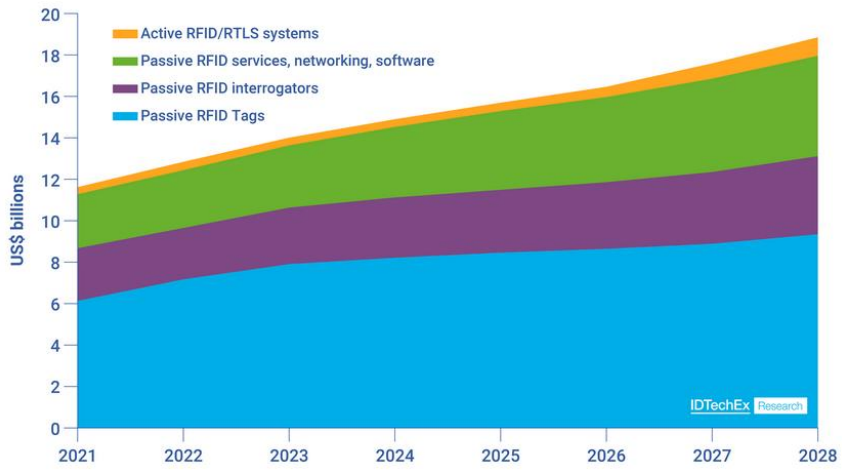
BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Dalam beberapa tahun terakhir, kemunculan teknologi *Internet of Things* (IoT) telah memberikan dampak yang signifikan di berbagai sektor industri, membawa kemajuan yang luar biasa dalam meningkatkan efisiensi dan konektivitas perangkat sehari-hari (Erwin dkk., 2023). Seiring dengan perkembangan tersebut, salah satu pengaplikasian yang banyak digunakan pada saat ini dari teknologi IoT adalah sistem RFID (*Radio-Frequency Identification*). Menonjolnya adopsi pengaplikasiannya tersebut selaras dengan data yang disajikan pada Gambar 1.1 bahwa pertumbuhan pasar RFID mencapai $14 miliar pada tahun 2023, yang termasuk *contactless card/tag*, *reader*, *keychain/fob*, layanan untuk label, dan semua faktor bentuk lainnya, baik untuk RFID pasif maupun aktif (Das & Chang, 2023). IDTechEx memperkirakan 10 tahun ke depan pada tahun 2033 untuk pertumbuhan pasar dari *tag* RFID berjenis pasif HF (*High Frequency*) meningkat pada pengaplikasian kartu tanda penduduk di berbagai negara dan kartu kredit modern dalam bentuk format yang dikenal sebagai "*contactless card*" atau "*tap-and-go*". Sekitar 3,1 miliar kartu/*tag* RFID diperkirakan ada pada tahun 2023 yang didorong karena masifnya kegiatan penggunaan seperti sistem layanan pembayaran, transit, dan autentikasi keamanan (Das & Chang, 2023).



Gambar 1.1 Data Pertumbuhan Pasar RFID (Das & Chang, 2023)

Berdasarkan data tersebut menekankan bahwasannya adopsi pengaplikasian dari sistem RFID saat ini masif digunakan di berbagai sektor industri, contohnya

seperti produk sistem pengamanan pintu RFID berbasis IoT yang dikomersilkan secara massal oleh Armada Integrasi Teknologi dengan nomor *series* BF-870 (Armada-IT, 2024). Didukung dengan penelitian terdahulu, sistem pengamanan pintu RFID berbasis IoT ini mewakili sebuah terobosan dalam solusi autentikasi keamanan pintar pada berbagai jenis pintu termasuk palang perumahan, kamar hotel, ruangan server, ruangan balita rumah sakit, laboratorium, gudang, dan brankas (Mubarok & Subali, 2020; Muthohir dkk., 2023; Nurwijaksana & Candra, 2021; Yulisman dkk., 2021). Dengan memanfaatkan sebuah *contactless card/tag* RFID, pengguna dapat memungkinkan integrasi fitur-fitur canggih ke dalam sistem pengamanan pintu. Integrasi ini mencakup mekanisme kontrol akses yang memfasilitasi pendekatan keamanan responsif seperti kemampuan pemantauan dan manajemen jarak jauh, yang memungkinkan pengguna untuk dapat memonitoring riwayat data akses masuk dan keluar pintu.

Namun, di era kemajuan ini, aspek keamanan dari teknologi IoT telah menjadi perhatian khusus tersendiri karena adanya kerentanan pada pengaplikasian sistem RFID yang berpotensi membahayakan integritas data dan privasi pengguna (Lounis & Zulkernine, 2020). Sistem pengamanan pintu RFID yang diintegrasikan dengan IoT, terutama dalam mekanisme kontrol akses, telah memperkenalkan tantangan baru terkait perlindungan data kunci sensitif. Salah satu kerantanan yang dikhawatirkan pada integrasi IoT ialah *insecure data transfer and storage*, sebuah kerentanan yang dimana kurangnya enkripsi terhadap data sensitif di dalam ekosistem, termasuk saat dalam penyimpanan, pemrosesan, atau selama perjalanan (Ferrara dkk., 2021).

Hal tersebut dapat terjadi dikarenakan sebagian besar integrasi IoT yang memakai protokol komunikasi MQTT (*Message Queuing Telemetry Transport*) tidak memiliki mekanisme keamanan data secara *default* yang membuat data sensitif diendus oleh penyerang melalui aplikasi *sniffer* atau bahkan memonitor lalu lintas jaringan (Hintaw dkk., 2023). Sehingga implementasinya membiarkan data penting terbuka tanpa enkripsi pun dapat terjadi pada lingkungan penyimpanan web dan *database* servernya (Ferrara dkk., 2021). Ada berbagai macam serangan pengendusan jaringan IoT pada *network* dan *middleware layer* yang terjadi dilakukan oleh penyerang pada *vulnerability* protokol komunikasi

MQTT, salah satunya ialah *network sniffing* dan MiTM (*Man-in-the-Middle*) (Chen dkk., 2020; Nandy dkk., 2019; Silveira & Gradvohl, 2021; Simsek & Atilgan, 2023). Dalam ranah sistem RFID, penyerang dapat memata-matai komunikasi jaringan untuk mendapatkan data *tag/*kartu RFID yang tidak terenkripsi dalam transmisi dari RFID *reader* ke sistem server/*broker* (Figueroa dkk., 2018). Pencurian data menggunakan teknik tersebut dapat memberikan akses yang tidak sah dan penyerang dapat menduplikasikan data *tag/*kartu RFID sang korban untuk disalahgunakan agar mengakses area ruangan yang seharusnya terlindungi (Shaikh dkk., 2019). Sehingga penyerang dapat dengan mudah mengelabui sistem pengamanan pintu RFID berbasis IoT, dan dengan leluasa dapat masuk ke dalam salah satu ruangan yang terotorisasi.

Kehadiran teknologi IoT dalam sistem pengamanan pintu RFID telah membuka banyak celah bagi para penyerang untuk mengeksploitasi. Dalam menghadapi ancaman ini, menegaskan pentingnya mengimplementasikan langkah-langkah keamanan yang kokoh dan enkripsi yang handal dalam upaya melindungi integritas sistem secara menyeluruh. Penelitian yang diusulkan ini melatarbelakangi untuk mengatasi masalah-masalah pada sistem RFID berbasis IoT yang berfokus pada implementasi kriptografi simetris menggunakan algoritma enkripsi *Advanced Encryption Standard* (AES-128) dalam kerangka kerja keamanan autentikasi pintu. AES-128, yang dikenal dengan kemampuan enkripsinya yang kuat, dimaksudkan untuk memperkuat keamanan sistem pengamanan pintu RFID berbasis IoT (Al-Mashhadani & Shujaa, 2022; Kaindl, 2021). Dengan memanfaatkan algoritma enkripsi simetris AES-128, penelitian ini berupaya menjaga integritas dan kerahasiaan data selama komunikasi antara perangkat dan unit kontrol pusat (Biswal dkk., 2022; Ravida & Santoso, 2020).

Urgensi penelitian ini digarisbawahi oleh meningkatnya kasus akses tidak sah, pelanggaran data, dan teknik peretasan menggunakan alat canggih yang menargetkan sistem keamanan berkemampuan IoT (Harbi dkk., 2021). Prevalensi insiden keamanan semacam itu menggarisbawahi kebutuhan kritis akan enkripsi tangguh dalam memitigasi risiko yang ditimbulkan dari serangan MiTM dan *network sniffing*. Dengan menerapkan enkripsi AES-128 pada proses pembacaan *reader* RFID di *microcontroller*, diharapkan dapat meminimalisir terjadinya

kerentanan sistem pengamanan pintu RFID berbasis IoT. Signifikansi dari penelitian ini terletak pada potensinya untuk berkontribusi pengembangan paradigma keamanan yang tangguh dalam protokol komunikasi MQTT melalui penerapan enkripsi AES-128 untuk transmisi data *reader* RFID di *microcontroller* ke dalam server/*broker*.

1.2 Rumusan Masalah Penelitian

Pada konteks sistem pengamanan pintu RFID yang terhubung dengan *Internet of Things* (IoT), penelitian ini berfokus pada beberapa permasalahan utama, yaitu:

1. Bagaimana mengembangkan sistem pengamanan pintu RFID berbasis IoT dengan implementasi AES-128 pada protokol komunikasi MQTT.
2. Bagaimana evaluasi performa kinerja sistem pengamanan pintu RFID berbasis IoT dengan implementasi AES-128 pada protokol komunikasi MQTT.

1.3 Batasan Penelitian

Batasan penelitian diperlukan pada penelitian ini untuk mengarahkan fokus penelitian agar menghindari risiko meluasnya ruang lingkup penelitian yang terlalu luas. Adapun batasan penelitian ini adalah sebagai berikut:

1. Penelitian ini menyempurnakan sistem yang telah ada pada produk yang dikomersilkan oleh Armada Integrasi Teknologi dengan nomor *series* BF-870 bernama *WebBased RFID MultiDoor Controller,* serta menyempurnakan penelitian terdahulu sebelumnya mengenai sistem pengamanan pintu RFID berbasis IoT.
2. Sistem yang dikembangkan berfokus pada celah kerentanan di jaringan IoT yaitu *insecure data transfer and storage* dalam serangan *network sniffing* dan MiTM untuk sistem RFID berbasis IoT dengan protokol komunikasi MQTT.
3. Penelitian ini berfokus melakukan pengembangan sistem pengamanan pintu RFID berbasis IoT dengan implementasi AES-128 pada protokol komunikasi MQTT.

4. Menambahkan opsi inputan selain RFID, yaitu *biometric fingerprint* sebagai strategi mitigasi risiko yang diperlukan, serta mengembangkan sistem manajemen web *dashboard* yang andal menggunakan Laravel.
5. Mengimplementasikan *kernel* sistem operasi FreeRTOS pada pengembangan sistem pengamanan pintu RFID berbasis IoT.
6. Purwarupa sistem pengamanan pintu RFID berbasis IoT yang dikembangkan ini menggunakan *microcontroller* ESP32 dan *reader* RFID MFRC 522 HF.
7. Penelitian ini berfokus melakukan pengujian performa kinerja sistem pengamanan pintu RFID berbasis IoT dengan implementasi AES-128 pada protokol komunikasi MQTT.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dirumuskan sebelumnya, maka penelitian ini bertujuan untuk:

1. Mengembangkan sistem pengamanan pintu RFID berbasis IoT dengan implementasi AES-128 pada protokol komunikasi MQTT.
2. Mengevaluasi performa kinerja sistem pengamanan pintu RFID berbasis IoT dengan implementasi AES-128 pada protokol komunikasi MQTT.

1.5 Manfaat Penelitian

Berdasarkan tujuan penelitian yang telah dipaparkan sebelumnya, diharapkan penelitian ini dapat bermanfaat bagi perkembangan teknologi terutama di bidang *Cyber Security* dan *Internet of Things*. Berikut beberapa manfaat dari penelitian ini diantaranya:

1.5.1 Manfaat Teoritis

1. Kontribusi terhadap keamanan IoT dalam memperluas pemahaman terhadap kerentanan pada sistem pengamanan pintu RFID yang terhubung dengan IoT, serta memberikan wawasan terkait strategi mitigasi risiko yang diperlukan.
2. Solusi kriptografi algoritma enkripsi simetris AES-128 sebagai landasan teoritis diharapkan mampu meningkatkan keamanan transmisi

data kartu/*tag* RFID ke dalam server/*broker* dengan konteks integrasi IoT.

1.5.2 Manfaat Praktis

1. Penyempurnaan sistem, dimana membantu dalam merancang dan mengembangkan sistem pengamanan pintu RFID yang lebih andal melalui penerapan teknologi kriptografi AES-128, serta mengidentifikasi risiko yang perlu diwaspadai.
2. Perlindungan data sensitif dalam meningkatkan keamanan dan privasi pengguna dengan mengurangi risiko pencurian data serta akses ilegal pada sistem pengamanan pintu RFID berbasis IoT.
3. Relevansi terhadap industri yang memberikan pandangan praktis bagi industri untuk meningkatkan sistem pengamanan pintu RFID berbasis IoT dengan mempertimbangkan solusi keamanan yang teruji.

1.6 Struktur Organisasi Skripsi

Sistematika penulisan karya tulis ilmiah ini terdiri atas 5 bagian diantaranya bagian pendahuluan, kajian pustaka, metode penelitian, temuan dan pembahasan, serta simpulan, implikasi, dan rekomendasi. Hal tersebut berdasar pada Peraturan Rektor UPI (Universitas Pendidikan Indonesia) Nomor. 7867/UN40/HK/2021 tentang Pedoman penulisan Karya Ilmiah Universitas Pendidikan Indonesia Tahun Akademik 2021. Adapun rincian setiap bagiannya sebagai berikut:

I. PENDAHULUAN

Dalam bab ini, penulis memperkenalkan konteks penelitian, mengidentifikasi permasalahan yang akan diselesaikan, dan merinci tujuan serta manfaat dari penelitian yang dilakukan. Struktur organisasi skripsi juga dijelaskan untuk memberikan gambaran menyeluruh tentang arah penulisan.

II. KAJIAN PUSTAKA

Bab kedua, yaitu Kajian Pustaka, menyoroti kajian teoritis yang relevan dari penelitian sebelumnya. Fokus utama bab ini adalah pada pemahaman keamanan sistem pengamanan pintu RFID berbasis IoT, protokol komunikasi MQTT pada IoT, serta kriptografi algoritma enkripsi

simetris AES-128. Penulis menguraikan konsep-konsep dari literatur yang mendukung kerangka konseptual penelitian, memberikan landasan kokoh untuk penelitian yang dilakukan.

III. METODOLOGI PENELITIAN

Bagian ketiga, yaitu Metodologi Penelitian, memaparkan secara rinci langkah-langkah yang dilalui dalam proses penelitian. Dimulai dari perancangan penelitian, implementasi, hingga pengujian model enkripsi AES-128 pada sistem pengamanan pintu RFID berbasis IoT. Pemilihan metode *Design Research Methodology* (DRM) dijelaskan untuk memberikan pemahaman yang jelas tentang pendekatan yang digunakan dalam pengumpulan data, pengembangan sistem, dan pengujian sistem.

IV. TEMUAN DAN PEMBAHASAN

Bab keempat, yang berjudul Temuan dan Pembahasan, menjadi wadah untuk mendiskusikan hasil temuan dari implementasi enkripsi AES-128 pada sistem pengamanan pintu RFID berbasis IoT. Evaluasi pengujian kinerja sistem menjadi fokus utama pembahasan. Dalam bagian ini, penulis menyoroti aspek-aspek kritis yang muncul selama penelitian dan memberikan pemahaman mendalam terhadap perlindungan data kunci kartu/*tag* RFID sensitif yang ditransmisikan oleh sistem pengamanan pintu RFID berbasis IoT.

V. SIMPULAN, IMPLIKASI, DAN REKOMENDASI

Bab terakhir, yaitu Simpulan, Implikasi, dan Rekomendasi, yang merangkum temuan penelitian. Simpulan dari hasil penelitian disajikan, diikuti dengan pembahasan implikasi dari penggunaan enkripsi AES-128 dalam sistem pengamanan pintu RFID berbasis IoT. Terakhir, penulis menyampaikan rekomendasi untuk pengembangan penelitian selanjutnya, memberikan arah bagi peneliti masa depan untuk mengembangkan konsep dan aplikasi lebih lanjut dalam bidang ini.