BAB 1
USULAN GAGASAN

1.1 Deskripsi Umum Masalah

Dalam beberapa tahun terakhir, perkembangan teknologi *Internet of Things* (IoT) telah menghadirkan revolusi dalam pengelolaan berbagai sektor, termasuk akuakultur. *My Intelligence Pond* (My I-Pond) merupakan sistem berbasis IoT yang dirancang untuk memantau kualitas air tambak ikan nila secara real-time, dengan tujuan utama untuk meningkatkan efisiensi pengelolaan tambak melalui data yang lebih akurat dan cepat. Sistem ini menggunakan sensor untuk mengukur parameter penting seperti pH, suhu, dan kekeruhan air, yang berperan dalam menjaga kesehatan ekosistem tambak serta meningkatkan produktivitas ikan. Namun, meskipun IoT menawarkan kemudahan dan efektivitas dalam pengelolaan, keamanan perangkat IoT dalam sistem ini menjadi tantangan besar yang perlu diatasi [1].

Kompleksitas masalah muncul karena My I-Pond mengandalkan jaringan terbuka untuk menghubungkan perangkat IoT dengan server pusat. Jaringan terbuka ini menimbulkan risiko keamanan yang signifikan, karena perangkat IoT rentan terhadap berbagai jenis serangan siber. Berdasarkan laporan *Zscaler ThreatLabz* tahun 2023, lalu lintas perangkat IoT meningkat sebesar 18% dibandingkan laporan sebelumnya, seiring dengan semakin banyaknya perangkat yang terhubung. Serangan malware IoT juga meningkat lebih dari 400%, dengan aktivitas botnet yang didominasi oleh keluarga malware Mirai dan Gafgyt, mencakup 66% dari seluruh serangan yang terdeteksi. Hal ini menunjukkan pentingnya perlindungan terhadap serangan yang menargetkan perangkat IoT [2]

Selain itu, pelaku kejahatan siber semakin sering mengeksploitasi kerentanan lama, dengan 34 dari 39 eksploit IoT paling umum ditujukan pada kerentanan yang telah ada selama lebih dari tiga tahun. Perangkat seperti router menjadi target utama, karena perannya sebagai pusat kontrol jaringan yang selalu terhubung. Ancaman semacam ini dapat berdampak pada My I-Pond, yang mengandalkan konektivitas jaringan untuk mengumpulkan dan mentransmisikan data real-time[2]

Salah satu ancaman yang paling umum adalah serangan *man-in-the-middle* (MITM), di mana penyerang dapat menyusup ke dalam komunikasi antara perangkat IoT dan server, mengakses, atau bahkan memodifikasi data yang dikirimkan[3]. Jika data real-time yang dikumpulkan, seperti suhu atau pH air, diubah secara tidak sah, hal ini bisa berujung pada

keputusan operasional yang salah, sehingga merusak ekosistem tambak secara keseluruhan. Dengan semakin banyaknya perangkat IoT yang terhubung, kebutuhan akan solusi keamanan yang komprehensif menjadi semakin mendesak untuk melindungi data dan menjaga keberlanjutan sistem tambak.

1.2 Analisis Masalah

Sistem IoT *My Intelligence Pond (*My I-Pond*)* menghadapi berbagai tantangan yang kompleks, terutama yang berkaitan dengan aspek keamanan sistem. Permasalahan ini dapat dianalisis dari sudut pandang teknis, ekonomi, dan lingkungan, di mana setiap aspek memiliki dampak yang signifikan terhadap keberlangsungan sistem dan operasional tambak.

1.2.1 Aspek Teknis

Dari segi teknis, My I-Pond menggunakan perangkat IoT yang beroperasi dalam jaringan terbuka untuk memantau kualitas air tambak. Proses pengiriman data antara perangkat IoT dan *cloud* masih menghadapi tantangan dalam memenuhi prinsip *Confidentiality, Integrity, Availability* (CIA). Salah satu tantangan utamanya adalah risiko serangan siber yang dapat terjadi pada berbagai lapisan jaringan menurut model OSI.

Pada lapisan jaringan (Network Layer), perangkat IoT rentan terhadap serangan *man-in-the-middle* (MITM), di mana penyerang dapat menyusup di antara komunikasi antara perangkat IoT dan server. Serangan ini memungkinkan penyerang untuk memantau dan memanipulasi data yang dikirimkan[4]. Pada sistem My I-Pond, MITM dapat menyebabkan perubahan pada data real-time seperti suhu atau pH air yang sedang dimonitor, yang jika tidak terdeteksi, akan berakibat pada penurunan kualitas air tambak dan potensi kerusakan ekosistem.

Ancaman utama pada Lapisan transport (*Transport Layer*), adalah serangan *Distributed Denial of Service* (DDoS), yang dapat menyebabkan server atau perangkat IoT tidak bisa diakses. Dalam konteks My I-Pond, serangan DDoS dapat mengakibatkan penghentian aliran data monitoring kualitas air, yang sangat penting untuk menjaga kondisi tambak. Jika komunikasi terganggu, sistem pemantauan dapat gagal memberikan data yang akurat dan tepat waktu, sehingga kondisi buruk dalam tambak tidak akan terdeteksi hingga terlambat.

Pada lapisan presentasi (*Presentation Layer*), masalah utamanya adalah kerahasiaan dan integritas data selama proses transmisi. Perangkat IoT dalam My I-Pond masih terbatas dalam hal daya dan komputasi, sehingga menerapkan enkripsi yang kuat menjadi tantangan. Kelemahan pada lapisan ini dapat membuka celah bagi pihak ketiga untuk mengakses atau memodifikasi data sensitif yang dikirimkan oleh perangkat IoT, berpotensi menyebabkan kebocoran data atau perubahan data yang kritis untuk pengambilan keputusan.

Masalah keamanan pada lapisan aplikasi (*Application Layer*), adalah terkait dengan antarmuka web yang digunakan untuk mengakses data dari perangkat IoT. Serangan seperti *ClickJacking* dan *cross-site scripting* (XSS) merupakan ancaman yang dapat mengakibatkan pengambilalihan sistem atau akses tidak sah ke data sensitif [4]. Kelemahan pada lapisan ini dapat menyebabkan kerusakan operasional, dimana penyerang dapat mengakses, memanipulasi, atau bahkan menghapus data penting yang digunakan untuk monitoring kualitas air.

1.2.2 Aspek Ekonomi

Dari sudut pandang ekonomi, permasalahan keamanan pada sistem My I-Pond dapat menimbulkan kerugian yang cukup serius, terutama dalam hal biaya perbaikan perangkat, hilangnya data penting, dan gangguan operasional tambak. Serangan siber yang berhasil dapat merusak perangkat IoT yang digunakan untuk monitoring kualitas air, yang memaksa pihak pengelola tambak mengeluarkan biaya tambahan untuk perbaikan atau penggantian perangkat yang rusak. Selain itu, hilangnya data real-time yang sangat penting bagi pengambilan keputusan operasional tambak dapat menyebabkan keputusan yang salah, seperti tidak mendeteksi perubahan kualitas air yang berbahaya bagi ikan. Akibatnya, produktivitas tambak bisa menurun secara drastis.

Selebihnya, downtime yang disebabkan oleh serangan atau kegagalan sistem dapat mengakibatkan gangguan pada aliran kerja tambak. Ketika data yang diperlukan untuk memonitor kondisi air tidak tersedia atau tidak akurat, penanganan masalah yang seharusnya dilakukan segera menjadi tertunda. Hal ini tidak hanya berdampak pada hasil produksi tambak dalam jangka pendek, tetapi juga dapat mempengaruhi reputasi tambak secara keseluruhan. Tambak yang bergantung pada sistem IoT seperti My I-Pond harus beroperasi dengan efisiensi tinggi, sehingga setiap gangguan atau downtime tidak dapat mempengaruhi hasil panen dan mengakibatkan kerugian finansial yang signifikan.

Selain itu, perlu dipertimbangkan pula dampak jangka panjang dari hilangnya kepercayaan terhadap sistem monitoring IoT. Jika sistem My I-Pond mengalami serangan berulang atau masalah keamanan yang tidak segera diatasi, hal ini dapat merugikan secara finansial dalam jangka panjang karena peningkatan biaya untuk langkah-langkah keamanan tambahan dan pemulihan sistem. Ketidakstabilan dalam sistem monitoring juga berisiko mengurangi keandalan tambak dalam menjaga kualitas air, yang dapat mengakibatkan kerugian lebih besar pada siklus produksi berikutnya.

1.2.3 Aspek Lingkungan

Masalah keamanan pada My I-Pond tidak hanya berdampak pada aspek teknis dan ekonomi, tetapi juga dapat merusak lingkungan. Perangkat IoT yang digunakan dalam sistem ini bertanggung jawab untuk memonitor kualitas air tambak, termasuk parameter penting seperti pH, suhu, dan kekeruhan. Jika sistem monitoring terganggu oleh serangan siber dan data yang dikumpulkan tidak akurat atau bahkan tidak tersedia, penanganan kualitas air menjadi tidak sesuai.

Kegagalan dalam mendeteksi perubahan kualitas air yang disebabkan oleh masalah keamanan dapat menyebabkan kerusakan pada ekosistem tambak. Misalnya, air yang terlalu asam atau keruh dapat menyebabkan kondisi tidak layak bagi ikan, yang pada akhirnya mengurangi populasi ikan dan merusak keseimbangan lingkungan tambak. Jika kualitas air terus memburuk tanpa intervensi yang tepat waktu, dampaknya bisa lebih luas, termasuk gangguan pada keanekaragaman hayati di sekitar tambak dan pencemaran air yang berpotensi menyebar ke lingkungan sekitarnya.

1.3 Analisis Solusi yang Ada

Berbagai solusi telah diajukan untuk mengatasi masalah keamanan pada perangkat IoT. Salah satu pendekatan yang paling umum adalah penerapan enkripsi data untuk melindungi komunikasi antara perangkat dan server. Protokol seperti TLS (*Transport Layer Security*) telah digunakan untuk memastikan bahwa data yang dikirim aman dari serangan *man-in-the-middle*. Namun, solusi ini sering kali membutuhkan daya komputasi yang besar, yang sulit diterapkan pada perangkat IoT yang memiliki keterbatasan daya dan memori [4]. Salah satu keunggulan enkripsi adalah yaitu melindungi data selama transmisi dan penyimpanan menggunakan metode simetris seperti AES maupun metode asimetris seperti RSA dan ECC. AE, seperti

Ascon, juga menawarkan keamanan tambahan dengan menggabungkan enkripsi dan autentikasi sekaligus, yang sangat efektif dalam mencegah serangan man-in-the-middle. Pengelolaan kunci skala besar juga sulit karena ada kemungkinan kebocoran data jika tidak dikelola dengan benar [5] [6].

Selain enkripsi, solusi seperti *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) telah digunakan untuk mendeteksi serangan pada perangkat IoT seperti serangan *Distributed Denial of Service* (DDoS) dan serangan *brute force*. Melalui metode deteksi tanda atau anomali, sistem ini dapat mengenali pola serangan baru. Namun, salah satu kelemahan sistem IDS/IPS adalah mereka seringkali tidak dapat mendeteksi secara real-time, yang berarti serangan dapat terjadi sebelum sistem dapat menanggapi. Selain itu, sistem IDS/IPS bergantung pada database tanda tangan, yang membuatnya kurang efektif dalam mendeteksi serangan yang belum terdaftar, seperti serangan *zero-day*. Selain itu, overhead yang disebabkan oleh IDS/IPS juga menjadi masalah, terutama pada perangkat IoT yang memiliki jumlah daya dan kapasitas yang terbatas [7].

1.4 Tujuan Tugas Akhir

Tujuan dari pelaksanaan tugas akhir ini adalah merancang dan mengimplementasikan sistem keamanan pada platform Internet of Things (IoT) berbasis edge computing yang mampu melindungi data dari serangan siber secara efisien. Sistem yang dikembangkan, bernama My-Ipond, difokuskan pada pemantauan kualitas air tambak secara real-time menggunakan sensor pH, suhu, dan kekeruhan, yang datanya dikirim melalui mikrokontroler ESP32 ke perangkat edge Raspberry Pi. Tujuan khusus dari penelitian ini adalah untuk menerapkan algoritma enkripsi AES-256 guna menjaga kerahasiaan data selama transmisi ke cloud, serta mengintegrasikan sistem Intrusion Prevention System (IPS) berbasis Suricata untuk mendeteksi dan mencegah ancaman jaringan secara lokal sebelum data dikirimkan. Selain itu, sistem juga diarahkan untuk menguji performa edge node terhadap berbagai parameter seperti latency, throughput, response time, efisiensi enkripsi, dan keandalan dalam menghadapi skenario serangan siber. Melalui tugas akhir ini, diharapkan dapat dihasilkan sebuah solusi IoT yang tidak hanya responsif dan efisien, tetapi juga aman dan dapat diterapkan pada lingkungan dengan keterbatasan sumber daya.

1.5 Batasan Tugas Akhir

Merangkum dari standar yang sudah ada, ISO 27001 dan NIST IR 8200 digunakan sebagai standar acuan utama untuk memastikan keamanan data pada sistem IoT. Standar ini menekankan perlunya penerapan kontrol keamanan yang melindungi kerahasiaan, integritas, dan ketersediaan data. Dalam konteks IoT, spesifikasi yang diterapkan harus disesuaikan dengan keterbatasan daya dan komputasi perangkat seperti ESP32. Penerapan ini mencakup enkripsi data, kontrol akses, dan deteksi ancaman menggunakan IDS/IPS, yang semuanya memerlukan adaptasi untuk menjaga efisiensi dan keandalan sistem. Selain itu, parameter Quality of Service (QoS) seperti latency, throughput, dan overhead kinerja juga menjadi aspek penting yang perlu diperhatikan. Latency mengukur waktu yang dibutuhkan data untuk mencapai tujuan, throughput mencerminkan kapasitas data yang berhasil ditransmisikan dalam periode tertentu, sedangkan overhead kinerja mengevaluasi beban tambahan pada sistem, baik dari sisi penggunaan CPU maupun memori. Ketiga parameter ini harus dioptimalkan agar sistem tetap responsif, efisien, dan mampu menjaga performa meskipun berada di bawah tekanan beban kerja atau ancaman siber.

Tabel 2. 1 Tabel Parameter IPS

Parameter	Deskripsi
Response Time	Waktu yang dibutuhkan sistem untuk merespons ancaman yang terdeteksi (misalnya, pemblokiran atau pengiriman peringatan).
Keandalan dan Ketahanan terhadap Serangan (*Reliability*)	kemampuan sistem dalam mempertahankan keamanan secara konsisten dan bertahan terhadap berbagai bentuk serangan.

Tabel 2. 2 Tabel Parameter Enkripsi

Parameter	Deskripsi
Kecepatan Enkripsi dan Dekripsi	Kecepatan enkripsi dan dekripsi data, mempengaruhi *latency* dan performa.

Avalanche Effects	Efek di mana perubahan kecil pada input (misalnya satu bit) menghasilkan perubahan signifikan pada output cipher. Parameter ini menunjukkan kekuatan difusi algoritma dan penting dalam menilai keamanan enkripsi.

Tabel 2. 3 Tabel Parameter Quality of Service

Parameter	Deskripsi
Latency	Kecepatan waktu pengiriman data dari IoT terhadap server *Edge Computing*.
Throughput	Kemampuan sistem dalam memproses data dalam jumlah besar tanpa penurunan kinerja.
Overhead kinerja	Dampak enkripsi terhadap kinerja sistem, terutama pada penggunaan CPU dan Memori
Scalability	kemampuan Suricata untuk menjaga performa deteksi dan mitigasi saat menghadapi peningkatan beban trafik atau jumlah perangkat.

Parameter-parameter yang disajikan pada Tabel 2.1 dan Tabel 2.2 merupakan ruang lingkup batasan yang digunakan dalam pelaksanaan tugas akhir ini. Batasan tersebut ditetapkan guna memberikan kejelasan terhadap aspek-aspek teknis yang menjadi fokus dalam proses implementasi dan evaluasi sistem keamanan berbasis IoT yang dirancang.