BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi *Internet of Things* (IoT) telah membawa dampak signifikan dalam berbagai aspek kehidupan, mulai dari industri hingga rumah tangga. IoT memungkinkan perangkat untuk saling terhubung dan berkomunikasi melalui internet, menciptakan ekosistem yang lebih efisien dan cerdas. Salah satu perangkat yang populer dalam pengembangan IoT adalah ESP32, sebuah modul mikrokontroler yang dilengkapi dengan kemampuan Wi-Fi dan *Bluetooth* (Michon et al., 2020). Dengan kemudahan penggunaan dan biaya yang relatif rendah, ESP32 menjadi pilihan menarik bagi pengembang dan peneliti. Namun, seiring dengan meningkatnya adopsi IoT, muncul pula tantangan besar terkait keamanan jaringan. Banyak perangkat IoT yang terhubung ke jaringan publik, sehingga rentan terhadap serangan siber. Keamanan data yang ditransmisikan melalui jaringan sangat penting untuk melindungi informasi sensitif dan mencegah akses tidak sah. Pada tahun 2023, tercatat lebih dari 1,5 miliar perangkat IoT di seluruh dunia menjadi target serangan siber, yang mengakibatkan kerugian besar (Najib et al., 2020). Untuk itu, penerapan protokol komunikasi yang aman menjadi suatu keharusan dalam pengembangan IoT, agar data yang dipertukarkan tetap terlindungi.

Protokol *HyperText Transfer Protocol* (HTTP) adalah salah satu protokol yang umum digunakan dalam komunikasi data di internet. Meskipun HTTP memungkinkan pengiriman data yang cepat dan efisien, protokol ini tidak menyediakan mekanisme keamanan yang memadai (Shafira Nur Alfiah Andina Aura Hayuningtyas, 2024). Protokol HTTP dipilih karena kemudahan implementasinya, kompatibilitas tinggi dengan perangkat IoT seperti ESP32, dan fleksibilitas dalam pengembangan sistem berbasis jaringan. Dibandingkan dengan protokol lain seperti MQTT atau CoAP, HTTP memiliki struktur komunikasi *request-response* yang sederhana dan tidak memerlukan *middlewar*e tambahan, sehingga lebih efisien untuk jaringan berskala kecil seperti *Local Area Network* (LAN). Masalah utama dari protokol HTTP adalah proses pengiriman HTTP *Request* dan HTTP *Response* dilakukan tanpa ada pengamanan sama sekali,

sehingga seseorang yang memiliki akses di jaringan mampu menyadap informasi yang dikirimkan dan bahkan bisa data *tampering* tanpa diketahui oleh kedua belah pihak (Prayama et al., 2021). Tanpa adanya enkripsi, data yang dikirimkan melalui HTTP dapat dengan mudah diintip oleh pihak ketiga. Oleh karena itu, penting untuk mengintegrasikan protokol yang lebih aman untuk memastikan integritas dan kerahasiaan data. Salah satu solusi untuk meningkatkan keamanan komunikasi adalah dengan menggunakan enkripsi TLS (Wahyudi, 2024). TLS adalah protokol yang dirancang untuk memberikan lapisan keamanan tambahan pada komunikasi jaringan, dengan cara mengenkripsi data yang dikirimkan. Dengan menggunakan TLS, pengembang dapat memastikan bahwa data yang dikirimkan antara perangkat IoT dan *server* aman dari potensi serangan, seperti penyadapan dan modifikasi data.

Implementasi TLS pada komunikasi berbasis HTTP dikenal sebagai HTTPS (HTTP *Secure*), yang menawarkan perlindungan lebih terhadap data yang ditransmisikan. Dalam konteks IoT berbasis ESP32, penerapan HTTPS dapat membantu melindungi komunikasi antara perangkat dan *server*, serta menjaga kepercayaan pengguna terhadap sistem yang dibangun (Tohir et al., 2022). Meskipun penerapan HTTPS dengan TLS memberikan banyak keuntungan, ada tantangan tersendiri dalam implementasinya, terutama pada perangkat dengan sumber daya terbatas seperti ESP32. Penggunaan enkripsi dapat mempengaruhi kinerja dan konsumsi daya perangkat. Oleh karena itu, perlu dilakukan penelitian dan pengembangan lebih lanjut untuk mengoptimalkan penggunaan TLS pada perangkat IoT, agar tetap efisien tanpa mengorbankan keamanan.

Dengan mempertimbangkan pentingnya keamanan dalam jaringan IoT dan potensi risiko yang ada, penelitian ini bertujuan untuk mengeksplorasi penerapan keamanan jaringan IoT berbasis ESP32 menggunakan protokol HTTP dan enkripsi TLS. Diharapkan, hasil penelitian ini dapat memberikan kontribusi signifikan terhadap pengembangan sistem IoT yang aman dan andal, serta meningkatkan kesadaran mengenai pentingnya menjaga keamanan data dalam ekosistem IoT yang terus berkembang.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka perumusan masalah dalam pembuatan proyek akhir ini adalah :

1. Bagaimana implementasi protokol HTTP dengan enkripsi *Transport Layer Security* (TLS) pada sistem monitoring IoT berbasis ESP32 menggunakan *Flask Server*?
2. Bagaimana pengaruh implementasi *Transport Layer Security* (TLS) terhadap performa komunikasi data yang meliputi latensi dan stabilitas koneksi dibandingkan dengan komunikasi HTTP tanpa TLS?
3. Bagaimana implementasi *Transport Layer Security* (TLS) dalam menjamin validitas sertifikat, keamanan komunikasi, dan integritas data yang dikirimkan dari sensor DHT11 pada ESP32 menuju *Flask Server*?

1.3 Batasan Masalah

Penelitian Tugas akhir ini diberikan Batasan masalah agar dalam penjelasannya menjadi terarah, dapat dipahami dan sesuai yang diharapkan serta terorganisasi dengan baik. Berikut batasan masalah dalam pembuatan proyek akhir ini sebagai berikut:

1. Fokus utama dari penelitian ini adalah pada aspek keamanan data yang ditransmisikan, termasuk pengamanan terhadap penyadapan dan modifikasi data.
2. Penelitian akan terbatas pada analisis penggunaan protokol HTTP dan HTTPS (dengan enkripsi TLS) dalam komunikasi data.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Adapun tujuan dari penelitian ini adalah:

1. Merancang sistem IoT berbasis ESP32 yang memanfaatkan protokol HTTP dan enkripsi TLS untuk meningkatkan keamanan data yang dikirimkan melalui jaringan.
2. Menerapkan enkripsi TLS pada komunikasi data untuk mencegah ancaman seperti *sniffing* dan *Man-in-the-Middle attack.*

3. Memastikan bahwa sistem pemantauan suhu menggunakan sensor DHT11 dapat mengirimkan data secara aman ke *server*

1.4.2 Manfaat

Manfaat yang diharapkan dari penilitian ini adalah:

1. Meningkatkan keamanan komunikasi data pada perangkat IoT agar terhindar dari potensi ancaman siber.
2. Memberikan panduan implementasi penggunaan TLS pada protokol HTTP di perangkat IoT, sehingga dapat diadopsi untuk berbagai kebutuhan sistem lainnya.

1.5 Metodologi Penelitian

Metode penelitian yang dipakai dalam pembuatan proyek akhir ini adalah:

1. Studi Pustaka

   Dalam penelitian ini akan dilakukan studi pustaka yanitu dengan cara menelaah, menggali, serta mengkaji teori yang mendukung dalam pemecahan masalah yang diteliti.
2. Identifikasi Masalah

   Mengidentifikasi masalah keamanan yang spesifik terkait dengan jaringan IoT berbasis ESP32 melalui studi literatur dan wawancara dengan ahli di bidang keamanan jaringan
3. Perancangan

   Merancang eksperimen untuk menguji efektivitas protokol HTTP dan penerapan TLS dalam komunikasi data
4. Implementasi

   Dalam tahap implementasi merupakan pengembangan prototipe jaringan IoT menggunakan ESP32 yang terhubung dengan *server*
5. Pengujian

   Dalam tahap melakukan pengujian keamanan untuk mengevaluasi kerentanan yang ada pada system jaringan yang menggunakan HTTP dan HTTPS untuk mengetahui apakah keamanan jaringan bekerja sesuai dengan scenario pada awal perancangan