BAB 1
PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) merupakan teknologi yang memungkinkan perangkat fisik saling terhubung dan bertukar data melalui internet. Teknologi ini terus berkembang pesat, dengan jumlah perangkat IoT aktif yang diproyeksikan mencapai 14,7 miliar pada tahun 2023 (Hercog et al., 2023). Namun, di balik potensi besar IoT, tantangan keamanan menjadi perhatian serius. "Serangan terhadap perangkat IoT, seperti *Distributed Denial of Service* (DDoS), *man-in-the-middle*, dan eksploitasi perangkat rentan, terus meningkat secara signifikan" (Wallarm, 2023).

Kerentanan IoT sebagian besar disebabkan oleh lemahnya protokol komunikasi dan kurangnya implementasi mekanisme keamanan yang memadai. Banyak perangkat IoT masih menggunakan protokol komunikasi tanpa enkripsi atau dengan enkripsi yang tidak aman, sehingga "berisiko disusupi oleh serangan siber, seperti penyadapan data" (Al-Mashhadani & Shujaa, 2022). Platform ESP32, yang banyak digunakan dalam pengembangan IoT, juga memiliki kerentanan terhadap serangan seperti replay attack dan packet sniffing akibat kurangnya pengamanan *end-to-end* yang kuat (Prasetyo Eka Putra et al., 2023).

Untuk mengatasi masalah ini, pemilihan protokol komunikasi yang tepat menjadi penting. *Advanced Message Queuing Protocol* (AMQP) merupakan salah satu protokol yang dirancang untuk memastikan keamanan dan keandalan komunikasi antarperangkat dalam jaringan IoT. "AMQP menawarkan fitur keamanan seperti autentikasi berbasis *Transport Layer Security* (TLS) dan mekanisme kontrol akses yang ketat" (CometChat, 2021). Selain itu, "AMQP juga mendukung interoperabilitas yang sangat baik untuk aplikasi IoT skala besar" (Hercog et al., 2023). Di sisi lain, *Transport Layer Security* (TLS) berperan sebagai fondasi dalam melindungi data selama transmisi. "TLS menyediakan tiga lapisan perlindungan utama, enkripsi data untuk mencegah penyadapan, autentikasi berbasis sertifikat digital untuk memverifikasi identitas perangkat, dan integritas data untuk mendeteksi manipulasi selama transmisi" (HPBN, 2023).

Dengan implementasi TLS, risiko pembobolan data dapat dikurangi hingga 92% (Al-Mashhadani & Shujaa, 2022).

Berdasarkan tantangan ini, penelitian ini bertujuan untuk menganalisis dan mengembangkan sistem keamanan jaringan IoT berbasis ESP32 dengan mengintegrasikan protokol AMQP dan TLS. Sistem ini dirancang untuk meningkatkan keamanan komunikasi data antarperangkat, menggunakan sensor DHT11 untuk pengumpulan data lingkungan, dan RabbitMQ sebagai message broker. Dengan pendekatan ini, diharapkan solusi yang dihasilkan dapat mengurangi risiko serangan siber, meningkatkan keandalan komunikasi, serta memberikan perlindungan menyeluruh terhadap data sensitif dalam sistem IoT.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah:

1) Bagaimana cara mengintegrasikan protokol *Advanced Message Queuing Protocol* (AMQP) dengan enkripsi *Transport Layer Security* (TLS) pada ESP32 untuk menjamin keamanan komunikasi pada jaringan IoT?
2) Bagaimana pengaruh penerapan enkripsi TLS terhadap kinerja sistem IoT, termasuk latensi komunikasi dan stabilitas sistem perangkat ESP32?
3) Bagaimana sistem dapat memastikan data yang dikirimkan dari sensor DHT11 melalui protokol *Advanced Message Queuing Protocol* (AMQP) tetap terenkripsi dan terlindungi dari ancaman keamanan?

1.3 Batasan Masalah

Agar ruang lingkup penelitian tidak terlalu luas, batasan masalah yang diterapkan adalah sebagai berikut:

1) Penelitian difokuskan pada pengembangan keamanan jaringan IoT berbasis ESP32 menggunakan protokol *Advanced Message Queuing Protocol* (AMQP) dan enkripsi *Transport Layer Security* (TLS).
2) Implementasi TLS dibatasi pada perlindungan data selama transmisi dalam sistem *monitoring* berbasis ESP32.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Adapun tujuan yang ingin dicapai dalam penelitian Proyek Akhir ini adalah:

1) Merancang sistem keamanan jaringan IoT berbasis ESP32 yang menggunakan protokol AMQP untuk memastikan data dari sensor DHT11 dienkripsi dan terlindungi dari ancaman keamanan.
2) Mengembangkan implementasi protokol AMQP dengan dukungan enkripsi *Transport Layer Security* (TLS) pada ESP32 untuk meningkatkan keamanan komunikasi antarperangkat IoT.
3) Menganalisis dampak penggunaan enkripsi TLS terhadap kinerja jaringan IoT, termasuk aspek latensi komunikasi, dan stabilitas sistem.

1.4.2 Manfaat

Hasil dari penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1) Memperoleh pemahaman mendalam mengenai penerapan *Advanced Message Queuing Protocol* (AMQP) dan enskripsi *Transport Layer Security* (TLS) untuk meningkatkan komunikasi yang aman dan andal pada aplikasi IoT.
2) Meningkatkan keandalan dan keamanan komunikasi data, memastikan bahwa data yang dikirim antar perangkat IoT lebih terlindungi dan minim gangguan dari ancaman eksternal, dengan memanfaatkan keamanan berbasis *Transport Layer Security* (TLS).
3) Menjamin keamanan komunikasi data pada jaringan IoT berbasis ESP32 melalui penerapan enkripsi *Transport Layer Security* (TLS), yang menyediakan perlindungan terhadap penyadapan dan manipulasi data.

1.5 Metode Penelitian

Metode penelitian yang dipakai dalam pembuatan proyek akhir ini adalah:

1) Studi Literatur

   Mengumpulkan informasi dari jurnal, buku, dan artikel terkait ESP32, protokol AMQP, dan enkripsi TLS, serta keamanan jaringan IoT.
2) Perancangan Sistem

Merancang arsitektur jaringan IoT berbasis ESP32 menggunakan protokol AMQP untuk komunikasi, serta enkripsi TLS untuk keamanan data.

3) Implementasi Sistem

   Mengembangkan sistem dengan memprogram ESP32 dan *Server* AMQP, serta mengintegrasikan enkripsi TLS untuk melindungi komunikasi antar perangkat.

4) Pengujian Sistem

   Melakukan uji kelemahan keamanan dengan simulasi serangan terhadap jaringan IoT, serta pengujian kinerja protokol AMQP dan TLS, untuk mengukur keandalan dan keamanan komunikasi data.

5) Analisis Data

   Menganalisis hasil uji keamanan dan performa untuk mengevaluasi dampak penerapan AMQP dan TLS pada sistem IoT.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini menjelaskan latar belakangmasalah, perumusan masalah ruang lingkup masalah, tujuan dan manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini membahas beberapa hasil penelitian terdahulu yang menjadi acuan dan perbandingan dalam penelitian ini. Selain itu akan dibahas pula landasan teori yang diperlukan untuk merancang sistem.

BAB III PERANCANGAN

Bab ini menjelaskan perancangan jaringan IoT berbasis ESP32, mencakup perangkat keras dan lunak. Penerapan protokol AMQP dan enkripsi TLS dijelaskan, termasuk metode pengujian yang digunakan untuk mengukur keandalan dan keamanan sistem.

BAB IV Jadwal dan Perkiraan Biaya

Bab ini berisi informasi mengenai jadwal pengerjaan proyek akhir dan perkiraan biaya yang dibutuhkan untuk pengerjaan proyek akhir.