Public Key User, UUID, UserID, Device ID, QRCode ke database FIDO, dan simpan QRCode dan UserID ke database utama.

Langkah 5: Pengguna melakukan perekaman wajah dan diminta untuk memverifikasi wajah. Bandingkan wajah di perekaman dengan data wajah yang akan diverifikasi.

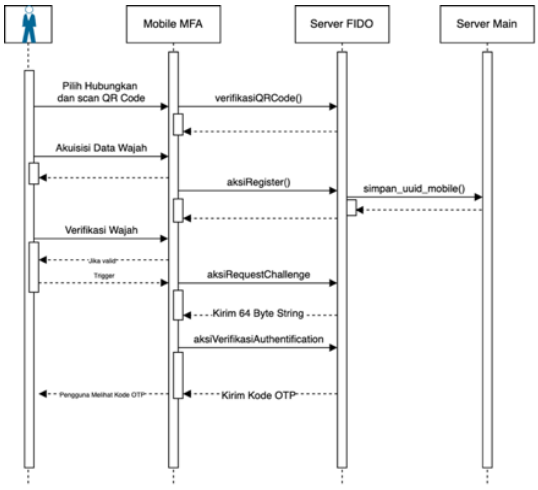
Langkah 6: Jika wajah cocok, Server FIDO memverifikasi tanda tangan digital berdasarkan tantangan yang diberikan dan menghasilkan *One-Time Password* (OTP) dari FIDO. Simpan *hash* OTP di database FIDO dan kirim OTP terenkripsi dengan kunci publik pengguna yang disimpan di Database FIDO ke perangkat. Tampilkan Kode OTP di perangkat dengan melakukan dekripsi menggunakan kunci privat.

Terakhir dalam Sequence Diagram terdapat contoh objek dan pesan yang berinteraksi di antara objek-objek tersebut. Diagram urutan yang ditampilkan pada Gambar 6 dan Gambar 7 mencakup jalannya proses pengguna dimulai dari tahap login di web sampai proses mendapatkan Kode OTP dan masuk ke aplikasi.



Sumber: (Hasil Penelitian, 2024)

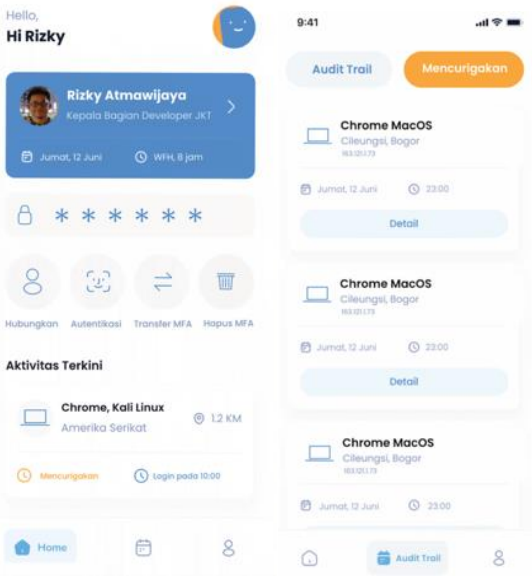
Gambar 6. Sequence Diagram di Web



Sumber: (Hasil Penelitian, 2024)

Gambar 7. Sequence Diagram di Mobile

Desain antarmuka pada aplikasi mobile MFA ini meliputi halaman beranda dan audit trail. Desain dibuat menggunakan *Affinity Designer* seperti yang ditampilkan pada Gambar 8.



Sumber: (Hasil Penelitian, 2024)

Gambar 8. Desain UX Mobile MFA

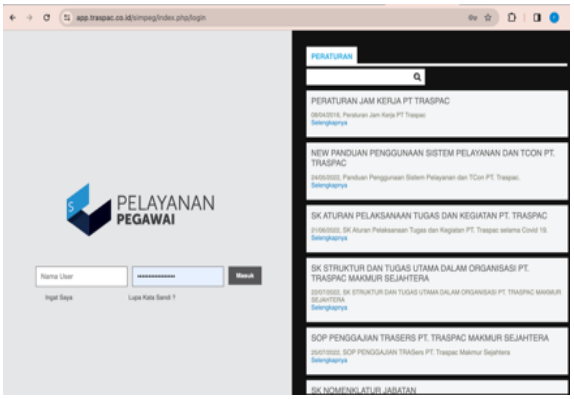
Pengguna memulai dengan mengaitkan akun MFA mereka dengan aplikasi web, melibatkan pemindaian QR Code setelah memasukkan username dan password. Proses ini melibatkan pertukaran data antara server dan perangkat mobile MFA, termasuk informasi seperti device id, UUID, publik key, dan lainnya. Setelah hubungan berhasil, perangkat mobile MFA siap digunakan untuk autentikasi. Ketika pengguna mengakses akun di aplikasi web, aplikasi mobile MFA terlibat dalam autentikasi tambahan. Pengguna diminta untuk melakukan autentikasi wajah pada perangkat mobile MFA, dan setelah berhasil, kode OTP (*One-Time Password*) muncul secara otomatis di aplikasi mobile, memberikan lapisan keamanan tambahan.

Selain fungsional MFA, pada Gambar 8 menampilkan informasi seperti nama, jabatan, foto profil, dan informasi terakhir pelaporan pekerjaan harian. Ini dikembangkan untuk memenuhi kebutuhan yang dijelaskan dalam rancangan *use case* sebelumnya.

C. Implementasi

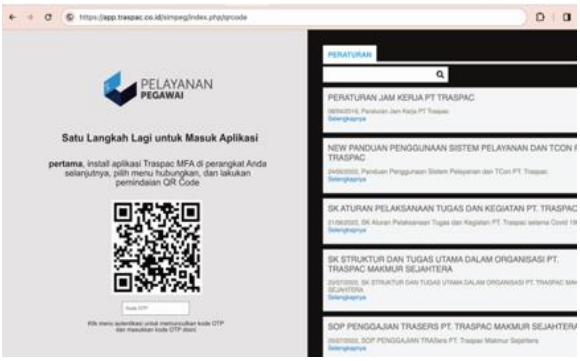
Tahap ini akan menampilkan hasil implementasi aplikasi ke dalam lingkungan PT. Traspac Makmur Sejahtera. Langkah-langkah ini mencakup presentasi mengenai hasil uji coba penggunaan aplikasi oleh pengguna. Pada Gambar 9 terdapat implementasi bagian autentikasi yaitu menu login pada Aplikasi Kepegawaian.

VOL. 19. NO. 1 AGUSTUS 2024
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Universitas Nusa Mandiri



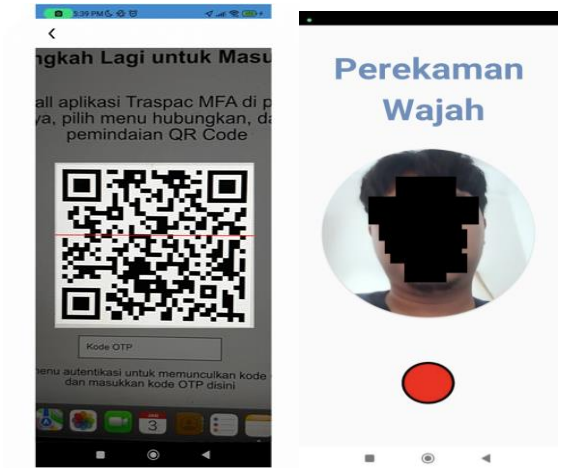
Sumber: (Hasil Penelitian, 2024)
Gambar 9. Halaman Login Aplikasi Kepegawaian

Sedangkan pada Gambar 10 menampilkan tahapan untuk registrasi perangkat dengan QR Code dan muncul inputan kode OTP di bawahnya.



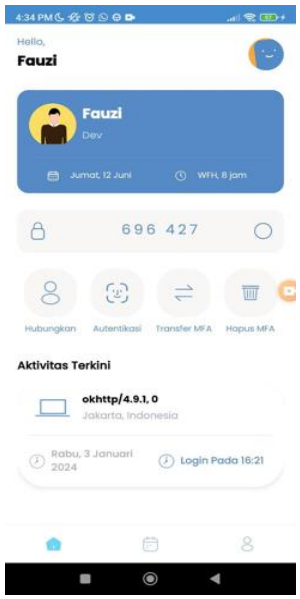
Sumber: (Hasil Penelitian, 2024)
Gambar 10. Halaman Login Aplikasi Kepegawaian

Kemudian pengguna melakukan registrasi perangkat dengan memindai kode QR Code tersebut melalui aplikasi Traspac MFA seperti terlihat pada Gambar 11.



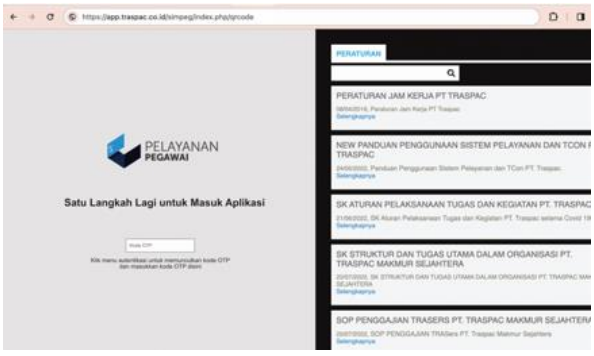
Sumber: (Hasil Penelitian, 2024)
Gambar 11. Scan QR dan Perekaman Wajah

Setelah perekaman data wajah, pengguna mengklik menu "autentikasi" di beranda. Jika verifikasi wajah berhasil, kode OTP muncul di halaman beranda dengan informasi waktu tersisa sebelum kadaluarsa. Pada Gambar 12 menampilkan kode OTP yang tampil setelah proses autentikasi berhasil.



Sumber: (Hasil Penelitian, 2024)
Gambar 12. Proses Setelah Autentikasi Wajah Berhasil

Pengguna hanya perlu memasukan kode OTP pada aplikasi web dan jika berhasil akan masuk ke aplikasi kepegawaian. Setelah fase registrasi perangkat dilalui selanjutnya di tampilan web pada Gambar 13 hanya menampilkan inputkan kode OTP.



Sumber: (Hasil Penelitian, 2024)
Gambar 13. Fase Autentikasi pada Web

C. Testing

Tahap pengujian ini telah dilakukan dengan menggunakan metode *black box testing*, *unit* dan *integration testing*, serta UAT dengan 6 responden karyawan PT. Traspac Makmur Sejahtera.

VOL. 19. NO. 1 AGUSTUS 2024
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Universitas Nusa Mandiri

INTI NUSA MANDIRI
DOI: https://doi.org/10.33480/inti.v19i1.5263

Pengujian ini dilakukan untuk mengukur kinerja autentikasi pengenalan wajah dengan berbagai skenario *test*. Mulai dari *test spoofing*, wajah salah, wajah benar dengan berbagai kondisi seperti pose, ekspresi, dan pencahayaan. Hasil pengujian dengan *black box* testing sesuai harapan. Pada pengujian ini dilakukan penghitungan *detection rate anti-spoofing* dan FAR (*False Accept Rate*) *Spoofing* seperti pada Tabel 1.

Tabel 1. Kompilasi UAT untuk *Detection Rate*

No	Tugas Pengujian	Gagal (*Anti-Spoofing*)	Gagal (Tidak Sah)	*False Accept* (Sah)
1	*Testing* Wajah yang muncul di monitor laptop	18	5	0
2	*Testing* Wajah yang muncul di HP	7	10	3
	Total	**25**	**15**	**3**

Sumber: (Hasil Penelitian, 2024)

$$\textit{Detection Rate} = \frac{Gagal\ (Anti-Spoofing)}{(Total\ Percobaan)} \times 10 \qquad (1)$$

$$\textit{Detection Rate} = \frac{25}{25+15+3} \times 100 \approx 58.14\ \%$$

Rumus: $$\text{FAR} = \frac{False\ Accept\ \ (Sah)}{(Total\ Percobaan)} \times 100$$

$$\text{FAR } \textit{Spoofing} = \frac{3}{25+15+3} \times 100 \approx 6.98\ \%$$

Sistem *anti-spoofing* dalam penelitian ini memiliki *Detection Rate* sebesar 58.14%, artinya algoritma berhasil menolak serangan sebanyak itu. Meski demikian, keamanan belum mencapai tingkat yang memadai. Sementara itu, tingkat keberhasilan serangan spoofing pada laptop dan handphone mencapai 6.98%.

Diperlukan Tingkat Penerimaan Palsu atau *False Accept Rate* (FAR) dari pengujian "Wajah Salah" seperti pada Tabel 2.

Tabel 2. Kompilasi UAT untuk FAR Wajah Salah

No	Pengguna	Merek HP	Masuk	Gagal
1	Ibnu	Xiaomi Poco MS	2	3
2	Fauzi	Sony Xperia	0	3
3	Kimi	Infinix Hot	0	1
4	Bendi	Xiaomi Poco X3 PRO	0	2
5	Raka	Infinix Hot	0	5
6	Alvio	Vivo 1918	0	6
	Total		**2**	**20**

Sumber: (Hasil Penelitian, 2024)

$$\text{FAR} = \frac{Kasus\ Masuk}{Kasus\ Masuk + Kasus\ Gagal} \times 100 \qquad (2)$$

$$\text{FAR} = \frac{2}{2+20} \times 100 \approx 9.09\ \%$$

Sistem menerima wajah yang seharusnya ditolak sebanyak 9.09%, tetapi hasilnya tidak sepenuhnya akurat karena ketidakseimbangan sampel pengujian. Pada Tabel 3 dilakukan penghitungan nilai *True Accept Rate* (TAR) keseluruhan, mempertimbangkan dampak penolakan *Anti-Spoofing* dari input data wajah yang benar.

Tabel 3. Kompilasi UAT untuk TAR Keseluruhan

No	Pengguna	Merek HP	Masuk	Gagal
1	Ibnu	Xiaomi Poco MS	8	10
2	Fauzi	Sony Xperia	9	7
3	Kimi	Infinix Hot	8	4
4	Bendi	Xiaomi Poco X3 PRO	8	16
5	Raka	Infinix Hot	10	7
6	Alvio	Vivo 1918	4	16
	Total		**47**	**60**

Sumber: (Hasil Penelitian, 2024)

$$\text{TAR} = \frac{Kasus\ Masuk}{Kasus\ Masuk + Kasus\ Gagal} \times 100 \qquad (3)$$

$$\text{TAR} = \frac{47}{47+60} \times 100 \approx 43.93\ \%$$

Tingkat Akurasi ini bisa dipengaruhi banyak faktor seperti *intra-personal variations* (perubahan ekspresi, pose dan kondisi pencahayaan), keragaman *device camera* yang digunakan pengguna, dan faktor lainnya seperti *anti-spoofing* dan lain-lain. Berdasarkan hasil pengukuran akurasi ini, tingkat akurasi TAR keseluruhan masih belum bisa memadai, akan tetapi cukup jika kondisi pencahayaan terang.

KESIMPULAN

Hasil penelitian menunjukkan bahwa layanan digital online rentan terhadap serangan siber tanpa autentikasi multi-faktor (MFA). Solusi diusulkan dengan MFA menggunakan teknologi pengenalan wajah FaceNet, namun potensi risiko privasi dapat diatasi dengan implementasi protokol FIDO. Pengguna melakukan verifikasi wajah secara lokal, sementara server memverifikasi autentikasi dengan enkripsi kunci publik dan *private*. Dengan MFA empat faktor (pengetahuan, biometrik, kepemilikan, lokasi) dan FIDO, keamanan autentikasi ditingkatkan sambil menjaga privasi biometrik. Sistem *anti-spoofing* dalam sistem usulan ini memiliki *Detection Rate* sebesar 58.14%, sementara tingkat keberhasilan serangan *spoofing* pada laptop dan *handphone* mencapai 6.98%. Pengujian juga mencatat Tingkat Penerimaan Palsu sebesar 9.09% dari sampel pengujian "Wajah Salah." Meskipun demikian, nilai *True Accept Rate* (TAR) keseluruhan sistem mencapai 43.93%, dengan akurasi yang

VOL. 19. NO. 1 AGUSTUS 2024
P-ISSN: 0216-6933 | E-ISSN: 2685-807X
Diterbitkan Oleh: LPPM Universitas Nusa Mandiri

dipengaruhi oleh berbagai faktor seperti variasi intra-personal dan perbedaan perangkat kamera. Untuk saran penelitian kedepan, tingkat akurasi bisa ditingkatkan baik dalam kondisi pencahayaan gelap, terang dan perubahan ekspresi wajah.

REFERENSI

Ali, G. (2023). *Development of a secure multi-factor authentication algorithm for mobile money applications*. https://dspace.nm-aist.ac.tz/handle/20.500.12479/2210

Anthony, P., Ay, B., & Aydin, G. (2021). A review of face anti-spoofing methods for face recognition systems. *2021 International Conference on INnovations in Intelligent SysTems and Applications, INISTA 2021 - Proceedings*. https://doi.org/10.1109/INISTA52262.2021.9548404

Arman, S. M., Yang, T., Shahed, S., Mazroa, A. Al, Attiah, A., & Mohaisen, L. (2024). A Comprehensive survey for privacy-preserving biometrics: Recent approaches, challenges, and future directions. *Computers, Materials and Continua*, *78*(2), 2087–2110. https://doi.org/10.32604/cmc.2024.047870

Baig, A. F., & Eskeland, S. (2021). Security, privacy, and usability in continuous authentication: A survey. In *Sensors* (Vol. 21, Issue 17). MDPI. https://doi.org/10.3390/s21175967

Cahyono, F. (2020). Pengenalan Wajah Menggunakan Model Facenet Untuk Presensi Pegawai (Doctoral dissertation, Institut Teknologi Sepuluh Nopember).

Feng, H., Li, H., Pan, X., & Zhao, Z. (2021). A Formal Analysis of the FIDO UAF Protocol. *28th Annual Network and Distributed System Security Symposium, NDSS 2021*. https://doi.org/10.14722/ndss.2021.24363

Jin, R., Li, H., Pan, J., Ma, W., & Lin, J. (2021). *Face Recognition Based on MTCNN and FaceNet*. www.aaai.org

Kim, H., Lee, D., & Ryou, J. (2020). User Authentication Method using FIDO based Password Management for Smart Energy Environment. *2020 International Conference on Data Mining Workshops (ICDMW)*, 707–710. https://doi.org/10.1109/ICDMW51313.2020.00100

Klieme, E., Wilke, J., Dornick, N. van, & Meinel, C. (2020). FIDOnuous: A FIDO2/WebAuthn Extension to Support Continuous Web Authentication. *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 1857–1867. https://doi.org/10.1109/TrustCom50675.2020.00254

Maheswari, V., Sari, C. A., Setiadi, D. R. I. M., & Rachmawanto, E. H. (2020). Face Recognition using FaceNet (Survey, Performance Test, and Comparison). *Proceedings - 2020 International Seminar on Application for Technology of Information and Communication: IT Challenges for Sustainability, Scalability, and Security in the Age of Digital Disruption, ISemantic 2020*, 55–60. https://doi.org/10.1109/iSemantic50169.2020.9234250

Meden, B., Rot, P., Terhorst, P., Damer, N., Kuijper, A., Scheirer, W. J., Ross, A., Peer, P., & Struc, V. (2021). Privacy-Enhancing Face Biometrics: A Comprehensive Survey. *IEEE Transactions on Information Forensics and Security*, *16*, 4147–4183. https://doi.org/10.1109/TIFS.2021.3096024

Ming, Z., Visani, M., Luqman, M. M., & Burie, J. C. (2020). A survey on anti-spoofing methods for facial recognition with rgb cameras of generic consumer devices. In *Journal of Imaging* (Vol. 6, Issue 12). MDPI. https://doi.org/10.3390/jimaging6120139

Otta, S. P., Panda, S., Gupta, M., & Hota, C. (2023). A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure. *Future Internet*, *15*(4). https://doi.org/10.3390/fi15040146

Taskiran, M., Kahraman, N., & Erdem, C. E. (2020). Face recognition: Past, present and future (a review). In *Digital Signal Processing: A Review Journal* (Vol. 106). Elsevier Inc. https://doi.org/10.1016/j.dsp.2020.102809

Wang, Q., & Wang, D. (2023). Understanding Failures in Security Proofs of Multi-Factor Authentication for Mobile Devices. *IEEE Transactions on Information Forensics and Security*, *18*, 597–612. https://doi.org/10.1109/TIFS.2022.3227753

Xin, T. Y., Katuk, N., & Arif, A. S. C. M. (2021). Smart Home Multi-Factor Authentication Using Face Recognition and One-Time Password on Smartphone. *International Journal of Interactive Mobile Technologies*, *15*(24), 32–48. https://doi.org/10.3991/IJIM.V15I24.25393