KEAMANAN KOMUNIKASI PADA PROTOKOL MQTT UNTUK MONITORING PERANGKAT *INTERNET OF THINGS* DENGAN METODE *ELLIPTIC CURVE CRYPTOGRAPHY*

TESIS

AXEL NATANAEL SALIM
TEKNIK INFORMATIKA
212420035

PROGRAM STUDI TEKNIK INFORMATIKA – S2
PROGRAM PASCASARJANA
UNIVERSITAS BINA DARMA
PALEMBANG
2024

KEAMANAN KOMUNIKASI PADA PROTOKOL MQTT UNTUK MONITORING PERANGKAT *INTERNET OF THINGS* DENGAN METODE *ELLIPTIC CURVE CRYPTOGRAPHY*

Tesis ini diajukan sebagai salah satu syarat
untuk memperoleh gelar

MAGISTER KOMPUTER

AXEL NATANAEL SALIM

TEKNIK INFORMATIKA

212420035

PROGRAM STUDI TEKNIK INFORMATIKA – S2

PROGRAM PASCASARJANA

UNIVERSITAS BINA DARMA

PALEMBANG

2024

Halaman Pengesahan Pembimbing Tesis

Judul Tesis : KEAMANAN KOMUNIKASI PADA PROTOKOL MQTT UNTUK MONITORING PERANGKAT INTERNET OF THINGS DENGAN METODE ELLIPTIC CURVE CRYPTOGRAPHY.

Oleh AXEL NATANAEL SALIM NIM 212420035 Tesis ini telah disetujui dan disahkan oleh Tim Penguji Program Studi Teknik Informatika – S2 Konsentrasi ENTERPRISE IT INFRASTRUCTURE, Program Pascasarjana Universitas Bina Darma pada 15 Maret 2024 dan telah dinyatakan LULUS.

Mengetahui,
Program Studi Teknin Informatika – S2
Universitas Bina Darma

Ketua,	Pembimbing,
.....	.....
M. Izman Herdiansyah, M.M., PhD.	**Dr. Tata Sutabri, S. Kom., M.M.S.I.**

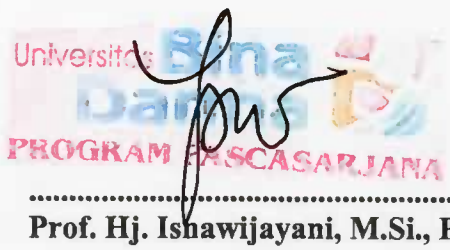
Halaman Pengesahan Penguji Tesis

Judul Tesis : KEAMANAN KOMUNIKASI PADA PROTOKOL MQTT UNTUK MONITORING PERANGKAT INTERNET OF THINGS DENGAN METODE ELLIPTIC CURVE CRYPTOGRAPHY.

Oleh AXEL NATANAEL SALIM NIM 212420035 Tesis ini telah disetujui dan disahkan oleh Tim Penguji Program Studi Teknik Informatika – S2 Konsentrasi ENTERPRISE IT INFRASTRUCTURE, Program Pascasarjana Universitas Bina Darma pada 15 Maret 2024 dan telah dinyatakan LULUS.

Palembang, 15 Maret 2024

Mengetahui,
Program Pascasarjana
Universitas Bina Darma
Direktur,



Prof. Hj. Ishawijayani, M.Si., Ph.D.

Tim Penguji :

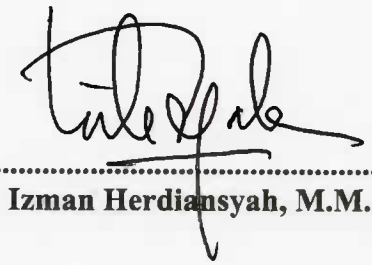
Penguji I,

Dr. Tata Sutabri, S.Kom., M.M.S.I.

Penguji II,

Prof. Dr. Edi Surya Negara, M.Kom.

Penguji III,



M. Izman Herdiansyah, M.M., PhD.

SURAT PERNYATAAN

Saya yang bertanda tangan dibawah ini:

Nama : AXEL NATANAEL SALIM
NIM : 212420035

Dengan ini menyatakan bahwa:

1. Karya tulis Saya Tesis ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik Magister di Universitas Bina Darma;
2. Karya tulis ini murni gagasan, rumusan dan penelitian Saya sendiri dengan arahan tim pembimbing;
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dikutip dengan mencantumkan nama pengarang dan memasukkan ke dalam daftar pustaka;
4. Karena yakin dengan keaslian karya tulis ini, Saya menyatakan bersedia Tesis yang Saya hasilkan di unggah ke internet;
5. Surat Pernyataan ini Saya tulis dengan sungguh-sungguh dan apabila terdapat penyimpangan atau ketidakbenaran dalam pernyataan ini, maka Saya bersedia menerima sanksi dengan aturan yang berlaku di perguruan tinggi ini.

Demikian Surat Pernyataan ini saya buat agar dapat dipergunakan sebagaimana mestinya.

Palembang, 15 Maret 2024
Yang Membuat Pernyataan,

AXEL NATANAEL SALIM
NIM: 212420035

ABSTRAK

Muculnya Internet of Things menjadi salah satu tren teknologi yang paling signifikan. Penerapan dari IoT ini untuk meningkatkan efisiensi, kenyamanan serta mempermudah manusia dalam melakukan beberapa aktifitas. Salah satu aspek kunci dalam pelaksanaan IoT adalah komunikasi yang efisien antara perangkat-perangkat tersebut, dan salah satu protokol yang paling umum digunakan dalam komunikasi antar perangkat adalah protokol Message Queuing Telemetry Transport. MQTT memungkinkan pengiriman data secara *real-time* atau berdasarkan peristiwa tertentu, namun masih terdapat beberapa tantangan yang perlu diatasi. Salah satu tantangan utama MQTT adalah masalah keamanan informasi, sehingga penelitian ini bertujuan untuk mengkaji solusi yang efektif untuk meningkatkan keamanan komunikasi dalam penggunaan IoT yang menggunakan protokol MQTT. Salah satu metode kemanan komunikasi antar perangkat IoT dapat menggunakan metode pengamanan komunikasi kriptografi yang ringan seperti metode ECC. Metode ECC digunakan karena menggunakan kunci yang lebih pendek tetapi tetap memberikan keamanan yang tinggi sehingga lebih efisien jika diimplementasikan pada perangkat IoT. Hasil yang didapat, data yang dikirimkan ke MQTT Broker tidak dapat dibaca dan dikonversi secara manual, sehingga data yang dikirim jauh lebih aman. Berdasarkan dari hasil pengujian, alat dapat bekerja dengan baik untuk membaca, memproses, dan mengirim data ke MQTT Broker. Pengukuran Qos pada sistem didapatkan bahwa data yang sudah dienkripsi dan dikirimkan dari subscriber ke MQTT Broker memiliki waktu rata-rata delay sebesar 54,1 ms, throughput 410,4 bps, packet loss sebesar 0% dan jitter sebesar 0,00 ms. Melihat dari hasil penelitian dapat disimpulkan bahwa metode ECC ini dapat menjadi solusi dari permasalah keamanan komunikasi data pada protokol MQTT.

Kata kunci: *DHT11, ECC, IoT, Keamanan Komunikasi, MQTT Broker, Wemos D1 Mini ESP8266.*

ABSTRACT

The emergence of the IoT has become one of the most significant technology trends. The application of IoT is aimed at enhancing efficiency, comfort, and facilitating various human activities. One key aspect of IoT implementation is efficient communication between devices, with one of the most commonly used protocols being MQTT protocol. MQTT enables the transmission of data in real-time or based on specific events, although there are still several challenges that need to be addressed. One of the main challenges of MQTT is information security issues, prompting this research to examine effective solutions to enhance communication security in IoT applications that utilize MQTT protocol. One method of securing communication between IoT devices can involve using lightweight cryptographic communication security methods such as ECC method. ECC method is chosen because it utilizes shorter keys while still providing high security, making it more efficient when implemented on IoT devices. The results obtained indicate that data sent to MQTT Broker cannot be read and converted manually, ensuring much safer data transmission. Based on the test results, the tool can effectively read, process, and send data to MQTT Broker. QoS measurements on the system revealed that data encrypted and sent from the subscriber to MQTT Broker had an average delay time of 54.1 ms, throughput of 410.4 bps, zero packet loss, and jitter of 0.00 ms. Looking at the research findings, it can be concluded that this ECC method could serve as a solution to data communication security issues in the MQTT protocol.

Kata kunci: *DHT11, ECC, IoT, Secure Communication, MQTT Broker, Wemos D1 Mini ESP8266.*

MOTTO DAN HALAMAN PERSEMBAHAN

"*Bagi Orang Yang Mau Berjuang,*

*Tidak Ada Jalan Yang Tidak Bisa Dilewati***"**

Kupersembahkan Tesis ini untuk:
1. Universitas Bina Darma Palembang
2. Keluarga Tercinta

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas rahmat dan karunia yang telah diberikan-Nya, sehingga penulis dapat menyelesaikan proposal tesis ini dengan judul "Keamanan Komunikasi Pada Protokol MQTT Untuk Monitoring Perangkat *Internet of Things* Dengan Metode *Elliptic Curve Cryptography*" dengan baik.

Penulis juga mengucapkan terima kasih yang sebesar-besarnya kepada Bapak Dosen Pembimbing, Dr. Tata Sutabri, S. Kom., M, M.S.I., atas bimbingan, arahan, dan dukungan yang telah diberikan dalam penyususan proposal tesis ini. Bimbingan dan masukan yang berharga dari Bapak sangat membantu penulis dalam mengembangkan ide-ide, menyusun kerangka penelitian, dan merumuskan metodologi yang tepat.

Penulis juga mengucapkan terima kasih kepada teman-teman yang telah memberikan masukan dan pendapatnya serta kepada pihak-pihak lain yang turut mendukung kelancaran penelitian ini. Tidak lupa, penulis menyampaikan rasa terima kasih kepada kedua orang tua dan keluarga penulis atas doa, dukungan, dan kasih sayang yang telah memberikan semangat dan motivasi dalam menyelesaikan studi ini.

Proposal tesis ini di susun dengan penuh dedikasi dan kerendahan hati, dengan harapan dapat memberikan kontribusi kecil bagi pengembangan ilmu pengetahuan di bidang teknik informatika, serta bermanfaat bagi pembaca yang mengkaji topik yang sama. Akhir kata, semoga tesis ini dapat diterima dan memberikan manfaat yang optimal, penulis menyadari bahwa masih banyak kekurangan dalam penulisan proposal ini, sehingga penulis membutuhkan kritik dan saran yang membangun untuk memperbaiki di masa mendatang.

Palembang, Desember 2023

Penulis,

Axel Natanael Salim

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN