JTIM : Jurnal Teknologi Informasi dan Multimedia

p-ISSN : 2715-2529
e-ISSN : 2684-9151
https://journal.sekawan-org.id/index.php/jtim

Evaluasi Keamanan Sistem Autentikasi Biometrik pada *Smartphone* dan Rekomendasi Implementasi Optimal

Felix Yeovandi [1], Sabariman[1], dan Stefanus Eko Prasetyo[1]*

[1] Program Studi Teknologi Informasi, Universitas Internasional Batam, Indonesia

* Korespondensi: stefanus@uib.ac.id

Sitasi: Yeovandi, F.; Sabariman, S.; Prasetyo, S. E. (**2025**). Evaluasi Keamanan Sistem Autentikasi Biometrik pada *Smartphone* dan Rekomendasi Implementasi Optimal. JTIM: Jurnal Teknologi Informasi Dan Multimedia, 7(1), 133-148. https://doi.org/10.35746/jtim.v7i1.653

Diterima: 06-12-2024
Direvisi: 27-12-2024
Disetujui: 03-01-2025

Abstract: Biometric authentication on smartphones is a modern solution for more practical and secure login security. This technology offers advantages such as speed of access and resistance to forgery compared to password-based methods. However, there are various weaknesses, such as the potential for exploitation through malware, spoofing, or brute force attacks that exploit security holes, such as Cancel-After-Match-Fail (CAMF) and Match-After-Lock (MAL). Additionally, hacked biometric data cannot be replaced, leaving users vulnerable to long-term security threats. To overcome these weaknesses, this article recommends a security approach based on Trusted Execution Environment (TEE), AES-256 encryption, spoofing detection based on liveness recognition, anti-tamper mechanisms, and the application of rate limiting. The secure authentication flow implementation is designed to protect biometric data locally without transmission to external servers, ensuring user integrity and privacy is maintained. This flow includes suspicious activity detection, login encryption, and data protection with advanced encryption. Through a combination of these technologies, the biometric authentication system is characterized as being able to significantly maximize security by minimizing the risk of attacks on user data. This research provides evaluation results that the DNN deep neural network model trained with AES-256 is characterized as being able to produce accuracy above 99.9% with less than 5,000 power traces. Then, the implementation of liveness detection is characterized as being able to produce an F1-Score of 97.78% and an HTER of 8.47% in the intra-dataset scenario, as well as an F1-Score of 74.77% and an HTER of 29.05% in the cross-dataset scenario. This combination of technologies provides secure and efficient biometric authentication without compromising user comfort.

Keywords: Biometric authentication, smartphone, data security

Abstrak: Autentikasi biometrik pada *smartphone* menjadi solusi modern untuk keamanan *login* yang lebih praktis dan aman. Teknologi ini menawarkan keunggulan seperti kecepatan akses dan resistensi terhadap pemalsuan dibandingkan dengan metode berbasis *password*. Namun, terdapat berbagai kelemahan, seperti potensi eksploitasi melalui *malware, spoofing*, atau serangan *brute force* yang memanfaatkan celah keamanan, seperti *Cancel-After-Match-Fail* (CAMF) dan *Match-After-Lock* (MAL). Selain itu, data biometrik yang diretas tidak dapat diganti, membuat pengguna rentan terhadap ancaman keamanan jangka panjang. Untuk mengatasi kelemahan tersebut, artikel ini merekomendasikan pendekatan keamanan berbasis *Trusted Execution Environment* (TEE), enkripsi AES-256, deteksi *spoofing* berbasis *liveness detection*, mekanisme *anti-tamper*, dan penerapan *rate limiting*. Implementasi alur autentikasi yang aman dirancang untuk melindungi data biometrik secara lokal tanpa transmisi ke server eksternal, memastikan integritas dan privasi pengguna tetap terjaga. Alur ini mencakup deteksi aktivitas mencurigakan, pembatasan percobaan *login*, dan perlindungan data dengan enkripsi tingkat lanjut. Melalui kombinasi teknologi tersebut, sistem autentikasi biometrik ditandai dapat memaksimalkan keamanan secara signifikan dengan meminimalisir risiko serangan pada data pengguna. Penelitian ini memberikan hasil evaluasi bahwa

model jaringan saraf dalam DNN yang dilatih dengan AES-256 ditandai dapat menghasilkan akurasi diatas 99,9% dengan kurang dari 5.000 jejak daya. Kemudian, implementasi liveness detection ditandai dapat menghasilkan F1-Score 97,78% serta HTER 8,47% dalam skenario intra-dataset, serta F1-Score 74,77% dan HTER 29,05% pada skenario cross-dataset. Kombinasi teknologi ini memberikan autentikasi biometrik yang aman dan efisien tanpa mengorbankan kenyamanan pengguna.

Kata kunci: Autentikasi biometrik, smartphone, keamanan data

1. Pendahuluan

Dalam era digital saat ini, penggunaan teknologi autentikasi biometrik semakin meluas, terutama pada perangkat *smartphone*. Autentikasi biometrik menawarkan solusi keamanan yang lebih canggih dibandingkan metode tradisional seperti kata sandi atau PIN [1]. Sistem ini memungkinkan pengguna untuk mengakses perangkat atau aplikasi dengan cara yang lebih cepat, praktis, dan aman, menggunakan karakteristik unik seperti sidik jari atau pengenalan wajah. Keunggulan ini telah membuat autentikasi biometrik menjadi pilihan utama bagi pengembang aplikasi untuk meningkatkan kenyamanan pengguna sekaligus mengurangi risiko pencurian data [2].

Namun, meskipun dianggap aman, autentikasi biometrik tidak luput dari berbagai tantangan dan risiko keamanan [3]. Penelitian menunjukkan bahwa sistem ini rentan terhadap berbagai serangan, seperti *spoofing*, *brute force*, dan eksploitasi *zero-day*, yang memanfaatkan kelemahan dalam implementasi sistem biometric [4]. Celah seperti *Cancel-After-Match-Fail* (CAMF) dan *Match-After-Lock* (MAL) memungkinkan peretas untuk mencoba berbagai kombinasi biometrik tanpa terdeteksi, sementara ancaman dari *malware* seperti *Chameleon* menunjukkan bagaimana perangkat lunak berbahaya dapat melumpuhkan kunci biometrik [5].

Masalah utama lainnya adalah sifat unik data biometrik yang tidak dapat diubah, berbeda dengan kata sandi atau PIN yang bisa diganti setelah terjadi pelanggaran. Hal ini menjadikan pelanggaran data biometrik sebagai risiko jangka panjang bagi pengguna. Selain itu, perangkat dengan sensor biometrik berkualitas rendah atau tanpa perlindungan tambahan juga lebih mudah dieksploitasi oleh penyerang [6]. Dalam upaya menghadapi tantangan tersebut, perlu diselenggarakan proses identifikasi secara mendalam mengenai kelemahan yang ditemui pada sistem autentikasi biometrik pada *smartphone*, sebagaimana yang telah menjadi fokus berbagai penelitian sebelumnya.

Penelitian seperti yang dilakukan oleh Chen et al. (2021) mengungkapkan bahwa kombinasi biometrik dengan TEE meningkatkan tingkat keberhasilan autentikasi hingga 95%, kemudian Mason et al. (2020) mencatat bahwa penggunaan *liveness detection* mengurangi tingkat keberhasilan *spoofing* sebesar 70% [13,24]. Dalam konteks ini, penelitian-penelitian sebelumnya telah banyak mengkaji berbagai kerentanannya, namun sebagian besar solusi yang ada masih terbatas dalam hal penerapan perlindungan secara lokal dan pengelolaan data biometrik secara lebih aman. Sebagian besar penelitian cenderung fokus pada penerapan enkripsi atau pengenalan biometrik saja, tanpa memperhatikan integrasi penuh dari berbagai teknologi yang dapat memperkuat keamanan sistem secara holistik [27-29].

Penelitian ini menempati posisi yang berbeda dengan riset-riset sebelumnya dengan mengusulkan pendekatan yang lebih komprehensif dan terintegrasi dalam mengatasi celah keamanan yang ada dalam sistem autentikasi biometrik. Pendekatan ini menggabungkan beberapa teknologi canggih, seperti *Trusted Execution Environment* (TEE), AES-256 *encryption, liveness detection, anti-tamper mechanisms*, serta penerapan *rate limiting*

untuk mencegah eksploitasi brute force. Salah satu kontribusi kebaruan penelitian ini adalah desain alur autentikasi biometrik yang menekankan perlindungan data secara lokal, tanpa melibatkan transmisi data biometrik ke *server* eksternal. Hal ini membedakan penelitian ini dari penelitian sebelumnya yang sering mengandalkan penyimpanan dan pemrosesan data biometrik di *server* eksternal, yang dapat menambah potensi risiko keamanan.

Adapun rumusan masalah yang diangkat dalam penelitian ini adalah, apa saja kelemahan sistem autentikasi biometrik pada *smartphone* yang dapat menjadi celah bagi kasus pembobolan perangkat(1), bagaimana langkah yang dapat diambil pengembang aplikasi dalam memastikan implementasi autentikasi biometrik yang aman dari potensi pembobolan *smartphone*(2), bagaimana alur autentikasi biometrik yang aman diterapkan pada aplikasi *smartphone* untuk memastikan tingkat keamanan yang optimal(3).

Penelitian ini bertujuan untuk menganalisis kelemahan-kelemahan tersebut dan mengusulkan solusi berbasis teknologi terkini, seperti enkripsi tingkat lanjut, *Trusted Execution Environment* (TEE), dan *liveness detection*. Dengan memahami tantangan dan solusi ini, autentikasi biometrik dapat diterapkan secara lebih aman tanpa mengorbankan kenyamanan pengguna dalam mengakses perangkat maupun aplikasi.

2. Bahan dan Metode

2.1. Konsep Autentikasi Biometrik

Autentikasi biometrik adalah proses verifikasi identitas individu berdasarkan karakteristik unik biologis atau perilaku, seperti sidik jari, wajah, dan iris mata. Menurut Jain et al. (2016), autentikasi biometrik menawarkan keunggulan berupa keamanan lebih tinggi dibandingkan metode tradisional seperti kata sandi atau PIN, karena karakteristiknya sulit dipalsukan dan tidak dapat dipindahtangankan. Dalam konteks *smartphone*, autentikasi biometrik menjadi fitur utama yang memberikan kenyamanan dan efisiensi pengguna.

2.2. Teknologi Autentikasi Biometrik pada Smartphone

Berbagai teknologi biometrik telah diintegrasikan ke dalam *smartphone*, seperti pengenalan sidik jari, wajah, dan iris mata. *Fingerprint recognition* merupakan teknologi yang paling umum digunakan karena tingkat akurasi tinggi dan kecepatan prosesnya [1]. Sementara itu, *facial recognition* mengandalkan teknologi pemetaan wajah 3D untuk analisis fitur wajah. *Iris recognition*, meskipun jarang digunakan, menawarkan akurasi tinggi dengan memanfaatkan pola unik iris mata. Setiap teknologi ini memiliki kekuatan dan kelemahannya, tergantung pada kualitas perangkat keras dan algoritma yang digunakan [8].

2.3. Kelemahan Autentikasi Biometrik pada Smartphone

Meski memberikan keamanan yang lebih baik, autentikasi biometrik memiliki beberapa kelemahan. Menurut Roy et al. (2021), ancaman utama autentikasi biometrik adalah *spoofing*, di mana penyerang menggunakan tiruan karakteristik biometrik untuk mengelabui sistem. Kelemahan lain meliputi sensor yang berkualitas rendah, sehingga cenderung rentan terhadap manipulasi. Kemudian, ketiadaan *liveness detection*, sehingga sistem tidak dapat membedakan data biometrik hidup dari tiruan. Selain itu, kelemahan lainnya ditemukan pada algoritma, dimana algoritma autentikasi dapat memiliki celah keamanan yang dimanfaatkan oleh peretas.

2.4. Upaya Mengatasi Kelemahan Sistem Biometrik

Untuk meningkatkan keamanan autentikasi biometrik, berbagai solusi telah diusulkan. Gonzalez et al. (2020) merekomendasikan penggunaan *Trusted Execution Environment* (TEE) yang memastikan data biometrik diproses di lingkungan yang aman. Tan et al. (2018) menekankan pentingnya *liveness detection*, yaitu teknologi yang mendeteksi

apakah data biometrik berasal dari sumber yang hidup. Selain itu, enkripsi data biometrik dinilai penting untuk melindungi data selama penyimpanan dan transmisi.

2.5. Implementasi Autentikasi Biometrik dalam Aplikasi Smartphone

Aplikasi smartphone dengan sistem autentikasi biometrik membutuhkan pendekatan keamanan yang komprehensif. Park et al. (2022) menyarankan penerapan autentikasi multi-faktor (*Multi-Factor Authentication*/MFA), yang mengombinasikan biometrik dengan faktor autentikasi lain, seperti kata sandi atau token fisik. Pendekatan ini dapat meningkatkan ketahanan sistem terhadap ancaman keamanan.

2.6. Kajian Empiris

Berbagai penelitian telah dilakukan untuk menguji efektivitas autentikasi biometrik pada *smartphone*. Studi oleh Chen et al. (2021) menunjukkan bahwa kombinasi biometrik dengan TEE meningkatkan tingkat keberhasilan autentikasi hingga 95%, sementara Mason et al. (2020) mencatat bahwa penggunaan *liveness detection* mengurangi tingkat keberhasilan *spoofing* sebesar 70%. Kajian ini membuktikan bahwa teknologi biometrik terus berkembang dan mampu mengatasi tantangan keamanan secara bertahap.

3. Metodologi

3.1. Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan analisis deskriptif. Pendekatan ini dipilih untuk memahami secara mendalam kelemahan sistem autentikasi biometrik pada *smartphone* serta langkah-langkah pengembangan yang dapat diambil untuk meningkatkan keamanan sistem.

3.2. Desain Penelitian

Metode studi literatur digunakan untuk mengumpulkan data, di mana data diperoleh melalui analisis sumber-sumber terpercaya seperti jurnal, buku, laporan teknis, dan dokumen ilmiah terkait dengan autentikasi biometrik. Selain itu, penelitian ini dilengkapi dengan simulasi teknis untuk memvalidasi model keamanan yang diusulkan.

3.3. Teknik Pengumpulan Data

Pengumpulan data dilakukan dalam dua tahap yaitu; Kajian Literatur, informasi dikumpulkan dari artikel jurnal, buku, laporan teknis, dan studi kasus untuk mengidentifikasi kelemahan dan solusi yang berkaitan dengan sistem autentikasi biometric. Simulasi Teknis, menggunakan dataset biometrik publik, seperti *Labeled Faces in the Wild* (LFW) atau *BioSecure Database*, untuk menguji dan memahami bagaimana kelemahan dalam sistem dapat dimanfaatkan.

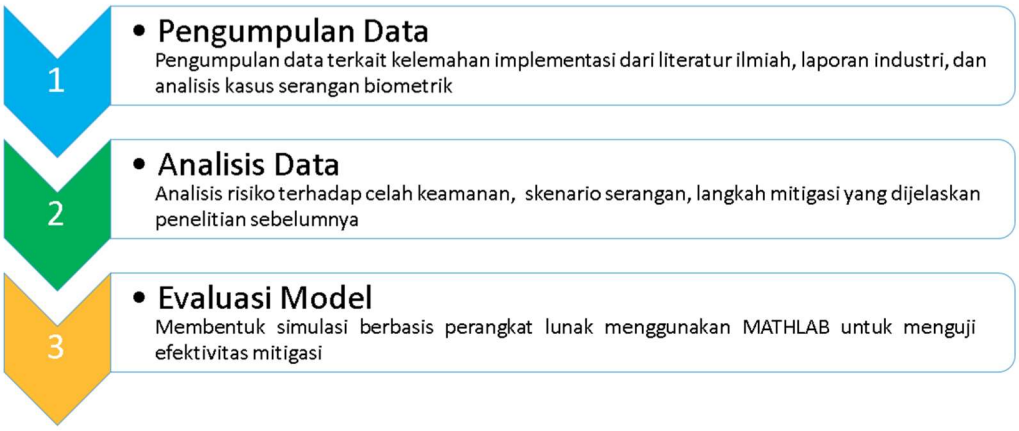
3.4. Teknik Analisis Data

Data dianalisis menggunakan dua metode yakni analisis konten serta analisis teknis. Analisis konten diperuntukkan dalam upaya menganalisis temuan yang didapatkan dari kajian literatur untuk mengelompokkan kelemahan autentikasi biometrik ke dalam kategori tertentu, seperti *spoofing*, kelemahan algoritma, dan sensor. Sementara itu, analisis teknis ditempuh dalam upaya menjalankan simulasi untuk menguji skenario eksploitasi kelemahan dan mengevaluasi efektivitas langkah mitigasi yang diusulkan.

3.5. Prosedur Penelitian

Prosedur penelitian diawali dengan upaya pengumpulan data terkait kelemahan implementasi dari literatur ilmiah, laporan industri, dan analisis kasus serangan biometrik yang dilaporkan. Peneliti juga menggunakan *dataset* biometrik terbuka seperti *fingerprint*, *iris scan*, atau *face recognition* yang telah tersedia untuk keperluan penelitian keamanan. *Dataset* ini diperuntukkan dengan tujuan penelitian keamanan dan untuk mengidentifikasi potensi kerentanannya dalam menghadapi serangan yang berbeda.

Prosesnya dilanjutkan dengan analisis data, sehubungan dengan upaya analisis risiko terhadap celah keamanan menggunakan *dataset* biometrik untuk mengidentifikasi pola kerentanan, menganalisa skenario serangan seperti *brute force* dan *spoofing* untuk dapat mengidentifikasikan efektivitas serangan tersebut terhadap sistem yang ada untuk dapat mengeksploitasi data biometrik palsu (seperti sidik jari palsu atau foto wajah) untuk memperoleh akses illegal, serta menganalisa langkah mitigasi yang diusulkan dalam penelitian sebelumnya, seperti enkripsi data maupun *liveness detection*. Kemudian, peneliti melaksanakan upaya evaluasi model dalam membentuk simulasi berbasis perangkat lunak menggunakan MATHLAB untuk menguji efektivitas mekanisme mitigasi, termasuk *Trusted Execution Environment* (TEE) serta *rate limiting* untuk membatasi jumlah percobaan autentikasi yang gagal dalam periode tertentu. Selanjutnya, peneliti juga melaksanakan eksperimen dengan upaya membandingkan tingkat keberhasilan serangan pada model autentikasi dengan maupun tanpa langkah mitigasi. Prosedur penelitian ini dijelaskan pada Gambar 1:



Gambar 1. Prosedur Penelitian

Melalui upaya menerapkan prosedur penelitian yang disajikan pada Gambar 1, penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai kelemahan autentikasi biometrik pada *smartphone*, serta solusi mitigasi yang berbasis pada analisis data beserta dengan simulasi yang dijalankannya. Identifikasi masalah akan difokuskan pada celah keamanan spesifik seperti *Cancel-After-Match-Fail* (CAMF) dan *Match-After-Lock* (MAL), yang dianalisis melalui data kasus serangan biometrik yang dilaporkan dan *dataset* biometrik terbuka. Proses analisis akan mengungkap pola kerentanan sistem biometrik, yang kemudian digunakan untuk merancang dan mengevaluasi langkah mitigasi, seperti implementasi *Trusted Execution Environment* (TEE), enkripsi AES-256, dan deteksi *spoofing* berbasis *liveness detection*. Hasil simulasi akan menjadi dasar dalam menilai efektivitas langkah-langkah ini, sehingga dapat diusulkan panduan teknis yang aplikatif bagi para pengembangnya.

3.6. Validitas dan Reliabilitas Data

Validitas dan reliabilitas penelitian dijaga dengan triangulasi data, yang meliputi perbandingan temuan dari berbagai sumber dan penggunaan *dataset* yang diakui untuk memastikan keandalan hasil simulasi. Evaluasi dari pakar keamanan informasi juga dilakukan untuk memvalidasi model keamanan yang diusulkan.

Penelitian ini diharapkan dapat memberikan rekomendasi praktis dan implementasi autentikasi biometrik yang lebih aman pada aplikasi *smartphone* untuk mengurangi risiko pembobolan perangkat.

4. Pembahasan

Penerapan sistem login dalam aplikasi *smartphone* ditandai memberikan solusi autentikasi yang lebih aman bagi penggunanya. Dalam konteks ini, sistem ini ditandai lebih rendah risiko pencurian data ataupun penyalahgunaan akses, mengingat autentikasi biometrik cenderung lebih sulit dipalsukan dibandingkan dengan metode berbasis *password* [9]. Selain itu, penggunaan biometrik memungkinkan penggunanya untuk mengakses akun mereka dengan cara yang lebih cepat dan praktis, cukup dengan sidik jari atau pemindaian wajah, tanpa perlu mengingat berbagai kombinasi *password* ataupun *pattern* yang kompleks [10].

Namun, meskipun mempunyai berbagai keunggulan, implementasi sistem *login* biometrik dalam aplikasi *smartphone* juga diperhadapkan dengan berbagai tantangan, karena adanya celah kelemahan tertentu [11]. Penelitian yang dilakukan oleh laboratorium siber global yang dinamakan Kaspersky Lab, menemukan adanya kelompok *hacker* yang mulai mencaritahu celah untuk dapat menembus sistem keamanan biometrik pada *smartphone*. Pengamatan dari Kaspersky Lab mengindikasikan bahwa terdapat 12 *hacker* yang telah menjual sistem *skimmer* khusus untuk melaksanakan pencurian data sidik jari. Dalam hal ini, terdapat diantaranya yang sudah menawarkan sistem untuk menembus autentikasi urat serta *iris recognition*. Kemudian, modus lainnya adalah dengan mengincar perangkat *mobile* untuk dapat melaksanakan pencurian atas identifikasi wajah seseorang. Hal ini juga dilancarkan dengan pengambilan foto seseorang yang sudah di*posting* di media sosial, untuk kemudian digunakan dalam rangka mengelabui sistem identifikasi wajah [6].

Masalah ini dapat menjadi semakin serius, mengingat sistem biometrik yang telah dibobol, data biometriknya tetap tidak dapat diganti seperti yang dapat dilakukan pada autentikasi *password*. Berbeda dengan *password* serta kode pin yang cenderung mudah untuk dimodifikasi, adalah suatu hal yang mustahil untuk mengubah sidik jari ataupun iris mata. Maka dari itu, apabila datanya diretas sekali saja, maka dapat mengakibatkan penggunanya sudah tidak aman menggunakan metode biometrik lagi [3].

Dalam hal ini, penggunaan sistem menembus autentikasi tersebut bukanlah satu-satunya celah, melainkan terdapat berbagai celah lainnya yang perlu diperhatikan, seperti halnya dengan yang dinyatakan oleh peneliti keamanan siber di Tencent Labs serta Zhejiang University mengugnkapkan bahwa perangkat android cenderung rentan untuk diretas pada fitur *fingerprint*nya. Dalam hal ini, peretas dapat membuka kunci pada sidik jari tersebut asalkan mempunyai akses ke *smartphone* secara langsung serta mempunyai waktu panjang (antara 2,9 hingga 13,9 jam) untuk melaksanakan pembobolan atasnya. Hal ini disebabkan karena ada 2 kerentanan *zero-day* pada perangkat Android, maupun perangkat yang didukung oleh AppleIOS serta Huawei HarmonyOS. Celah tersebut ditandai sebagai *Cancel-After-Match-Fail* (CAMF) dan *Match-After-Lock* (MAL) [12].

Dalam konteks ini, CAMF terjadi pada saat sistemnya memungkinkan pengguna dalam membatalkan proses autentikasi beberapa kali setelah percobaannya gagal, tetapi tidak mampu membersihkan riwayat dari percobaan sebelumnya [5]. Pada skenario ini, penyerang cenderung memanfaatkan kelemahan tersebut dengan menggunakan berbagai percobaan kombinasi biometrik, contohnya seperti sidik jari atau wajah, hingga mereka menemukan pola yang berhasil. Contohnya dengan memanfaatkan cetakan palsu atau rekayasa data biometrik, celah CAMF dapat memperpanjang waktu percobaan penyerang tanpa memicu sistem keamanan yang lebih tinggi, seperti penguncian total perangkat [13].

Disamping sisi, MAL dapat mengacu pada situasi ketika sistemnya memungkinkan pelaksanaan autentikasi biometrik diselenggarakan, bahkan sesudah perangkat dinyatakan terkunci. Hal ini terjadi karena adanya desain sistem yang cenderung tidak membatasi akses menuju fungsi biometrik secara efektif mengingat adanya batasan tertentu

yang telah terpenuhi [14]. Hal ini mengakibatkan penyerangnya dapat mencoba serangkaian percobaan biometrik tanpa harus membuka kunci utama perangkat, sehingga meningkatkan peluang keberhasilan eksploitasi, terutama jika perangkat menggunakan sensor biometrik dengan kualitas atau standar keamanan rendah [9].

Kedua celah ini dapat merepresentasikan kurangnya mekanisme pengamanan yang memadai dalam pengelolaan proses autentikasi biometrik. Dalam upaya mengatasi kelemahan tersebut, sistemnya perlu untuk dirancang supaya lebih ketat, contohnya dengan membatasi jumlah percobaan biometrik yang diperbolehkan sebelum perangkatnya terkunci sepenuhnya ataupun membutuhkan metode autentikasi lain seperti PIN atau kata sandi [1]. Selain itu, sistem harus mampu mendeteksi dan menolak percobaan autentikasi yang mencurigakan, serta memiliki fitur enkripsi untuk melindungi data biometrik dari manipulasi. Pengguna juga harus memahami pentingnya memilih perangkat yang menawarkan perlindungan keamanan biometrik tingkat tinggi untuk mengurangi risiko eksploitasi [10].

Dalam hal ini, para peneliti berhasil untuk membuat Android mengizinkan upaya pemindaian sidik jari pada jumlah yang tidak terbatas, ataupun menggunakan *database* yang diemukan, kebocoran data biometrik, serta sebagainya. Serangan tersebut disebut dengan istilah *BrutePrint* serta mengklaim bahwa perangkat yang memiliki lebih banyak rekaman sidik jari akan lebih mudah untuk dibobol [15].

Celah lainnya berupa *malware*, yang mana dapat memiliki kemampuan untuk dapat melumpuhkan kunci biometrik, seperti yang dinamakan dengan *malware Chameleon*, yang mana berkemampuan lebih tinggi. Versi sebelumnya dari *malware* tersebut sudah pernah digunakan untuk dapat meniru badan pemerintahan, pusat pertukaran kripto, hingga perbankan. Dalam hal ini, malware jenis tersebut disebarkan lewat layanan *Zombinder* maupun menyamar sebagai *Google Chrome* supaya dapat lolos dari deteksi *Google Play Protect* serta aplikasi antivirus [16].

Dalam konteks ini, *Malware* mampu memanfaatkan layanan *Accessibility* untuk dapat memaksa penggunanya untuk dapat membuka kunci perangkatnya. *Malware Chameleon* juga dilengkapi dengan fitur penjadwalan via *API AlarmManager*, sehingga *malware*nya tidak aktif pada saat ponsel yang terinfeksi aktif. Cara tersebut juga dapat membantu *malware* tetap tersembunyi serta tidak terdeteksi [38-39].

4.1. Perbandingan Pendekatan Keamanan Data dalam Memitigasi Potensi Pembobolan Smartphone

Setiap pendekatan, baik itu pendekatan konvensional dengan kata sandi maupun PIN sederhana, biometrik dasar yang mencakup sidik jari sertapengenalan wajah, biometrik dengan server eksternal, dengan pendekatan yang diusulkan pada penelitian ini, mencakup kombinasi dari metode TEE, AES-256, *Liveness Detection* cenderung memiliki kelebihan, kekurangan, beserta dengan fitur-fitur yang berbeda. Adapun peneliti menyajikan perbandingan pendekatan-pendekatan tersebut dalam tabel berikut:

Tabel 1. Perbandingan Pendekatan Keamanan Data

Pendekatan	Metode	Kelebihan	Kekurangan	Fitur Utama	Penelitian Terdahulu
Konvensional (*Password*/PIN)	*Password*, PIN sederhana	Mudah diterapkan, tidak memerlukan perangkat tambahan, dan familiar bagi semua pengguna	Rentan terhadap serangan *brute force*, *shoulder surfing*, pencurian informasi, dan sharing kredensial	Tidak memanfaatkan biometrik, mudah dilupakan oleh pengguna	[23-28]

Pendekatan	Metode	Kelebihan	Kekurangan	Fitur Utama	Penelitian Terdahulu
Biometrik Dasar	Sidik jari, *face recognition*, *iris recognition*	Akses cepat, praktis, tidak memerlukan ingatan pengguna, dan mulai diadopsi di berbagai perangkat	Rentan terhadap *spoofing*, rekayasa data biometrik, dan celah pada proses verifikasi	Verifikasi sederhana tanpa deteksi aktivitas hidup (*liveness detection*)	[29-34].
Biometrik dengan *Server* Eksternal	Data biometrik disimpan di *server*	Memungkinkan pengelolaan data terpusat dan sinkronisasi lintas perangkat	Risiko pelanggaran privasi tinggi, ketergantungan pada keamanan jaringan dan *server*	Data tidak diproses secara lokal, rentan terhadap kebocoran data	[35-40].
Usulan Penelitian Ini	TEE, AES-256, *Liveness Detection*	Tingkat keamanan tinggi, mencegah *spoofing*, menjaga privasi dengan memproses data secara lokal	Kompleksitas implementasi lebih tinggi dan memerlukan perangkat khusus	*Rate limiting*, *anti-tamper*, enkripsi tingkat lanjut untuk proteksi maksimal	[17-22].

Pendekatan yang digunakan dalam penelitian ini didasarkan pada analisis mendalam terhadap kelemahan pendekatan sebelumnya yang telah dijelaskan dalam berbagai penelitian terdahulu. Pendekatan konvensional seperti penggunaan password atau PIN, sebagaimana diungkap oleh Market et al. (2021) dan Wang et al. (2020), mudah diimplementasikan namun memiliki kelemahan signifikan, seperti rentan terhadap serangan *brute force*, *shoulder surfing*, dan pencurian informasi. Sementara itu, pendekatan biometrik dasar seperti sidik jari dan pengenalan wajah, Li et al. (2020) dan Arora & Bhatia (2020).menawarkan kecepatan dan kenyamanan pengguna, tetapi terbukti rentan terhadap serangan *spoofing*, seperti penggunaan cetakan silikon atau foto untuk menipu sistem.

Penelitian oleh Bodepudi & Manjunath (2020) dan Kumar et al. (2022) juga mengeksplorasi penggunaan *cloud biometrics*, yang memungkinkan pengelolaan data biometrik secara terpusat dan lintas perangkat. Namun, pendekatan ini meningkatkan risiko pelanggaran privasi akibat ketergantungan pada jaringan dan *server* yang rentan terhadap serangan seperti man-*in-the-middle* atau kebocoran data di *server* (Anthony et al., 2022; Shibel et al., 2021; Ebihara et al. (2021). Kemudian, Marutotamtama et al. (2022) mengusulkan alternatif yang lebih aman dengan memanfaatkan *Trusted Execution Environment* (TEE), yang memungkinkan data biometrik diproses secara lokal tanpa harus dikirim ke server eksternal, mengurangi risiko kebocoran data.

Penelitian ini memperluas pendekatan penelitian sebelumnya oleh Lalouani et al. (2023; Xu et al. (2024); Das et al., 2020; Marsiani et al. (2021) dengan menambahkan fitur seperti enkripsi AES-256 untuk melindungi data biometrik, deteksi *spoofing* berbasis *liveness detection* untuk mencegah serangan dengan material tiruan, mekanisme *anti-tamper* untuk melindungi perangkat keras dan perangkat lunak, serta *rate limiting* untuk membatasi jumlah percobaan *login*. Maka dari itu, penelitian ini tidak hanya mengatasi kelemahan dari pendekatan sebelumnya, tetapi juga menawarkan solusi yang lebih komprehensif dan aman untuk melindungi privasi serta keamanan pengguna dalam sistem autentikasi biometrik pada *smartphone*.

4.2. Langkah yang Dapat Diambil Pengembang Aplikasi Dalam Memastikan Implementasi Autentikasi Biometrik yang Aman Dari Potensi Pembobolan Smartphone

Dalam rangka memastikan keamanan dan perlindungan data pengguna *smartphone* dari segala risiko pembobolan, maka pengembang aplikasi perlu mempertimbangkan implementasi beberapa teknik yang dibuktikan telah efektif dalam memaksimalkan keamanan data biometrik. Salah satu pendekatan utama adalah penggunaan enkripsi AES-

256, yang terbukti sangat kuat dalam melindungi data biometrik selama penyimpanan dan transmisi. Penelitian oleh Das et al. (2020) menunjukkan bahwa *Machine Learning side-channel attacks* (SCA), khususnya dalam bentuk *deep learning side-channel attacks* (DLSCA) telah dibuktikan efektif dalam mengekstraksi rahasia kriptografi, dan berpotensi mengungkap kunci hanya dari satu jejak. Efektivitas ini sebagian besar disebabkan oleh fase pembuatan profil, di mana model mempelajari korelasi antara pola kebocoran dan kunci rahasia.

Penelitian tersebut memperkenalkan perangkat keras redaman tanda tangan domain saat ini (CDSA), yang mengintegrasikan mesin AES256 yang dibuat dalam teknologi CMOS 65nm. CDSA secara efektif mengurangi tanda tangan saat ini lebih dari 350× sebelum mencapai pin catu daya, sehingga kurang dapat diakses oleh penyerang. Hasil eksperimennya menunjukkan bahwa model jaringan saraf dalam (DNN) untuk DLSCA dapat dilatih sepenuhnya dengan akurasi pengujian lebih dari 99,9% menggunakan kurang dari 5.000 jejak daya dari AES256 yang tidak dilindungi. Sebaliknya, model DNN untuk AES256 yang dilindungi CDSA tidak dapat dilatih bahkan dengan 10 juta jejak. Temuan penelitiannya menggarisbawahi pentingnya tindakan pencegahan di tingkat perangkat keras dalam meningkatkan keamanan perangkat kriptografi terhadap serangan berbasis pembelajaran mesin tingkat lanjut.

Selain itu, penerapan *liveness detection*, seperti yang dijelaskan oleh Sthevanie et al. (2020), memainkan peran penting dalam mencegah serangan *spoofing*, dengan memastikan bahwa data biometrik yang digunakan berasal dari pengguna asli, bukan rekayasa seperti foto atau cetakan sidik jari palsu. Teknologi ini dapat memanfaatkan sensor tambahan, seperti sensor kedalaman atau inframerah, untuk membedakan antara pengguna yang hidup dan tiruan.

Secara lebih jelas, penelitian tersebut memperkenalkan sebuah sistem yang dapat melaksanakan pendeteksian atas serangan spoofing menggunakan metode *Local Derivative Pattern* dari *Three Orthogonal Planes. Dataset* yang dimanfaatkan bersumber dari empat dataset publik yang berbeda yakni *Idiap Replay-Attack Database*, *MSU MFSD Database*, *Casia FASD Database* dan *NUAA Imposter Database* yang *format*nya adalah video. Hasil pengujian pada *intra-dataset* mendapatkan nilai performansi terbaik dengan rata-rata *F1-Score* 97.77% dan rata-rata HTER 8.47%, sedangkan pada skenario *cross-dataset* rata-rata *F1-Score* 74.77% dan rata-rata HTER 29.05% [22].

Di sisi lain, mekanisme *anti-tamper*, yang menggunakan teknik seperti *checksum* dan tanda tangan digital, dapat memastikan integritas data biometrik, seperti yang diungkapkan oleh Jacob & Samuel (2020), sehingga mencegah manipulasi data oleh pihak luar. Dalam konteks ini, penelitian ini membahas berbagai jenis *tamper*, seperti *tamper* pembalikan, *tamper grounding*, *tamper* penutup terbuka, *tamper* magnetik, *tamper* kawat tunggal, *tamper* korsleting jalur fasa, dan *tamper bypass* meteran yang merusak. Berdasarkan analisis matematis, simulasi dilakukan menggunakan perangkat lunak MATLAB untuk memvisualisasikan arus, bentuk gelombang tegangan, serta gelombang daya dan energi yang dikonsumsi oleh beban, serta daya dan energi yang tercatat oleh pengukur energi. Selain itu, dikembangkan sebuah *flowchart* yang memungkinkan sistem pengukuran konvensional untuk mendeteksi pencurian energi, mengklasifikasikannya, dan mengirimkan data pengukuran tersebut ke pusat layanan [21].

Sementara itu, *Trusted Execution Environment* (TEE), yang dijelaskan oleh Busch et al. (2020), memberikan lapisan perlindungan dengan menyimpan dan memproses data biometrik dalam area yang terisolasi dan aman, sehingga data tidak dapat diakses oleh aplikasi atau perangkat lunak berbahaya [18]. Lebih lanjut, penelitian ini mengidentifikasi kerentanan signifikan dalam sistem *keystore* dan mengungkap kebocoran kunci yang dilindungi ekspor dari TEE yang melemahkan keamanan enkripsi *disk* penuh. Selain itu, penelitian ini menemukan kelemahan kerusakan memori pada *keymaster* TA Huawei,

yang memungkinkan eksekusi kode arbitrer dalam *ARM TrustZone* pada tingkat hak istimewa tertinggi. Memanfaatkan kerentanan ini memerlukan melewati beberapa langkah keamanan, seperti *stack canaries* dan *Address Space Layout Randomization* (ASLR), yang semuanya terbukti tidak efektif karena kelemahan dalam desain TEE.

Sementara itu, penerapan *rate limiting*, yang dibahas oleh Huszar et al. (2021) efektif dalam mencegah serangan *brute force* dengan memberikan pembatasan atas jumlah percobaan autentikasi yang gagal, sehingga mengurangi risiko eksploitasi [38].

Kombinasi dari berbagai metode ini, terletak pada enkripsi yang kuat, *liveness detection*, *anti-tamper*, TEE, dan *rate limiting*, sehingga dapat menyediakan solusi autentikasi biometrik yang lebih aman dan efektif, menjaga data pengguna tetap terlindungi tanpa mengorbankan kenyamanan atau kecepatan akses. Dalam konteks ini, BR-PET (*Biometric recognition privacy-enhancing technologies*), yaitu PET yang dirancang khusus untuk sistem pengenalan biometrik, memerlukan persyaratan privasi yang disesuaikan dengan konteks spesifik data biometrik. Persyaratan ini mengadaptasi prinsip-prinsip perlindungan data tertentu untuk meningkatkan privasi informasi biometrik, seperti yang diilustrasikan dalam Gambar 2. Secara khusus, prinsip integritas dan kerahasiaan mengharuskan pemrosesan data untuk menjamin keamanan data pribadi yang memadai. Dalam hal data biometrik, konsep irreversibility dan unlinkability memperkenalkan persyaratan tambahan yang spesifik pada konteks, berdasarkan prinsip integritas dan kerahasiaan yang lebih luas. Dalam ISO/IEC 24745, kerahasiaan adalah persyaratan privasi informasi biometrik pada tingkat ireversibilitas dan *unlinkability* yang sama.

Dalam kaitannya dengan mekanisme *rate limiting*, penerapan prinsip-prinsip privasi dalam BR-PET juga melibatkan kontrol terhadap jumlah dan frekuensi akses ke data biometrik. *Rate limiting*, yang mengatur batasan berapa banyak kali data biometrik dapat diakses atau diproses dalam jangka waktu tertentu, berfungsi sebagai mekanisme penting untuk mencegah penyalahgunaan data dan serangan *brute force*. Dengan membatasi jumlah permintaan yang dapat dilakukan oleh entitas tertentu, *rate limiting* membantu menjaga integritas dan kerahasiaan data biometrik, memastikan bahwa data pribadi tidak dapat diekspos melalui percakapan yang berlebihan atau permintaan yang mencurigakan.

Maka dari itu, pendekatan yang direkomendasikan peneliti dalam merancangkan implementasi keamanan biometrik yang dapat meminimalisir risiko serangan, seperti *spoofing* dan *brute force* tanpa mengorbankan kenyamanan pengguna, diungkapkan pada Tabel 2 berikut:

Tabel 2. Langkah Keamanan Dalam Implementasi Autentikasi Biometrik

No.	Langkah Keamanan	Deskripsi	Manfaat Keamanan
1	Penggunaan *Trusted Execution Environment* (TEE) atau *Secure Enclave*	Data biometrik disimpan di lingkungan yang aman (TEE/*Secure Enclave*) untuk melindungi data sensitif dari aplikasi atau sistem operasi yang tidak terotorisasi [17].	Mencegah eksploitasi melalui *malware* atau akses tidak sah oleh aplikasi pihak ketiga [18].
2	Penerapan Enkripsi Tingkat Lanjut (AES-256)	Data biometrik selalu dienkripsi dengan algoritma AES-256 selama penyimpanan dan transmisi untuk melindungi kerahasiaan data [35,37].	Menjamin data biometrik tetap aman meskipun dicuri, karena hanya dapat dibaca dengan kunci enkripsi yang benar [19].
3	Penggunaan Mekanisme *Anti-Tamper*	Menggunakan teknologi untuk mendeteksi dan memblokir manipulasi kode atau perangkat keras yang mencoba mengakses data biometrik,	Mencegah manipulasi data biometrik yang dapat merusak integri-

No.	Langkah Keamanan	Deskripsi	Manfaat Keamanan
		seperti *checksum* atau tanda tangan digital [25,28].	tas data dan mengurangi ancaman pencurian data [21].
4	*Rate Limiting* pada Proses Autentikasi	Pembatasan jumlah percobaan autentikasi biometrik yang gagal dalam periode tertentu, misalnya setelah tiga kali gagal [33].	Mengurangi risiko serangan *brute-force* dengan membatasi upaya yang dapat dilakukan oleh penyerang [20].
5	Pengenalan Sistem Deteksi *Spoofing* (*Liveness Detection*)	Teknologi yang membedakan biometrik asli dari pengguna hidup dan data palsu seperti foto atau cetakan sidik jari, menggunakan sensor tambahan (inframerah, kedalaman) [38].	Mengurangi risiko serangan *spoofing* dengan memastikan bahwa data biometrik yang digunakan berasal dari pengguna asli [22].

Berdasarkan Tabel 2 diatas, peneliti memberikan penjelasan sebagai berikut:

1. Penggunaan *Trusted Execution Environment* (TEE) atau *Secure Enclave*

Pengembang aplikasi harus memastikan bahwa data biometrik disimpan di dalam lingkungan yang aman seperti *Trusted Execution Environment* (TEE) atau *Secure Enclave*. Hal ini ditandai sebagai area yang terisolasi secara fisik dan logis dalam *processor* yang dirancang untuk melindungi data sensitif dari gangguan oleh aplikasi atau bahkan sistem operasi utama [17]. Dengan menggunakan TEE atau *Secure Enclave*, data biometrik tidak akan dapat diakses oleh perangkat lunak yang tidak terotorisasi, sehingga mengurangi risiko pencurian data. Langkah ini sangat penting karena mencegah eksploitasi melalui malware atau akses langsung oleh aplikasi pihak ketiga [18].

2. Penerapan Enkripsi Tingkat Lanjut

Data biometrik harus mampu untuk selalu dienkripsi menggunakan algoritma enkripsi yang kuat seperti AES-256 selama penyimpanan dan transmisi. Hal ini memastikan bahwa meskipun data berhasil dicuri, penyerang tidak dapat membacanya tanpa kunci enkripsi [19]. Selain itu, pengembang harus mengimplementasikan *end-to-end encryption* untuk memastikan bahwa data biometrik tetap aman saat dipindahkan antara modul sistem. Dengan langkah ini, risiko intersepsi data biometrik oleh penyerang selama proses komunikasi dapat diminimalkan [20].

3. Penggunaan *Anti-Tamper Mechanisms*

Dalam rangka mencegah akses ilegal atau manipulasi data biometrik, pengembang aplikasi harus menerapkan mekanisme *anti-tamper*. Hal ini termasuk dengan pemanfaatan teknologi yang mampu mendeteksi dan memblokir modifikasi kode atau manipulasi perangkat keras yang mencoba mengakses data sensitif. Selain itu, pengembang dapat menggunakan metode integritas data seperti *checksum* ataupun tanda tangan digital untuk memverifikasi bahwa data biometrik tetap utuh dan tidak dimodifikasi oleh pihak luar [21].

4. *Rate Limiting* pada Proses Autentikasi

Pengembang harus mampu menerapkan pembatasan jumlah percobaan autentikasi biometrik dalam periode tertentu untuk mencegah serangan *brute force*. Misalnya, setelah tiga kali percobaan gagal, sistem dapat mengunci proses autentikasi untuk sementara

waktu atau memerlukan metode autentikasi tambahan, seperti PIN atau *password*. Pendekatan ini memastikan bahwa bahkan jika ada celah dalam sistem, waktu dan upaya yang dibutuhkan untuk mengeksploitasi sistem menjadi tidak praktis [20].

5. Pengenalan Sistem Deteksi *Spoofing*

Sistem autentikasi biometrik harus dilengkapi dengan teknologi *liveness detection*, yang mana dapat membedakan antara biometrik asli dari pengguna yang hidup dan data palsu seperti cetakan sidik jari, foto, atau rekaman video. Teknologi ini dapat memanfaatkan sensor tambahan, seperti sensor kedalaman atau inframerah, untuk memvalidasi keberadaan fisik pengguna secara *real-time*. Dengan mengintegrasikan deteksi *spoofing*, pengembang dapat mengurangi risiko serangan berbasis rekayasa biometrik [22].

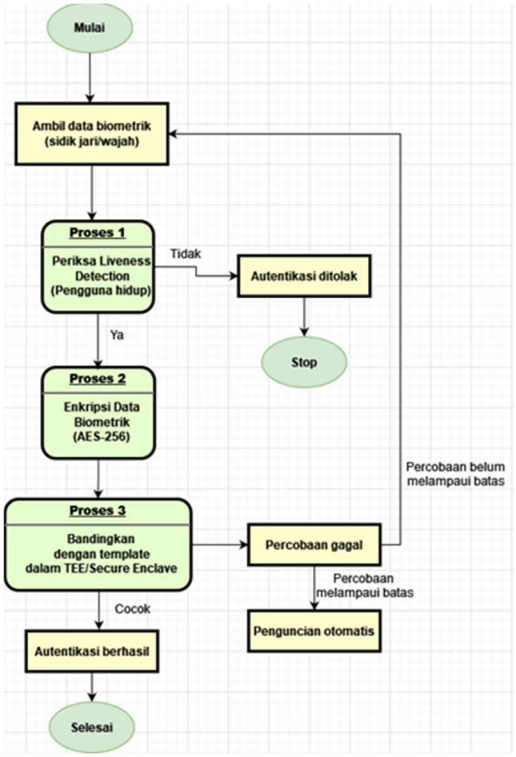
4.3. Alur Autentikasi Biometrik yang Aman Diterapkan pada Aplikasi Smartphone

Dalam rangka menghindari potensi pembobolan, maka alur autentikasi biometrik yang aman pada aplikasi *smartphone* dapat dirancang sebagai berikut. Pada saat penggunanya memulai autentikasi biometrik, data biometrik (misalnya, sidik jari atau wajah) diambil melalui sensor perangkat. Data ini kemudian dikirim ke *Trusted Execution Environment* (TEE) atau *Secure Enclave* untuk diproses, di mana data tersebut dienkripsi menggunakan algoritma seperti AES-256. Dalam TEE, data biometrik yang diambil dibandingkan dengan template biometrik yang telah disimpan sebelumnya, yang juga dienkripsi [18].

Apabila ditemukan adanya ketidakcocokan, mekanisme *rate limiting* akan membatasi jumlah percobaan yang dapat dilakukan dalam periode tertentu. Setelah beberapa percobaan gagal, autentikasi akan terkunci sementara atau memerlukan metode tambahan seperti PIN untuk melanjutkan. Selain itu, selama proses ini, *teknologi liveness detection* memverifikasi bahwa data biometrik berasal dari pengguna yang hidup untuk mencegah serangan dengan cetakan palsu atau foto [20]. Seluruh data dari biometrik diproses dan disimpan secara lokal dalam area aman, tanpa mentransmisikannya ke *server* eksternal, untuk memastikan privasi pengguna. Alur kerjanya dijelaskan sebagai berikut:

1. Mulai
2. Ambil Data Biometrik (sidik jari/wajah)
3. Periksa *Liveness Detection* (Pengguna Hidup?)
    - Jika tidak, autentikasi ditolak.
    - Jika ya, lanjutkan.
4. Enkripsi Data Biometrik (AES-256)
5. Bandingkan dengan *Template* dalam TEE/*Secure Enclave*
    - Jika cocok, autentikasi berhasil.
    - Jika tidak cocok, lanjutkan.
6. Hitung Percobaan Gagal
    - Jika melampaui batas percobaan, aktifkan penguncian sementara.
    - Jika belum melampaui batas, ulangi dari langkah 2.
7. Selesai

Secara lebih jelasnya, dinyatakan pada bagan *flowchart* berikut ini:



Gambar 2. Flowchart Autentikasi Biometrik yang Aman

Dalam konteks ini, dapat dinyatakan bahwa implementasi alur autentikasi biometrik yang aman pada aplikasi *smartphone*, dengan memanfaatkan enkripsi AES-256, TEE, dan *liveness detection*, menyediakan proteksi perlindungan yang kuat terhadap data pribadi pengguna serta mencegah serangan berbasis *spoofing* dan *brute-force*. Proses yang dilakukan sepenuhnya di perangkat memastikan bahwa data biometrik tetap terlindungi dan tidak rentan terhadap ancaman dari server eksternal [17]. Dengan mekanisme *rate limiting*, penguncian sementara, dan penerapan metode autentikasi alternatif seperti PIN setelah beberapa percobaan gagal, sistem ini juga dapat berguna memastikan keseimbangan antara keamanan dan kenyamanan pengguna [21]. Maka dari itu, alur autentikasi biometrik ini dapat menjadi solusi yang efektif dan aman untuk aplikasi *smartphone*, dengan menyajikan lapisan perlindungan yang lebih baik tanpa mengorbankan pengalaman pengguna.

5. Kesimpulan

Penelitian ini mengidentifikasi sejumlah kelemahan pada sistem autentikasi biometrik *smartphone* yang dapat menjadi celah bagi potensi pembobolan perangkat. Kelemahan utama meliputi teknik *spoofing*, seperti penggunaan gambar, rekaman, atau model 3D untuk menipu sensor biometrik, serta potensi manipulasi data sensor dan pengungkapan data biometrik melalui serangan *cyber*. Selain itu, analisis menunjukkan bahwa teknologi biometrik yang berbasis pada satu jenis sensor, seperti pemindaian wajah atau sidik jari tunggal, rentan terhadap penyusupan.

Hasil penelitian juga menekankan pentingnya pengembang aplikasi untuk mengintegrasikan langkah-langkah keamanan tambahan, seperti autentikasi multi-faktor (MFA), serta penggunaan algoritma pembelajaran mesin untuk mendeteksi anomali yang tidak biasa pada data biometrik. Implementasi prosedur pembaruan perangkat lunak secara berkala juga menjadi langkah penting dalam menjaga keamanan dari potensi eksploitasi celah keamanan yang ditemukan seiring waktu.

Selanjutnya, penelitian ini menekankan bahwa alur autentikasi biometrik yang aman harus melibatkan proses pengenalan pengguna yang lebih canggih, seperti penggunaan

data multispektral dan verifikasi tambahan berbasis perilaku pengguna. Penerapan sistem semacam itu dapat membantu mengurangi risiko pembobolan dan memastikan tingkat keamanan yang lebih tinggi.

Secara keseluruhan, untuk memastikan integritas dan keamanan data biometrik pengguna, diperlukan kombinasi teknologi canggih, kebijakan keamanan yang ketat, serta pengawasan yang terus-menerus terhadap potensi risiko. Implementasi langkah-langkah ini akan membantu menjaga kepercayaan pengguna terhadap teknologi biometrik pada *smartphone* dan mencegah potensi ancaman yang dapat merugikan pengguna.

Penelitian lebih lanjut dapat diselenggarakan untuk dapat mengeksplorasi teknik *spoofing* yang lebih canggih, seperti serangan menggunakan *deepfake* atau model AI lainnya yang semakin berkembang. Selain itu, penggunaan data multispektral yang melibatkan sensor berbagai jenis, seperti inframerah dan sensor gerakan, perlu dieksplorasi lebih jauh untuk memaksimalkan ketahanan terhadap teknik spoofing. Penelitian selanjutnya juga harus mempertimbangkan penggunaan teknologi kriptografi dalam autentikasi biometrik untuk memberikan lapisan tambahan perlindungan terhadap potensi kebocoran data biometrik yang sifatnya sensitif.

Ucapan Terima Kasih: Penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada kepala prodi, dosen pembimbing atas dukungan teknis, administratif, dan logistik yang diberikan selama penelitian ini berlangsung. Penulis juga mengucapkan terima kasih kepada orangtua dan teman-teman penulis yang telah memberikan dukungan yang sungguh berarti baik secara moral maupun materi. Akhir kata, terima kasih kepada semua pihak yang secara langsung maupun tidak langsung telah membantu keberhasilan penelitian ini.

Referensi

[1] X. Zhang, D. Cheng, P. Jia, Y. Dai, and X. Xu, "An Efficient Android-Based Multimodal Biometric Authentication System with Face and Voice," *IEEE Access*, vol. 8, pp. 102757–102772, 2020, doi: 10.1109/ACCESS.2020.2999115.

[2] B. L. Ortiz, J. W. Chong, V. Gupta, M. Shoushan, K. Jung, and T. Dallas, "A Biometric Authentication Technique Using Smartphone Fingertip Photoplethysmography Signals," *IEEE Sens. J.*, vol. 22, no. 14, pp. 14237–14249, 2022, doi: 10.1109/JSEN.2022.3176248.

[3] Z. A. Zukarnain, A. Muneer, and M. K. Ab Aziz, "Authentication Securing Methods for Mobile Identity: Issues, Solutions and Challenges," *Symmetry (Basel).*, vol. 14, no. 821, pp. 1–17, 2022, doi: 10.3390/sym14040821.

[4] Z. Shen, S. Li, X. Zhao, and J. Zou, "IncreAuth: Incremental-Learning-Based Behavioral Biometric Authentication on Smartphones," *IEEE Internet Things J.*, vol. 11, no. 1, pp. 1589–1603, 2024, doi: 10.1109/JIOT.2023.3289935.

[5] O. Silasai and W. Khowfa, "The Study on Using Biometric Authentication on Mobile Device," *Int. J. Sci.*, vol. 17, no. 1, pp. 90–110, 2020, [Online]. Available: https://www.sci.nu.ac.th/sciencejournal/index.php/sci/article/view/ID457 .

[6] S. A. Lone and A. H. Mir, "Smartphone-based Biometric Authentication Scheme for Access Control Management in Client-server Environment," *Int. J. Inf. Technol. Comput. Sci.*, vol. 14, no. 4, pp. 34–47, 2022, doi: 10.5815/ijitcs.2022.04.04.

[7] N. Nurazela and T. Wibowo, "PERANCANGAN DAN IMPLEMENTASI ABSENSI KARYAWAN BERBASIS BIOMETRIC PADA PT. BANGUN SEJAHTERA ABADIJAYA," *Conf. Business, Soc. …*, vol. 1, no. 1, pp. 329–335, 2020, [Online]. Available: https://ojs.digitalartisan.co.id/index.php/cbssit/article/view/1433.

[8] N. Mamuriyah, S. E. Prasetyo, and A. O. Sijabat, "Rancangan Sistem Keamanan Jaringan dari serangan DDoS Menggunakan Metode Pengujian Penetrasi," *J. Teknol. Dan Sist. Inf. Bisnis*, vol. 6, no. 1, pp. 162–167, 2024, doi: 10.47233/jteksis.v6i1.1124.

[9] V. Kumar, A. M. Ali Al-Tameemi, A. Kumari, M. Ahmad, M. W. Falah, and A. A. Abd El-Latif, "PSEBVC: Provably Secure ECC and Biometric Based Authentication Framework Using Smartphone for Vehicular Cloud Environment," *IEEE Access*, vol. 10, pp. 84776–84789, 2022, doi: 10.1109/ACCESS.2022.3195807.

[10] J. Lee, S. Park, Y. G. Kim, E. K. Lee, and J. Jo, "Advanced authentication method by geometric data analysis based on user behavior and biometrics for iot device with touchscreen," *Electron.*, vol. 10, no. 21, p. 2583, 2021, doi: 10.3390/electronics10212583.

[11] R. Alrawili, A. A. S. AlQahtani, and M. K. Khan, "Comprehensive survey: Biometric user authentication application, evaluation, and discussion," *Comput. Electr. Eng.*, vol. 119, no. 3, p. 109485, 2024, doi: 10.1016/j.compeleceng.2024.109485.

[12] T. Yudha, "Punya Celah, Sistem Keamanan Fingerprint Ternyata Masih Bisa Dibobol," *https://tekno.sindonews.com/*, 2023. https://tekno.sindonews.com/read/1106543/122/punya-celah-sistem-keamanan-fingerprint-ternyata-masih-bisa-dibobol-1684847153.

[13] J. Mason, R. Dave, P. Chatterjee, I. Graham-Allen, A. Esterline, and K. Roy, "An Investigation of Biometric Authentication in the Healthcare Environment," *Array*, vol. 8, p. 100042, 2020, doi: 10.1016/j.array.2020.100042.

[14] S. Alwahaishi and J. Zdralek, "Biometric Authentication Security: An Overview," in *Proceedings - 2020 IEEE International Conference on Cloud Computing in Emerging Markets, CCEM 2020*, 2020, pp. 87–91, doi: 10.1109/CCEM50674.2020.00027.

[15] Y. Chen and Y. He, "BrutePrint: Expose Smartphone Fingerprint Authentication to Brute-force Attack," *ArXiv*, vol. abs/2305.1, pp. 1–15, 2023, doi: 10.48550/arXiv.2305.10791.

[16] Sun, Ruimin, et al. "A praise for defensive programming: Leveraging uncertainty for effective malware mitigation." *IEEE Transactions on Dependable and Secure Computing* vol 19(1), 2020, pp 353-369. doi: 10.1109/TDSC.2020.2986112

[17] T. Geppert, S. Deml, D. Sturzenegger, and N. Ebert, "Trusted Execution Environments: Applications and Organizational Challenges," *Front. Comput. Sci.*, vol. 4, pp. 1–6, 2022, doi: 10.3389/fcomp.2022.930741.

[18] M. Marcel Busch and T. Westphal, Johannes Mueller, "Unearthing the TrustedCore: A Critical Review on Huawei's Trusted Execution Environment," in *14th USENIX Workshop on Offensive Technologies (WOOT 20)*, 2002.

[19] D. Das, J. Danial, A. Golder, S. Ghosh, A. Raychowdhury, and S. Sen, "Deep Learning Side-Channel Attack Resilient AES-256 using Current Domain Signature Attenuation in 65nm CMOS," in *Proceedings of the Custom Integrated Circuits Conference*, 2020, pp. 1–4, doi: 10.1109/CICC48029.2020.9075889.

[20] E. S. Marsiani, I. Setiadi, and A. Cahyo, "Implementasi Sistem Keamanan AES 256-Bit GCM Guna Mengamankan Data Pribadi," *JRKT (Jurnal Rekayasa Komputasi Ter.*, vol. 1, no. 2, 2021, pp. 108–114, doi: 10.30998/jrkt.v1i02.4096.

[21] A. J. Jacob and I. T. Samuel, "Development of mechanism for meter tamper detections and counter measures," *J. Multidiscip. Eng. Sci. Technol.*, vol. 7, no. 7, pp. 13641–13652, 2020, [Online]. Available: https://www.jmest.org/wp-content/uploads/JMESTN42353763.pdf.

[22] F. Sthevanie, A. Dwi, Y. #2, K. Nur, and R. #3, "Deteksi Spoofing Wajah Manusia Berbasis Video menggunakan Metode Local Derivative Pattern-Three Orthogonal Planes," *Ind. J. Comput.*, vol. 5, no. 1, pp. 53–62, 2020, doi: 10.21108/indojc.2020.5.1.376.

[23] Markert, Philipp, et al. "On the security of smartphone unlock pins." *ACM Transactions on Privacy and Security (TOPS)* vol 24(4), 2021, pp 1-36, doi: 10.1145/3473040

[24] Wang, Chen, et al. "User authentication on mobile devices: Approaches, threats and trends." *Computer Networks* 170, 2020, doi: 10.1016/j.comnet.2020.107118

[25] Markert, Philipp, et al. "This pin can be easily guessed: Analyzing the security of smartphone unlock pins." *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020. doi: 10.1109/SP40000.2020.00100

[26] Li, Zengpeng, Ding Wang, and Eduardo Morais. "Quantum-safe round-optimal password authentication for mobile devices." *IEEE transactions on dependable and secure computing* vol 19(3), 2020, pp 1885-1899, doi: 10.1109/TDSC.2020.3040776

[27] Arora, Shefali, and MP S. Bhatia. "Fingerprint spoofing detection to improve customer security in mobile financial applications using deep learning." *Arabian journal for science and engineering* vol 45(4), 2020, pp 2847-2863. https://link.springer.com/article/10.1007/s13369-019-04190-1

[28] Sudeep, Sista Venkata Naga Veerabhadra Sai, et al. "An overview of biometrics and face spoofing detection." *ICCCE 2020: Proceedings of the 3rd International Conference on Communications and Cyber Physical Engineering*. Springer Singapore, 2021. doi: 10.1007/978-981-15-7961-5_82

[29] Kumar, Sandeep, et al. "Face spoofing, age, gender and facial expression recognition using advance neural network architecture-based biometric system." *Sensors* vol 22(14), 2022. doi: 10.3390/s22145160

[30] Bodepudi, Anusha, and Manjunath Reddy. "Spoofing attacks and mitigation strategies in biometrics-as-a-service systems." *Eigenpub Review of Science and Technology* vol 4(1), 2020, pp 1-14. https://studies.eigenpub.com/index.php/erst/article/view/10

[31] Ebihara, Akinori F., Kazuyuki Sakurai, and Hitoshi Imaoka. "Efficient face spoofing detection with flash." *IEEE Transactions on Biometrics, Behavior, and Identity Science* vol 3(4), 2021, pp 535-549. doi: 10.1109/TBIOM.2021.3076816

[32] .Anthony, Peter, Betul Ay, and Galip Aydin. "A review of face anti-spoofing methods for face recognition systems." *2021 International Conference on INnovations in Intelligent SysTems and Applications (INISTA)*. IEEE, 2021. 10.1109/INISTA52262.2021.9548404

[33] Shibel, Ahmed Muthanna, et al. "Deep learning detection of facial biometric presentation attack." *Life-Sciences* 8.2 (2022): 01-18. doi: 10.20319/lijhls.2022.82.0118

[34] Marutotamtama, Jane Chrestella, and Iwan Setyawan. "Face Recognition and Face Spoofing Detector for Attendance System." *2022 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*. IEEE, 2022. 10.1109/ISRITI56927.2022.10052985

[35] Kim, Seung-Hyun, Su-Min Jeon, and Eui Chul Lee. "Face biometric spoof detection method using a remote photoplethysmography signal." *Sensors* vol 22(8), 2022. doi: 10.3390/s22083070

[36] Ebihara, Akinori F., Kazuyuki Sakurai, and Hitoshi Imaoka. "Efficient face spoofing detection with flash." *IEEE Transactions on Biometrics, Behavior, and Identity Science* vol 3(4), 2021 535-549. doi: 10.1109/TBIOM.2021.3076816

[37] Kaur, Harkeerat, and Pritee Khanna. "Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing." *Future Generation Computer Systems* vol 102, 2020, 30-41. doi: 10.1016/j.future.2019.07.023

[38] Huszár, Viktor Dénes, and Vamsi Kiran Adhikarla. "Live spoofing detection for automatic human activity recognition applications." *Sensors* vol 21(21), 2021. doi: 10.3390/s21217339

[39] Xu, Xiang, et al. "Principles of Designing Robust Remote Face Anti-Spoofing Systems." *arXiv preprint arXiv:2406.03684*, 2024. doi: 10.48550/arXiv.2406.03684

[40] Lalouani, Wassila, Yi Dang, and Mohamed Younis. "Mitigating voltage fingerprint spoofing attacks on the controller area network bus." *Cluster Computing* vol 26(2), 2023, pp 1447-1460. https://link.springer.com/article/10.1007/s10586-022-03821-x