Implementasi Kriptografi Hibrida Ascon AEAD dan ECDH pada Sistem Pemantauan Elektrokardiogram Jarak Jauh

Mochammad Fatchur Rochman
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
13519009@std.stei.itb.ac.id

Rinaldi Munir
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
rinaldi@staff.stei.itb.ac.id

***Abstrak*— Sistem pemantauan elektrokardiogram (EKG) jarak jauh adalah sistem yang melakukan pemantauan kondisi jantung secara jarak jauh untuk deteksi dini terhadap segala jenis kelainan jantung. Data EKG yang dibawa sistem bersifat sensitif sehingga kebocoran, modifikasi, atau akses tidak sah dapat berdampak serius terhadap privasi dan keselamatan pasien. Tugas akhir ini mengusulkan implementasi kriptografi hibrida menggunakan Ascon AEAD (Authenticated Encryption with Associated Data) dan ECDH (Elliptic-curve Diffie–Hellman) pada sistem pemantauan EKG jarak jauh. Ascon AEAD digunakan untuk menjaga kerahasiaan dan integritas data, sedangkan ECDH memastikan data EKG dikirimkan pada pihak yang tepat dengan membentuk kunci enkripsi dan dekripsi yang hanya diketahui oleh pengirim dan penerima. Evaluasi dilakukan melalui pengujian latensi, serta uji penyadapan dan modifikasi data. Hasil menunjukkan metode ini mampu melindungi kerahasiaan dan integritas data EKG dengan rata-rata latensi 29,0840 ms pada 500 sampel, yang memenuhi batasan latensi untuk skenario pemantauan kesehatan yang ditargetkan.**

Kata Kunci—Sistem pemantauan EKG jarak jauh, kriprografi hibrida, Ascon AEAD, ECDH

I. PENDAHULUAN

Sistem pemantauan EKG jarak jauh bekerja dengan membaca sinyal listrik jantung melalui sensor EKG, kemudian mengirimkannya secara nirkabel ke aplikasi pengguna. Data EKG merupakan informasi medis yang bersifat sensitif karena digunakan sebagai dasar untuk melakukan deteksi kelainan pada segala jenis penyakit jantung dari pemilik data EKG. Kebocoran, modifikasi, atau akses tidak sah terhadap data EKG dapat menimbulkan dampak serius, baik dari sisi privasi seperti terungkapnya informasi kesehatan maupun dari sisi keselamatan, seperti terjadinya kesalahan diagnosis akibat manipulasi data.

Ascon AEAD adalah algoritma yang telah ditetapkan sebagai standar enkripsi terotentikasi ringan oleh NIST pada 2023, menawarkan enkripsi terotentikasi dengan efisiensi tinggi untuk menjaga kerahasiaan dan integritas data, bahkan pada perangkat dengan keterbatasan sumber daya. Sementara itu, Elliptic Curve Diffie–Hellman (ECDH) menyediakan metode pertukaran kunci yang aman untuk membentuk kunci rahasia bersama, yang kemudian digunakan dalam proses enkripsi dan dekripsi, sekaligus mendukung autentikasi antar pihak yang berkomunikasi.

Dengan mengimplementasikan kriptografi hibrida Ascon AEAD dan ECDH pada sistem pemantauan EKG jarak jauh dapat menjaga kerahasiaan, integritas dan autentikasi dari data EKG yang dikirimkan. Pada penelitian ini akan berfokus pada perancangan arsitektur sistem pemantauan EKG yang aman dan optimal.

II. ANALISIS MASALAH

Arsitektur sistem pemantauan EKG jarak jauh berdasarkan Ciuffoletti, 2019 ataupun Bushnag, 2022 [4][5] secara terdiri dari tiga entitas utama, yaitu IoT (sensor dan mikrokontroler) untuk membaca dan mengirim data EKG, backend (server/cloud) untuk analisis, penyimpanan, menyampaikan data EKG ke frontend/antarmuka, serta frontend sebagai antarmuka pengguna untuk menampilkan data EKG. Sehingga data EKG akan melewati setidaknya dua proses transmisi data yaitu ketika data EKG dikirimkan dari IoT ke *backend* dan dari *backend* ke *frontend*.

Sistem pemantauan EKG jarak jauh umumnya beroperasi secara real-time untuk memastikan deteksi kelainan jantung. Protokol MQTT dan websocket adalah protokol yang didesain untuk menangani komunikasi yang berjalan secara real-time, namun kedua protokol tersebut memiliki kasus penggunaan yang berbeda, MQTT cocok digunakan untuk pengiriman data pada perangkat berdaya rendah seperti IoT, sedangkan websocket cocok sebagai protokol komunikasi aplikasi web aplikasi web dan perangkat yang tidak dibatasi oleh bandwidth rendah, seperti *backend* dengan *frontend*.

Saat ini, pengamanan data EKG pada sebagian besar arsitektur sistem pemantauan EKG jarak jauh umumnya hanya mengandalkan penggunaan protokol SSL/TLS untuk melindungi data selama transmisi. Penggunaan SSL/TLS pada protokol MQTT terbatas melindungi data EKG pada saat transmisi yaitu saat IoT ke broker dan broker ke *subscriber*, pada saat di MQTT broker data EKG dalam keadaan tidak terenkripsi [6].

III. ANALISIS SOLUSI

Berdasarkan analisis masalah yang telah dijelaskan pada subab II, diusulkan untuk menerapkan enkripsi ujung ke ujung dengan melakukan enkripsi data EKG pada sistem pemantauan EKG jarak jauh, enkripsi ujung ke ujung dilakukan pada komunikasi antara pengiriman data EKG antara perangkat IoT dengan backend dan pada komunikasi pengiriman data EKG antara backend dengan frontend.

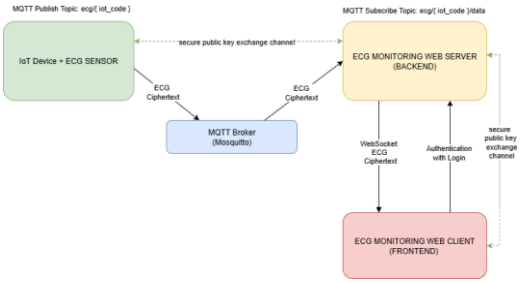
Penelitian sebelumnya telah mengeksplorasi skema kriptografi hibrida untuk mengamankan komunikasi IoT. Karmous et al. (2024) menggabungkan AES-GCM dan ECC pada infrastruktur Software Defined Network untuk mencegah serangan man-in-the-middle [1]. Chanal & Kakkasageri (2021) mengusulkan kombinasi ECC, AES, dan MD5 untuk meningkatkan kerahasiaan data pada perangkat IoT [3]. Raheja & Kumar Manocha (2022) memanfaatkan kombinasi 3-DES dan Water Cycle Optimization untuk memastikan keamanan dan autentikasi data EKG yang dikirimkan melalui IoT[2].

Skema kriptografi hibrida yang akan digunakan pada penelitian ini mengacu pada penelitian Kamous et al., 2024, dibandingkan dengan skema kriptografi yang dilakukan oleh Raheja & Kumar Manocha, 2022 karena skema Karmous et al., 2024 memungkinkan untuk pembentukkan kunci sesi yang berbeda antara IoT dengan backend maupun backend dengan frontend, sehingga tidak ada penyimpanan kunci yang bersifat statis pada sisi yang berisiko bocor seperti pada IoT dan frontend.

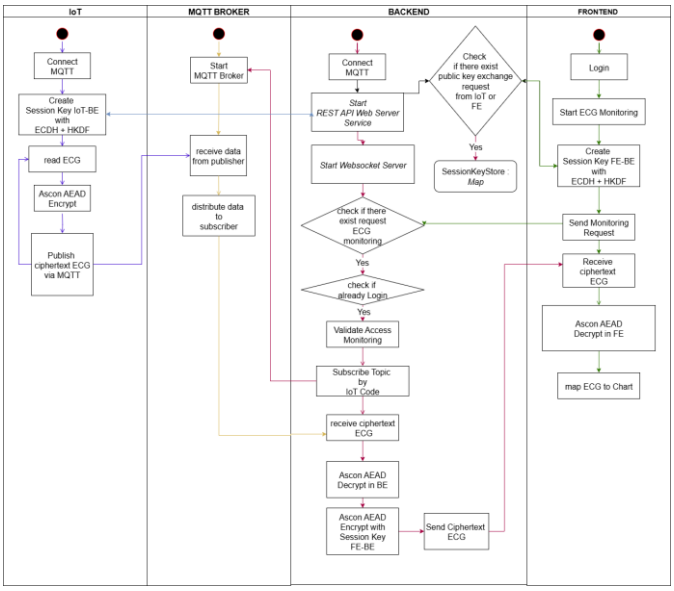
IV. RANCANGAN SOLUSI

A. *Arsitektur Umum Sistem*

Arsitektur sistem pemantauan EKG terdiri dari 4 entitas Utama yaitu perangkat IoT atau mikrokontroler, MQTT Broker, backend, dan frontend. Arsitektur Sistem dapat ditunjukkan pada Gambar 1. dan untuk proses yang dilakukan oleh setiap entitas dapat ditunjukkan pada Gambar 2.



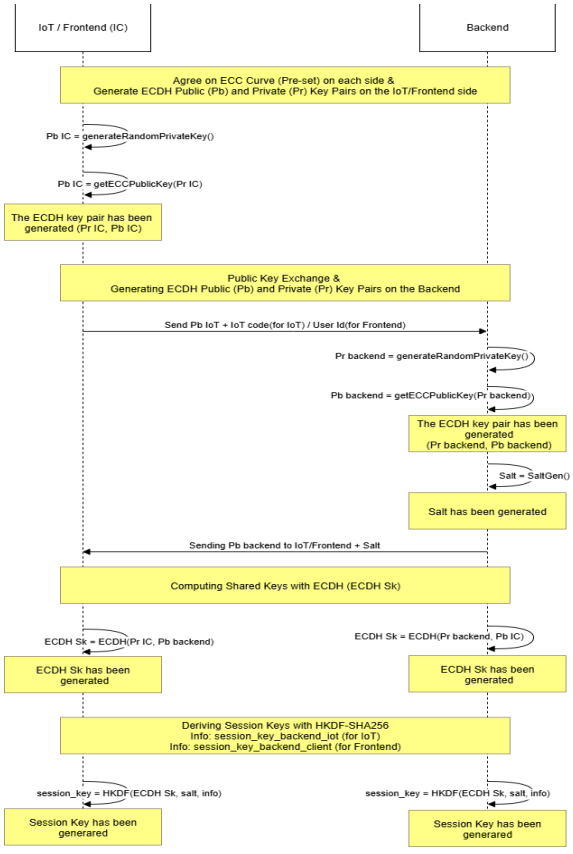
Gambar 1. Arsitektur Sistem



Gambar 2. Diagram Aktivitas Arsitektur Sistem

B. *Pembangkitan dan Derivasi Kunci Sesi*

Proses pembangkitan dan derivasi kunci menggunakan kombinasi algoritma ECDH untuk menghitung kunci bersama dan algoritma HKDF untuk melakukan derivasi kunci sesi. Proses pembangkitan kunci sesi dapat dilihat pada Gambar 3.



Gambar 3. Proses Pembangkitan Kunci Sesi

C. *Enkripsi & Decrypt*

Enkripsi data EKG dengan algoritma Ascon AEAD dapat ditunjukkan dengan persamaan 1, sedangkan proses dekripsi dapat ditujunkkan pada persamaan 2.

$$(C, T, A, N) = ASCON\_ENCRYPT(Ke,P,A,N) \quad (1)$$

$$P = ASCON\_DECRYPT(Kd,C,A,N) \quad (2)$$

Keterangan :
C adalah ciphertext dari EKG
P adalah plaintext dari EKG
T adalah tag autentikasi
A adalah data terkait
N adalah *Nonce*

Ke adalah kunci sesi untuk enkripsi yang mana memiliki dua jenis:
Kunci sesi enkripsi IoT-BE
Kunci sesi enkripsi FE-BE

Kd adalah kunci sesi untuk dekripsi yang mana memiliki dua jenis:
Kunci sesi dekripsi IoT-BE
Kunci sesi dekripsi FE-BE

V. IMPLEMENTASI

Implementasi dilakukan pada lingkungan pengembangan yang dapat ditunjukkan pada Table I dan menggunakan kakas teknologi yang dapat ditunjukkan pada Tabel II.

TABEL I. Spesifikasi Komputer dan Mikrokontroler

Spesifikasi Komputer	
Merk	Lenovo Ideapad Gaming 3
Processor	Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz 2.59 GHz
RAM	8 GB
Sistem Operasi	Windows
Tipe Sistem	64-bit operating system, x64-based processor
Spesifikasi Mikrokontroler	
Merk	ESP-WROOM-32
Microprocessor	two low-power Xtensa® 32-bit LX6
SRAM	520 kB
ROM	448 kB

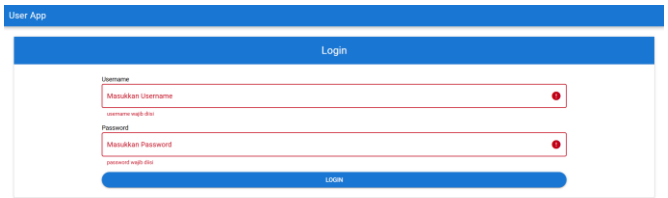
TABEL II. Teknologi Pengembangan yang digunakan

	Frontend	*Backend*	IoT
Bahasa Pemrograman	Javascript	Javascript	C++
Framework	QuasarJS	ExpressJs	PlatformIO Arduino
Pustaka fungsional	-	ellipticJs, CryptoJs	MbedTLS, esp, Crypto, CryptoLw
Basis Data	-	PostgresSQL	-

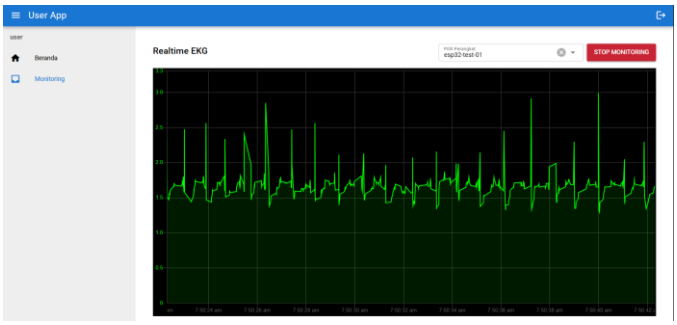
Implementasi pada sisi frontend dapat dilihat pada Table II dan Gambar 4. Sampai Gambar 6.

TABEL III. Implementasi pada sisi Frontend

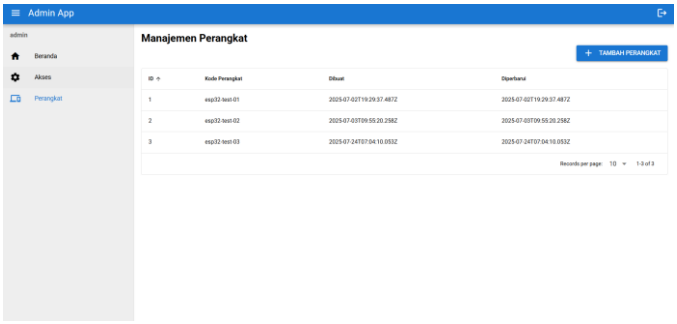
Kode	Nama	Role	Deskripsi
H-1	Halaman Login	-	Antarmuka untuk Pengguna Login / melakukan autentikasi diri
H-2	Halaman Pemantauan EKG	User	Antarmuka untuk pengguna melakukan pemantauan (*monitoring*) EKG pada perangkat tertentu
H-3	Halaman Manajemen Perangkat	Admin	Antarmuka untuk Admin mendaftarkan perangkat
H-4	Halaman Manajemen Akses Pemantauan	Admin	Antaramuka untuk Admin memberikan akses pemantauan EKG pada pengguna ke suatu perangkat



Gambar 4. Halaman Login



Gambar 5. Halaman Pemantaun EKG



Gambar 6. Halaman Manajemen Perangkat

VI. PENGUJIAN

Pengujian yang dilakukan adalah pengujian latensi dan pengujian scenario serangan penyadapan dan serangan modifikasi data/tampering data. Hasil pengujian latensi dapat dilihat pada Tabel IV dan hasil pengujian keamanan transmisi data EKG dapat dilihat pada Tabel V dan Tabel VI.

TABEL IV. Pengujian Latensi

Banyaknya data EKG yang telah sampai di *frontend*	Rata-rata Latensi (ms)
100	29.5100
200	28.7150
300	29.6233
400	28.6975
500	29.0840

Hasil pengujian latensi menunjukkan rata-rata dari pengiriman lima ratus data EKG dari IoT ke frontend adalah 29.0840 milisekon. Berdasarkan kebutuhan latensi oleh Qureshi et al., 2022, hasil pengujian latensi menunjukkan memenuhi untuk kebutuhan perangkat pemantauan tanda vital yaitu kurang dari satu detik (29.0840 ms < 1 s), dan memenuhi juga untuk kebutuhan pemantauan pada penyakit kronis yaitu kurang dari lima puluh milisekon (29.0840 ms < 50 ms) [7].

Hasil Tabel V dan Tabel VI menunjukkan skema kriptografi hibrida Ascon dan ECC yang diterapkan mampu melindungi pengiriman data EKG dari serangan penyadapan maupun modifikasi ciphertext.

TABEL V. Pengujian keamanan transmisi IoT ke backend

Kode	Skenario Pengujian	Hasil	Status Pengujian
T-IS1	Penyadapan transmisi data	Data EKG yang diamati terenkripsi	Valid
T-IS2	Tidak memodifikasi data	Data EKG sampai di *frontend* dan bisa didekripsi oleh *frontend*	Valid
T-IS3	Memodifikasi *ciphertext* data EKG yang dikirimkan	*Ciphertext* data EKG tidak dapat didekripsi	Valid

TABEL VI. Pengujian keamanan transmisi backend ke frontend

Kode	Skenario Pengujian	Hasil	Status Pengujian
T-SC1	Penyadapan transmisi data	Data EKG yang diamati terenkripsi	Valid
T-SC2	Tidak memodifikasi data	Data EKG sampai di *frontend* dan bisa didekripsi oleh *frontend*	Valid
T-SC3	Memodifikasi *ciphertext* data EKG yang dikirimkan	*Ciphertext* data EKG tidak dapat didekripsi	Valid

VII. KESIMPULAN

1. Arsitektur sistem pemantauan EKG jarak jauh terdiri dari 4 entitas utama, yaitu perangkat IoT (membaca data EKG dari sensor, penerbit data EKG), MQTT Broker (mendistribusikan data EKG dari penerbit ke pelanggan), Backend (menerima data EKG dari IoT dan memvalidasi otentikasi dan akses ke akses pemantauan data EKG), dan Frontend (antarmuka pengguna).
2. Implementasi kriptografi hybrid Ascon AEAD dan ECDH dapat dilakukan dengan melakukan proses enkripsi dengan algoritma Ascon AEAD dengan kunci yang telah disepakati antara kedua belah pihak dengan algoritma ECDH.
3. Hasil pengujian menunjukkan bahwa implementasi kriptografi hibrid Ascon AEAD dan ECDH dapat melindungi kerahasiaan dan integritas data serta memiliki latensi rata-rata 29,0840 ms pada 500 sampel yang memenuhi persyaratan latensi sistem pemantauan data kesehatan.

REFERENSI

[1] Karmous, N., Hizem, M., Ben Dhiab, Y., Ould-Elhassen Aoueileyine, M., Bouallègue, R., & Youssef, N. (2024). Hybrid Cryptographic End-to-End Encryption Method for Protecting IoT Devices Against MitM Attacks. Radioengineering, 33(4), 583–592. https://doi.org/10.13164/re.2024.0583.

[2] Raheja, N., & Kumar Manocha, A. (2022b). IOT based ECG monitoring system with encryption and authentication in Secure Data Transmission for Clinical Health Care Approach. Biomedical Signal Processing and Control, 74, 103481. https://doi.org/10.1016/j.bspc.2022.103481

[3] P. M. Chanal and M. S. Kakkasageri, "Hybrid Algorithm for Data Confidentiality in Internet of Things," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-5, doi: 10.1109/ICCCNT45670.2019.8944565.

[4] Bushnag, A. (2022). A wireless ECG Monitoring and analysis system using the IOT Cloud. Intelligent Automation & Soft Computing, 33(1), 51–70. https://doi.org/10.32604/iasc.2022.024005I.

[5] Ciuffoletti, A. (2019). Design of an open remote electrocardiogram (ECG) service. Future Internet, 11(4), 101. https://doi.org/10.3390/fi11040101 Qureshi, H. N., Manalastas, M., Ijaz, A., Imran, A., Liu, Y., & Al Kalaa, M. O. (2022). Communication requirements in 5G-enabled healthcare applications: Review and Considerations. Healthcare, 10(2), 293. https://doi.org/10.3390/healthcare10020293.

[6] A. R. Alkhafajee, A. M. A. Al-Muqarm, A. H. Alwan and Z. R. Mohammed, "Security and Performance Analysis of MQTT Protocol with TLS in IoT Networks," 2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA), Najaf, Iraq, 2021, pp. 206-211, doi: 10.1109/IICETA51758.2021.9717495.

[7] Qureshi, H. N., Manalastas, M., Ijaz, A., Imran, A., Liu, Y., & Al Kalaa, M. O. (2022). Communication requirements in 5G-enabled healthcare applications: Review and Considerations. Healthcare, 10(2), 293. https://doi.org/10.3390/healthcare10020293.