Skema Autentikasi Berbasis Elliptic Curve Cryptography untuk Internet of Medical Things

Michelle Theresia - 13518050
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
michelle.theresia17@gmail.com

***Abstract*—Istilah Internet of Medical Things (IoMT) mulai bermunculan dengan adanya teknologi Internet of Things (IoT) namun spesifik untuk meningkatkan kualitas medis. Akan tetapi, data medis di IoMT rentan karena banyak perangkat lain yang juga terhubung dengan IoT. Salah satu ancaman terbesar adalah akses ilegal. Oleh sebab itu, dibutuhkan sebuah sistem autentikasi akses berbasis Elliptic Curve Cryptography (ECC) untuk IoMT.**

Keywords—Internet of Medical Things (IoMT); Authentication; Elliptic Curve Cryptography (ECC)

I. Pendahuluan

Perkembangan komunikasi nirkabel, sensor miniatur dan biaya komputasi awan terjangkau menyebabkan kesuksesan penerapan *Internet of Medical Things* (IoMT) [1]. IoMT adalah berbagai sistem perawatan kesehatan (perangkat medis, perangkat lunak aplikasi dan layanan, dll.) untuk menyediakan transmisi data terkait kesehatan yang aman antara perangkat pintar yang membantu dokter, penyedia layanan, pusat tes medis yang berlokasi jauh untuk menyimpan dan bertukar data kesehatan secara elektronik [2]. Saat ini, miliaran perangkat telah terhubung dengan IoT untuk berbagai jenis aplikasi, termasuk kesehatan. Peningkatan tersebut menyebabkan privasi dan keamanan pengguna menjadi masalah dalam IoT, terutama IoMT, dan membutuhkan pertimbangan penting. Beberapa contoh ancaman sistem perawatan kesehatan antara lain, akses data pasien oleh pihak yang tidak memiliki izin, modifikasi data kesehatan, membajak perangkat medis, mendapatkan akses ke jaringan rumah sakit dan eksploitasi informasi yang tersimpan dan ditukar mengancam keselamatan pasien. Oleh sebab itu, dibutuhkan mekanisme dengan keamanan dan privasi yang layak untuk melindungi informasi medis pasien yang sensitif dari akses yang tidak resmi. Salah satu algoritma kriptografi yang dapat digunakan untuk melindungi akses IoMT adalah elliptic curve cryptography (ECC).

II. Dasar Teori

A. Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan [3]. Tujuan dari kriptografi adalah untuk menjaga keamanan yang artinya terjaga kerahasiaannya (*confidentiality*), terjaga keasliannya (*data integrity*), memastikan pengirim pesan asli bukan pihak ketiga yang menyamar (authentication), pengirim pesan tidak dapat menyangkal telah mengirim pesan (non repudiation) [3].

B. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) adalah kriptografi kunci-publik yang menggunakan kurva eliptik [4]. Komputasi dengan kurva eliptik menawarkan keamanan yang sama dengan algoritma-algoritma lain namun dengan ukuran yang lebih kecil, seperti panjang kunci ECC lebih pendek daripada kunci RSA namun memiliki tingkat keamanan yang sama dengan RSA [4].

C. Internet of Things (IoT)

IoT adalah infrastruktur objek pintar yang terhubung seperti sensor, aktuator, tag RFID, prosesor mikro, perangkat komunikasi, sumber daya, dll. disebut sebagai *things* yang dihubungkan melalui koneksi nirkabel maupun kabel untuk komunikasi data [5].

References

[1] K. Sowjanya, M. Dasgupta and S. Ray, "Elliptic Curve Cryptography based authentication scheme for Internet of Medical Things", *Journal of Information Security and Applications*, vol. 58, p. 102761, 2021. Available: https://www.sciencedirect.com/science/article/pii/S2214212621000120. [Accessed 20 December 2021].

[2] N. Garg, M. Wazid, A. Das, D. Singh, J. Rodrigues and Y. Park, "BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment", *IEEE Access*, vol. 8, pp. 95956-95977, 2020. Available: https://ieeexplore.ieee.org/abstract/document/9097179. [Accessed 20 December 2021].

[3] R. Munir, *Informatika.stei.itb.ac.id*, 2021. [Online]. Available: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2021-2022/Pengantar-Kriptografi-(2021).pdf. [Accessed: 20- Dec- 2021].

[4] R. Munir, *Informatika.stei.itb.ac.id*, 2021. [Online]. Available: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/ECC-2020-Bagian1.pdf. [Accessed: 20- Dec- 2021].

[5] S. Majumder, S. Ray, D. Sadhukhan, M. Khan and M. Dasgupta, "ECC-CoAP: Elliptic Curve Cryptography Based Constraint Application Protocol for Internet of Things", *Wireless Personal Communications*, vol. 116, no. 3, pp. 1867-1896, 2020. Available: https://link.springer.com/article/10.1007/s11277-020-07769-2. [Accessed 20 December 2021].

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 26 April 2021

Michelle 13518050