Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN: 2548-964X
Vol. 4, No. 1, Januari 2020, hlm. 166-173 http://j-ptiik.ub.ac.id

Implementasi Mekanisme *End-To-End Security* Menggunakan Algoritma AES dan HMAC pada Pengiriman Data Sensor ECG Berbasis LoRa

Al Ghitha Aulia Rahman[1], Eko Sakti Pramukantoro[2], Kasyful Amron[3]

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]alghithaa@student.ub.ac.id, [2].ekosakti@ub.ac.id, [3].kasyful@ub.ac.id

Abstrak

LoRa (Long Range) merupakan salah satu media transmisi nirkabel yang dirancang untuk perangkat dengan keterbatasan sumberdaya seperti sensor dan hanya perlu mentransmisikan sejumlah kecil data dalam jarak jauh. Penerapan media transmisi LoRa pada IoT seperti pemantauan ECG (*electrocardiogram*) akan sangat membantu pasien. Namun, salah satu tantangan utama dalam menerapkan IoT ialah keamanan pada data saat ditransmisikan. Terlebih lagi, data sensor seperti data ECG dinilai bersifat sensitif karena menjadi dasar diagnosis suatu penyakit oleh tenaga medis. Oleh karena itu, salah satu solusi dari kerentanan tersebut ialah menerapkan mekanisme keamanan antar *endpoints* (*end-to-end security*). Mekanisme *end-to-end security* dapat implementasi menggunakan kriptografi. Pada penelitian ini akan menerapkan mekanisme *end-to-end security* menggunakan algoritma kriptografi AES dan HMAC. Pemilihan kedua algoritma tersebut didasari pada keterbatasan sumberdaya perangkat yang digunakan. Mekanisme tersebut diterapkan pada *node sensor* dan *gateway* sebagai *endpoints* pengiriman data ECG. Hasil dari penelitian ini didapatkan bahwa mekanisme *end-to-end security* berhasil diterapkan. Namun, penerapan mekanisme tersebut memiliki dampak yaitu kenaikan *end-to-end delay* melebihi waktu *delay* yang ditoleransi oleh data ECG. Sehingga mekanisme tersebut tidak direkomendasikan untuk diterapkan.

Kata kunci: Kriptografi, LoRa, AES, HMAC, ECG, IoT

Abstract

LoRa (Long-Range) is a wireless transmission media that was designed to be used on low-powered devices such as sensors and only needs to transmit small data over long distances. The application of LoRa in IoT-based ECG (Electrocardiogram) monitoring will assist patients. However, one of the main challenges in implementing IoT is its data security. Moreover, health data such as ECG data are considered to be sensitive because they are used in medical diagnosis. Therefore, a solution to this vulnerability is implementing a security mechanism between endpoints (end-to-end security). End-to-end security mechanisms can be implemented using cryptography. In this research, an end-to-end security using AES and HMAC algorithm is implemented. AES and HMAC is chosen because the devices that is used are low-powered and only have limited resources. That mechanism is applied to sensor nodes and gateway because they are the endpoints.In this research, an end-to-end security mechanism has been implemented successfully. But, the application of this end-to-end security mechanism has an impact, that is an increase in end-to-end delay that exceeds the tolerated delay limit in ECG data transmission. So, this mechanism isn't recommended to be applied in ECG data transmission.

Keywords: *Cryptography, LoRa, AES, HMAC, ECG, IoT*

1. PENDAHULUAN

Sekarang ini sudah banyak pemantauan kondisi jantung pasien menggunakan alat *electrocardiogram* (ECG) yang diterapkan menggunakan arsitektur IoT (*Internet of Things*) (Yang et al., 2016). Konsep dari IoT merupakan gabungan dari perangkat konkret maupun virtual yang dapat terhubung melalui media transmisi (Pramukantoro et al., 2019). LoRa (Long Range) merupakan salah satu media transmisi nirkabel yang sudah banyak diterapkan dalam IoT. LoRa sering digunakan kerena media transmisi tersebut dirancang untuk perangkat dengan keterbatasan sumberdaya seperti perangkat sensor dan hanya perlu mentransmisikan sejumlah kecil data dalam jarak jauh (Devalal and Karthikeyan, 2018). Menurut Agustin

(2016), media transmisi LoRa tepat untuk digunakan dalam berbagai aplikasi seperti pemantauan kesehatan, pemantauan kondisi lingkungan, dan lain-lain.

Tantangan dalam menerapkan IoT bukan hanya soal keterbatasan sumberdaya. Namun, keamanan pada data juga menjadi salah satu tantangan utama dalam menerapkan pemantauan jarak jauh menggunakan transmisi via nirkabel (Pinto et al., 2018). Pengembangan IoT yang tidak mempertimbangkan keamanan akan membuat informasi dari data tersebut menjadi rentan terkena serangan oleh pihak yang tidak bertanggungjawab (Alassaf, Alkazemi and Gutub, 2017). Terlebih lagi, data sensor seperti data ECG dinilai bersifat sensitif karena menjadi dasar diagnosis suatu penyakit oleh tenaga medis. Data ECG yang tidak dijaga keamananya dapat dilihat dan diubah oleh pihak tertentu pada saat transmisi. Hal ini dapat berakibat fatal seperti salah diagnosis yang berujung pada kematian (Al-janabi et al., 2016).

Salah satu solusi dari kerentanan tersebut adalah dengan menerapkan mekanisme *end-to-end security* pada sistem berbasis IoT (Pramukantoro et al., 2019). Metode *end-to-end security* dapat diimplemetasikan dengan menggunakan kriptografi. Kriptografi merupakan sebuah seni penulisan yang bertujuan untuk menjaga kerahasiaan dari suatu pesan (Stallings, 2010). Namun, penerapan mekanisme keamanan akan mempengaruhi kinerja pengiriman datanya. Maka dari itu, penerapan mekanisme *end-to-end security* juga harus memperhatikan pengaruhnya terhadap kinerja transmisi (Pramukantoro et al., 2019).

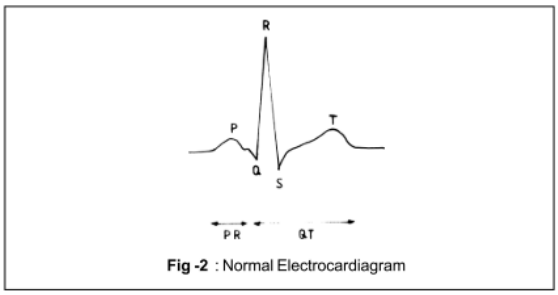
Salah satu algoritma yang cukup sering digunakan pada sistem dengan keterbatasan sumberdaya adalah AES (*Advanced Encryption Standard*). AES merupakan salah satu algoritma *block cipher* yang mengunakan operasi subtitusi dan permutasi pada blok 128 *bits*. AES memiliki keunggulan kecepatan dan kemanan yang sangat baik dengan pengunaan sumberdaya paling efisien (Alassaf, Alkazemi and Gutub, 2017). Data yang dikirimkan pada komunikasi antar *endpoints* juga harus terjamin keasliannya dan tidak dimodifikasi. Oleh karena itu, dibutuhkan metode seperti HMAC (*Keyed-Hash Message Authentification Code*) yang dapat menjamin autentikasi dan integritas data dengan konsumsi sumberdaya yang minim (Khemissa and Tandjaoui, 2016).

Berdasarkan uraian sebelumnya, fokus dari penelitian ini adalah mengimplementasikan mekanisme *end-to-end security* untuk mengamankan data *sensor* ECG. Mekanisme tersebut akan diimplementasikan pada *node sensor* dan *gateway* yang menjadi *endpoints* sistem pengiriman data sensor ECG. Penelitian ini menggunakan jaringan sensor nirkabel mengacu pada standar LoRa. Skema yang diterapkan antar *endpoints* menggunakan algoritma kriptografi AES (*Advanced Encryption standart*) kunci 128 bits dan HMAC (*Keyed-Hash Message Authentication Code*) dengan algoritma *hash* SHA-256.

2. DASAR TEORI

2.1 *Electrocardiogram* (ECG)

Electrocardiogram atau ECG adalah alat diagnostik yang sangat penting pada dunia kedokteran. Alat ECG mengukur aktivitas listrik yang dihasilkan dari detak jantung yang didapatkan dari permukaan kulit. Aliran listrik yang dimaksud adalah ketika jantung mulai memompa darah masuk dan keluar melalui sistem peredaran darah. Elektroda pada alat ECG digunakan untuk *sensing bio-electric* yang disebabkan oleh sel otot dan saraf (Gawali and Wadhai, 2015). Perekaman menggunakan ECG dulakukan untuk mendiagnosa kondisi jantung dari seorang pasien. Frekuensi optimal yang dibutuhkan pada pengambilan data sampel ECG berkisar antara 100Hz hingga 500Hz. Tujuannya adalah agar data yang diterekam dapat dianalisis (Kwon, Jeong and Kim, 2018). Selain itu, waktu perekaman data ECG agar dapat dianalisis dilakukan selama 10 detik atau lebih (Hodgart and Macfarlane, 2004). Nilai *delay* yang dapat ditoleransi pada kondisi *non-critical* sampai dengan 4 detik. Sedangkan, nilai *delay* toleransi terhadap kondisi *critical* hanya sampai 3 detik (Alesanco and García, 2010).



Gambar 1. Grafik Electrocariogram Normal
Sumber: (Gawali & Wadhai, 2015)

Rekaman ECG akan diperiksa oleh dokter yang secara visual memeriksa fitur yang terdapat

di dalam sinyal dan memperkirakan parameter-parameter penting dari sinyal tersebut dokter dapat menilai status seorang pasien. Parameter standar dari gelombang ECG adalah gelombang PQRS dan gelombang T. Tetapi, sebagian besar informasi terletak di sekitar R puncak. Jadi, apa yang direkam oleh ECG, dapat mengatakan apakah aktivitas jantung tersebut normal atau tidak (Gawali and Wadhai, 2015).

2.2 Long Range (LoRa)

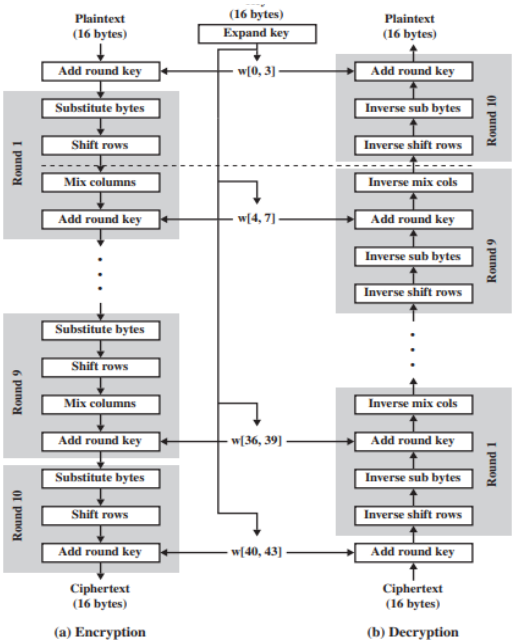
LoRa (*Long Range*) adalah konektivitas IoT nirkabel dikembangkan oleh perusahaan Semtech. LoRa baru-baru ini berevolusi dan mendapatkan popularitas karena tepat pada aplikasi dengan keterbatasan sumber daya dan hanya perlu mentransfer sejumlah kecil data dalam jarak jauh. (Devalal and Karthikeyan, 2018). LoRa memiliki maksimum jumlah *payload* pada setiap transmisi sebesar 2-255 *byte*. Modulasi pada LoRa menggunakan spread spectrum, spread spectrum sendiri adalah variasi dari Chirp Spread Spectrum (CSS). Bandwith yang ditawarkan oleh LoRa di USA: 915MHz, UE: 433MHz dan 868MHz (Augustin et al., 2016).

Gambar berikut merupakan struktur frame LoRa *physical*, dimulai dengan *preamble*, dilanjutkan dengan *header* (opsional), *payload* yang dapat menampung informasi sebesar 255 *bytes* dan 16 *bits* CRC (*Cyclic Redudancy Check*) yang bersifat opsional.

Gambar 2. Struktur LoRa frame
Sumber: (Augustin et al., 2016)

2.3. Advanced Encryption tandard (AES)

Advanced Encryption Standart (AES) merupakan kriptografi algoritma kunci simetrimetris dengan panjang kunci dari AES bisa 16, 24, 32 *bytes* (128, 192 atau 256 bits). Perbedaan panjang kunci akan mempengaruhi jumlah round yang akan diimplementasikan pada algoritma AES. Pada gambar dibawah ini menunjukkan urutan algoritma enkripsi dan dekripsi dari AES kunci 128 bit. Algoritma enkripsi AES terdiri dari operasi *Sub-Bytes*, *Shift-Rows*, *MIX-Columns*, dan *Add-key*. Di putaran terakhir operasi *Mix-Columns* ditiadakan (Stallings, 2010).

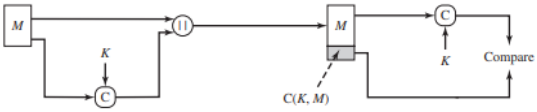


Gambar 3. Algoritma AES-128 *bit*
Sumber: (Stallings, 2010)

2.4 Keyed-Hash Message Authentication Code (HMAC)

MAC atau *Message Authentication Code* adalah satu teknik autentikasi yang melibatkan penggunaan kunci untuk menghasilkan blok data berukuran tetap (*fixed-size block*). Sedangkan HMAC adalah teknik dari MAC dengan memanfaatkan fungsi *hash* terhadap pesan dan kemudian mengenkripsi pesan tersebut dengan sebuah kunci yang hanya diketahui oleh pengirim dan penerima (Stallings, 2010).

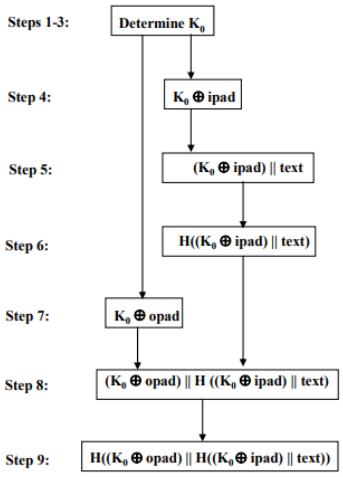
Secara umum, pesan yang dikirimkan oleh pengirim (*sender*) dapat divalidasi sebagai otentik (tidak dimodifikasi oleh pihak lain) oleh pihak penerima (*receiver*).



Gambar 4. Prosedur MAC
Sumber: (Stallings, 2010)

Secara matematis HMAC dirumuskan sebagai:

$$HMAC = ((H((K_o \oplus opad)) \,||\, H((K_o \oplus ipad)) \,||\, text)) \quad (1)$$



Gambar 5. Metode HMAC
Sumber: (FISP PUB 198-1, 2008)

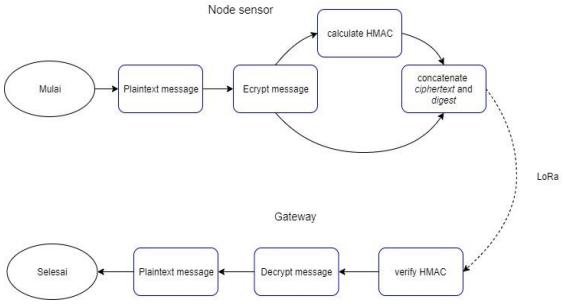
Adapun langkah-langkah meknisme HMAC yang telah dijabarkan di atas dapat dijelaskan pada tabel 2.4 di bawah ini:

Tabel 1. Penjelasan Mekanisme dari HMAC

	DEKRIPSI
Step 1	Jika panjang K = B (K sama dengan B). Maka, set K_o = B. Lalu, lanjut ke *step* 4.
Step 2	Jika panjang K > B (K lebih dari B), hash K untuk mendapatkan nilai L *string byte*, kemudian *append* dengan (B-L) angka 0 untuk mendapatkan string byte K_o yang panjangnya sama dengan B. Lalu, lanjut ke *step* 4.
Step 3	Jika panjang K < B (K kurang dari B), *append* angka 0 sebanyak (B-K) untuk mendapatkan *string byte* K_o yang panjangnya sama dengan B. Lalu, lanjut ke Step 4.
Step 4	Lakukanlah XOR K_o dengan *ipad* untuk menghasilkan *string byte* sepanjang B.
Step 5	*Append* hasil dari K_o □ *ipad* pada *step* 4 dengan *string text*.
Step 6	Lakukan H (*Hashing*) untuk string yang dihasilkan pada *step* 5.
Step 7	Lakukanlah XOR K_o dengan *opad.*
Step 8	*Append* hasil pada step 7 dengan hasil *hash* pada step 6.
Step 9	Lakukan H dari hasil yang dihasilkan pada *step* 8.

3. PERANCANGAN

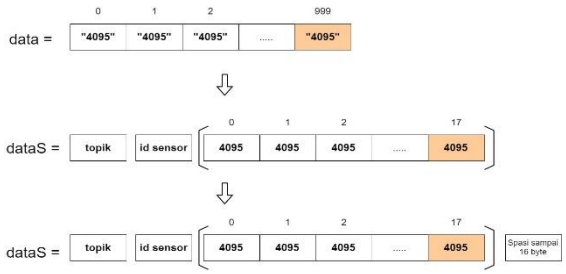
Perancangan dimulai dengan membuat perancangan alur data mekanisme *end-to-end security* pada sistem secara umum yang dapat dilihat pada gambar 6. Sebelum data ditransmisikan terlebih dahulu data di proses menggunakan algoritma AES kunci 128 *bits* hingga menjadi *ciphertext.* Selanjutnya, *ciphertext* digunakan sebagai masukan pada proses HMAC untuk mendapatkan nilai *digest*. Hasil dari keduanya kemudian digabungkan dan ditransmisikan menggunakan media transmisi LoRa. Data yang kemudian diterima oleh *gateway* akan menjalankan proses verifikasi dengan cara membandingkan nilai *digest* yang diterima dengan nilai *digest* yang telah terhitung pada *gateway.* Selanjutnya, pesan yang cocok akan masuk kedalam proses dekripsi *ciphertext* yang dibawa oleh pesan tersebut hingga menjadi *plaintext/* data ECG.



Gambar 6. Perancangan Alur Mekanisme

3.1. Perancangan Alur Pada Node Sensor

Proses bermula dari *node sensor* yang telah merekam data ECG dengan frekuensi 100Hz sehingga menghasilkan 1000 data. , data dengan jumlah 1000 tersebut berupa *list* dibagi menjadi 18 data pertransmisi untuk selanjutnya dienkripsi dengan AES. Pembagian data tersebut bertujuan untuk memaksimalkan ukuran *payload* yang dapat ditampung oleh LoRa yaitu sekitar 255 *bytes* sekali transmisi. Gambar 7 merupakan ilustrasi dari data telah terbagi menjadi 18 data ditambahkan dengan topik dan id sensor sebagai identitas dari sensor pengirim.



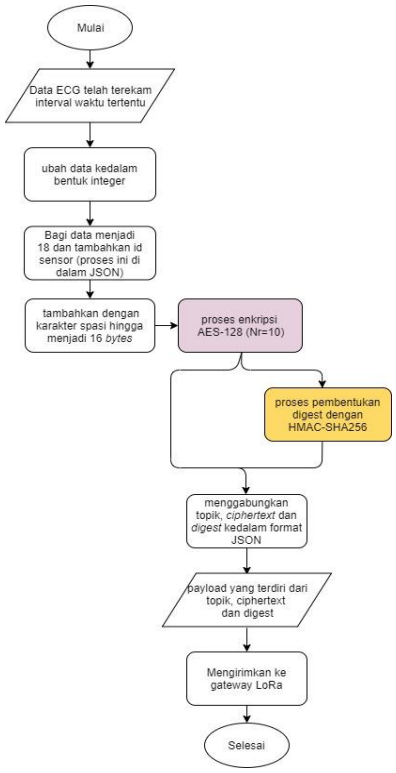
Gambar 7. Ilustrasi Pembagian Data

Data pada gambar diatas, data kemudian di enkripsi menggunakan algoritma AES-128 dan menghasilkan *ciphertext* dalam bentuk *byte*. *Ciphertext* hasil dari proses enkripsi AES diubah kedalam bentuk ASCII terlebih dahulu sebelum digunaan sebagai masukan untuk proses HMAC.

Proses HMAC menghasilkan *digest* sebesar 256 *bits*/ 64 karakter heksadesimal. *Ciphertext* dan *digest* hasil proses enkripsi dan *hashing*

kemudian digabungkan kedalam format JSON bersama dengan. *Payload* tersebut kemudian sitransmisikan ke *gateway* menggunakan media transmisi LoRa.

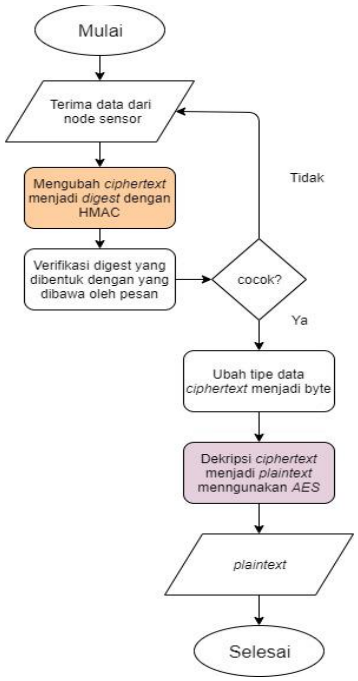
Ciphertext dan *digest* hasil proses enkripsi dan hashing kemudian digabungkan kedalam format JSON bersama dengan topik dan id sensor. *Payload* tersebut kemudian sitransmisikan ke *gateway* menggunakan LoRa.



Gambar 8. Alur Mekanisme Pada Node Sensor

3.2. Perancangan Pada *Gateway*

Payload yang telah diterima oleh *gateway* diverifikasi dengan cara menghitung nilai *digest* menggunakan HMAC yang telah diinisialisasikan dengan algoritma *hash* SHA-256 (*H*), *input* yang digunakan adalah *ciphertext* yang diterima oleh *gateway* (*B*), kunci yang diinisialisasikan sama dengan yang ada pada *node sensor* (*k2*). *Digest* hasil keluaran HMAC pada *gateway* di verifikasi dengan *digest* yang ada didalam paket data dari *node sensor* bersama dengan *ciphertext*, proses ini adalah untuk mengautentikasi pesan yang masuk pada *gateway*. Selanjutnya, jika kedua digest telah terverifikasi dan hasilnya valid/ cocok, *ciphertext* dapat didekripsi menjadi data ECG semula. Proses pada penjelasan tersebut dapat dilihat pada gambar 9.



Gambar 9. Alur Mekanisme Pada Node Sensor

4. PENGUJIAN

4.1 Pengujian Hasil Implementasi Mekanisme *End-To-End Security*

Hasil implementasi mekanisme *end-to-end security* yang telah dilakuka kemudian diuji dan dilihat berdasarkan *otput* yang dikeluarkan oleh masing-masing proses.

Tabel 2. Hasil Implementasi Mekanisme

Pengujian Hasil Implementasi	
Pembagian Data Sensor	Valid
Implementasi Enkripsi AES	Valid
Implementasi HMAC	Valid
Implementasi Autentikasi	Valid
Implementasi Dekripsi AES	Valid

Tabel 2 merupakan kesimpulan hasil dari implementasi tiap proses mekanisme *end-to-end security*. Seluruh proses meknisme end-to-end security dapat berjalan dan mengeluarkan output yang diharapkan.

4.2 Pengujian Validasi Enkripsi dan Dekripsi

Pengujian validasi enkripsi dan dekripsi pada penelitian ini, dilakukan dengan tujuan memastikan data ECG yang diproses menggunakan mekanisme *end-to-end security* tidak berubah ketika sampai pada *gateway*. Pengujian ini menggunakan 3 kelompok data skunder ECG pertama dari satu siklus. Ketiga

kelompok data tersebut masing-masing terdiri dari 18 data ECG beserta topik dan id sensor. Kemudian, ketiga data tersebut diujikan menggunakan mekanisme *end-to-end security* yang telah diimplementasikan.

Ketiga kelompok data ECG yang dikirimkan oleh *node sensor* diterima oleh *gateway* dengan hasil dan urutan yang sama. Proses enkripsi dan dekripsi yang dilakukan menggunakan sebuah *private key* sepanjang 128 *bits*. Jadi, dapat disimpulkan hasil dari pengujian validasi enkripsi dan dekripsi pada penelitian ini menghasilkan kecocokan antara plaintext sebelum dienkripsi pada node sensor dan plaintext sesudah *didekripsi* pada *gateway.*

4.3 Pengujian Kinerja Mekanisme *End-To End Delay*

Pengujian *end-to-end delay* akan dilakukan terhadap lima kali percobaan pengiriman data ECG. Satu kali percobaan tersebut terdiri dari 1000 data skunder ECG. Data yang diujikan dibagi menjadi dua kategori, yaitu data yang tidak menggunakan mekanisme dan yang menggunakan mekanisme *end-to-end security.* Kedua kategori tersebut sama-sama ditransmisikan menggunakan media transmisi LoRa. Kemudian, dilakukan selisih nilai *delay* dari kedua kategori tersebut untuk dianalisis.

Pada pengujian ini data ECG tersebut dibagi menjadi satu kelompok berjumlah 18 data sekali transmisi untuk skenario menggunakan mekanisme *end-to-end security*, yang artinya akan dilakukan 56 kali transmisi. Sedangkan, untuk skenario pengujian tanpa menggunakan mekanisme *end-to-end security* dilakukan dengan membagi 1000 data tersebut menjadi 39 data pertransmisi, yang artinya akan dilakukan 26 kali transmisi. Hal ini dilakukan karena ke-39 data tersebut dapat ditampung oleh *payload* LoRa yang berjumlah 255 *bytes*.

Tabel 3. Delay Pengiriman Data Tanpa Mekanisme

Percobaan	Delay Pengiriman Data Tanpa Mekanisme (s)
Percobaan ke-1	25,2040
Percobaan ke-2	25,18647
Percobaan ke-3	25,19766
Percobaan ke-4	25,25532
Percobaan ke-5	25,14987

Tabel 3 merupakan waktu yang diperlukan oleh *node sensor* untuk mengirim data ke *gateway* tanpa mekanisme *end-to-end security*. Nilai yang ditampilkan pada tabel tersebut merupakan nilai selisih saat data pertama dalam satu siklus dikirimkan oleh *node senor* hingga data terakhir diterima oleh *gateway*.

Pada percobaan pertama, selisih nilai yang didapat dari pengiriman data tanpa mekanisme keamanan melalui LoRa sebesar 25,2040 detik. Pada percobaan kedua, selisih nilai yang didapat dari pengiriman tanpa mekanisme keamanan melalui LoRa sebesar 25,18647 detik. Pada percobaan ketiga, selisih nilai yang didapat dari pengiriman data tanpa mekanisme keamanan melalui LoRa sebesar 25,19766 detik. Pada percobaan keempat, selisih nilai yang didapat dari pengiriman tanpa mekanisme keamanan melalui LoRa sebesar 25,25532 detik. Terakhir, Pada percobaan kelima, selisih nilai yang didapat dari pengiriman data tanpa mekanisme keamanan melalui LoRa sebesar 25,14987 detik. Nilai rata-rata selisih dari kelima percobaan yang telah dilakukan sebesar 25,19866 detik.

Tabel 4 merupakan selisih dari waktu yang diperlukan oleh sistem untuk memproses data ECG menggunakan mekanisme *end-to-end security* antar *node sensor* hingga ke *gateway* menggunakan media transmisi LoRa. Nilai yang ditampilkan pada tabel tersebut merupakan selisih waktu saat data pertama dienkripsi menggunakan AES pada *node sensor* hingga data terakhir diterima dan didekripsi pada *gateway*.

Tabel 4. Delay Pengiriman Data dengan Mekanisme

Percobaan	Delay Pengiriman Data dengan Mekanisme (s)
Percobaan ke-1	81,4640
Percobaan ke-2	81,18796
Percobaan ke-3	81,34976
Percobaan ke-4	81,02446
Percobaan ke-5	81,35003

Pada percobaan pertama, selisih nilai yang didapat dari pengiriman data menggunakan mekanisme keamanan sebesar 81,4640 detik. Pada percobaan kedua, selisih nilai yang didapat dari pengiriman menggunakan mekanisme keamanan sebesar 81,18796 detik. Pada percobaan ketiga, selisih nilai yang didapat dari pengiriman menggunakan mekanisme keamanan sebesar 81,34976 detik. Pada percobaan keempat, selisih nilai yang didapat dari pengiriman menggunkan mekanisme

keamanan sebesar 81,02446 detik. Terakhir, Pada percobaan kelima, selisih nilai yang didapat dari pengiriman data tanpa mekanisme keamanan melalui LoRa sebesar 81,02446 detik. Nilai rata-rata selisih dari kelima percobaan yang telah dilakukan sebesar 81,2752 detik.

Berdasarkan hasil dari pengujian *end-to-end delay* menggunakan lima kali percobaan, didapat *delay* yang dihasilkan oleh skenario menggunakan mekanisme keamanan lebih tinggi dibanding skenario yang tidak menggunakan mekanisme keamanan. Nilai tersebut terbukti dari rata-rata *delay* pada masing-masing skenario pengujian adalah 25,19866 detik untuk skenario pengujian yang tidak menggunakan mekanisme keamanan dan 81,2752 detik untuk skenario pengujian yang menggunakan mekanisme keamanan. Penerapan mekanisme *end-to-end security* berdampak pada kenaikan *delay* sebesar 224% kali lebih besar dari *end-to-end delay* pada pengiriman tanpa menggunakan mekanisme keamanan. Hal tersebut dikarenakan proses dari algoritma AES dan HMAC antara *node sensor* dan *gateway*. Perbedaan pada jumlah data yang dikirimkan antara skenario pengujian ada dan tanpa mekanisme *end-to-end security* disebabkan oleh nilai *digest* yang juga ditransmisikan bersama *payload*. Hal ini juga mempengaruhi perbedaan pada jumlah transmisi yang dilakukan oleh sistem untuk dapat mentransmisikan 1000 data ECG tiap siklus.

5. KESIMPULAN

Implementasi mekanisme *end-to-end security* pada pengiriman data ECG berbasis jaringan LoRa dinilai kurang tepat. Hal ini dikarenakan waktu yang dibutuhkan oleh sistem untuk memproses dan mengirimkan seluruh data ECG satu siklus hingga ke *gateway* melebihi waktu baik *critical* maupun non-*critical* yang harus diterima oleh tenaga medis. Oleh karena itu, penulis memberikan saran untuk penelitian selanjutnya dari penelitian yang dilakukan, yaitu penggunaan variasi mekanisme keamanan mendatang yang mempunyai kelebihan dari segi kecepatan dan penggunaan sumberdaya dibanding dengan mekanisme yang diterapkan.

6. DAFTAR PUSTAKA

Al-janabi, S., Al-shourbaji, I., Shojafar, M. and Shamshirband, S., 2016. *Survey Of Main Challenges (Security And Privacy) In Wireless Body Area Networks For Healthcare Applications*. *Egyptian Informatics Journal*. [online] Available at: <http://dx.doi.org/10.1016/j.eij.2016.11.001>.

Alassaf, N., Alkazemi, B. and Gutub, A., 2017. *Applicable Light-Weight Cryptography To Secure Medical Data In Iot Systems*. (April).

Alesanco, Á. and García, J., 2010. *Clinical Assessment Of Wireless ECG Transmission In Real-Time Cardiac Telemonitoring*. *IEEE Transactions on Information Technology in Biomedicine*, 14(5), pp.1144–1152.

Augustin, A., Yi, J., Clausen, T. and Townsley, W.M., 2016. *A Study Of Lora: Long Range & Low Power Networks For The Internet Of Things*. *Sensors (Switzerland)*, 16(9), pp.1–18.

Devalal, S. and Karthikeyan, A., 2018. *LoRa Technology - An Overview*. *Proceedings of the 2nd International Conference on Electronics, Communication and Aerospace Technology, ICECA 2018*, (Iceca), pp.284–290.

Gawali, D.H. and Wadhai, V.M., 2015. *Implementation Of ECG Sensor For Real Time Signal Processing Applications. 2014 International Conference on Advances in Electronics, Computers and Communications, ICAECC 2014*.

Hodgart, E. and Macfarlane, P.W., 2004. *10 Second heart rate variability*. *Computers in Cardiology*, 31, pp.217–220.

Khemissa, H. and Tandjaoui, D., 2016. *A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things. Proceedings - NGMAST 2015: The 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, pp.90–95.

Kwon, O., Jeong, J. and Kim, H. Bin, 2018. *ECG Sampling Frequency for HRV Analysis. Healthcare Informatics Research*, [online] 24(3), pp.198–206. Available at: <www.e-hir.org>.

Pramukantoro, E.S., Bakhtiar, F.A., Aji, A.L.B. and Dewa, D.H.P., 2019. I*mplementasi Mekanisme End-To-End Security pada IoT Middleware. Jurnal Teknologi Informasi dan Ilmu Komputer*, 6(3), p.335.

Ribeiro Pinto, J., Cardoso, J.S. and Lourenco, A., 2018. *Evolution, Current Challenges, And Future Possibilities In ECG Biometrics. IEEE Access*, 6(c), pp.34746–34776.

Stallings, W., 2010. *Cryptography and Network Security: Principles and Practice, 5th edition. Cryptography and Network Security: Principles and Practice, 5th edition*, .

Yang, Z., Zhou, Q., Lei, L., Zheng, K. and Xiang, W., 2016. *An IoT-cloud Based Wearable ECG Monitoring System for Smart Healthcare*. *Journal of Medical Systems*, [online] 40(12). Available at: <http://dx.doi.org/10.1007/s10916-016-0644-9>.