P-ISSN : 2580-4316
https://doi.org/10.37817/ikraith-informatika.v10i2 E-ISSN : 2654-8054

Perancangan dan Implementasi Sistem Pembangkitan Kunci Kriptografi Deterministik Berbasis Biometrik Sidik Jari pada Android

[1]Imam Faozi, [2]M. Imam Sulistyo Sarjowo, [3]M. Agus Sunandar
[123]Program Studi Teknik Informatika, Sekolah Tinggi Teknologi Wastukancana, Purwakarta

E-mail: [1]imamfaozi1220@gmail.com

ABSTRAK

Keamanan data digital pada platform Android bergantung pada kriptografi, namun metode autentikasi konvensional seperti kata sandi rentan terhadap serangan dan risiko terlupa. Autentikasi biometrik sidik jari merupakan solusi yang lebih aman, namun memiliki kendala pada sifat data biologis yang fuzzy atau tidak konsisten, yang bertentangan dengan kebutuhan kunci kriptografi yang deterministik. Selain itu, sensor smartphone modern memiliki keterbatasan luas area sensor yang hanya mampu menangkap 10–15% area sidik jari secara parsial. Penelitian ini bertujuan merancang dan membangun aplikasi menggunakan framework Flutter yang memanfaatkan Trusted Execution Environment (TEE) Android untuk memvalidasi sidik jari. Metode pengembangan menggunakan model Waterfall yang mencakup tahap analisis, desain, implementasi, dan pengujian. Sistem mendelegasikan validasi biometrik ke TEE untuk menjamin privasi. Setelah autentikasi berhasil, sistem menarik Helper Data dari basis data cloud (Supabase) dan menggabungkannya dengan identitas pengguna menggunakan algoritma SHA-256 untuk menghasilkan kunci privat. Hasil pengujian Black-Box menunjukkan bahwa sistem berhasil membangkitkan kunci kriptografi 256-bit yang 100% konsisten pada setiap pemindaian yang divalidasi oleh TEE. Pendekatan ini efektif mengatasi batasan hardware sensor tanpa mengekspos data biologis mentah, sehingga andal sebagai mekanisme passwordless tingkat tinggi pada perangkat mobile.

Kata kunci : Kriptografi, Biometrik Sidik Jari, Deterministik, SHA-256, Trusted Execution Environment (TEE), Flutter.

ABSTRACT

Digital data security on Android platforms relies heavily on cryptography, yet conventional authentication methods such as passwords are increasingly vulnerable to cyberattacks and prone to user forgetfulness. Fingerprint biometric authentication offers a secure alternative, but it faces inherent constraints due to the fuzzy nature of biological data, which is inconsistent with the rigid requirements of deterministic cryptographic keys. Furthermore, modern smartphone sensors have physical limitations, capturing only 10 to 15 percent of the fingerprint area partially. This research aims to design and build a mobile application using the Flutter framework to bridge these biometric reading inconsistencies. The development process utilizes the Waterfall model, including analysis, design, implementation, and testing phases. The system delegates biometric validation to the Android native Trusted Execution Environment (TEE) to ensure data privacy. Upon successful authentication, the system retrieves Helper Data from a cloud database (Supabase) and concatenates it with the user's identity. This combination is then fused using the SHA-256 one-way hash algorithm to generate a private key. Black-Box testing results demonstrate that the system

P-ISSN : 2580-4316
E-ISSN : 2654-8054 https://doi.org/10.37817/ikraith-informatika.v10i2

successfully generates a 256-bit private cryptographic key that is 100% consistent for every scan validated by the TEE. This architectural approach effectively overcomes hardware sensor limitations without exposing raw biological data, making it highly reliable as a high-level passwordless security mechanism on mobile devices.

Keyword : Cryptography, Fingerprint Biometrics, Deterministic, SHA-256, Trusted Execution Environment (TEE), Flutter.

1. PENDAHULUAN

1.1 Latar Belakang

Keamanan data digital pada platform Android kini menjadi kebutuhan vital seiring tingginya volume pertukaran informasi sensitif setiap harinya. Kriptografi merupakan pilar utama perlindungan data melalui enkripsi, namun efektivitasnya sangat bertumpu pada pengelolaan kunci. Penggunaan metode autentikasi konvensional seperti kata sandi atau PIN dinilai tidak lagi efektif di dunia nyata karena rentan terhadap serangan siber dan risiko terlupa.

Autentikasi biometrik sidik jari hadir sebagai solusi potensial menggantikan sandi konvensional. Namun, terdapat kontradiksi ketika karakteristik biometrik diadopsi untuk membangkitkan kunci kriptografi yang bersifat deterministik. Data sidik jari secara alamiah bersifat *fuzzy* dan tidak pernah identik 100% pada setiap pemindaian. Kondisi ini diperparah oleh keterbatasan fisik sensor *smartphone* yang rata-rata hanya mampu menangkap 10–15% area sidik jari secara parsial dalam satu waktu.

Guna menjembatani celah tersebut, penelitian ini mengusulkan rancang bangun aplikasi *mobile* menggunakan *framework* Flutter yang memanfaatkan validasi *Trusted Execution Environment* (TEE) bawaan Android. Sistem dirancang untuk mengintegrasikan logika penanganan data penunjuk (*helper data*) dengan fungsi *hash* deterministik untuk mengatasi masalah pembacaan sensor parsial.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, rumusan masalah dalam penelitian ini adalah:

a. Bagaimana merancang arsitektur sistem pembangkit kunci kriptografi yang memanfaatkan validasi biometrik *native* Android melalui TEE untuk menjembatani masalah inkonsistensi pembacaan akibat keterbatasan luas sensor ?

b. Bagaimana merancang sistem yang mampu menghasilkan kunci kriptografi yang selalu identik meskipun sensor hanya mampu membaca 10–15% dari total luas permukaan jempol pengguna ?

c. Bagaimana tingkat konsistensi kode output (deterministik) yang dihasilkan sistem dari berbagai posisi pemindaian jari yang berbeda-beda ?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah:

a. Merancang arsitektur sistem pembangkit kunci kriptografi yang memanfaatkan validasi biometrik *native* Android melalui TEE.

b. Membangun sistem yang mampu membangkitkan kunci kriptografi yang selalu identik secara presisi dengan integrasi *helper data*.

c. Menganalisis tingkat konsistensi kode *output* (deterministik) yang dihasilkan sistem melalui pengujian dengan berbagai variasi posisi pemindaian jari.

P-ISSN : 2580-4316
https://doi.org/10.37817/ikraith-informatika.v10i2 E-ISSN : 2654-8054

2. LANDASAN TEORI

Sistem keamanan data digital yang handal sangat dibutuhkan, terutama dalam pengembangan aplikasi *mobile* di platform Android. Untuk membangun sistem tersebut, diperlukan pemahaman mendalam mengenai konsep-konsep dasar yang mendukung arsitektur perlindungan informasi.

2.1 Kriptografi dan Pembangkitan Kunci

Kriptografi merupakan teknik mengamankan data dengan menyamarkan data asli (*plaintext*) menjadi data tersandi (*ciphertext*). Dalam implementasinya, efektivitas kriptografi bergantung pada proses pembangkitan kunci (*key generation*), yaitu proses menghasilkan untaian biner acak berentropi tinggi yang berfungsi sebagai instrumen utama enkripsi dan dekripsi.

Sifat deterministik sangat krusial dalam kriptografi. Deterministik memastikan bahwa sebuah algoritma akan selalu menghasilkan keluaran yang konsisten jika diberikan masukan yang sama persis. Perubahan satu bit pada *input* akan menyebabkan kegagalan total sistem.

2.2 Autentikasi Biometrik Sidik Jari

Sistem berbasis biometrik memverifikasi identitas menggunakan karakteristik fisik atau perilaku unik, menawarkan keamanan yang lebih tinggi dibandingkan kata sandi konvensional. Sidik jari adalah modalitas biometrik yang umum digunakan. Meskipun polanya permanen, hasil pembacaan sensor fisiknya selalu berubah-ubah (*fuzzy*) akibat pengaruh lingkungan dan posisi jari.

2.3 Fungsi Hash SHA-256 dan Fuzzy Extractor

Algoritma SHA-256 (*Secure Hash Algorithm 256-bit*) memproses masukan menjadi nilai *hash* sepanjang 256 bit. Algoritma ini bersifat deterministik dan satu arah (*one-way*), menjadikannya ideal untuk pembangkitan kunci kriptografi karena data asli tidak dapat direkayasa balik.

Untuk mengatasi variasi (*fuzzy*) pada data biometrik, sistem menggunakan konsep *Fuzzy Extractor* dan *Helper Data*. *Helper Data* membantu merekonstruksi kunci secara deterministik tanpa perlu menyimpan data biometrik asli, sehingga menjaga privasi pengguna.

2.4 Keamanan Perangkat Keras Android (TEE)

Android *Keystore* dan *Trusted Execution Environment* (TEE) adalah modul keamanan *hardware* pada sistem Android. Eksekusi sensitif seperti pemadanan pola biometrik diisolasi dalam TEE, mencegah ekstraksi data kunci oleh aplikasi pihak ketiga atau *malware*. Aplikasi hanya menerima nilai verifikasi tanpa pernah mengekspos *raw data* biometrik.

2.5 Pengembangan Aplikasi Mobile

Aplikasi dibangun menggunakan *framework* Flutter, *UI toolkit* dari Google yang mendukung pengembangan lintas platform dengan performa tinggi. Bahasa pemrograman utama yang digunakan adalah Dart, yang mendukung kompilasi *Ahead-Of-Time* (AOT) untuk eksekusi algoritma kriptografi yang cepat dan efisien. Data pembantu (*Helper Data*) disimpan secara aman menggunakan layanan *Backend-as-a-Service* (BaaS) Supabase, sebuah basis data relasional berbasis PostgreSQL.

Pengembangan perangkat lunak mengikuti model *Software Development Life Cycle* (SDLC) Waterfall, yang sistematis dan sekuensial, sangat cocok untuk penelitian kriptografi yang

P-ISSN : 2580-4316
E-ISSN : 2654-8054 https://doi.org/10.37817/ikraith-informatika.v10i2

membutuhkan presisi tinggi dari tahap analisis hingga *deployment*.

3. METODOLOGI

Dalam melaksanakan penelitian ini, penulis menggunakan metode penyelesaian masalah yang mengacu pada kerangka kerja *Software Development Life Cycle* (SDLC) dengan model *Waterfall*. Pendekatan ini memastikan bahwa pengembangan model dilakukan secara sistematis, mulai dari memahami masalah hingga menerapkan solusi perangkat lunak yang dapat digunakan secara nyata.

Tahapan penelitian meliputi:

3.1 Analysis

Tahap ini merupakan fase awal yang menggabungkan proses komunikasi dan *Requirements Gathering* (pengumpulan kebutuhan). Pada tahap ini dilakukan identifikasi masalah utama, yaitu ketidakstabilan data sidik jari yang menyebabkan kunci kriptografi menjadi tidak konsisten. Berdasarkan analisis, kebutuhan sistem dirancang untuk menghasilkan kunci deterministik dari pindaian sidik jari yang bersifat *noisy*.

3.2 Data Requirement

Tahap ini berfokus pada penyiapan komponen data tanpa mengekspos data biologis mentah. Kebutuhan data mencakup *token* validasi otentikasi yang diekstraksi dari API biometrik *native* Android melalui modul *local_auth*, parameter *Helper Data* kriptografi yang disimpan di *cloud database* (Supabase), serta *Email* anonim. Kombinasi data ini dipersiapkan untuk diproses menjadi representasi heksadesimal yang stabil.

3.3 Modeling

Tahap *Modeling* mencakup perancangan arsitektur pembangkitan kunci dan manajemen keamanan pada Android *Keystore*. Alur logika dirancang di mana keberhasilan otentikasi biometrik dari *Trusted Execution Environment* (TEE) memicu penggabungan parameter *Helper Data* dan *Email*, yang kemudian diproses melalui fungsi *hash* deterministik (SHA-256).

Proses pembangkitan kunci tidak dilakukan secara acak, melainkan menggunakan penggabungan linier antara identitas pengguna dan data pembantu, dengan rumus:

$$Kpriv = SHA - 256(IDuser \parallel HD)$$

3.4 Coding

Tahap ini merupakan proses pengembangan aplikasi menggunakan *framework* Flutter dan bahasa Dart serta integrasi sensor biometrik. Implementasi teknis dilakukan dengan memanfaatkan pustaka *local_auth* untuk komunikasi dengan sensor fisik. Fokus utama adalah sinkronisasi antara deteksi sidik jari dengan proses pembangkitan kunci di latar belakang sistem.

3.5 Evaluation

Evaluasi dilakukan dengan pendekatan *Black Box Testing* untuk menguji stabilitas dan determinisme kunci yang dihasilkan. Pengujian difokuskan pada observasi *output string* heksadesimal saat dilakukan berbagai variasi pemindaian jari yang sama, guna memastikan keandalan mekanisme penanganan inkonsistensi biometrik.

3.6 Deployment

Tahap akhir penelitian meliputi finalisasi aplikasi menjadi *file* APK, pengujian kompatibilitas sistem secara langsung melalui uji coba lintas perangkat (*multi-device testing*), dan penyusunan laporan. Aplikasi diuji pada perangkat dengan berbagai spesifikasi *hardware* dan sensor untuk memastikan algoritma

https://doi.org/10.37817/ikraith-informatika.v10i2
P-ISSN : 2580-4316
E-ISSN : 2654-8054

pembangkitan kunci berjalan dengan konsisten.

4. HASIL DAN PEMBAHASAN

Hasil dan pembahasan pada bagian ini menguraikan implementasi sistem yang telah dibangun serta analisis dari pengujian fungsionalitas dan konsistensi algoritma pembangkitan kunci kriptografi berbasis biometrik sidik jari.

4.1 Implementasi Algoritma dan Program

Implementasi algoritma pada sistem ini berfokus pada sinkronisasi antara perangkat keras sensor sidik jari dengan logika komputasi di latar belakang. Sistem mendelegasikan validasi biometrik sepenuhnya ke dalam *Trusted Execution Environment* (TEE). Setelah TEE memvalidasi kecocokan sidik jari, sistem akan menarik *Helper Data* dari *cloud database* (Supabase).

Tahapan selanjutnya adalah melakukan penggabungan (*concatenation*) antara identitas *Email* pengguna dan *Helper Data*. Hasil gabungan tersebut kemudian dikonversi menjadi susunan *byte* dan dilebur menggunakan fungsi *hash* SHA-256 untuk menghasilkan Kunci Privat 256-bit. Algoritma inti pembangkitan kunci privat tersebut dapat dilihat seperti di bawah ini.

```
import 'dart:convert';
 import 'package:crypto/crypto.dart';

 String generatePrivateKey(String email, String helperData) {
   // Melakukan concatenation (Email + Helper Data)
   String combinedInput = email + helperData;

   // Mengonversi string menjadi bytes
   var bytes = utf8.encode(combinedInput);

   // Mengeksekusi algoritma hash SHA-256
   var digest = sha256.convert(bytes);

// Mengembalikan output Kunci Privat dalam bentuk String hex
return digest.toString();
}
```

4.2 Hasil Pengujian Sistem

Pengujian sistem dilakukan dengan menggunakan metode *Black-Box Testing* yang berfokus pada fungsionalitas dan keluaran (*output*) aplikasi. Berdasarkan skenario pengujian, sistem terbukti berhasil memvalidasi format surel, mendaftarkan *Device ID*, serta merekam status aktif sensor sidik jari ke dalam basis data.

Pengujian pada fitur utama "Generate Kunci Privat" menunjukkan bahwa ketika pengguna memasukkan surel yang valid dan melakukan pindaian sidik jari yang cocok, sistem berhasil menarik *Helper Data*, mengeksekusi algoritma SHA-256, dan menampilkan kunci privat berbentuk QR Code maupun teks *string* heksadesimal 64 karakter. Selain itu, fitur "Keluar Aplikasi" (*logout*) juga berjalan sesuai prosedur dengan menghapus data sesi sementara (*cache*) dari memori sehingga keamanan tetap terjaga setelah sesi berakhir.

4.3 Pembahasan (Evaluasi Deterministik)

Tantangan terbesar dalam penggunaan sidik jari sebagai basis kunci kriptografi adalah karakteristik biometrik yang bersifat *fuzzy* (tidak konsisten) serta keterbatasan fisik sensor *smartphone* modern. Rata-rata sensor hanya mampu menangkap 10–15% area sidik jari secara

P-ISSN : 2580-4316
E-ISSN : 2654-8054 https://doi.org/10.37817/ikraith-informatika.v10i2

parsial dalam satu waktu, yang berpotensi menghasilkan *output* yang berubah-ubah pada setiap pemindaian.

Hasil evaluasi secara langsung menggunakan lintas perangkat (perangkat keras yang berbeda) membuktikan bahwa sistem yang dirancang berhasil mengatasi masalah ini. Penggabungan *Helper Data* berentropi tinggi sebagai *cryptographic salt* dengan identitas pengguna memastikan bahwa fungsi *hash* selalu memproses masukan yang sama persis selama TEE memberikan persetujuan (nilai *True*).

Hasilnya, algoritma secara konsisten memproduksi Kunci Privat 256-bit yang 100% identik mutlak pada setiap pemindaian jari yang sah. Pendekatan ini secara efektif memisahkan data biologis mentah dari memori aplikasi (mengadopsi konsep *Zero-Knowledge*), memberikan tingkat deterministik yang sempurna untuk kebutuhan kriptografi, serta memitigasi risiko keamanan konvensional akibat kelalaian kata sandi.

5. KESIMPULAN

Berdasarkan hasil analisis, perancangan, implementasi, serta pengujian yang telah dilakukan, dapat disimpulkan bahwa arsitektur sistem pembangkit kunci kriptografi berhasil dirancang dengan memanfaatkan validasi biometrik *native* Android melalui *Trusted Execution Environment* (TEE). Pendekatan ini efektif menjembatani masalah inkonsistensi pembacaan data mentah sidik jari dengan mendelegasikan proses pemadanan pola ke tingkat keamanan perangkat keras, tanpa perlu mengekspos data biologis pengguna ke memori aplikasi. Sistem terbukti mampu membangkitkan kunci kriptografi privat yang 100% konsisten secara presisi, meskipun sensor fisik pemindai memiliki keterbatasan dalam membaca luas permukaan jempol pengguna secara utuh. Melalui skema penggabungan (*concatenation*) identitas pengguna dan *Helper Data* yang dilebur menggunakan fungsi *hash* SHA-256, *output* berupa *string* heksadesimal 256-bit menunjukkan tingkat deterministik yang sempurna, menjadikan sistem ini sangat andal sebagai alternatif mekanisme keamanan *passwordless* pada perangkat *mobile*.

6. UCAPAN TERIMA KASIH

Penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada Sekolah Tinggi Teknologi Wastukancana Purwakarta, khususnya Bapak Dr. Ir. Apang Djafar Shieddieque, S.T., M.T. IPM., ASEAN Eng. (Ketua STT Wastukancana) dan Bapak Teguh Iman Hermanto, S.Kom, M.Kom. (Ketua Program Studi Teknik Informatika), atas fasilitas dan dukungan institusional yang diberikan. Terima kasih juga dihaturkan secara khusus kepada Bapak M. Imam Sulistyo Sarjowo, S.Si, M.Si. selaku pembimbing utama, dan Bapak M. Agus Sunandar, S.T, M.Kom. selaku pembimbing pendamping, atas arahan, diskusi ilmiah, bimbingan, serta evaluasi komprehensif yang sangat berarti selama proses penelitian dan penyusunan naskah ilmiah ini berlangsung.

DAFTAR PUSTAKA

Al-Fedaghi, O. (2021). UML Sequence Diagram: An Alternative Model. *International Journal of Advanced Computer Science and Applications*, *12*(5), 1–10.

Alwajeeh, M. S., Sufyan, M., AlSarori, M. H., Al-Asaly, M. S., & AlMaamari, G. A. A. (2025). A

systematic review of cognitive passwords: Limitations, challenges, and solutions. *Journal of Intelligent Communication*.

Chao, L., Nazaré, T. E., & Nepomuceno, E. (2023). Key generation from fingerprint biometric. Dalam *2023 15th IEEE International Conference on Industry Applications (INDUSCON)* (hlm. 611–612). São Paulo, Brazil.

Gupta, N. K., Meena, S., Kumar, P., Dobhal, V. C., & Kaur, M. (2021). Template security using fuzzy extractor: A review. Dalam *Proceedings of the International Conference on Computer Science* (hlm. 809–825).

Hidayat, R., Pratama, A., & Kurniawan, B. (2023). Integrasi Android Keystore dan Fingerprint API untuk pengamanan aplikasi mobile. *JUTI: Jurnal Ilmiah Teknologi Informasi*, *21*(1), 45–53.

Imran, A., & Bianchi, A. (2024). Automated detection of cryptographic inconsistencies in android's keymaster implementations. Dalam *Proceedings of the IEEE Symposium on Security and Privacy (S&P)* (hlm. 1–15).

Koç, H., Erdoğan, A. M., Barjakly, Y., & Peker, S. (2021). UML diagrams in software engineering research: A systematic literature review. *MDPI Proceedings*, *74*(1), 13.

Kusuma, W., Saputra, D., & Hidayat, R. (2020). Peningkatan keamanan data melalui penggabungan SHA-256 dan data biometrik pengguna. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, *5*(3), 211–218.

Maspupah, A. (2024). Literature review: advantages and disadvantages of black box and white box testing methods. *Jurnal Techno Nusa Mandiri*, *21*(2), 151–162.

Pratama, A., Wibowo, B., & Santoso, C. (2022). Implementasi keamanan data menggunakan kriptografi AES dan autentikasi biometrik pada Android. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *6*(4), 654–661.

Putra, G. R., Situmorang, B. H., & Hidayatullah, S. (2023). Identifikasi biometrika menggunakan ekstraksi minutiae pada citra sidik jari. *Jurnal Teknoinfo*, *17*(1), 15–24.

Rahmawati, D., & Kurniawan, A. (2024). Pengamanan transmisi data menggunakan kombinasi cipher simetris dan identitas perangkat (Device ID). *JSI: Jurnal Sistem Informasi*, *16*(1), 89–97.

Santhosh, A., Tiji, A., Anuraj, T. R., Thomas, N., Anoop, A., & Varghese, T. (2024). Cross-platform innovation: The rise and impact of flutter in modern app development. *Deleted Journal*, *2*(12), 3560–3569.

Saputra, H., & Wijaya, K. (2024). Evaluasi keamanan sistem autentikasi biometrik pada aplikasi mobile berbasis Flutter. *Jurnal Teknologi dan Sistem Komputer*, *12*(2), 112–120.

Septiansyah, A., Hasanah, S., Permatasari, V. N., & Yuliawati, A. (2024). Sistem informasi otomatisasi pelaporan data

penjualan toko buku nazwa yang masuk dan yang keluar. *IKRAITH-INFORMATIKA*, *8*(1), 108–116.

Setiawan, B., & Nugroho, A. (2021). Penerapan fuzzy extractor untuk pembangkitan kunci kriptografi berbasis sidik jari. *JNTETI (Jurnal Nasional Teknik Elektro dan Teknologi Informasi)*, *10*(3), 234–241.

Susanto, E., & Aryanto, D. (2023). Model keamanan kriptografi berbasis partial fingerprint matching di lingkungan smartphone. *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, *9*(1), 55–63.

Syahid, M., Wahid, N., Najafi, A. M., Sihaj, A., Alik, R., Az, A., & Irsani, Z. (2023). TECHNES: Penyedia layanan jasa service berbasis aplikasi android. *Jurnal Teknologi dan Sistem Informasi Bisnis*, *5*(1), 20–28.

Voronova, A., & Ivanov, A. (2021). The influence of the accuracy of data representation on the cryptographic properties of digital encryption systems. Dalam *Proceedings of the International Conference on Information Security* (hlm. 10–15).

Yuliana, S., Pratama, R., & Kusuma, A. (2025). Rancang bangun sistem passwordless berbasis biometrik sidik jari pada aplikasi pendataan. *JuTISI (Jurnal Teknik Informatika dan Sistem Informasi)*, *11*(1), 34–42.