

Sistem *Monitoring* Security Building Berbasis E-KTP dan NodeMCU ESP8266

Muh. Kharis Faahmi¹, Ibrahim Nawawi¹, dan Risky Via Yuliantari^{1*}

¹Universitas Tidar, Magelang, Indonesia

*Email: rviay@untidar.ac.id

Abstrak—Artikel ini telah membahas sistem *monitoring* keamanan pada bangunan berbasis Internet of Things (IoT) yang dirancang untuk memantau pintu utama dengan menggunakan protokol MQTT (*Message Queuing Telemetry Transport*), sebuah teknologi yang memungkinkan pengiriman data jarak jauh dengan konsumsi daya yang sangat rendah. Keunggulan utama dari sistem ini adalah efisiensinya dalam hal penggunaan energi, menjadikannya ideal untuk aplikasi keamanan yang memerlukan pemantauan jangka panjang tanpa menguras sumber daya. Sistem ini bekerja dengan cara mengumpulkan data dari sensor yang dipasang pada pintu utama dan mengirimkannya ke *web server*, di mana data tersebut disimpan dan dapat dipantau secara *real-time* oleh pengguna. Hal ini memungkinkan pengelola bangunan untuk dengan cepat mendeteksi dan merespons potensi ancaman keamanan, seperti upaya akses tidak sah atau gangguan pada pintu utama. Selain memberikan pemantauan yang akurat, sistem ini juga memberikan perlindungan andal, meningkatkan keamanan keseluruhan bangunan. Kemampuan untuk merespons secara cepat terhadap ancaman menjadikan sistem ini sebagai solusi keamanan yang efektif dan dapat diandalkan dalam menjaga keselamatan properti.

Kata kunci: *Database*, MQTT, RFID, *Security Monitoring*

Abstract—This article discusses a building security *monitoring* system based on the Internet of Things (IoT), designed to monitor the main door using the MQTT (*Message Queuing Telemetry Transport*) protocol, a technology that enables long-distance data transmission with very low power consumption. The main advantage of this system is its energy efficiency, making it ideal for security applications that require long-term *monitoring* without draining resources. The system works by collecting data from sensors installed on the main door and sending it to a *web server*, where the data is stored and can be monitored in real-time by users. This allows building managers to quickly detect and respond to potential security threats, such as unauthorized access or disturbances at the main door. In addition to providing accurate *monitoring*, the system also offers reliable protection, enhancing the overall security of the building. The ability to respond quickly to threats makes this system an effective and dependable security solution for safeguarding property.

Keywords: *Database*, MQTT, RFID, *Security Monitoring*

I. PENDAHULUAN

SISTEM pemantauan keamanan bangunan diciptakan sebagai respons terhadap kebutuhan untuk memastikan keamanan gedung-gedung yang dinilai penting. Sistem ini mengintegrasikan berbagai teknologi seperti sensor, akses terkendali, dan perangkat lunak analitik untuk memantau dan mengidentifikasi potensi ancaman atau aktivitas yang mencurigakan. Tujuan utamanya adalah melindungi orang, properti, dan informasi yang ada di dalam gedung, serta memberikan respons cepat terhadap situasi darurat dan peristiwa keamanan yang mungkin terjadi. Dalam hal ini sistem *monitoring* pada pintu sangat berperan untuk meningkatkan keamanan dalam pengelolaan sebuah gedung, terutama gedung yang memiliki nilai tinggi seperti museum, hotel, bank dan rumah – rumah mewah. *Monitoring* bertujuan untuk mempermudah pelaksanaan suatu kegiatan yang berlandaskan pada perencanaan, *monitoring* juga memungkinkan untuk menilai apakah sumber daya yang tersedia berada dalam kondisi yang aman. [1].

Terdapat peningkatan ancaman pada keamanan yang meliputi serangan teroris, pencurian, vandalisme, dan bencana alam, yang mendorong kebutuhan akan suatu sistem yang dapat memantau dan melindungi bangunan secara langsung. Seperti yang diberitakan oleh BBC tentang pencurian di museum Kendari, Sulawesi Tenggara pada tanggal 9 Februari 2021 [2]. Menurut pengakuan pengelola museum tersebut, pencurian barang – barang bersejarah ini terjadi karena kurangnya petugas keamanan dan belum adanya fasilitas keamanan yang andal. Kurangnya fasilitas keamanan ini tentunya tidak terjadi di satu tempat saja. Menurut data BPS pada tahun 2020 saja, kasus pencurian barang tanpa kekerasan mencapai 73.264 kejadian dan pencurian barang dengan kekerasan mencapai 6.538 [3]. Hal ini membuktikan bahwa kasus pencurian di Indonesia masih sangat sering terjadi, sehingga perlu peningkatan pada sistem keamanan.

Semakin kompleks suatu bangunan, pengawasan secara manual oleh manusia saja tidak akan memberikan keamanan yang maksimal dikarenakan terdapat banyak batasan pada manusia. Manusia memiliki keterbatasan fisik dan konsentrasi yang membuat sulit untuk memantau area yang luas secara efisien dan terus-menerus. Manusia dapat lelah, kurang fokus, atau terganggu oleh faktor lingkungan, sehingga meningkatkan risiko kesalahan atau kegagalan dalam mendeteksi ancaman keamanan. Sehingga diperlukan sistem *monitoring* keamanan untuk memungkinkan pengawasan tujuh kali 24 jam dengan teknologi otomatis, mengurangi kesalahan manusia, dan memberikan respons yang cepat terhadap situasi darurat.

E-KTP dapat digunakan untuk mendukung sistem keamanan yang dirancang. Penggunaan e-KTP dalam sistem keamanan bangunan berbasis RFID memberikan keunggulan berupa tingkat keamanan dan otentikasi yang tinggi, integrasi data yang mudah dengan *database* kependudukan, kemudahan pengelolaan hak akses, multi-fungsi sebagai kartu akses dan identifikasi personal, serta meningkatkan ketertiban dan pemantauan di dalam bangunan [4]. Keamanan tinggi e-KTP, yang dilengkapi menggunakan teknologi *chip* RFID, mengurangi risiko pemalsuan atau penyalahgunaan. Selain itu, kenyamanan, kecepatan, dan keterkaitan dengan sistem pemerintah menjadi alasan kuat untuk mengadopsi teknologi ini, walaupun perlindungan privasi dan implementasi keamanan yang baik tetap menjadi prioritas utama. Penggunaan kunci solenoid berbasis teknologi RFID sangat memungkinkan untuk menggantikan kunci konvensional yang ada, sehingga menjadi sangat sulit untuk diduplikasi. [5]

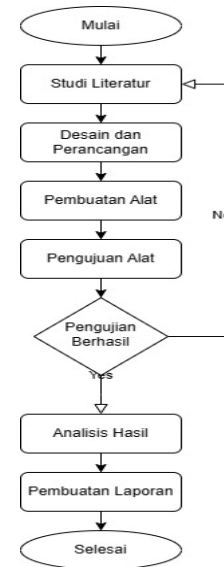
Mohamad Erzio Ardimas melakukan penelitian tentang Perancangan sistem pengendalian dan pemantauan simulasi palang pintu otomatis menggunakan teknologi *Radio Frequency Identification* (RFID) dan sensor ultrasonik berbasis *Programmable logic controller* (PLC) serta perangkat lunak Vijeo Designer [6]. Pada penelitian ini dilakukan perancangan alat untuk melakukan *monitoring* dan mengontrol palang pintu pada perumahan, sehingga tidak menyulitkan penghuni yang ingin masuk dengan cepat. Proses kontrol dan *monitoring* menggunakan alat *programmable logic controller* sedangkan perangkat lunak aplikasi ini dirancang menggunakan *software* Vijeo Designer. Kekurangan dari sistem ini adalah kegagalan sistem RFID dalam membaca atau mendeteksi *tag* RFID dengan akurasi yang tinggi. Penting juga untuk diperhatikan bahwa untuk mengurangi kemungkinan terjadinya tindak kriminal, seperti pencurian di dalam ruangan atau rumah, diperlukan sistem kunci pintu yang sulit dirusak serta dilengkapi dengan sistem notifikasi yang dapat segera memberi tahu pengguna jika ada upaya untuk mengakses pintu [7]. Mengenai keamanan pada E-KTP, mengetahui nomor RFID pada E-KTP tidak secara langsung memungkinkan akses ke data di dalamnya. *Chip* RFID pada E-KTP menyimpan data yang di enkripsi. Hanya perangkat dengan sistem kunci resmi

yang dapat mendekripsi kode RFIDnya.

II. METODE

A. Diagram Alir Penelitian

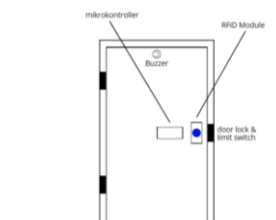
Tahapan Penelitian dimulai dengan studi literatur, desain dan perancangan alat, pembuatan alat, implementasi alat, pengujian alat, analisis data, dan kesimpulan. Diagram alir penelitian ditunjukkan pada Gambar 1.



Gambar. 1. Diagram alir penelitian

B. Perancangan Desain

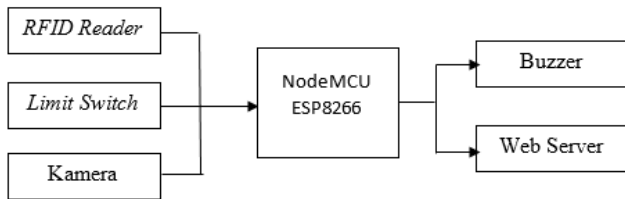
Tahap perancangan desain dan sistem pada *monitoring* pintu merujuk pada proses rinci dan strategis di mana solusi teknologi dikonseptualisasikan dan dirancang. Tahap ini melibatkan analisis mendalam terhadap kebutuhan sistem, merancang antarmuka pengguna yang informatif, memilih dan mengintegrasikan komponen seperti sensor, serta mengembangkan perangkat lunak untuk menyajikan informasi yang relevan. Selama tahap ini, arsitektur teknis dibentuk agar sistem dapat memberikan pengawasan pintu yang akurat, responsif, dan handal sesuai dengan tujuan pemantauan yang ditetapkan. Gambaran umum alat yang akan dibuat dapat dilihat pada Gambar 2.



Gambar. 2. Rancangan desain

C. Diagram Blok Sistem

Monitoring Pintu pada gedung ini dirancang dengan beberapa sistem yang terdiri dari tiga bagian utama yaitu masukan, proses, dan keluaran [8]. Berikut ini adalah diagram blok alat yang ditunjukkan pada Gambar 3. Diagram blok ini menunjukkan masukan yang dipicu oleh RFID reader dan limit switch, secara sederhana RFID akan mengidentifikasi siapa yang mengakses pintu, jika akses diterima maka limit switch akan mati dan tidak memicu buzzer untuk menyala serta pintu akan terbuka. Jika pintu dibuka paksa limit switch akan terpicu, buzzer akan menyala dan kamera akan secara otomatis menangkap gambar. Setiap kondisi tersebut terpenuhi maka laporan akan dikirim ke web server.



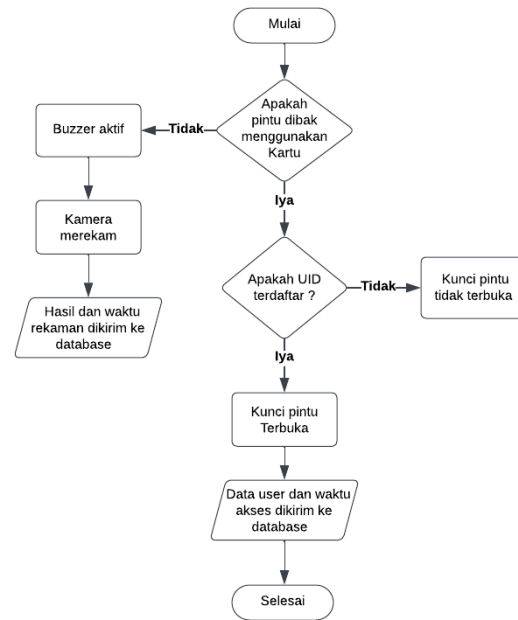
Gambar. 3. Diagram blok sistem

D. Flowchart Kerja Alat

Sinyal yang diterima dari RFID akan diteruskan ke mikrokontroler untuk kemudian diolah menggunakan logika matematis untuk menentukan tindakan yang akan dilakukan sistem, semua data yang telah diolah akan ditampilkan ke user interface berupa website yang memiliki sistem login khusus untuk user yang menggunakan perangkat keamanan ini. Untuk lebih jelasnya proses kerja alat dapat dilihat pada Gambar 4.

Terdapat hubungan antara mikrokontroler ESP8266 dan program pada komputer yang berfungsi mengatur kamera. Program dengan ekstensi ino akan menangkap sinyal dari RFID dan switch [9]. ketika pintu dibuka tanpa menggunakan kartu atau dibuka paksa, switch akan terpicu, kemudian program ino akan mengirimkan sinyal integer bernilai 1, yang akan ditransmisikan menggunakan protokol MQTT, kemudian data tersebut akan diteruskan dan ditangkap oleh program python pada komputer. Ketika python mendeteksi nilai 1 dari MQTT maka python memerintahkan komputer untuk membuka kamera dan merekam saat itu juga. Program python juga menyimpan data rekaman ke server XAMPP yang kemudian akan ditampilkan pada website.

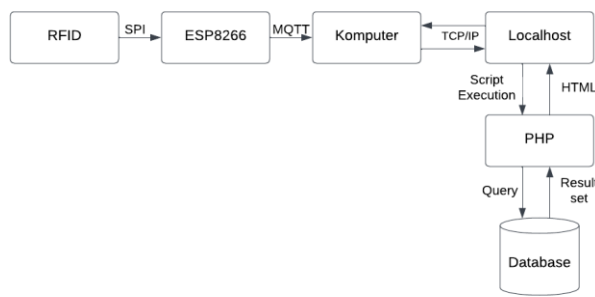
Ketika RFID berhasil membace kartu, program ino akan mengirimkan sinyal integer bernilai 2, yang akan ditransmisikan menggunakan protokol MQTT, kemudian data tersebut akan diteruskan dan ditangkap oleh program python pada komputer. Ketika python mendeteksi nilai 2 dari MQTT, python akan mengirim data dari kartu yang telah di deteksi ke server, yang kemudian akan ditampilkan pada web.



Gambar. 4. Flowchart kerja alat

E. Diagram Blok Komunikasi

Komunikasi yang digunakan antara RFID dan ESP adalah komunikasi SPI [10]. SPI (Serial Peripheral Interface) adalah protokol komunikasi serial yang digunakan untuk mentransfer data antara perangkat mikrokontroler dan perangkat keras eksternal seperti RFID [11]. Komunikasi SPI melibatkan beberapa saluran komunikasi, termasuk MOSI (Master Out Slave In), MISO (Master In Slave Out), dan SCLK (Serial Clock). Komunikasi yang digunakan ESP8266 dan komputer untuk mengaktifkan kamera adalah MQTT. MQTT (Message Queuing Telemetry Transport) adalah protokol komunikasi ringan yang menggunakan model publish/subscribe, dirancang khusus untuk aplikasi Internet of Things (IoT) dan lingkungan dengan bandwidth terbatas [12]. Protokol ini memungkinkan perangkat atau aplikasi untuk mengirim (publish) dan menerima (subscribe) pesan ke dan dari topik tertentu dengan overhead data minimal, efisien dalam penggunaan sumber daya, serta mendukung tingkat kehandalan yang dapat disesuaikan atau Quality of Service dan fitur-fitur seperti Last Will and Testament serta Retained Messages. Untuk lebih jelasnya dapat dilihat pada Gambar 5.



Gambar. 5. Diagram blok komunikasi

III. HASIL DAN PEMBAHASAN

A. Hasil Perakitan Komponen

Alat yang telah berhasil dirancang akan diuji dalam serangkaian pengujian yang sistematis, pengujian – pengujian tersebut terdiri dari pengujian alat secara fisik berupa koneksi tiap alat pada mikrokontroler serta keberhasilan tiap alat dalam melakukan pekerjaannya. Selanjutnya pengujian pada program arduino yang telah diupload pada mikrokontroler, pengujian hubungan antara mikrokontroler dan MQTT, pengujian hubungan MQTT dan program python, pengujian fungsi pada program python untuk mengetahui apakah tiap fungsi berjalan dengan baik, pengujian server dan database dan terakhir pengujian sistem yang bekerja pada website. Alat yang akan diuji dapat dilihat pada Gambar 6.



Gambar. 6. Hasil Perakitan Komponen

B. Perancangan Sistem Arduino

Pada tahap ini, perancangan sistem arduino akan diawali dengan pembuatan program terlebih dahulu. Program akan dibuat dan dites menggunakan aplikasi arduino IDE, dengan menambahkan beberapa library pendukung untuk komponen yang digunakan. Library yang dipakai antara lain, MFRC522, SPI, WiFi, dan PubSubClient. Cara kerja dari sistem arduino ini adalah ketika RFID card digunakan, dan berhasil dibaca oleh sistem, maka akan memicu doorlock untuk terbuka selama beberapa detik, sehingga pintu dibuka dengan normal. Riwayat pembacaan RFID card juga akan disimpan pada database dan

ditampilkan pada website. Sedangkan ketika pintu dibuka tanpa RFID atau dibuka paksa maka switch akan aktif dan memicu buzzer, kemudian sinyal akan dikirim melalui MQTT untuk mengaktifkan kamera menggunakan program python dan merekam kejadian. Semua data kejadian tadi akan dikirim ke server untuk ditampilkan di website. Semua algoritma dan program tersebut telah diverifikasi terlebih dahulu menggunakan perangkat lunak Arduino IDE, dan proses pengunggahan (upload) dapat dilakukan dengan lancar.

Program arduino dapat dikatakan berhasil berfungsi setelah memastikan tidak ada error yang terjadi dan alat dapat bekerja seperti yang diharapkan. Komponen – komponen yang digunakan antara lain, ESP8266, limit switch, trafo stepdown, seolenoid doorlock, relay, RFID reader, buzzer dan kamera. Selanjutnya adalah uji konektifitas antara mikrokontroler dan broker MQTT. Kedua sistem dapat dikatakan terhubung apabila MQTT berhasil menangkap sinyal keluaran yang tampil di serial monitor, ada juga indikator terhubungnya wifi pada serial monitor, sehingga dapat diketahui status koneksi ke wifi ataupun MQTT. Gambar 7. adalah proses konektifitas yang ditampilkan pada serial monitor.

```

20:43:10.656 -> Connecting to WiFi...
20:43:11.149 -> Connecting to WiFi...
20:43:11.671 -> Connecting to WiFi...
20:43:11.671 -> Connected to WiFi
20:43:12.687 -> Connected to MQTT broker
20:43:12.732 -> 1
20:43:23.397 -> Card Registered!
20:43:28.377 -> Sending MQTT message: 2
  
```

Gambar. 7. Status koneksi mikrokontroler

C. Perancangan Program Python

Program python pada sistem ini tidak hanya berperan untuk menangkap sinyal dari broker MQTT, tetapi juga untuk aktivasi kamera serta menyimpan data yang sudah didapat ke server serta database. Untuk menghubungkan ke broker MQTT, python menggunakan library paho.mqtt.client. Dengan ini pengguna dapat menggunakan kelas dan fungsi yang disediakan oleh Paho MQTT untuk membuat dan mengelola klien MQTT dalam aplikasi Python. Sedangkan untuk aktivasi kamera serta menyimpan rekaman ke server lokal, python menggunakan library cv2 dan os. Modul cv2 (OpenCV) adalah library komputer vision yang digunakan untuk berbagai tugas pengolahan gambar dan video. Fungsi-fungsi dalam modul ini mencakup pembacaan dan penulisan gambar, pemrosesan gambar, deteksi objek, dan banyak lagi. Dalam program ini cv2 berfungsi untuk mengendalikan kamera dan memproses rekaman. Sedangkan modul os menyediakan berbagai fungsi untuk melakukan interaksi dengan sistem operasi, seperti manipulasi direktori, membaca atau menulis ke file, dan lainnya, dalam program ini modul os digunakan untuk menyimpan video hasil rekaman ke direktori server lokal.

Gambar 8. menunjukk proses yang dijalankan program python.

```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
PS C:\Users\USER\Documents\Skripsi\python> & C:/Users/USER/AppData/Local/Programs/Python/Py
Koneksi MQTT berhasil!
Menerima pesan: 1
Menerima pesan untuk membuka kamera dan merekam...
Rekaman video disimpan: D:\xampp\htdocs\skripsi\vid\video_2024-02-01_12-22-40.mp4
Informasi nama file video disimpan ke dalam database.
Video dapat diakses melalui: http://localhost/skrripsi/vid/video_2024-02-01_12-22-40.mp4
Menutup kamera dan database...
PS C:\Users\USER\Documents\Skripsi\python>
    
```

Gambar 8. Proses pada Pythom

D. Perancangan Situs Web

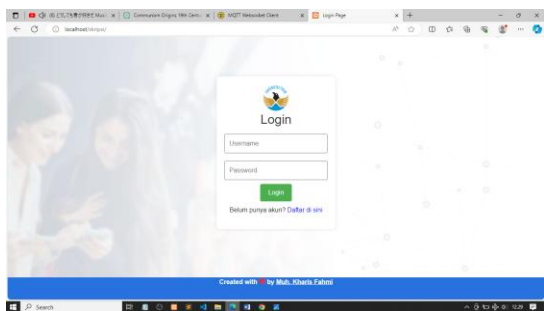
Pengembangan situs *web* adalah proses merancang, membangun, dan memelihara situs untuk keperluan *online*. Ini melibatkan serangkaian langkah, mulai dari perencanaan dan desain visual hingga pengkodean, implementasi fungsionalitas, dan pengujian. Pengembang *web* menggunakan teknologi-teknologi serta bahasa pemrograman seperti PHP, JavaScript, CSS, dan HTML sebagai bagian pada *backend frameworks* agar menciptakan situs yang responsif dan interaktif. Selain itu, pengembangan situs *web* juga melibatkan integrasi dengan basis data, optimisasi performa, dan keamanan untuk memastikan pengalaman pengguna yang baik.

Pada *website* ini, untuk meningkatkan keamanan, terdapat sistem registrasi dan *login user*. Selain itu password juga dienkripsi mebggunakan metode hash yang sudah disediakan PHP.

```

$newPassword= password_hash($_POST["newPassword"],
PASSWORD_DEFAULT);
    
```

baris program di atas adalah proses enkripsi password menggunakan metode **hash**. Dalam contoh tersebut, nilai dari **\$_POST["newPassword"]** (kata sandi yang dikirimkan melalui formulir HTML dengan metode POST) di-hash menggunakan sebuah algoritma default yang disarankan oleh sistem (**PASSWORD_DEFAULT**). Hasil dari hash tersebut disimpan dalam variabel **\$newPassword**. Proses ini secara efektif menghasilkan string hash yang unik dan sulit untuk di-decode kembali ke kata sandi aslinya. Untuk fitur yang ada pada *website* dapat dilihat pada gambar 9. sistem *login* dan registrasi, 11. daftar riwayat akses oleh *user*, dan 10. hasil tangkapan kamera keamanan.



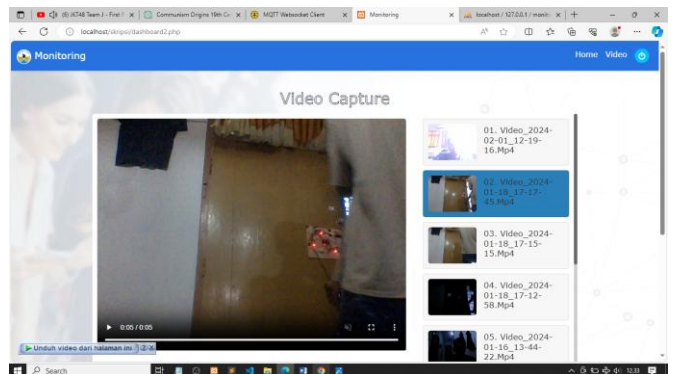
Gambar 9. Sistem login dan registrasi *website*

Dapat dilihat juga pada Gambar 10. terdapat halaman yang memuat *user* yang telah mengakses sistem, halaman ini memuat tabel yang berisi nama *user*, UID dan waktu akses. Ini dapat memudahkan pemantauan karena sistem mencatat tindakan akses oleh siapa saja yang menggunakan sistem ini.

NO	Nama	UID	Waktu
1	fahmi1	593520400	2024-01-18 17:18:13
2	fahmi1	593520400	2024-01-18 17:17:58
3	fahmi1	593520400	2024-01-18 17:16:07
4	fahmi1	593520400	2024-01-18 17:15:51
5	fahmi1	593520400	2024-01-18 17:15:26
6	fahmi1	593520400	2024-01-18 17:13:39
7	fahmi1	593520400	2024-01-16 13:45:18
8	fahmi1	593520400	2024-01-16 13:44:31
9	fahmi1	593520400	2024-01-08 13:57:04
10	fahmi2	-1277434225	2024-01-08 13:57:01

Gambar 10. Daftar riwayat akses oleh *user*

Gambar 11. Menunjukkan rekaman yang terkirim ketika sistem berhasil ditembus. Jadi ketika sistem di tembus, selain *buzzer* aktif, kamera juga akan menangkap video kejadian dan akan dikirim ke dataase dan ditampilkan pada *website* untuk dapat ditinjau.



Gambar 11. Hasil tangkapan kamera keamanan

E. Pengujian Sensor RC522

Pengujian pembacaan sensor RC522 melibatkan penerapan dan pengujian modul RFID RC522 untuk membaca data dari *tag* RFID. Pengujian terhadap sensor RC522 melibatkan penempatan berbagai benda sebagai penghalang. Selain itu, uji jarak dilakukan untuk mengevaluasi jangkauan kemampuan pembacaan UID RFID dan identifikasi jenis kartu yang dapat dibaca oleh pembaca RFID. Tujuan dari pengujian ini adalah untuk menilai sejauh mana sensor RC522 dapat membaca *tag* RFID dalam kondisi yang berbeda dan untuk mengidentifikasi batasan-batasan serta keandalan pembacaan pada jarak.

Pengujian RC522 pada halangan yang dijelaskan Tabel 1:

TABEL I
PENGUJIAN RC522 TERHADAP HALANGAN

Penghalang	Terbaca	Tidak terbaca
Kertas	v	-
Kantong plastik	v	-
Kardus	v	-
Logam	-	v

Pengujian RC522 terhadap jenis kartu yang dijelaskan Tabel 3:

TABEL II
PENGUJIAN RC522 TERHADAP JENIS KARTU

Jenis Kartu	Terbaca	Tidak terbaca
Kartu RFID (Mifare)	v	-
RFID key chain	v	-
SIM	-	v
E-KTP	v	-
Kartu ATM	-	-
Kartu Mahasiswa	-	-

Pengujian RC522 terhadap jarak yang dijelaskan Tabel 4:

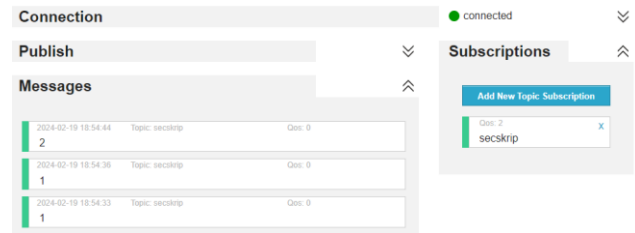
TABEL III
PENGUJIAN RC522 TERHADAP JARAK

Jarak	Terbaca	Tidak terbaca
1cm	v	-
2cm	v	-
3cm	v	-
4cm	v	-
5cm	-	v

Dari hasil pengujian pada Tabel 1, dapat disimpulkan bahwa logam merupakan satu-satunya materi yang secara signifikan menghambat pembacaan sensor. Hal ini dapat disebabkan karena struktur logam yang efektif menghalangi atau memblokir sinyal elektromagnetik. Selain itu, ketebalan benda juga memainkan peran penting; kertas dan kardus dengan ketebalan beberapa sentimeter dapat menghambat sinyal. Pengaruh jarak terhadap pembacaan tag RFID juga terlihat signifikan, dengan sinyal yang melemah seiring dengan peningkatan jarak, seperti tercatat di Tabel 3, di mana jarak maksimal pembacaan RFID hanya mencapai sekitar 4 cm. Terakhir, pengujian jenis kartu yang dapat dibaca oleh RFID Reader menunjukkan bahwa kartu Mifare, RFID key chain, dan E-KTP dapat terbaca, sementara kartu SIM, Kartu Debit, dan Kartu Tanda Mahasiswa tidak dapat terbaca. Ini disebabkan oleh fakta bahwa RFID Reader hanya dapat membaca kartu dengan chip yang beroperasi pada frekuensi 13,56 Hz.

F. Pengujian Konektifitas Database

Pengujian ini akan dilakukan untuk memastikan terhubungnya semua program hingga data dikirim ke database dan ditampilkan pada website. Pertama adalah pengiriman sinyal data dari ESP8266 yang dikirim menggunakan broker MQTT, dapat dilihat pada Gambar 7 bahwa ESP8266 berhasil terhubung dengan broker MQTT dan berhasil mengirim pesan. Sedangkan di sisi broker, seperti yang dapat dilihat pada Gambar 12.



Gambar. 12. Broker MQTT menerima pesan dari ESP

Pada gambar dapat dilihat bahwa broker dapat menerima dengan baik pesan yang dikirim oleh ESP8266, dapat dilihat juga dengan delay yang hanya beberapa detik, membuat komunikasi ini sangat cocok untuk digunakan pengujian selanjutnya dilakukan pada hubungan program python yang menerima masukan oleh broker MQTT hingga pengirimannya ke database. Program python menggunakan baris kode berikut untuk menerima pesan.

```
def on_message(client, userdata, msg):
    global last_record_time
    message = msg.payload.decode()
    print(f"Menerima pesan: {message}")
```

Fungsi **on_message** adalah callback yang dipanggil setiap kali ada pesan baru yang diterima oleh klien MQTT. Ketika sebuah pesan diterima, fungsi ini mengakses pesan tersebut menggunakan parameter msg, mendekode payload pesan menjadi string menggunakan metode **decode()**, dan kemudian mencetak pesan tersebut ke konsol dengan menggunakan fungsi **print()**. Variabel global **last_record_time** juga digunakan dalam fungsi ini untuk mencatat waktu pesan diterima. Dan ketika python menerima pesan tertentu maka kamera akan otomatis aktif dan merekam, kemudian video dikirim ke direktori server lokal seperti gambar 8.

Kemudian pada sisi database seperti yang ditunjukkan pada gambar 13 dan 14, database berhasil menyimpan data aktifitas penggunaan RFID dan hasil rekaman yang diambil pada direktori server lokal. Semua data pada database akan berhasil ditampilkan pada website dengan urutan waktu terbaru seperti pada gambar perancangan situs website.

	id	nama	uid	waktu
<input type="checkbox"/>	1	fahmi1	593520400	2024-01-07 16:34:44
<input type="checkbox"/>	2	fahmi2	-1277424225	2024-01-07 16:34:57
<input type="checkbox"/>	3	fahmi1	593520400	2024-01-08 13:56:33
<input type="checkbox"/>	4	fahmi2	-1277424225	2024-01-08 13:56:43
<input type="checkbox"/>	5	fahmi1	593520400	2024-01-08 13:56:46
<input type="checkbox"/>	6	fahmi2	-1277424225	2024-01-08 13:56:49
<input type="checkbox"/>	7	fahmi1	593520400	2024-01-08 13:56:52
<input type="checkbox"/>	8	fahmi2	-1277424225	2024-01-08 13:56:55
<input type="checkbox"/>	9	fahmi1	593520400	2024-01-08 13:56:58
<input type="checkbox"/>	10	fahmi2	-1277424225	2024-01-08 13:57:01

Gambar. 13. Tabel user pada database

Selanjutnya sistem juga dapat menyimpan data video pada server yang akan ditulis pada tabel di database, seperti pada Gambar 14.

	id	nama	waktu
<input type="checkbox"/>	28	video_2024-01-12_15-22-13.mp4	2024-01-12 15:22:13
<input type="checkbox"/>	29	video_2024-01-12_18-54-16.mp4	2024-01-12 18:54:16
<input type="checkbox"/>	30	video_2024-01-15_12-22-45.mp4	2024-01-15 12:22:45
<input type="checkbox"/>	31	video_2024-01-16_13-44-22.mp4	2024-01-16 13:44:22
<input type="checkbox"/>	32	video_2024-01-18_17-12-58.mp4	2024-01-18 17:12:58
<input type="checkbox"/>	33	video_2024-01-18_17-15-15.mp4	2024-01-18 17:15:15
<input type="checkbox"/>	34	video_2024-01-18_17-17-45.mp4	2024-01-18 17:17:45
<input type="checkbox"/>	35	video_2024-02-01_12-19-16.mp4	2024-02-01 12:19:16

Gambar. 14. Tabel video pada database

G. Analisis malfungsi pada sistem

Malfungsi dalam sistem keamanan pintu dan jendela berbasis RFID, e-KTP, dan solenoid doorlock dapat terjadi karena masalah teknis atau operasional. Solusi melibatkan pemeliharaan rutin, pemeriksaan perangkat keras dan perangkat lunak secara berkala, serta penggunaan komponen cadangan untuk menghindari downtime. Penyelesaian masalah secara cepat dan sistematis akan memastikan sistem tetap berfungsi dengan baik dan aman. Ada beberapa kemungkinan malfungsi yang akan terjadi, list malfungsi dan solusi yang ditemukan ketika penelitian dijelaskan sebagai berikut:

1) RFID tidak terbaca atau terdeteksi,

Penyebabnya bisa berupa kartu RFID yang rusak, jarak pembacaan yang tidak sesuai, atau gangguan elektromagnetik dari perangkat lain. Solusinya adalah memastikan kartu dalam kondisi baik, memeriksa antena pembaca, dan memilih pembaca RFID yang lebih tahan terhadap interferensi.

2) Solenoid doorlock Tidak Membuka atau Terkunci,

Masalah ini sering disebabkan oleh kerusakan solenoid atau kelistrikan yang tidak stabil. Pastikan solenoid dalam kondisi baik, periksa koneksi listrik, dan lakukan pemeliharaan rutin seperti pelumasan untuk mencegah macet.

3) Gangguan pada Sistem Elektronik (Power Failure),

Kegagalan daya atau arus listrik yang tidak stabil bisa menyebabkan sistem gagal berfungsi. Solusinya adalah menggunakan sumber daya cadangan seperti UPS atau baterai untuk menjaga sistem tetap berjalan saat terjadi pemadaman listrik.

4) Gangguan Jaringan (Sistem Berbasis Cloud),

Jika sistem bergantung pada jaringan internet atau cloud, gangguan pada jaringan dapat menghambat operasional. Gunakan sistem cadangan lokal agar tetap dapat berfungsi meskipun ada gangguan jaringan.

5) Pengguna Tidak Terdaftar atau Terblokir,

Jika pengguna mencoba mengakses sistem menggunakan RFID atau e-KTP yang tidak terdaftar atau diblokir, maka akses akan ditolak. Pastikan hanya pengguna terotorisasi yang terdaftar dalam sistem, dan lakukan verifikasi data serta pemantauan log secara rutin.

IV. KESIMPULAN

Berdasarkan penelitian yang sudah dilaksanakan, penelitian dengan judul “Sistem Monitoring Security Building Berbasis E-KTP dan Nodemcu Esp8266” didapat kesimpulan bahwa delay yang dihasilkan dari semua proses tidak sampai lima detik, sehingga masalah ini tidak mempengaruhi kinerja sistem jika berjalan pada server lokal. Halangan yang tebal dan padat dapat mengganggu pembacaan kartu rfid, tetapi masalah seperti ini tidak akan menjadi persoalan penting selama kartu tidak rusak. Ada juga kartu cadangan yang disiapkan ketika kartu rusak atau tidak bekerja. Selama pengujian kita menggunakan tiga kartu, sehingga memungkinkan sistem untuk memiliki lebih dari satu kartu sebagai cadangan kunci. Untuk sistem website yang digunakan, akan sangat mempermudah dalam pemantauan karena bisa diakses melalui berbagai perangkat dan data akan otomatis mengupdate. Penerapan sistem pada pintu dan jendela bekerja dengan baik dan alat berjalan dengan sempurna tanpa terjadi malfungsi. Keamanan data pada E-KTP juga terjamin, karena sistem hanya mengambil nomor pada chip RFID, nomor tersebut tidak dapat disalahgunakan kecuali menggunakan dekriptor dari pemerintah.

REFERENSI

- [1] M. Fadly, D. R. Muryana and A. T. Priandika, "Sistem *Monitoring* Penjualan bahan Bangunan Menggunakan Pendekatan Key Performance Indicator," *Journal of Social Sciences and Technology for Community Service (JSSTCS)*, pp. 15-20, 2020.
- [2] J. Antara, "Kisah di balik pencurian ratusan koleksi Museum Sulawesi Tenggara," BBC, Kendari, Sulawesi Tenggara, 2021.
- [3] Suhariyanto, "Kasus Pencurian Barang di Indonesia," Badan Pusat Statistik, Jakarta Pusat, Jakarta, 2021.
- [4] M. Akbar and I. Effendy, "Implementasi aplikasi kehadiran perkuliahan dikelas menggunakan pembaca RFID pada e-KTP. Jurnal Informatika," *Jurnal Pengembangan IT*, vol. III, no. 1, pp. 31-35, 2018.
- [5] A. Mubarak, I. Sofyan, A. A. Rismayadi and I. Najiyah, "Sistem Keamanan Rumah Menggunakan RFID, Sensor PIR dan Modul GSM Berbasis Mikrokontroler," *Jurnal Khatulistiwa Informatika*, vol. V, no. 1, pp. 137-144, 2018.
- [6] M. E. Adimas, "Perancangan Pengontrolan dan *Monitoring* Simulasi Palang Pintu Otomatis Menggunakan Radio Frequency Identification (RFID) dan Sensor Ultrasonik Berbasis *Programmable logic controller* (PLC) Schneider TM221CE16R dan Vijeo Designer," *Doctoral Dissertation, Undip Vocation*, 2019.
- [7] M. M. R. N. Rifai and R. Yuliantari, "Analisis Perancangan Sistem Pengaman Pintu Otomatis Menggunakan Rfid Dan Bot Telegram," *SEMASTER*, *Seminar Nasional Riset Teknologi Terapan*, vol. II, pp. 1-5, 2021.
- [8] A. Ipanhar, T. K. Wijaya and P. Gunoto, "Perancangan Sistem *Monitoring* Pintu Otomatis Berbasis IoT Menggunakan ESP32-CAM," *SIGMA TEKNIKA*, vol. V, no. 2, pp. 333-350, 2022.
- [9] N. K. Daulay and M. N. Alamsyah, "*Monitoring* sistem keamanan pintu menggunakan rfid dan fingerprint berbasis *web* dan *database*," *Jusikom: Jurnal Sistem Komputer Musirawas*, vol. IV, no. 2, pp. 85-92, 2019.
- [10] D. Nataliana, F. Hadiatna and A. Fauzi, " Rancang Bangun Sistem Keamanan RFID *Tag* menggunakan Metode Caesar Cipher pada Sistem Pembayaran Elektronik," *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika*, vol. VII, no. 3, pp. 427-433, 2019.
- [11] N. R. Prayogi, I. Siradjuddin and D. Radianto, "Implementasi Modular Papan Kontroler Swerve Drive: Komunikasi SPI," *Journal of Mechanical and Electrical Technology*, vol. III, no. 3, pp. 116-124, 2024.
- [12] H. Arijuddin, A. Bhawiyuga and K. Amron, "Pengembangan Sistem Perantara Pengiriman Data Menggunakan Modul Komunikasi LoRa dan Protokol MQTT Pada Wireless Sensor Network," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. III, no. 2, pp. 1655-1659, 2019.