Rancang Bangun Sistem Keamanan Pemetaan Situasi Menggunakan Metode MFA (*Multi-Factor Authentication*) Berbasis Biometrik Sidik Jari

Gabriel Bilthon Nikijuluw[1)], Gatut Yulisusianto [2)] Muhammad Ridwan[3)]
[1), 2), 3)]Prodi Teknik Telekomunikasi Militer. Politeknik Angkatan Darat
Jl.Raya Anggrek No.1 Junrejo, Batu, Indonesia
E - mail : propagasi30@gmail.com[1)], mr.gatut@gmail.com[2),]
ridwan.mtte20@gmail.com[3)]

Situation Mapping Security System Design Using the MFA (Multi-Factor Authentication) Method Fingerprint Biometric Based

Abstract: *Current situation mapping security systems are often vulnerable to illegal access and misuse of data. This research proposes the design of a stronger security system using the Multi-Factor Authentication (MFA) method based on fingerprint biometrics. The main objective of this research is to improve access validation and data integrity in situation mapping systems. By combining multiple authentication factors, the system is designed to minimize the risk of unauthorized access and ensure that only verified users can access sensitive information. This research uses an object-oriented system development (OOD) methodology with an iterative and incremental approach. Fingerprint biometrics are integrated as a second factor in the authentication process, after the user enters standard credentials (username and password). Fingerprint data is encrypted and stored securely in a database. System testing is carried out to evaluate system performance and reliability in various usage scenarios.Test results show that the fingerprint-based MFA system has succeeded in significantly increasing the level of security. The system response time in the authentication process is also relatively fast and efficient. This system provides a reliable and practical security solution for situation mapping systems, and has the potential to be implemented in various other applications that require a high level of security. This research makes an important contribution to the development of safer and more reliable security systems.*
Keywords*: MFA, Fingerprint biometrics, Security system, Situation mapping*

Abstrak: Sistem keamanan pemetaan situasi saat ini seringkali rentan terhadap akses ilegal dan penyalahgunaan data. Penelitian ini mengusulkan rancangan sistem keamanan yang lebih kuat menggunakan metode *Multi-Factor Authentication* (MFA) berbasis biometrik sidik jari. Tujuan utama penelitian ini adalah untuk meningkatkan validasi akses dan integritas data dalam sistem pemetaan situasi. Dengan menggabungkan beberapa faktor autentikasi, sistem ini dirancang untuk meminimalkan risiko akses tidak sah dan memastikan bahwa hanya pengguna terverifikasi yang dapat mengakses informasi sensitif. Penelitian ini menggunakan metodologi pengembangan sistem berorientasi objek (OOD) dengan pendekatan iteratif dan inkremental. Biometrik sidik jari diintegrasikan sebagai faktor kedua dalam proses otentikasi, setelah pengguna memasukkan kredensial standar (nama pengguna dan kata sandi). Data sidik jari dienkripsi dan disimpan dengan aman dalam database. Pengujian sistem dilakukan untuk mengevaluasi kinerja dan keandalan sistem dalam berbagai skenario penggunaan. Hasil pengujian menunjukkan bahwa sistem MFA berbasis sidik jari berhasil meningkatkan tingkat keamanan secara signifikan. Waktu respon sistem dalam proses autentikasi juga relatif cepat dan efisien. Sistem ini memberikan solusi keamanan yang andal dan praktis untuk sistem pemetaan situasi, serta berpotensi untuk diimplementasikan pada berbagai aplikasi lain yang memerlukan tingkat keamanan tinggi. Penelitian ini memberikan kontribusi penting terhadap pengembangan sistem keamanan yang lebih aman dan andal.
Kata kunci: MFA, Biometrik Sidik Jari, Sistem Keamanan, Pemataan Situasi

PENDAHULUAN

Keamanan digital merupakan isu yang semakin krusial di era informasi saat ini.[1] Dengan perkembangan teknologi yang cepat, terutama dalam sistem pemetaan situasi yang digunakan untuk memantau kondisi tertentu, kompleksitas ancaman di dunia siber juga semakin meningkat. Sistem pemetaan situasi, yang banyak diterapkan di bidang keamanan militer, menghadapi tantangan signifikan akibat ancaman akses tidak sah yang terus berkembang.

Selain itu, dalam beberapa tahun terakhir, frekuensi serangan siber telah meningkat secara drastis.[1] Kelemahan yang melekat dalam metode autentikasi tradisional, umumnya bergantung pada kombinasi username dan password, membuka peluang besar bagi penyerang untuk mengeksploitasi akses tidak sah. Fenomena ini menunjukkan betapa rentannya pengguna terhadap potensi penipuan dan kerugian yang dapat merugikan individu maupun organisasi.

Menyadari urgensi permasalahan ini, terdapat kebutuhan mendesak untuk mengembangkan dan menerapkan mekanisme autentikasi yang lebih kuat. Dalam hal ini, teknologi keamanan modern seperti Multi-Factor Authentication (MFA) berbasis biometrik sidik jari telah muncul sebagai salah satu solusi yang menjanjikan. Dengan mengintegrasikan beberapa faktor identifikasi, MFA tidak hanya meningkatkan lapisan keamanan tetapi juga memberikan proteksi tambahan yang sulit ditembus oleh penyerang.[2] Sidik jari, sebagai salah satu metode biometrik, menawarkan tingkat keamanan yang tinggi berkat sifat unik masing-masing individu, sehingga sulit untuk dipalsukan. Implementasi MFA berbasis biometrik sidik jari dalam sistem pemetaan situasi diharapkan dapat menjaga integritas data dan identitas pengguna, serta menciptakan lingkungan digital yang lebih aman.

Namun, tantangan tetap ada dalam pengembangan sistem keamanan berbasis MFA dan biometrik. Permasalahan perlindungan data biometrik yang rawan disalahgunakan, kebutuhan akan kompatibilitas dengan perangkat keras yang beragam, dan kebutuhan untuk menemukan keseimbangan antara keamanan dan kenyamanan pengguna merupakan beberapa isu yang perlu diselesaikan. Oleh karena itu, penelitian ini bertujuan untuk merancang dan membangun sistem keamanan pemetaan situasi menggunakan MFA berbasis biometrik sidik jari. Diharapkan hasil dari penelitian ini dapat meningkatkan keamanan akses serta mengurangi risiko penyalahgunaan data, yang pada gilirannya dapat menjadi referensi berharga untuk pengembangan sistem keamanan yang lebih efisien di masa mendatang.

Melalui kajian ini, peneliti dapat mengidentifikasi posisi penelitian yang akan dilakukan serta mengumpulkan informasi yang relevan untuk mendukung argumen dan temuan yang akan dihasilkan.

Berdasarkan penelitian berjudul “Decentralized Identity Authentication Mechanism: Integrating FIDO and Blockchain for Enhanced Security,” hasil penelitian menunjukkan bahwa kerangka kerja autentikasi identitas yang dikembangkan dengan menggabungkan FIDO2 dan teknologi blockchain merupakan solusi yang aman dan efisien. Kerangka ini menawarkan beberapa keunggulan, seperti pengurangan biaya pembuatan sistem dan kemudahan dalam pengelolaan izin karena semua izin dapat dikelola melalui blockchain, bukan satu per satu. Selain itu, dengan integrasi metode Access Control List (ACL), kerangka ini meningkatkan keamanan dan fungsionalitas autentikasi identitas. Penelitian ini juga menunjukkan bahwa sistem ini dapat beroperasi dengan baik dalam praktik. Untuk penelitian ke depan, disarankan untuk mengeksplorasi penggunaan arsitektur Passkey, yang dapat memberikan pengalaman login yang lebih mudah dan fleksibel bagi pengguna. Namun, sebelum menerapkan teknologi ini, sangat penting untuk melakukan evaluasi dan pengujian yang menyeluruh untuk memastikan bahwa sistem tetap aman dan dapat diandalkan.[3]

Dalam penelitian lain, mengkaji tentang " Enhanced Cloud Computing Security Using Application-Based Multi-Factor Authentication (MFA) for Communication Systems ". Hasil penelitian menunjukkan bahwa layanan digital online rentan terhadap serangan siber tanpa penerapan autentikasi multi-faktor (MFA). Solusi yang diusulkan adalah penggunaan MFA yang mengintegrasikan teknologi pengenalan wajah FaceNet, dengan penanganan potensi risiko privasi melalui implementasi protokol FIDO. Dalam metode ini, pengguna melakukan verifikasi wajah secara lokal, sedangkan server melakukan verifikasi autentikasi menggunakan enkripsi kunci publik dan privat. Dengan menggunakan MFA yang terdiri dari empat faktor (pengetahuan, biometrik, kepemilikan, lokasi) dipadukan dengan FIDO, keamanan autentikasi dapat ditingkatkan sambil tetap menjaga privasi data biometrik. Sistem anti-spoofing yang diusulkan menunjukkan Detection Rate sebesar 58,14%, sedangkan tingkat keberhasilan serangan spoofing pada perangkat laptop dan handphone mencapai 6,98%. Pengujian menunjukkan adanya Tingkat Penerimaan Palsu sebesar 9,09% dari sampel pengujian "Wajah Salah." Meskipun demikian, nilai True Accept Rate (TAR) keseluruhan sistem adalah 43,93%, dengan akurasi yang dipengaruhi oleh berbagai faktor, termasuk variasi intra-personal dan perbedaan jenis perangkat kamera. Untuk penelitian yang akan datang, disarankan agar tingkat akurasi dapat ditingkatkan dalam berbagai kondisi pencahayaan, baik di lingkungan gelap maupun terang, serta dalam menghadapi perubahan ekspresi wajah.[4]

Selanjutnya, penelitian yang berjudul "You still use the password after all - Exploring FIDO2 Security Keys in a Small Company". Hasil penelitian penelitian ini, penulis menganalisis bagaimana komponen inti FIDO2, yaitu WebAuthn dan CTAP, dapat menjadi alternatif yang lebih aman dibandingkan skema autentikasi tradisional berbasis nama pengguna dan kata sandi yang umum digunakan. Kunci keamanan FIDO2, yang berbentuk token perangkat keras berbasis USB, dijelaskan sebagai faktor autentikasi yang kuat dan tahan terhadap serangan phishing, sehingga cocok untuk meningkatkan keamanan aplikasi web. Studi ini menyoroti bahwa sementara kebanyakan peserta menemukan penggunaan kunci keamanan itu praktis, beberapa dari mereka memilih untuk tidak terus menggunakan kunci tersebut karena kecepatan login yang lebih lambat dibandingkan dengan pengelola kata sandi yang sudah mereka gunakan di peramban mereka. Selain itu, banyak manfaat keamanan yang diharapkan dari kunci keamanan dianggap tidak terwujud atau tidak terlalu penting bagi pengguna. Kesulitan lain adalah kurangnya dukungan dari beberapa peramban dan sistem operasi saat studi ini dilakukan, yang menghalangi adopsi yang lebih luas. Sebagai kesimpulan, jurnal ini menunjukkan bahwa dalam rangka menggantikan metode autentikasi berbasis nama pengguna dan kata sandi dengan FIDO2, perlu ada upaya untuk mengatasi berbagai hambatan adopsi ini supaya kunci keamanan dapat diterima dan diterapkan secara efektif di perusahaan.[5]

Sistem keamanan informasi adalah aspek yang sangat vital dalam era digital saat ini, di mana data berfungsi sebagai aset berharga bagi organisasi dan individu. Perlindungan terhadap informasi sangat penting untuk mencegah ancaman siber yang dapat merugikan reputasi, kepercayaan pengguna, dan integritas data. Oleh karena itu, investasi dalam sistem keamanan yang handal bukan hanya menjadi kebutuhan, tetapi juga merupakan langkah strategis untuk memastikan keberlangsungan dan keamanan di dunia yang semakin terhubung.[6] Kerahasiaan data pengguna adalah upaya perlindungan terhadap informasi sensitif agar hanya dapat diakses oleh pihak yang berwenang. Menjaga kerahasiaan ini sangat penting karena informasi merupakan aset yang berharga dalam Keamanan Sistem Informasi, dan kebocoran data dapat mengakibatkan kerugian finansial, reputasi, serta kepercayaan pengguna. Dengan memastikan kerahasiaan data, organisasi dapat melindungi diri dan penggunanya

dari potensi risiko dan ancaman yang merugikan [7].

Keamanan database melibatkan serangkaian tindakan untuk memastikan bahwa data hanya tersedia bagi pihak yang berwenang, dan tidak dapat diakses oleh pihak yang tidak berwenang. Keterjangkauan data bagi pengguna yang memiliki hak akses adalah kunci untuk menjaga integritas dan keamanan informasi sensitif [8]. Ancaman Terhadap Keamanan Informasi merupakan tindakan yang memanfaatkan kerentanan untuk merusak keamanan sistem informasi atau infrastruktur teknologi, sehingga berdampak negatif pada elemen tertentu dari sistem tersebut [9]. Data pribadi merupakan informasi yang dapat mengidentifikasi individu secara unik, termasuk nama, alamat, nomor telepon, alamat email, kesehatan, dan data keuangan. Informasi ini memiliki nilai penting untuk berbagai tujuan, mulai dari layanan personalisasi hingga analisis selanjutnya, keberadaannya dalam sistem digital menciptakan peluang inovasi serta peningkatan efisiensi di berbagai sektor.

Selain itu, data pribadi juga mencakup aspek lain dari identitas seseorang, seperti usia, jenis kelamin, latar belakang pendidikan, pekerjaan, dan posisi dalam keluarga [10]. Di era digital saat ini, data pribadi menjadi salah satu aset yang paling berharga, dan kehilangan atau penyalahgunaannya dapat mengakibatkan konsekuensi yang fatal. Oleh karena itu, penelitian ini bertujuan untuk mengidentifikasi risiko yang ada serta memberikan rekomendasi strategis untuk meminimalkan ancaman tersebut. Hal ini dapat dilihat dari kasus di Desa Donowarih, Jawa Timur, di mana data pribadi warga dimanfaatkan secara tidak benar untuk penipuan online [11]. Pentingnya melindungi data pribadi di era digital sangatlah krusial, terutama ketika melihat Studi Kasus Desa Pematang Jering yang mencerminkan tantangan keamanan digital yang dihadapi oleh masyarakat desa di seluruh Indonesia. Penelitian ini bertujuan untuk memberikan kontribusi nyata dalam meningkatkan literasi digital dan keamanan data pribadi, sehingga masyarakat dapat lebih merasa aman dan terlindungi saat menggunakan media sosial [12]. "Karena semua data disimpan secara digital, pengguna tidak perlu khawatir kehilangan sertifikat selama proses validasi."Kalimat ini mempertahankan makna asli namun dengan sedikit perbaikan pada struktur untuk meningkatkan kelancaran baca [13].

Di era digital yang terus berkembang, kebutuhan akan sistem keamanan informasi yang handal dan efektif semakin mendesak.[14] Semakin kompleksnya ancaman siber dan meningkatnya ketergantungan pada teknologi informasi membuat organisasi, perusahaan, dan individu rentan terhadap serangan peretas, pencurian data, dan pelanggaran privasi. Konsep dasar keamanan sistem informasi mencakup beberapa komponen penting :

(1) Kerangka Kerja Keamanan
Keamanan sistem informasi memerlukan pendekatan yang terstruktur dan sistematis, yang dikenal sebagai kerangka kerja keamanan. Ini mencakup kebijakan, prosedur, dan standar untuk melindungi aset informasi.

(2) Tiga Pilar Keamanan

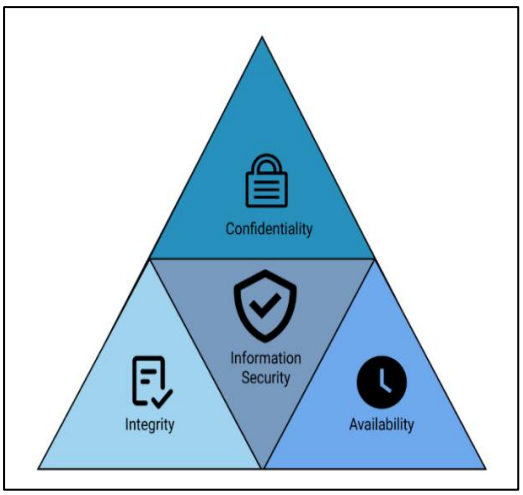
Gambar 1. CIA TRIAD

Tiga pilar utama keamanan informasi dikenal dengan istilah "CIA Triad," yang terdiri dari :

a) Confidentiality (Kerahasian) yaitu melindungi data agar hanya dapat diakses oleh pihak yang berwenang.
b) Integrity (Integritas) yaitu memastikan data tidak dirubah atau dimodifikasi oleh pihak yang tidak berwenang.
c) Availability (Ketersediaan) yaitu memastikan bahwa data dan sistem tersedia dan dapat diakses oleh pengguna yang berhak ketika dibutuhkan.

(3) Ancaman dan Kerentanan
Identifikasi ancaman seperti peretasan, malware, dan serangan phishing, serta kerentanan sistem, adalah langkah awal dalam merancang strategi keamanan. Strategi tersebut harus mencakup

kebijakan keamanan yang ketat,



Gambar 1.1 CIA TRIAD [38]

teknologi terbaru, dan pelatihan kesadaran bagi pengguna.[15]

(4) Kontrol Keamanan
Meliputi langkah-langkah dan teknik yang digunakan untuk melindungi sistem informasi. Ini dapat mencakup pengenalan sistem keamanan fisik, kontrol akses, enkripsi, dan perangkat lunak keamanan.

(5) Pemantauan dan Audit
Pemantauan dan audit sistem secara teratur membantu mengidentifikasi pelanggaran keamanan atau anomali yang dapat menunjukkan potensi ancaman.

Otentikasi Multifaktor (MFA)

Otentikasi Multifaktor (MFA) adalah metode keamanan yang memerlukan pengguna untuk menjalani beberapa langkah verifikasi identitas sebelum mengakses sistem, aplikasi, atau data.[16] MFA menggabungkan faktor otentikasi kategori "sesuatu yang tahu" (seperti kata sandi), "sesuatu yang memiliki" (seperti token fisik), dan "sesuatu yang adalah" (seperti biometrik). Dengan menambahkan lapisan perlindungan ini, MFA meningkatkan keamanan, mengurangi risiko peretasan dan serangan sosial, serta membantu organisasi memenuhi standar keamanan informasi. Selain itu, MFA meningkatkan kepercayaan pengguna terhadap sistem yang aman, mendorong adopsi lebih luas terhadap aplikasi sensitif.[17]

WebAuth (*Web Authentication*)

WebAuth (*Web Authentication*) adalah standar otentikasi yang dikembangkan oleh W3C dan FIDO *Alliance* untuk menyediakan pengalaman autentikasi yang aman dan bebas kata sandi di *web*.[18] Dengan memanfaatkan kunci kriptografi, *WebAuth* memungkinkan aplikasi menggunakan otentikasi multifaktor dan biometrik serta beroperasi di atas protokol FIDO2, yang dirancang untuk mengatasi kelemahan kata sandi tradisional seperti pembobolan akun dan serangan *phishing*. Prosesnya meliputi pendaftaran perangkat autentikasi, di mana sepasang kunci kriptografi dihasilkan; saat login, server mengirim tantangan yang ditandatangani pengguna menggunakan kunci privat, dan tanda tangan tersebut diverifikasi dengan kunci publik yang disimpan. Dengan demikian, *WebAuth* memastikan keamanan tinggi tanpa penggunaan kata sandi, mengandalkan kepemilikan perangkat autentikasi untuk akses.

Biometrik

Biometrik adalah teknologi yang menggunakan karakteristik fisik atau perilaku individu untuk otentikasi, termasuk sidik jari, pengenalan wajah, pemindaian iris, suara, dan pola vena.[19] Sidik jari merupakan salah satu bentuk biometrik paling umum karena pola yang unik untuk setiap individu. Proses otentikasi sidik jariiputi pengambilan gambar sidik jari menggunakan pemindai, ekstraksi fitur biometrik seperti pola garis dan titik bifurkasi, penyimpanan fitur yang diubah menjadi template digital dalam database, dan verifikasi identitas dengan membandingkan sidik jari yang dipindai dengan template yang tersimpan untuk memberikan akses jika ada kecocokan.

Keamanan data di era digital sangat penting karena meningkatnya serangan siber.[20] Integrasi (MFA) dan *WebAuth* FIDO2 menjadi solusi efektif. MFA

memerlukan verifikasi ganda, sedangkan *WebAuth* FIDO2 memungkinkan autentikasi tanpa kata sandi menggunakan kunci fisik atau biometrik. Penggabungan keduanya menciptakan sistem autentikasi yang lebih aman dan mengurangi risiko pencurian identitas.[21]

METODE PENELITIAN

Studi literatur pada sistem ini dilakukan untuk memahami konsep dasar dan teknologi yang mendukung autentikasi berbasis *WebAuthn* dan FIDO2 dalam sistem keamanan pemetaan situasi. Studi ini mencakup tentang standar *WebAuthn* dan FIDO2, autentikasi MFA, serta biometrik sidik jari. Selain itu, akan menganalisis penelitian terdahulu terkait keamanan autentikasi tanpa *password*, *WebAuthn* yang diimplementasikan ke *website*, serta tantangan penggunanya. Pemahaman konsep pada penelitian sebelumnya akan memudahkan untuk mengidentifikasi keunggulan dan keterbatasan *WebAuthn* untuk mengimplementasikan keamanan sistem pemetaan situasi.

Penelitian ini mengeksplorasi integrasi *Multifactor Authentication* (MFA) dan *WebAuthn* FIDO2 untuk meningkatkan keamanan *website* dan aplikasi *mobile*. Metode yang digunakan meliputi pengujian fungsional untuk memastikan fitur bekerja dengan baik, pengujian keamanan untuk mengidentifikasi kerentanan, dan evaluasi fleksibilitas untuk menilai kemudahan penggunaan.

Laporan akhir akan menyajikan analisis, temuan, dan rekomendasi untuk pengembangan lebih lanjut. Penelitian ini bertujuan menjadi referensi untuk meningkatkan sistem keamanan dan kepercayaan pengguna dalam layanan digital.

Dalam penelitian ini, kami menggunakan pendekatan penelitian dan pengembangan *Research and Development* (R&D) dengan tujuan menciptakan sistem keamanan yang inovatif dalam konteks pemetaan situasi. Pendekatan ini diambil untuk menjawab tantangan yang semakin mendesak menjaga keamanan informasi. Di tengah meningkatnya ancaman siber dan kompleksitas serangan, seperti phishing dan malware, penting bagi organisasi dan individu untuk memiliki solusi keamanan yang tidak hanya efektif tetapi juga adaptif terhadap berbagai jenis ancaman yang muncul.

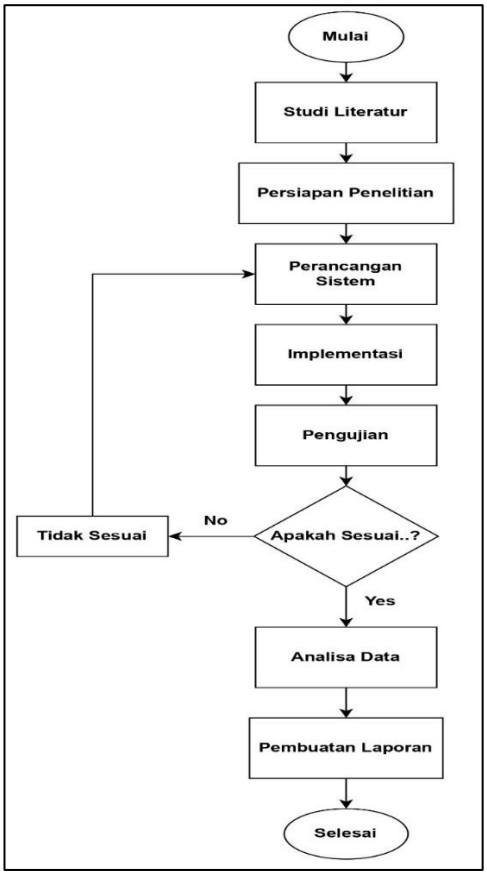
Proses penelitian dimulai dengan melakukan wawancara mendalam dan observasi terhadap pengguna. Lewat wawancara ini, kami berusaha memahami berbagai tantangan yang dihadapi pengguna dalam menjaga keamanan informasi sensitif mereka. Kami tidak hanya mengumpulkan data teknis, tetapi juga menggali preferensi dan kekhawatiran pengguna mengenai fitur-fitur sistem keamanan yang ideal. Observasi langsung di lapangan memberikan gambaran nyata tentang bagaimana pengguna berinteraksi dengan sistem yang ada, dan membantu kami mengidentifikasi potensi risiko serta area yang memerlukan perbaikan.

Menerapkan metode pengembangan sistem *Prototype* untuk menciptakan solusi keamanan informasi yang dapat menyesuaikan dengan kebutuhan pengguna dalam pemetaan situasi, berfokus pada iterasi cepat dan keterlibatan pengguna. Proses dimulai dengan analisis kebutuhan yang melibatkan wawancara, observasi, serta survei untuk mengidentifikasi tantangan dan keinginan pengguna. Selanjutnya, *prototipe* dirancang dengan model arsitektur sistem, antarmuka pengguna yang intuitif, dan desain database yang aman.

Pengembangan dilakukan melalui pengkodean fungsionalitas utama dan integrasi teknologi keamanan, seperti *Multi-Factor Authentication* (MFA). *Prototipe* kemudian diuji untuk menilai fungsionalitas dan keamanan, diikuti dengan revisi berdasarkan umpan balik pengguna. Terakhir, sistem diimplementasikan secara nyata dengan pelatihan pengguna dan pemantauan kinerja berkelanjutan, memastikan sistem selalu *up-to-date* dan aman dari ancaman.

(1) Variabel Terikat

Variabel terikat adalah variabel yang dipengaruhi oleh variabel bebas. Dalam penelitian ini,abel terikat meluti:



a) Tingkat keamanan sistem (Keamanan mencegah akses tidak sah)
b) Kemudahan dan kepuasan pengguna saat melakukan autentikasi.
c) Waktu autentikasi (Kemudahan pengguna terhadap perjalanan autentikasi)

(2) Variabel Bebas

Variabel bebas atau variabel independen merupakan variabel yang berdiri sendiri tanpa dipengaruhi oleh variabel lainnya. Variabel bebas dapat dikatakan sebagai variabel pengaruh karena akan memberikan pengaruh terhadap variabel lainnya. Adapun variabel bebas dari penelitian ini adalah :

a) Metode autentikasi yang digunakan mengintegrasikan *WebAuthn* dengan MFA berbasis sidik jari, memberikan keamanan yang jauh lebih baik dibandingkan metode tradisional yang hanya menggunakan kata sandi.
b) Penggunaan *WebAuthn* FIDO2 yaitu penerapan autentikasi tanpa kata sandi melalui biometrik dan kunci keamanan.
c) Penggunaan perangkat keras tambahan tidak atau tanpa kunci keamanan fido2

Gambar 2. Diagram Alir Penelitian

Diagram alir adalah representasi grafis langkah-langkah prosedur dalam suatu program untuk memudahkan pemahaman alat. Proses penelitian dimulai dari tahap Mulai, di mana peneliti merumuskan pertanyaan, lalu dilanjutkan dengan Studi Literatur untuk mengumpulkan informasi. Pada tahap Persiapan Penelitian, peneliti merancang rencana pengumpulan data. Selanjutnya, pada tahap Perancangan Sistem, sistem dirancang, lalu dilakukan Implementasi untuk pengujian.

Hasil pengujian dievaluasi, dan jika sesuai, peneliti melanjutkan ke Analisa Data. Penelitian diakhiri di tahap Selesai, dengan laporan hasil yang diarsipkan dan dipublikasikan, bertujuan menghasilkan temuan yang *valid* dan berkontribusi pada ilmu pengetahuan.

Perancangan Sistem

Sistem yang diusulkan didesain terintegrasi dengan beberapa komponen yang secara umum dapat dikategorikan sebagai sistem keamanan pemetaan situasi menggunakan MFA berbasis biometrik sidik jari.

(1) Pengguna Mengakses Halaman Login

Proses login dimulai ketika pengguna membuka aplikasi atau situs web yang telah dilengkapi dengan fitur keamanan canggih. Ketika halaman login muncul, pengguna akan disajikan dengan antarmuka yang bersih dan mudah digunakan, yang terdiri dari dua kolom input: satu kolom untuk nama pengguna (username) dan satu kolom untuk kata sandi (password). Desain halaman ini mencakup elemen-elemen visual yang

mendukung pengalaman pengguna, seperti logo aplikasi atau pesan pengantar yang menyatakan tujuan login. Ini membantu menciptakan suasana aman dan ramah pengguna

(2) Pengisian Username dan Password
Pada halaman login, pengguna diminta untuk memasukkan informasi yang relevan untuk akses akun mereka. Di kolom pertama, pengguna harus mengisi nama pengguna yang terdaftar, sementara di kolom kedua, mereka memasukkan kata sandi mereka. Penting bagi pengguna untuk memastikan bahwa kedua informasi ini diisi dengan tepat, karena kesalahan kecil dalam pengetikan dapat mengakibatkan kegagalan proses login. Selain itu, aplikasi memberikan penjelasan tentang pentingnya menggunakan kata sandi yang kuat dan saran untuk tidak membagikannya kepada siapa pun, sehingga meningkatkan keamanan.

(3) Pengiriman Data ke Server
Setelah semua kolom terisi, pengguna klik tombol untuk mengirim data ke server. Sistem menggunakan permintaan HTTP dengan metode POST, yang mengizinkan pengiriman data dengan cara yang aman dan menyembunyikan informasi sensitif dari URL. Dalam permintaan ini, data yang dikirim mencakup nama pengguna dan kata sandi. Pengiriman data berlangsung dalam beberapa detik, dengan pengaturan yang memberi umpan balik visual kepada pengguna, seperti animasi loading atau perubahan warna tombol saat data sedang diproses.

(4) Penerimaan dan Pengolahan Data oleh Server
Begitu server menerima data dari pengguna, langkah pertama yang dilakukan adalah memvalidasi keakuratan data. Server mencocokkan informasi nama pengguna dan kata sandi dengan data yang tersimpan dalam database. Jika validasi berhasil, server kemudian menyiapkan informasi yang dibutuhkan untuk proses otentikasi berikutnya, termasuk instruksi biometrik yang akan digunakan untuk otentikasi sidik jari. Dalam keadaan di mana validasi gagal, server memberikan respons kesalahan yang menjelaskan kesalahan, sehingga pengguna dapat memahami dan memperbaikinya.

(5) Permintaan Otentikasi Biometrik
Setelah server siap, aplikasi akan mengarahkan pengguna untuk menggunakan metode autentikasi sidik jari. Pada langkah ini, teknologi FIDO2 mengambil peran penting dalam menjamin bahwa semua komunikasi antara aplikasi dan server dilakukan dengan aman. Server mengirimkan instruksi yang diperlukan kepada aplikasi tentang cara beralih ke mode input sidik jari, dan aplikasi akan menampilkan antarmuka yang kompatibel untuk proses verifikasi biometrik.

(6) Pengguna Memindai Sidik Jari
Di langkah ini, pengguna diminta untuk melakukan pemindaian sidik jari mereka menggunakan perangkat sensor sidik jari yang terintegrasi dengan perangkat. Antarmuka pengguna memberikan instruksi tentang bagaimana cara memindai sidik jari dengan benar, termasuk posisi jari yang tepat pada sensor. Dengan sensor yang menangkap pola sidik jari, data ini diubah menjadi format digital yang dapat digunakan untuk otentikasi. Teknologi FIDO2 berperan dalam menjaga keamanan data biometrik dengan melindunginya melalui enkripsi, sehingga informasi ini tidak mudah diakses oleh pihak yang tidak berwenang.

(7) Memulai Proses Autentikasi
Setelah sidik jari berhasil dipindai, perangkat akan memulai proses verifikasi menggunakan instruksi dan data biometrik yang telah dikirim sebelumnya dari server. Sistem menggunakan algoritma verifikasi untuk membandingkan data sidik jari yang baru dipindai dengan data yang sudah terdaftar di dalam database. Pada tahap ini, FIDO2 memastikan bahwa semua data yang dikirimkan

dan diterima tetap terjaga kerahasiaannya, sehingga data aman dari upaya penyadapan.

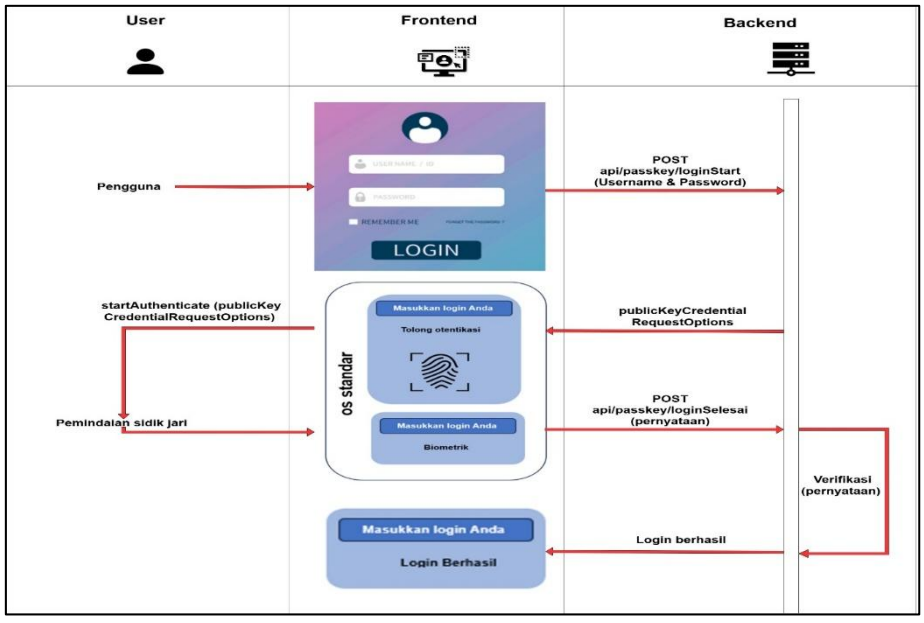
(8) Pengiriman Data Biometrik ke Server
Jika pemindaian sidik jari berhasil dan pengguna memberikan konfirmasi melalui antarmuka aplikasi, data sidik jari yang telah dipindai akan dikirimkan kembali ke server untuk menyelesaikan proses login. Proses pengiriman ini dilakukan melalui permintaan HTTP POST untuk memastikan bahwa informasi sensitif tetap aman dan tidak terlihat di URL. Data ini dikirim melalui endpoint yang diketahui, seperti "loginSelesai," yang siap untuk menerima dan memeriksa informasi biometrik.

(9) Proses Verifikasi di Server
Setelah server menerima data otentikasi sidik jari, server memverifikasi apakah data tersebut sesuai dengan data yang ada dalam sistem. Proses verifikasi ini melibatkan pemeriksaan yang cepat untuk memastikan keakuratan data. Jika sidik jari yang dipindai cocok dengan data yang tersimpan, proses verifikasi dianggap berhasil, dan server bersiap untuk mengirimkan respons positif. Jika tidak, server akan mengirimkan pesan kesalahan yang menjelaskan ketidakcocokan, sehingga pengguna dapat mengulangi proses otentikasi

(10) Pemberitahuan Login Berhasil
Setelah verifikasi berhasil, server akan mengirimkan respons positif kepada aplikasi bahwa pengguna telah berhasil login. Respons ini mencakup token otentikasi yang memberikan akses lebih lanjut ke sistem tanpa perlu login ulang selama sesi itu aktif. Server juga dapat mengirim informasi tambahan yang relevan tentang pengguna, yang memungkinkan aplikasi untuk menyesuaikan pengalaman mereka dengan preferensi pengguna

(11) Tampilan Pemberitahuan Kepada Pengguna
Setelah menerima respons dari server, aplikasi akan menampilkan notifikasi kepada pengguna bahwa proses login mereka telah berhasil. Aplikasi kemudian akan mengarahkan pengguna ke halaman utama atau dashboard, di mana mereka dapat mulai menggunakan fitur dan layanan yang tersedia. Pemberitahuan ini penting untuk memberi tahu pengguna bahwa data mereka tetap aman selama proses autentikasi.

Konsep dari sistem yang diusulkan ditunjukkan pada Gambar 3.



Gambar 3. Alur Sistem

Pengambilan Data

Pengambilan Data Primer yang penulis lakukan yaitu dengan melakukan proses penelitian lapangan dan eksperimen. Dalam konteks penelitian ini, data primer meliputi :

(1) Wawancara dilakukan kepada pengguna kridensial yaitu staff Intelijen kodim mendapatkan kebutuhan sistem, standar keamanan MFA dan pengalaman pengguna menggunakan sidik jari.

Pengambilan Data Sekunder yang penulis lakukan dalam penelitian ini yaitu melakukan proses pengumpulan data informasi dari berbagi macam sumber terpercaya dan yang sudah ada sebelumnya yang dimana sumber ini meliputi sebagai berikut :

(1) Study Literatur yaitu seperti jurnal, artikel ilmiah, laporan tugas akhir, dan buku yang membahas tentang proses autentifikasi dengan menerapkan FIDO2.
(2) Buku Petunjuk Induk mengenai Adminsitrasi Intelijen Militer yang telah disahkan dengan Skep Kasad Nomor Skep/692/VIII/2018 tanggal 8 Agustus 2018. Dengan memadukan data primer dan sekunder, peneliti dapat memperoleh pemahaman yang lebih komprehensif tentang topik yang penulis akan teliti, serta meningkatkan kredibilitas dan relevansi dari hasil penelitian
(3) Spesifikasi Yang Diharapkan
Spesifikasi yang diharapkan untuk sistem “Rancang Bangun Sistem Ke Pemetaan Situasi Menggunakan Metode MFA Berbasis Biometrik Sidik Jari” mencakup penerapan keamanan data yang canggih melalui enkripsi biometrik dan autentikasi multifaktor (MFA) menggunakan kombinasi kata sandi dan sidik jari. Sistem ini harus dirancang dengan antarmuka yang intuitif dan menarik, serta memberikan akses penuh sepanjang waktu, serta kompatibel dengan berbagai platform tanpa memerlukan perangkat keras tambahan. Selain itu, perlu ada dokumentasi yang baik dan pelatihan pengguna, disertai dengan fitur pemantauan dan pencatatan aktivitas untuk audit keamanan, sambil memastikan kepatuhan terhadap regulasi perlindungan data yang berlaku.

RELEVANSI

Rancangan sistem keamanan pemetaan situasi yang memanfaatkan metode Multi-Factor Authentication (MFA) dan FIDO2 berbasis biometrik sidik jari memiliki relevansi yang mendalam bagi instansi TNI Angkatan Darat, khususnya pada satuan kewilayahan seperti Komando Rayon Militer (Koramil). Dalam menjaga ketertiban dan keamanan di wilayah teritorial, Koramil menghadapi berbagai tantangan yang kompleks, terutama dalam pengelolaan data dan informasi yang sensitif. Oleh karena itu, penerapan sebuah sistem yang canggih dan terintegrasi seperti ini tidak hanya penting, tetapi juga mendesak untuk meningkatkan efektivitas operasional mereka.

MFA berperan sebagai lapisan keamanan pertama yang mengharuskan pengguna untuk melakukan autentikasi melalui beberapa faktor, terdiri dari username dan password sebagai langkah awal. Dalam dunia digital yang semakin berkembang, metode ini menyediakan perlindungan dasar. Namun, potensi serangan siber masih tetap ada. Di sinilah FIDO2 memasuki peran penting, dengan menawarkan autentikasi berbasis biometrik. Melalui penerapan sidik jari sebagai bentuk otentikasi, sistem ini menambahkan tingkat keamanan yang lain, yang jauh lebih sulit untuk dipalsukan. Sinergi antara MFA dan FIDO2 tidak hanya menawarkan perlindungan yang lebih baik, tetapi juga menciptakan pengalaman pengguna yang lebih intuitif; pengguna cukup melakukan dua langkah autentikasi untuk mendapatkan akses ke informasi kritis.

Keunggulan dari sistem keamanan ini terletak pada kemampuannya untuk mempercepat proses pengambilan keputusan, terutama dalam situasi darurat. Dengan pemetaan situasi yang diintegrasikan, Koramil dapat

mengumpulkan dan menganalisis data dalam waktu nyata. Ini memberi personel Koramil informasi yang diperlukan untuk merespons ancaman, mengelola bencana, atau mengatasi gangguan sosial dengan lebih efektif. Sebagai contoh, selama terjadi bencana alam, akses cepat dan akurat ke informasi dapat memfasilitasi mobilisasi bantuan yang diperlukan dan penyampaian peringatan kepada masyarakat secara efektif.

Lebih jauh, penerapan sistem ini juga menunjukkan komitmen TNI-AD untuk beradaptasi dengan kemajuan teknologi modern. Dalam dunia yang semakin digital, kepercayaan masyarakat terhadap keamanan dan kinerja institusi pemerintahan sangat dipengaruhi oleh transparansi dan akuntabilitas yang mereka tunjukkan. Dengan menggunakan teknologi yang canggih, Koramil dapat membangun hubungan yang lebih kuat dengan masyarakat. Ketika publik melihat bahwa TNI menggunakan metode yang aman dan efisien untuk menjaga keamanan, mereka akan lebih cenderung berpartisipasi aktif dalam mendukung program-program keamanan dan ketertiban.

Secara keseluruhan, rancang bangun sistem keamanan pemetaan situasi yang memanfaatkan MFA dan FIDO2 berbasis biometrik sidik jari bukan hanya merupakan langkah evolusioner dalam menjaga keamanan, tetapi juga merupakan pendekatan strategis yang berorientasi pada masa depan. Dengan kemampuan untuk meningkatkan efektivitas operasional, merespons ancaman secara cepat, dan membangun kepercayaan masyarakat, sistem ini memberikan kontribusi yang signifikan terhadap tugas dan tanggung jawab Koramil dalam menciptakan lingkungan yang aman dan stabil. Melalui inovasi ini, TNI-AD tak hanya melangkah seiring dengan perkembangan teknologi, tetapi juga menjawab tantangan yang ada dengan kepercayaan diri dan kemampuan tingkat tinggi dalam menjaga keamanan nasional.

DAFTAR PUSTAKA

[1] Abdullah Mubarak Lubis, Gladis Jelita, Syafira Okta Vionna Wirya, and Nurbaiti Nurbaiti, “Tantangan dan Keamanan Teknologi Informasi pada Manajemen Bank Syariah,” Switch : Jurnal Sains dan Teknologi Informasi, vol. 3, no. 1, pp. 148–162, Jan. 2025, doi: 10.62951/switch.v3i1.344.

[2] M. Agreindra, H. Yopi, H. Akbar, F. Mahardika, Y. Hidayatul, and A. Link, “Keamanan Teknologi Informasi: Teori, Risiko, dan Strategi Pertahanan di Era Digital,” 2024.

[3] H. H. Ou, C. H. Pan, Y. M. Tseng, and I. C. Lin, “Decentralized Identity Authentication Mechanism: Integrating FIDO and Blockchain for Enhanced Security,” Applied Sciences (Switzerland), vol. 14, no. 9, May 2024, doi: 10.3390/app14093551.

[4] R. Atmawijaya and U. Radiyah, “PERANCANGAN AUTENTIKASI MULTI FAKTOR DENGAN PENGENALAN WAJAH DAN FIDO (FAST IDENTITY ONLINE),” INTI Nusa Mandiri, vol. 19, no. 1, pp. 46–53, Jul. 2024, doi: 10.33480/inti.v19i1.5263.

[5] Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security (SOUPS 2020) : August 10 - 11, 2020,. USENIX Association, 2020.

[6] Victor Benny Alexsius Pardosi, “Bernadete Deta, Fifto Nugroho, dan Arnes Yuli Vandika, SISTEM KEAMANAN INFORMASI,” ISBN: 978-623-8606-34-4, 2024 .

[7] S. Nurul, S. Anggrainy, and S. Aprelyani, “FAKTOR-FAKTOR YANG MEMPENGARUHI KEAMANAN SISTEM INFORMASI: KEAMANAN INFORMASI, TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE REVIEW SIM),” vol. 3, no. 5, 2022, doi: 10.31933/jemsi.v3i5.

[8] A. M. Ujung, M. Irwan, and P. Nasution, “Pentingnya Sistem Keamanan Database untuk

melindungi data pribadi," JISKA: Jurnal Sistem Informasi Dan Informatika, vol. 1, no. 2, p. 44, 2023, [Online]. Available: http://jurnal.unidha.ac.id/index.php/jteksis

[9] A. Fauzi et al., "Keamanan Cyber dan Peretasan Etis: Pentingnya Melindungi Data Pengguna," vol. 2, no. 1, doi: 10.38035/jim.v2i1,2023.

[10] Y. Daeng, J. Levin, M. Razzaq Prayudha, N. Putri Ramadhani, S. Imanuel, and A. Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia Yusuf Daeng, "2023".

[11] S. Nurul, S. Anggrainy, and S. Aprelyani, "FAKTOR-FAKTOR YANG MEMPENGARUHI KEAMANAN SISTEM INFORMASI: KEAMANAN INFORMASI, TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE REVIEW SIM)," vol. 3, no. 5, 2022, doi: 10.31933/jemsi.v3i5.

[12] A. Putri, N. Sari, P. Fajrina, and S. Aisyah, "Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering)," Jurnal Pengabdian Nasional (JPN) Indonesia, vol. 6, no. 1, pp. 38–52, Nov. 2024, doi: 10.35870/jpni.v6i1.1097.

[13] H. Wijayanto, "Aplikasi Verifikasi Sertifikat Berbasis Website Menggunakan Blockchain," JURNAL SAINS DAN KOMPUTER, vol. 8, no. 02, pp. 35–42, Aug. 2024, doi: 10.61179/jurnalinfact.v8i02.586.

[14] Siti Mutia Kosassy 1,Arnal Yanuardi 2,Marzalisman 3,Marwandizal 4,Yurismen 5, "ANALISIS TRANSFORMASI KUALITAS PELAYANAN BERBASIS DIGITAL DI ERA VUCA," P-2655-710X e-ISSN 2655-6022, 2025.

[15] Tri Ginanjar Laksana1, Sri Mulyani2, "PENGETAHUAN DASAR IDENTIFIKASI DINI DETEKSI SERANGAN KEJAHATAN SIBERUNTUK MENCEGAH PEMBOBOLAN DATA PERUSAHAAN," https://doi.org/10.56127/jukim.v3i01.1143, 2024.

[16] P. D. Firmansyah et al., "Manajemen Sekuriti Dalam Era-Digital untuk Mengoptimalisasi Perlindungan Data dengan Teknologi Lanjutan", doi: 10.38035/jkmt.v2i2, 2024.

[17] U. Budi, and A. Sujarwo, "Penerapan JSON Web Token sebagai Strategi Pengamanan Data pada Aplikasi MultiMasjid," E-ISSN 2807-4238 and P-ISSN 2807-4246, 2023.

[18] M. Febrian Aska, D. pratama Putta, and C. Julyana Magdalena Sinambela, "Strategi Efektif Untuk Implementasi Keamanan Siber di Era Digital," Journal of Information and Information Security (JIFORTY), vol. 5, no. 2, pp. 187–200, 2024, [Online]. Available: http://ejurnal.ubharajaya.ac.id/index.php/jiforty

[19] Z. K. Kadir, "Volume 12 Nomor 2 Februari 2025 Kejahatan Berbasis Identitas Digital: Menggagas Kebijakan Kriminal untuk Dunia Metaverse."

[20] M. Tantrinesia1, L. F. Amelia2, and H. A. Sidarwaya, "Prosiding Seminar Nasional Pengaruh M-banking Terhadap Pola Belanja Masyarakat di Surabaya".

[21] Fakhrur Rozi, "Fakhrur Rozi.,PERANCANGAN SISTEM PENYEDIAAN STOK DARAH DALAM BLOOD SUPPLY CHAIN MANAGEMENT BERBASIS BLOCKCHAIN PADA PMI SLEMAN YOGYAKARTA.,(2024)," PERANCANGAN SISTEM PENYEDIAAN STOK DARAH DALAM BLOOD SUPPLY CHAIN MANAGEMENT BERBASIS BLOCKCHAIN PADA PMI SLEMAN YOGYAKARTA, Jul. 2024.