

KEAMANAN DAN IMPLEMENTASI IOT DALAM LINGKUNGAN INDUSTRI

Muhammad Fatih Muhana, Evans Fuad

Teknik Informatika, Universitas Muhammadiyah Riau

Jalan Tuanku Tambusai Kota Pekanbaru, Indonesia

mfatihmuhana@gmail.com

ABSTRAK

Perkembangan cepat Internet of Things (IoT) telah membawa dampak signifikan di sektor industri, menciptakan peluang untuk peningkatan efisiensi operasional dan inovasi. Namun, tantangan serius muncul terkait aspek keamanan informasi, di mana potensi serangan dapat mengganggu operasional dan membahayakan keselamatan pekerja. Penelitian ini bertujuan untuk menyajikan pemahaman mendalam mengenai sistem keamanan IoT dalam lingkungan industri, dengan menganalisis temuan terkini dari jurnal-jurnal terakreditasi. Metode yang digunakan adalah studi pustaka, yang mencakup pengumpulan dan analisis data dari sumber-sumber seperti jurnal, buku, dan publikasi ilmiah, dengan fokus pada jurnal yang terakreditasi SINTA 1 hingga SINTA 5, antara tahun 2018 hingga 2023. Proses ini melibatkan pembacaan dan pencatatan informasi, serta sintesis dari sepuluh jurnal relevan untuk merumuskan kesimpulan yang mendalam. Hasil penelitian menunjukkan bahwa fokus utama dalam keamanan IoT meliputi penerapan teknologi seperti pengaturan cerdas, deteksi gas dan gerakan, pengenalan wajah, serta penggunaan Raspberry Pi. Selain itu, penerapan pemantauan jarak jauh dan solusi keamanan menyeluruh seperti QR code dan teknologi RFID menunjukkan potensi inovasi dalam menjaga integritas dan kerahasiaan data. Dengan pemahaman ini, diharapkan dapat membangun dasar yang kokoh untuk sistem keamanan IoT yang lebih efektif di masa depan.

Kata kunci : *IoT, Sistem, Keamanan, Industri*

1. PENDAHULUAN

Perkembangan cepat Internet of Things (IoT) memiliki dampak yang besar di berbagai sektor, termasuk lingkungan industri. Penerapan IoT di industri membuka peluang baru untuk meningkatkan efisiensi operasional dan menggalakkan inovasi. Namun, seiring dengan manfaat yang dihadirkan oleh integrasi ini, juga muncul tantangan serius terkait dengan aspek keamanan.

Dalam konteks ini, tujuan dari peninjauan literatur ini adalah untuk menyajikan pemahaman yang mendalam tentang sistem keamanan IoT di lingkungan industri. Dengan menguraikan temuan-temuan terkini dari jurnal-jurnal utama, kita dapat menyelidiki perkembangan terkini, kerangka kerja keamanan yang diterapkan, serta solusi-solusi inovatif yang telah diajukan oleh penelitian sebelumnya.

Kehadiran perangkat terkoneksi di sektor industri memberikan kontribusi pada peningkatan produktivitas dan efisiensi, namun sekaligus membawa risiko serius terhadap keamanan informasi. Potensi serangan terhadap sistem IoT di industri dapat mengakibatkan gangguan operasional, mengancam kelangsungan produksi, dan bahkan membahayakan keselamatan pekerja. Karena itu, penelitian dan pengembangan keamanan IoT di lingkungan industri menjadi perhatian utama.

Melalui penelaahan literatur ini, penulis akan menyelidiki kerangka kerja keamanan yang telah diusulkan, teknologi keamanan yang diterapkan, serta tantangan dan peluang yang dihadapi dalam menjaga integritas dan kerahasiaan data di lingkungan industri yang terhubung. Dengan pemahaman mendalam terhadap pandangan yang telah dihasilkan oleh

penelitian sebelumnya, kita dapat membangun dasar yang kokoh untuk merancang dan menerapkan sistem keamanan IoT yang efektif dan adaptif di masa depan industri.

2. TINJAUAN PUSTAKA

2.1. Pengertian IoT

Internet of Things (IoT) merupakan gagasan di mana objek fisik, perangkat, atau sistem yang terhubung ke internet memiliki kemampuan untuk berkomunikasi dan bertukar data secara otomatis. Dengan kata lain, IoT menciptakan suatu ekosistem di mana berbagai perangkat dapat terkoneksi, saling berbagi informasi, dan berinteraksi untuk mencapai tujuan tertentu tanpa memerlukan campur tangan manusia[1].

2.2. Penelitian Terdahulu

Pada penelitian [2] menyajikan analisis menyeluruh mengenai keamanan dan privasi dalam ekosistem pertanian cerdas. Artikel ini menjelaskan arsitektur berlapis yang relevan dengan pertanian presisi serta membahas isu-isu keamanan dan privasi dalam lingkungan maya yang dinamis dan terdistribusi. Selain itu, penelitian ini juga mengidentifikasi potensi skenario serangan siber dan menyoroti tantangan penelitian yang masih terbuka serta arah pengembangan di masa depan.

Pada penelitian [3] membahas perkembangan pesat Internet of Things (IoT) dan aplikasinya di berbagai sektor, seperti konsumen, kesehatan, dan pertanian. Penelitian ini mencakup kondisi ekosistem IoT saat ini, manfaat utama, dan tantangan yang dihadapi. Arsitektur IoT dibagi menjadi tiga lapisan:

perangkat, gateway, dan platform, serta empat tahap tata letak: sensor, gateway, pemrosesan data edge, dan cloud. Arsitektur ini memungkinkan pengumpulan dan analisis data untuk solusi otomatis yang efisien. Di masa depan, IoT akan menjadi dasar banyak teknologi, dengan pembelajaran mesin semakin berperan dalam berbagai industri.

2.3. Sistem Keamanan

Perlindungan perangkat, data, dan jaringan dalam ekosistem Internet of Things (IoT) melibatkan sejumlah protokol, teknologi, dan kebijakan untuk mengamankan sistem dari potensi ancaman keamanan. Pentingnya keamanan ini diperlihatkan oleh kerentanannya perangkat terhubung terhadap berbagai jenis serangan, termasuk serangan siber dan risiko penyalahgunaan data[4].

2.4. Perkembangan IoT dalam Sistem Keamanan

Evolusi yang signifikan dalam usaha melindungi perangkat, data, dan jaringan di dalam ekosistem Internet of Things (IoT) tercermin dalam kemajuan keamanan sistem. Salah satu kemajuan utama adalah penerapan teknologi keamanan yang lebih canggih, termasuk peningkatan dalam penggunaan enkripsi, otentikasi yang kuat, dan pemantauan keamanan secara real-time[5].

Standarisasi protokol juga menjadi fokus yang penting, memfasilitasi integrasi perangkat dari berbagai produsen sambil menjaga tingkat keamanan yang konsisten. Di samping itu, meningkatnya kesadaran terhadap risiko keamanan yang terkait dengan implementasi IoT telah mendorong pengembangan kebijakan dan praktik keamanan yang lebih matang[6].

2.5. Keamanan IoT di Lingkungan Industri

Keamanan IoT di sektor industri menjadi isu yang sangat penting dan membutuhkan perhatian khusus, terutama mengingat perkembangan cepat Internet of Things (IoT) dalam konteks industri. Pentingnya aspek keamanan semakin meningkat sejalan dengan peningkatan konektivitas perangkat dan sistem di lingkungan industri, yang dapat meningkatkan potensi kerentanan terhadap berbagai serangan siber dan ancaman keamanan lainnya[7].

Aspek krusial dalam menghadapi kompleksitas konektivitas dan integrasi perangkat di sektor industri adalah keamanan Internet of Things (IoT)[8]. Fokus analisis risiko keamanan yang spesifik pada potensi dampak terhadap operasional dan keselamatan mendorong kebutuhan akan strategi keamanan yang canggih dan menyeluruh.

Tantangan unik muncul, termasuk risiko gangguan operasional yang dapat berdampak negatif pada produktivitas, potensi ancaman terhadap keselamatan karyawan, dan risiko potensial kerugian data yang signifikan[9]. Pentingnya memahami dan mengatasi risiko-risiko ini menjadi landasan kunci dalam perancangan dan implementasi solusi keamanan

yang adaptif, memastikan kelancaran operasional dan tingkat keamanan yang optimal di lingkungan industri yang semakin terkoneksi.

2.6. Protokol dan Teknologi Keamanan

Peran vital protokol dan teknologi keamanan dalam mendukung keamanan sistem Internet of Things (IoT) di lingkungan industri memiliki signifikansi yang besar. Dengan mengevaluasi protokol keamanan yang umum digunakan, dapat dipastikan bahwa keamanan data yang dikirim antar perangkat IoT melalui jaringan tetap terjaga. Terus berkembangnya teknologi keamanan, seperti penggunaan enkripsi tingkat lanjut dan penerapan mekanisme otentikasi yang kuat, memberikan tingkat perlindungan tambahan terhadap perangkat dan informasi yang beroperasi dalam konteks industri yang terus berkembang.[10]. Dengan memperhatikan aspek-aspek ini, implementasi protokol dan teknologi keamanan yang sesuai menjadi kunci utama untuk menjaga integritas dan keandalan operasional dalam lingkungan IoT industri yang semakin terkoneksi

2.7. Tantangan dan Peluang

Tantangan dan peluang yang muncul seiring dengan implementasi Internet of Things (IoT) di lingkungan industri menciptakan situasi yang kompleks dalam mengelola aspek keamanan dan efisiensi operasional. Tantangan tersebut terkait dengan risiko gangguan operasional yang dapat berdampak negatif pada produktivitas dan kelangsungan operasional, sementara juga menuntut manajemen akses yang efektif untuk menjaga integritas data

Meskipun di dalam tantangan tersebut terdapat risiko, terbuka pula peluang untuk mengembangkan solusi inovatif, meningkatkan otomatisasi proses, dan memanfaatkan data yang dihasilkan oleh perangkat IoT guna meningkatkan efisiensi keseluruhan. Dengan pemahaman yang mendalam terhadap tantangan dan penerimaan terhadap peluang tersebut, organisasi dapat merancang strategi yang adaptif dan holistik untuk mendukung kesuksesan penerapan IoT di konteks lingkungan industri

2.8. Kasus Studi Keamanan IoT Industri

Penelitian kasus mengenai keamanan IoT di sektor industri memiliki peran yang sangat penting dalam mengevaluasi serta memahami tantangan konkret dan solusi yang dapat diterapkan di lingkungan yang semakin terkoneksi. Salah satu contoh studi yang mencerminkan kompleksitas dan kebutuhan keamanan di dunia industri adalah penerapan sistem otomatisasi di sebuah pabrik manufaktur besar.[11]

Dalam situasi tersebut, pabrik menggunakan berbagai perangkat IoT dengan tujuan meningkatkan efisiensi dan memonitor langsung proses produksi. Tantangan keamanan timbul akibat konektivitas yang melibatkan sejumlah besar perangkat, sehingga

membuka peluang celah bagi serangan siber dan ancaman terhadap integritas data produksi. Manajemen pabrik menghadapi risiko potensial terhadap gangguan operasional, kemungkinan kebocoran data rahasia produksi, dan manipulasi perangkat yang dapat terjadi[12].

Solusi keamanan yang diterapkan melibatkan penggunaan protokol enkripsi yang kuat, pemantauan jaringan secara langsung, serta penerapan sistem manajemen akses yang ketat. Selain itu, pihak manajemen juga mengenalkan prosedur pengujian keamanan secara berkala dan melibatkan karyawan dalam pelatihan keamanan siber

Melibatkan diri dalam kasus studi semacam ini memungkinkan pengamatan terhadap bagaimana penerapan IoT di sektor industri menimbulkan tantangan keamanan yang khusus, dan bagaimana langkah-langkah perlindungan yang sesuai dapat menjaga integritas, kerahasiaan data, dan kelancaran operasional. Penelitian ini menyediakan wawasan berharga untuk pengembangan strategi keamanan yang lebih efektif dalam konteks industri yang kompleks[13]

3. METODE PENELITIAN

Dalam penelitian ini, peneliti mengadopsi metode literatur review atau studi pustaka sebagai dasar untuk membimbing proses penulisan karya ilmiah. Proses ini melibatkan langkah-langkah seperti pengumpulan data, membaca, dan mencatat informasi dari berbagai sumber pustaka, termasuk jurnal, buku, dan publikasi ilmiah, bersama dengan dokumen lainnya. Data-literatur yang terkumpul kemudian diproses dan digunakan sebagai landasan untuk pembahasan serta sebagai dasar untuk hasil penelitian.



Gambar 1. Alur Penelitian

Peneliti juga memilih untuk memfokuskan pada jurnal-jurnal yang terakreditasi SINTA 1 - SINTA 5 dengan rentang tahun publikasi antara 2018 hingga 2023. Pendekatan studi pustaka ini merupakan suatu bentuk penelitian yang menggali sumber-sumber pustaka yang beragam, termasuk jurnal, buku, dan publikasi ilmiah, yang kemudian melibatkan analisis terhadap 10 jurnal yang akan diulas. Pendekatan ini digunakan untuk melihat kondisi masa lalu dan saat ini yang relevan dengan topik penelitian dengan tujuan utama menghasilkan kesimpulan yang mendalam melalui sintesis informasi dari sumber-sumber tersebut

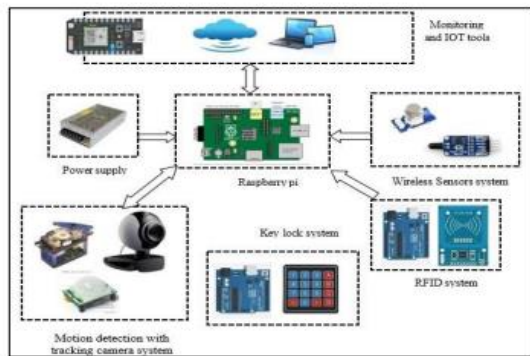
4. HASIL DAN PEMBAHASAN

Dari berbagai kajian Pustaka yang sudah di kumpulkan maka didapatkan beberapa system keamanan teknologi IoT pada bidang industri, yaitu sebagai berikut:

4.1. Sistem Keamanan Home Security

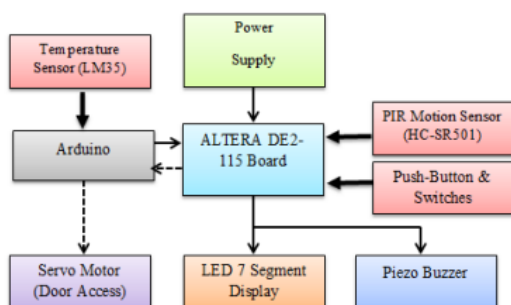
Menurut [14][15][16][17][18][19] Dalam menghadapi peningkatan kasus perampokan secara global, penerapan sistem keamanan rumah konvensional dianggap tidak optimal. Oleh karena itu, perhatian utama beralih ke pengembangan sistem keamanan rumah pintar yang berbasis Internet of Things (IoT). Teknologi terkini, seperti integrasi jaringan sirkuit terpadu, digunakan untuk menyediakan solusi keamanan yang lebih mutakhir, terutama dalam mencegah penyusupan dan insiden kebakaran. Proyek konkret dalam bidang ini melibatkan perancangan dan pembangunan sistem pintar dengan fitur keamanan digital, termasuk pintu kunci otomatis dan sensor pendeteksian gerakan dan suhu. Sistem ini didesain untuk meningkatkan keamanan rumah secara menyeluruh, menyertakan teknologi penguncian otomatis, sensor gerak PIR, dan sensor suhu.

Selain itu, proyek lainnya melibatkan sistem deteksi dini perumahan dengan memanfaatkan Smart Home berbasis IoT, termasuk kamera dan sensor pintu magnetik. Secara keseluruhan, solusi-solusi ini membuktikan keefektifannya dalam meningkatkan keamanan rumah dengan memberikan pemberitahuan langsung melalui aplikasi smartphone Android kepada pemilik rumah. Integrasi teknologi seperti identifikasi wajah dengan ESP32Cam dan penggunaan kunci pintu elektromagnetik pada Raspberry Pi juga diterapkan untuk mengurangi risiko keamanan. Dengan demikian, proyek-proyek ini mencerminkan inovasi dan kemajuan dalam meningkatkan tingkat keamanan rumah melalui pendekatan yang terintegrasi, adaptif, dan mudah digunakan, sesuai dengan perkembangan teknologi saat ini



Gambar 2. Diagram Blok Sistem Akses Keamanan Rumah Pintar [4]

Pada Gambar 2, diimplementasikan sistem keamanan akses pintu yang menggunakan tombol tekan dan sakelar sebagai input. Sistem ini mengoperasikan motor servo untuk membuka pintu dengan memasukkan kode rahasia. Selain itu, deteksi keamanan ditingkatkan dengan memanfaatkan sensor gerak dan suhu PIR. Sensor suhu berfungsi untuk memonitor suhu ruangan, sementara sensor gerak PIR mendeteksi gerakan yang tidak teratur dalam jangkauan tertentu. Jika suhu melewati batas yang ditentukan atau terdeteksi gerakan tidak teratur, sistem alarm akan diaktifkan, memberikan peringatan melalui bel sebagai demo perangkat alarm, terutama dalam konteks insiden kebakaran. Integrasi semua kompone ini menyusun sistem keamanan yang komprehensif dan responsif.

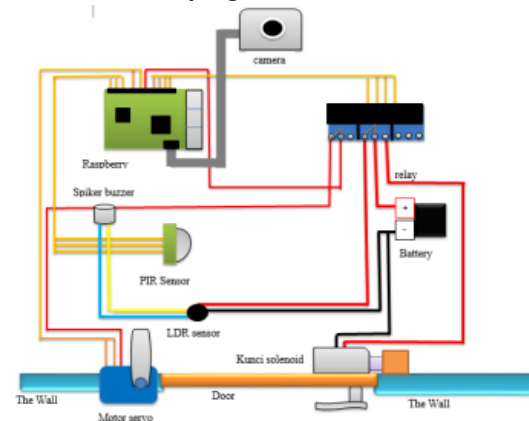


Gambar 3. Diagram blok sistem keamanan rumah [5]

Sistem keamanan rumah pada Gambar 3 memiliki fungsi serbaguna yang mencakup penggunaan sensor nirkabel, sistem pelacakan gerakan dengan kamera, dan sistem identifikasi RFID. Sensor nirkabel terdiri dari berbagai jenis seperti suhu, kelembaban, sensor gas, dan sensor flam, yang berkomunikasi secara nirkabel antara pemancar dan penerima menggunakan Arduino Uno dan transceiver NRF24L01.

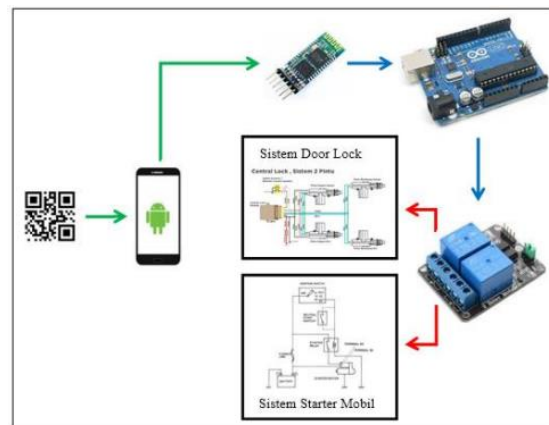
Sistem pelacakan gerakan melibatkan dua sensor PIR, servo, dan kamera, yang secara otomatis mengambil gambar dan mengunggah data ke Internet of Things (IoT) melalui Raspberry Pi saat gerakan mencurigakan terdeteksi. Sistem identifikasi RFID, dengan menggunakan buzzer, LED hijau dan merah,

dan Arduino Uno, memberikan lampu hijau untuk akses yang benar dan lampu merah dengan peringatan suara untuk akses yang tidak sah.



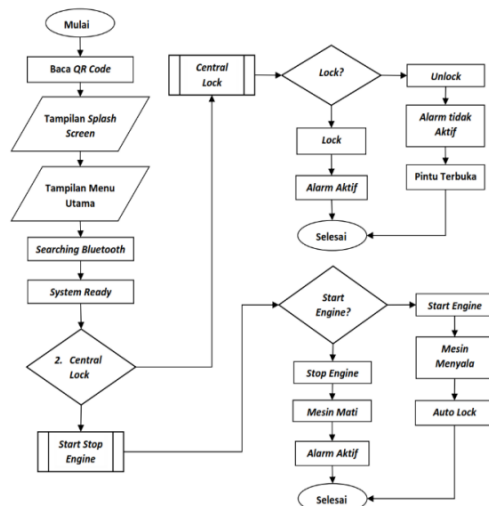
Gambar 4. Rangkaian kerja Sistem Keamanan [6]

Selain itu, sistem dapat mengirimkan SMS kepada pengguna melalui IoT sebagai tindak lanjut. Dengan melibatkan perangkat keras seperti Arduino Uno, Raspberry Pi, partikel foton, RFID, keypad, kamera IP, LCD, motor servo, dan NRF24L01, keseluruhan sistem ini dirancang untuk memberikan tingkat keamanan yang tinggi melalui integrasi teknologi yang efektif.



Gambar 5. Rangkaian Pembuatan Perangkat [10]

Sistem keamanan rumah pada gambar 4 berbasis pengontrol mikro ini digunakan untuk mengendalikan relay yang terkoneksi ke berbagai antarmuka keamanan rumah, termasuk kunci solenoid, sensor PIR, modul kamera, sensor LDR, motor servo, dan speaker buzzer. Fungsi relay di sistem ini terutama bertugas mengubah fungsi objek yang akan diaktifkan melalui kontrol dari smartphone Android. Sensor LDR membaca setiap kali pintu terbuka melalui paparan cahaya yang semula gelap, mengaktifkan sakelar relay yang terhubung ke speaker buzzer untuk menghasilkan suara alarm.



Gambar 6. Flowchart Pembuatan Aplikasi [10]

Ketika pintu dibuka, relay beralih ke mode aktif, menyebabkan sensor LDR mati dan kunci solenoid menyala, memungkinkan pintu terbuka tanpa suara alarm karena relay tidak lagi terhubung dengan sensor LDR. Selanjutnya, sensor PIR di area pintu menjadi aktif saat pintu dibuka, mengirim perintah ke kamera melalui Raspberry Pi untuk mengambil gambar dengan cepat, memastikan bahwa foto orang yang masuk selalu dapat terlihat dan diidentifikasi.

4.2. Sistem Keamanan Mobil

Menurut [20] Dalam konteks pertumbuhan jumlah pengguna kendaraan bermotor di Indonesia, penelitian ini menekankan peningkatan kasus tindak kriminal terhadap pemilik kendaraan. Untuk mengatasi tantangan ini, penelitian ini berhasil mengembangkan prototipe sistem keamanan mobil yang menggunakan quick response code sebagai kontrol akses otentikasi, dengan basis Android dan integrasi Arduino. Penelitian ini dilaksanakan melalui dua fase, yakni pembuatan aplikasi Android dan pengembangan perangkat sistem keamanan mobil.

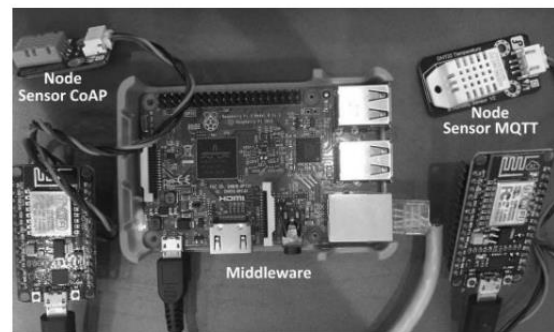
Metode pengujian aplikasi Android menggunakan black box testing berhasil memverifikasi fungsionalitas aplikasi, sementara pengujian perangkat menunjukkan bahwa sistem dapat beroperasi secara normal dan memiliki daya tahan yang baik. Dengan demikian, penelitian ini memberikan sumbangan penting dalam menciptakan solusi keamanan khusus untuk kendaraan bermotor, sesuai dengan pertumbuhan penggunaan kendaraan dan tantangan keamanan yang terkait.

Pada tahap pembuatan aplikasi, proses dimulai dengan tampilan baca QR Code, dan setelah QR Code terbaca sesuai dengan kata sandi, muncul splash screen. Langkah berikutnya melibatkan pembuatan tampilan menu utama, yang terdiri dari dua menu utama: sistem kendali central lock dan sistem kendali engine mobil. Sebelum memasuki salah satu menu, aplikasi melakukan pencarian bluetooth, dan jika berhasil, koneksi antara aplikasi dan perangkat terjadi.

Menu sistem kendali central lock memiliki fungsi untuk mengunci dan membuka kunci pintu mobil, dengan pilihan mengaktifkan alarm saat mengunci. Sementara itu, menu sistem kendali engine mobil digunakan untuk menghidupkan dan mematikan mesin mobil, dengan opsi mengaktifkan auto lock pintu saat mesin dihidupkan.

Pembuatan aplikasi dan perangkat dilakukan dengan mengikuti flowchart tertentu dan menggunakan Arduino Uno R3, modul bluetooth, dan relay. Arduino Uno R3, sebagai papan mikrokontroler, memiliki berbagai pin dan fitur yang mendukung proses ini. Modul bluetooth HC-06 berfungsi sebagai perantara komunikasi antara aplikasi Android dan Arduino melalui koneksi nirkabel pada frekuensi 2.4 GHz. Relay digunakan sebagai penghubung antara sistem central lock dan start-stop engine, dengan catu daya 5 V. Penelitian ini memberikan penekanan pada penggunaan teknologi Arduino dalam berbagai aplikasi, seperti smart home dan wireless sensor networking, serta memanfaatkan komunikasi bluetooth untuk interaksi nirkabel yang efektif.

4.3. Sistem Keamanan Middleware

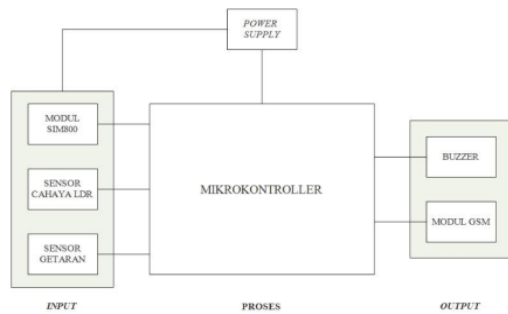


Gambar 7. Prototipe IoT Middleware [11]

Menurut Menurut [21] Penelitian sebelumnya berhasil mengembangkan middleware yang mengadopsi pendekatan event-driven untuk mendukung interoperabilitas perangkat sensor dalam lingkungan Internet of Things (IoT). Walaupun demikian, skema komunikasi pada middleware tersebut masih memiliki kekurangan dalam aspek keamanan dan rentan terhadap ancaman seperti eavesdropping. Penelitian ini menyajikan solusi untuk mengatasi permasalahan tersebut dengan menerapkan mekanisme keamanan end-to-end. Dalam konteks ini, diterapkan algoritme kriptografi AES-CBC 128 pada saluran komunikasi antara node sensor dan middleware, sementara mekanisme TLS digunakan pada komunikasi antara middleware dan aplikasi berbasis IoT.

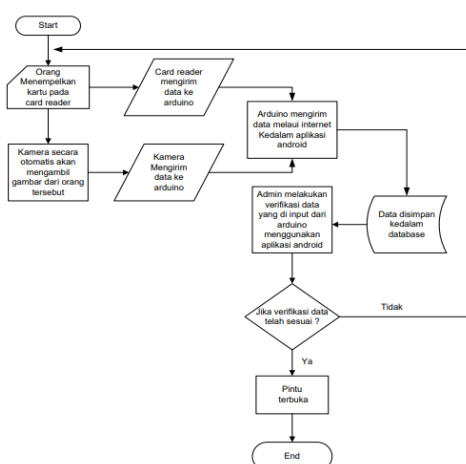
Hasilnya menunjukkan bahwa keamanan end-to-end berbasis kriptografi pada pola pub/sub efektif dalam menjamin kerahasiaan data melalui enkripsi payload, meskipun topik masih terlihat. Di sisi lain, TLS/SSL mampu menjamin kerahasiaan seluruh data yang dikirim. Implementasi mekanisme ini tidak berdampak secara signifikan pada keterlambatan

pengiriman data, dengan waktu delay tetap di bawah 1 detik.



Gambar 8. Diagram Blok sistem [12]

Dari ilustrasi pada Gambar 8, terlihat dua perangkat sensor yang berfungsi sebagai pengirim data menggunakan protokol MQTT dan CoAP. Kedua perangkat sensor ini dibuat menggunakan nodeMCU esp8266 dan dilengkapi dengan sensor DHT22. Data yang dikirim memiliki topik yang spesifik, sebagai contoh, "home/kitchen". Proses pengiriman data dilakukan melalui suatu broker, yang pada penelitian ini diimplementasikan menggunakan Redis. Data yang dikirim oleh perangkat sensor disimpan sementara di dalam broker dan selanjutnya diminta oleh penerima data (subscriber) melalui protokol WebSocket. Setelah itu, data diteruskan ke aplikasi lain untuk mendapatkan analisis lebih lanjut. Pertukaran data antara perangkat sensor dan middleware dilakukan melalui jaringan nirkabel atau wireless LAN yang disediakan oleh middleware. Di sisi lain, komunikasi antara middleware dan penerima data menggunakan jaringan LAN, terutama dalam lingkup jaringan kampus sesuai dengan konteks penelitian ini. Informasi yang dikirim oleh perangkat sensor mencakup data mengenai perangkat sensor itu sendiri, seperti jenis protokol yang digunakan, timestamp, topik, dan payload sensor.



Gambar 9. Flowchart Cara Kerja Sistem Pada Client [12]

4.4. Sistem Keamanan Ruang

Menurut [22] Dalam menghadapi meningkatnya tingkat kejahatan pencurian data, penting untuk memiliki sistem keamanan ruangan yang efektif guna melindungi data instansi atau organisasi. Sistem keamanan yang optimal adalah yang dapat dimonitor dan dikendalikan dari jarak jauh melalui internet, yang lebih dikenal sebagai Internet of Things (IoT). Tujuan penelitian ini adalah merancang sistem keamanan ruangan berbasis IoT dengan menggunakan aplikasi Android. Sistem ini melibatkan beberapa modul, seperti modul RFID (Radio Frequency Identification), modul kamera, dan solenoid door lock.

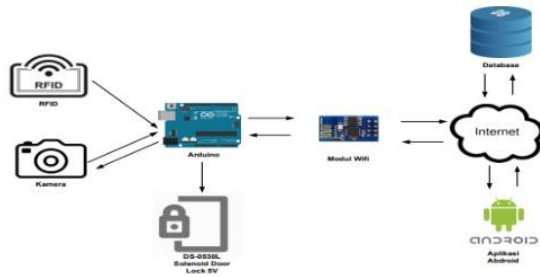
Dalam operasinya, kartu RFID pada modul RFID berperan sebagai alat identifikasi untuk mengenali orang yang ingin memasuki ruangan. Modul RFID juga berfungsi sebagai pemicu kamera, yang mengambil gambar orang yang akan memasuki ruangan. Data yang dihasilkan oleh kedua modul tersebut akan dikirimkan ke aplikasi Android. Admin ruangan dapat melakukan verifikasi untuk memberikan atau menolak akses kepada orang yang hendak memasuki ruangan.

Hasil pengujian sistem menunjukkan kinerja yang optimal saat kecepatan internet dari akses point berjalan dengan cepat dan stabil. Namun, sistem kurang optimal ketika kecepatan internet dari akses point berjalan dengan lambat. Dengan demikian, sistem ini menyajikan solusi keamanan ruangan yang dapat diakses secara remote melalui IoT, dengan catatan bahwa kinerjanya bergantung pada kecepatan dan stabilitas koneksi internet.

Ketika seseorang menggunakan kartu pada card reader RFID, card reader secara otomatis memberikan instruksi kepada Arduino untuk mengambil gambar individu yang akan memasuki ruangan melalui kamera di bagian atas pintu. Setelah gambar berhasil diambil, Arduino melakukan pemrosesan data yang berasal dari kartu dan gambar tersebut, dan kemudian mengirimkan data tersebut ke aplikasi Android. Secara simultan, Arduino juga mengirimkan notifikasi ke aplikasi Android untuk memulai proses verifikasi data yang dilakukan oleh admin ruangan. Notifikasi di aplikasi Android mencakup informasi seperti nama, nomor identitas, nomor kartu, dan gambar orang yang berencana memasuki ruangan.

Admin ruangan memiliki kewenangan untuk memberikan izin atau menolak akses kepada orang tersebut melalui aplikasi Android. Setelah izin diberikan, admin dapat memasukkan data tersebut ke dalam database. Pentingnya, pada saat akses masuk, admin memasang keypad di depan pintu ruangan. Keypad berfungsi sebagai kata sandi saat koneksi internet mati, untuk mencegah kegagalan dalam proses verifikasi data. Kata sandi ini hanya diketahui oleh admin ruangan dan digunakan sebagai alternatif untuk memasuki ruangan ketika koneksi internet mati.

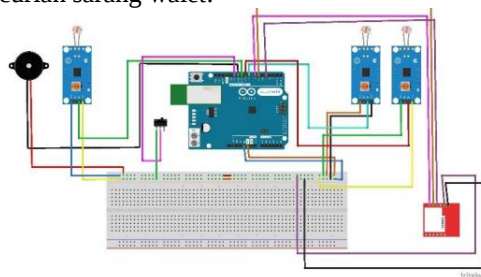
4.5. Sistem Keamanan Rumah Wallet



Gambar 10. Sistem Keamanan

Menurut [23] pencurian sarang walet merupakan permasalahan serius bagi pengusaha rumah walet. Karena rumah walet umumnya terletak di lokasi terpencil, pengendalian keamanan menjadi kurang efektif, dan kerugian finansial yang ditimbulkan dapat mencapai puluhan juta rupiah. Oleh karena itu, diperlukan pengembangan sistem keamanan berbasis sensor cahaya dan sensor getaran yang terhubung dengan SMS Notifikasi. Sistem ini melibatkan perangkat seperti Arduino Uno, Light Dependent Resistor (LDR) atau sensor cahaya, sensor getaran, buzzer, modul SIM800L, dan notifikasi melalui SMS.

Dengan penerapan sistem keamanan ini, diharapkan para pengusaha rumah walet dapat menerima pemberitahuan melalui SMS jika terdeteksi aktivitas mencurigakan di rumah walet. Hal ini diharapkan dapat membantu dalam mencegah dan mengurangi potensi kerugian yang lebih besar akibat pencurian sarang walet.



Gambar 11. Skema Perangkat Sistem Keamanan Rumah Walet [13]

Setelah dilakukan pengujian baik black box maupun pengujian pengguna, hasil analisis dan pembahasan mengenai Sistem Keamanan Rumah Walet yang Menggunakan Sensor Cahaya dan Sensor Getaran yang Diintegrasikan dengan SMS Notifikasi menghasilkan kesimpulan sebagai berikut:

- Implementasi Sistem Keamanan Rumah Walet dengan Sensor Cahaya dan Sensor Getaran yang Diintegrasikan dengan SMS Notifikasi dapat menjadi opsi tambahan sebagai langkah keamanan yang efektif.
- Pemanfaatan teknologi mikrokontroler sebagai pengendali sistem terbukti sangat sederhana dan mudah digunakan, memberikan kemudahan dalam proses implementasi dan pengoperasian.
- Sistem Keamanan Rumah Walet yang menggunakan Sensor Cahaya dan Sensor Getaran

yang Diintegrasikan dengan SMS Notifikasi ini dapat memberikan informasi dini kepada pengguna (user/owner) tentang kejadian di rumah walet, sehingga dapat membantu dalam upaya pencegahan pencurian sarang walet.

5. KESIMPULAN DAN SARAN

Dari 10 literatur yang direview tersebut memberikan kontribusi dalam mengembangkan sistem keamanan yang cerdas untuk rumah, Internet of Things (IoT), dan kendaraan. Fokus utamanya mencakup pengaturan cerdas, deteksi parameter seperti gas dan gerakan, pengenalan wajah, penggunaan Raspberry Pi, pemantauan jarak jauh dengan sensor magnetic switch, pengamanan pintu dengan QR code, penerapan keamanan menyeluruh pada middleware IoT, teknologi RFID, dan solusi keamanan rumah walet menggunakan sensor cahaya dan getaran dengan notifikasi SMS.

Saran untuk Penelitian Lebih Lanjut: Eksplorasi lebih lanjut integrasi teknologi terbaru seperti kecerdasan buatan atau blockchain untuk meningkatkan keamanan dan efektivitas sistem keamanan rumah. Penelitian lebih lanjut untuk mencari cara agar teknologi keamanan rumah dapat lebih terjangkau, memungkinkan adopsi oleh sebanyak mungkin orang. Penelitian terkait dengan pengembangan sistem keamanan rumah yang lebih ramah lingkungan, seperti pemanfaatan sumber energi terbarukan atau penggunaan material daur ulang.

DAFTAR PUSTAKA

- [1] Y. Bin Zikria, R. Ali, M. K. Afzal, and S. W. Kim, "Next-Generation Internet of Things (IoT): Opportunities, Challenges, and Solutions," pp. 1–7, 2021.
- [2] M. Gupta, M. Abdelsalam, and S. Mittal, "Security and Privacy in Smart Farming: Challenges and Opportunities," *IEEE Access*, vol. 8, pp. 34564–34584, 2020, doi: 10.1109/ACCESS.2020.2975142.
- [3] T. Sutikno and D. Thalmann, "Insights on the internet of things: past, present, and future directions," vol. 20, no. 6, pp. 1399–1420, 2022, doi: 10.12928/TELKOMNIKA.v20i6.22028.
- [4] A. Boy *et al.*, "Implementasi nodemcu esp8266 dalam rancang bangun sistem keamanan sepeda motor berbasis iot," vol. 4, no. 2, pp. 163–170, 2021.
- [5] S. Megawati and A. Lawi, "Pengembangan Sistem Teknologi Internet of Things Yang Perlu Dikembangkan Negara Indonesia," vol. 05, pp. 19–26, 2021.
- [6] H. Marcos and M. Reza, "Implementasi IoT Pada Rancang Bangun Aplikasi Mobile Sistem Keamanan Dan Pelacak Sepeda Motor 1,2," vol. 8, no. 1, pp. 170–180, 2021.
- [7] Solehudin, "TANTANGAN KEAMANAN DAN PRIVASI DALAM SISTEM IOT: TINJAUAN KOMPREHENSIF," vol. 2, no. 4,

- 2022.
- [8] D. R. Sari, "Analisis Keamanan Sistem Informasi dalam Era Internet of Things (IoT)," vol. 1, no. 2, pp. 1–10, 2024.
 - [9] V. No *et al.*, "Sosialisasi Kesadaran Keamanan Digital di Era Revolusi Industri 4 . 0," vol. 5, no. 1, 2024.
 - [10] A. Irawan, W. Hamzah, N. Fadholi, Z. Erikamaretha, and F. Sinlae, "Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT," vol. 06, no. 01, pp. 114–119, 2024.
 - [11] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: Requirements, challenges, and solutions," *Internet of Things (Netherlands)*, vol. 14, p. 100129, 2021, doi: 10.1016/j.iot.2019.100129.
 - [12] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W. C. Hong, "Internet of things: Evolution, concerns and security challenges," *Sensors*, vol. 21, no. 5, pp. 1–35, 2021, doi: 10.3390/s21051809.
 - [13] N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," *IEEE Access*, vol. 9, pp. 59353–59377, 2021, doi: 10.1109/ACCESS.2021.3073408.
 - [14] S. Bin Saleh *et al.*, "Smart home security access system using field programmable gate arrays," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 11, no. 1, pp. 152–160, 2018, doi: 10.11591/ijeecs.v11.i1.pp152-160.
 - [15] H. H. Qasim, A. E. Hamza, L. Audah, H. H. Ibrahim, H. A. Saeed, and M. I. Hamzah, "Design and implementation home security system and monitoring by using wireless sensor networks WSN/internet of things IoT," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 3, pp. 2617–2624, 2020, doi: 10.11591/ijece.v10i3.pp2617-2624.
 - [16] A. Setiawan and A. I. Purnamasari, "Pengembangan Smart Home Dengan Microcontrollers ESP32 Dan MC-38 Door Magnetic Switch Sensor Berbasis Internet of Things (IoT) Untuk Meningkatkan Deteksi Dini Keamanan Perumahan," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 3, no. 3, pp. 451–457, 2019, doi: 10.29207/resti.v3i3.1238.
 - [17] B. Yanto, B. Basorudin, S. Anwar, A. Lubis, and K. Karmi, "Smart Home Monitoring Pintu Rumah Dengan Identifikasi Wajah Menerapkan Camera ESP32 Berbasis IoT," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 11, no. 1, pp. 53–59, 2022, doi: 10.32736/sisfokom.v11i1.1180.
 - [18] W. Kurniasih, A. Rakhman, and I. Salamah, "Sistem Keamanan Jendela Rumah Berbasis IoT," *J. Ris. Sist. Inf. Dan Tek. Inform.*, vol. 5, no. 2, pp. 2527–5771, 2021.
 - [19] E. Riyanto, "SISTEM KEAMANAN RUMAH BERBASIS ANDROID DENGAN RASBERRY Pi," *J. Inform. Upgris*, vol. 5, no. 1, pp. 55–59, 2019, doi: 10.26877/jiu.v5i1.3214.
 - [20] K. Indartono and A. Jahir, "Prototype Sistem Keamanan Mobil Dengan Menggunakan Quick Prototype of Car Scurity System Using Quick Response Code Based," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 3, pp. 235–244, 2019, doi: 10.25126/jtiik.20186964.
 - [21] E. S. Pramukantoro, F. A. Bakhtiar, A. L. B. Aji, and D. H. P. Dewa, "Implementasi Mekanisme End-To-End Security pada IoT Middleware," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 3, p. 335, 2019, doi: 10.25126/jtiik.2019631401.
 - [22] K. H. R. , H. Subrata, and F. Gozali, "Sistem Keamanan Ruangan Berbasis Internet Of Things Dengan Menggunakan Aplikasi Android," *TESLA J. Tek. Elektro*, vol. 20, no. 2, p. 127, 2019, doi: 10.24912/tesla.v20i2.2989.
 - [23] B. Sokhi and E. A. Kadir, "Sistem Keamanan Rumah Walet Menggunakan Sensor Cahaya dan Sensor Getaran Diintegrasi Dengan SMS Notifikasi," *IT J. Res. Dev.*, vol. 3, no. 1, pp. 1–10, 2019, doi: 10.25299/itjrd.2019.vol3(1).xxxx.