



Sistem Keamanan IoT dengan Sensor RFID dan Kamera ESP32 untuk Verifikasi Identitas dan Visual

Imam Gunawan¹, Khairil Hamdi^{2*}, Joyo Kilat Moko³, Budi Sunaryo⁴

^{1,2,3}Sistem Informasi, STMIK Jaya Nusa Padang

⁴Teknologi Rekayasa Komputer Jaringan, Fakultas Teknologi Industri, Universitas Bung Hatta
khairilhamdi@jayanusa.ac.id

Abstract

The main problem faced by the madrasah is the lack of visual evidence that can cause a number of problems, including misuse of access cards and the inability to identify perpetrators using fake cards if they want to adopt RFID technology as a security system. This study aims to develop an Internet of Things (IoT)-based security system at Madrasah Ibtidaiyah Wathoniyah Sumber Makmur by utilizing RFID sensors and ESP32 cameras. The system developed is designed to automatically verify identity and provide visual notifications sent via Telegram. The research process began with the collection of qualitative data through direct observation and interviews with the principal, which provided in-depth insights into the existing problems, history, and vision, mission, and organizational structure of the madrasah. Library research was also conducted to collect information from various relevant books and scientific articles, providing the theoretical basis needed for system development. In addition, laboratory research focused on testing and validating prototypes involving hardware components such as ESP32, ESP32 Cam, and PN532 sensors as well as software developed using software such as Arduino IDE, Telegram, and Visual Studio Code. The development method in this study uses a prototyping method that involves active collaboration between designers and end users to ensure that the resulting solution is in accordance with user needs and expectations. The conclusion is that the developed system significantly improves security and access management in madrasahs. This system has proven effective in reducing the risk of access card misuse by providing the necessary visual evidence and accurately detecting illegal access attempts, and can identify perpetrators in illegal access attempts with fake access cards that can be spam.

Keywords: Security System, IoT, RFID, ESP32 Camera, Prototyping

Abstrak

Masalah utama yang dihadapi oleh madrasah adalah tidak adanya bukti visual yang dapat menyebabkan sejumlah masalah, termasuk penyalahgunaan kartu akses dan ketidakmampuan untuk mengidentifikasi pelaku yang menggunakan kartu palsu apabila hendak mengadopsi teknologi RFID sebagai sistem keamanan. Penelitian ini bertujuan untuk mengembangkan sistem keamanan berbasis Internet of Things (IoT) di Madrasah Ibtidaiyah Wathoniyah Sumber Makmur dengan memanfaatkan sensor RFID dan kamera ESP32. Sistem yang dikembangkan dirancang untuk melakukan verifikasi identitas secara otomatis dan memberikan notifikasi visual yang dikirimkan melalui Telegram. Proses penelitian ini dimulai dengan pengumpulan data kualitatif melalui observasi langsung dan wawancara dengan kepala sekolah, yang memberikan wawasan mendalam mengenai masalah yang ada, sejarah, serta visi, misi, dan struktur organisasi madrasah. Penelitian perpustakaan juga dilakukan untuk mengumpulkan informasi dari berbagai buku dan artikel ilmiah yang relevan, memberikan dasar teori yang diperlukan untuk pengembangan sistem. Selain itu, penelitian laboratorium berfokus pada pengujian dan validasi prototipe dengan melibatkan komponen perangkat keras seperti ESP32, ESP32 Cam, dan sensor PN532 serta perangkat lunak yang dikembangkan menggunakan software seperti Arduino IDE, Telegram, dan Visual Studio Code. Metode pengembangan dalam penelitian ini menggunakan metode prototyping yang melibatkan kolaborasi aktif antara perancang dan pengguna akhir untuk memastikan bahwa solusi yang dihasilkan sesuai dengan kebutuhan dan harapan pengguna. Kesimpulannya adalah sistem yang dikembangkan secara signifikan meningkatkan keamanan dan pengelolaan akses di madrasah. Sistem ini terbukti efektif dalam mengurangi risiko penyalahgunaan kartu akses dengan menyediakan bukti visual yang diperlukan dan mendeteksi upaya akses ilegal secara akurat, dan dapat mengetahui pelaku dalam percobaan pengaksesan ilegal dengan kartu akses palsu yang dapat bersifat spam.

Kata kunci: Sistem Keamanan, IoT, RFID, Kamera ESP32, Prototyping

1. Pendahuluan

Keamanan di lingkungan sekolah menjadi salah satu aspek krusial yang memerlukan perhatian khusus karena termasuk dalam parameter kepuasan siswa dan juga

orang tua siswa terhadap sarana dan prasarana sekolah [1], terutama di era digital di mana teknologi dapat memberikan solusi inovatif untuk meningkatkan keamanan [2][3], sehingga guru dan siswa dapat melaksanakan kegiatan pembelajaran dengan aman dan

nyaman [4]. Salah satu teknologi yang mulai banyak digunakan adalah Radio Frequency Identification (RFID) [5][6]. Teknologi ini memungkinkan akses cepat dan efisien ke fasilitas sekolah, berkat kemampuannya dalam mengidentifikasi individu melalui kartu atau tag berbasis frekuensi radio [7]. RFID dikenal sebagai teknologi yang mudah diintegrasikan dan memberikan kenyamanan dalam penggunaannya [8].

Meskipun RFID memiliki berbagai keunggulan, ada beberapa tantangan yang muncul ketika teknologi ini diterapkan di lingkungan sekolah. Salah satu tantangan utamanya adalah risiko penyalahgunaan akses. Ketika kartu akses jatuh ke tangan yang tidak berhak, tanpa adanya sistem verifikasi tambahan seperti biometrik atau identifikasi visual, kemungkinan terjadinya akses ilegal menjadi lebih besar [9]. Hal ini dapat menimbulkan kerentanan keamanan yang bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Selain itu, kelemahan lain dari sistem RFID adalah tidak adanya bukti visual yang dapat mengidentifikasi pengguna kartu [10]. RFID saat ini hanya berfungsi sebagai alat berbasis frekuensi tanpa memberikan data visual dari pengguna sebenarnya [11]. Hal ini meningkatkan risiko pemalsuan kartu atau penyalahgunaan, di mana sistem tidak dapat memastikan siapa pengguna yang sesungguhnya [12]. Sistem RFID juga rentan terhadap serangan seperti spam atau aktivitas merusak, yang tidak memberikan informasi tentang pelaku yang mencoba mengakses fasilitas secara tidak sah [13].

Untuk mengatasi tantangan tersebut, teknologi Internet of Things (IoT) yang mengintegrasikan sensor RFID dengan kamera ESP32 dan bot Telegram menjadi solusi yang potensial [14]. IoT memungkinkan perangkat RFID dan kamera untuk beroperasi secara real-time [15], sehingga tidak hanya mencatat akses fisik, tetapi juga menghasilkan bukti visual yang dapat dikirim langsung melalui bot Telegram sebagai notifikasi [16]. Dengan sistem ini, setiap akses menggunakan RFID akan disertai dengan tangkapan gambar dari pengguna oleh kamera ESP32, yang kemudian dikirimkan ke administrator melalui Telegram [17]. Hal ini memberikan keamanan lebih tinggi dengan jejak digital dan visual yang dapat dilacak [18].

Penerapan sistem keamanan berbasis RFID, IoT, kamera ESP32, dan bot Telegram diharapkan dapat secara signifikan meningkatkan efisiensi dan keamanan di lingkungan sekolah. Kombinasi teknologi ini mampu mengatasi berbagai kekurangan dari sistem RFID tradisional, sekaligus memberikan solusi yang lebih terintegrasi dan efektif untuk menjaga keamanan fasilitas sekolah.

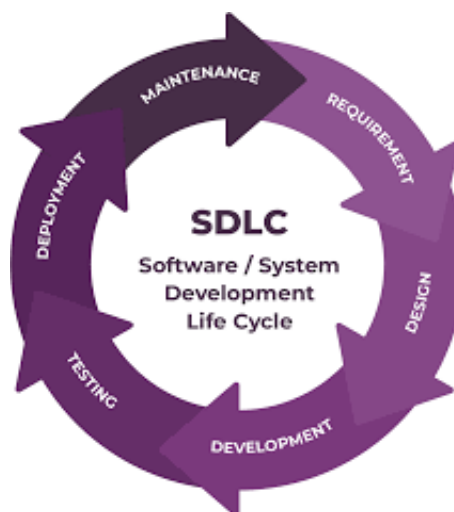
Langkah implementasi sistem keamanan RFID ini adalah sebuah inovasi progresif untuk meningkatkan keamanan dan efisiensi di lingkungan sekolah. Namun, tantangan seperti risiko penyalahgunaan akses harus diantisipasi. Misalnya, jika kartu akses jatuh ke pihak

yang tidak berhak, sistem harus dilengkapi dengan verifikasi tambahan. Selain itu, kelemahan lain adalah kurangnya bukti visual, yang dapat membuka celah bagi penyalahgunaan kartu palsu atau serangan spam yang bertujuan merusak sistem tanpa identifikasi pelaku.

Tujuan dari pengembangan sistem ini adalah membantu staf sekolah, khususnya guru, untuk memantau secara visual siapa yang mengakses fasilitas tertentu. Sistem ini juga dirancang untuk menambahkan lapisan keamanan lebih pada fasilitas sekolah yang membutuhkan perlindungan lebih tinggi. Dengan pendekatan ini, diharapkan keamanan di lingkungan sekolah dapat ditingkatkan secara signifikan.

2. Metode Penelitian

Metode penelitian ini menggunakan paradigma pengembangan system secara prototyping. Model Prototype adalah metode proses pembuatan sistem yang dibuat secara terstruktur dan memiliki beberapa tahap-tahap yang harus dilalui pada pembuatannya, namun jika tahap final dinyatakan bahwa sistem yang telah dibuat belum sempurna atau masih memiliki kekurangan, maka sistem akan dievaluasi kembali dan akan melalui proses dari awal [19]. Pendekatan Prototyping adalah proses interative yang melibatkan hubungan kerja yang dekat antara perancang dan pengguna [20]. Proses prototyping melalui beberapa tahapan pada Gambar 1.



Gambar 1. Metode SDLC

2.1. Perencanaan

Tahap awal dalam pembuatan sistem berbasis alat dan Telegram adalah perencanaan. Pada tahap ini, langkah pertama adalah mengidentifikasi kebutuhan dengan memahami tujuan sistem yang ingin dicapai. Salah satu contohnya adalah mengintegrasikan alat fisik, seperti sensor atau mikrokontroler, dengan platform Telegram untuk mendukung komunikasi dan pengendalian.

2.2. Analisis Kebutuhan

Tahap berikutnya adalah analisis kebutuhan. Dalam tahap ini, fungsionalitas sistem didefinisikan secara rinci, seperti kemampuan untuk mengirim notifikasi alat melalui Telegram atau menjalankan perintah yang diterima dari bot Telegram. Selain itu, spesifikasi teknis alat fisik dan langkah-langkah keamanan untuk memastikan komunikasi antara alat, server, dan Telegram juga dirumuskan.

2.3. Perancangan Sistem

Selanjutnya, perancangan sistem dilakukan. Pada tahap ini, desain arsitektur sistem dibuat, termasuk bagaimana alat fisik, server, dan API Telegram saling berinteraksi. Contohnya adalah alat mengirimkan data ke server, yang kemudian diteruskan ke bot Telegram, atau sebaliknya. Jika diperlukan, desain struktur database dan wireframe untuk antarmuka pengguna juga dirancang.

2.4. Pengembangan

Tahap pengembangan mencakup pemrograman perangkat fisik agar dapat berkomunikasi dengan server atau Telegram. Selain itu, bot Telegram dikembangkan menggunakan API dengan logika yang memungkinkan penerimaan dan pemrosesan perintah dari pengguna. Setelah itu, semua komponen sistem diintegrasikan untuk memastikan fungsionalitas berjalan dengan baik.

2.5. Pengujian

Pengujian menjadi langkah penting untuk memastikan semua bagian sistem berfungsi sesuai harapan. Pengujian meliputi unit testing untuk setiap komponen, integration testing untuk memastikan komunikasi antara alat, server, dan Telegram berjalan lancar, serta user acceptance testing oleh pengguna akhir. Stress testing juga dilakukan untuk menilai kemampuan sistem dalam menghadapi beban besar.

2.6. Implementasi

Setelah tahap pengujian selesai, sistem mulai diterapkan di lingkungan produksi. Proses ini mencakup pemasangan perangkat fisik dan bot Telegram yang sudah siap digunakan oleh pengguna. Jika diperlukan, pelatihan juga diberikan untuk membantu pengguna memahami cara kerja sistem, termasuk mengirimkan perintah melalui Telegram.

2.7. Pemeliharaan

Pemeliharaan dilakukan untuk memastikan sistem tetap berfungsi optimal. Ini meliputi pemantauan berkala, perbaikan bug, dan penambahan fitur baru sesuai kebutuhan yang berkembang. Proses pemeliharaan ini penting untuk menjamin keberlanjutan sistem.

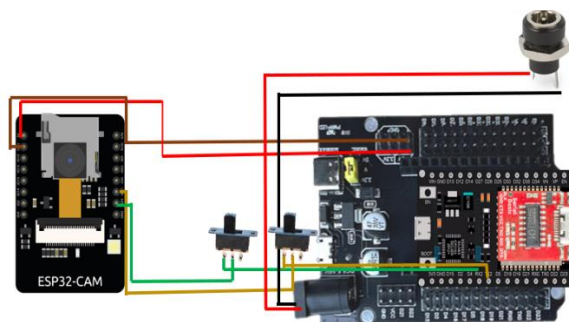
2.8. Evaluasi dan Pengembangan

Langkah terakhir dalam proses ini adalah evaluasi dan pengembangan lebih lanjut. Pada tahap ini, kinerja sistem ditinjau secara menyeluruh untuk mengevaluasi

efektivitasnya dalam memenuhi tujuan yang telah ditetapkan. Selain itu, masukan dari pengguna dikumpulkan dan dianalisis sebagai bahan untuk merancang peningkatan sistem di masa depan.

3. Hasil dan Pembahasan

Komunikasi serial digunakan untuk memungkinkan kedua mikrokontroler saling membaca data secara serial. Metode yang digunakan adalah UART, yang hanya memerlukan beberapa pin untuk menghubungkan kedua perangkat agar dapat berkomunikasi. Rangkaian komunikasi antara mikrokontroler tersebut dapat dilihat pada Gambar 2.



Gambar 2. Komunikasi UART

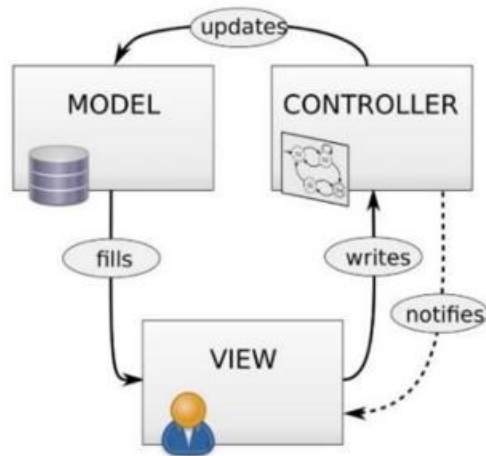
Tabel 1 menjelaskan konfigurasi pin komunikasi UART antara ESP32 dan ESP32Cam yang melibatkan penggunaan dua saklar (Switch 1 dan Switch 2). Pin VCC pada ESP32 dan ESP32Cam digunakan sebagai sumber daya positif, sementara pin GND berfungsi sebagai ground. Jalur TX pada ESP32 dihubungkan ke kaki 1 Switch 1, sedangkan RX dihubungkan ke kaki 2 Switch 2, yang kemudian terhubung ke pin UOR dan UOT pada ESP32Cam. Dengan konfigurasi ini, komunikasi serial antara ESP32 dan ESP32Cam dapat dilakukan secara fleksibel melalui pengaturan posisi saklar untuk memastikan jalur komunikasi berfungsi dengan baik.

Tabel 1. Pin Komunikasi UART

Power	ESP32	Switch 1	Switch 2	ESP32Cam
+	VCC			
-	GND			
	5V			5V
	GND			GND
	TX	Kaki 1		
		Kaki 2		UOR
	RX		Kaki 1	
			Kaki 2	UOT

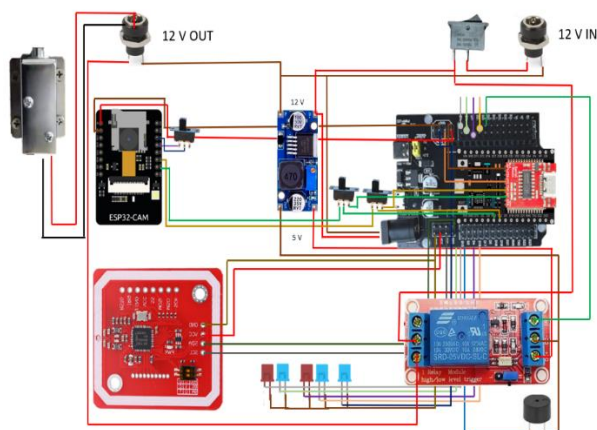
Bot Telegram menyediakan fitur custom button keyboard untuk klien, yang mempermudah interaksi antara bot dan penggunanya. Telegram menggunakan format JavaScript Object Notation (JSON) untuk mengirimkan data kepada klien, sehingga pengembang bot dapat menggunakan bahasa pemrograman apa pun yang mereka kuasai, karena semua bahasa pemrograman

mendukung pembuatan dan pembacaan JSON. JSON, yang diciptakan oleh Douglas Crockford, adalah format pertukaran data yang ringan dan berfokus pada representasi data di situs web. Format ini dirancang untuk menyederhanakan proses pertukaran data pada situs web dan merupakan pengembangan dari fungsi-fungsi JavaScript.



Gambar 3. Konsep VC

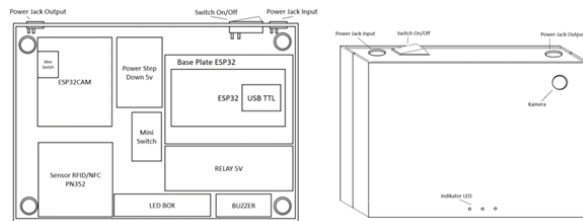
Berdasarkan Gambar 3, ketika pengguna mengirim pesan ke bot, seperti perintah /start, pesan tersebut diterima oleh bot dalam format JSON melalui webhook dari API Telegram. Controller kemudian memproses JSON tersebut, memeriksa perintah /start, dan mengambil data yang diperlukan dari Model. Model bertugas menyiapkan data yang dibutuhkan, seperti menyimpan informasi pengguna atau membuat pesan selamat datang. Setelah data tersedia, Controller mengirimkan data tersebut ke View untuk dirancang menjadi pesan balasan. View kemudian merender pesan tersebut ke dalam format JSON yang dapat dikenali oleh API Telegram, dan bot mengirimkan balasan tersebut kepada pengguna.



Gambar 4. Diagram Blok Sistem

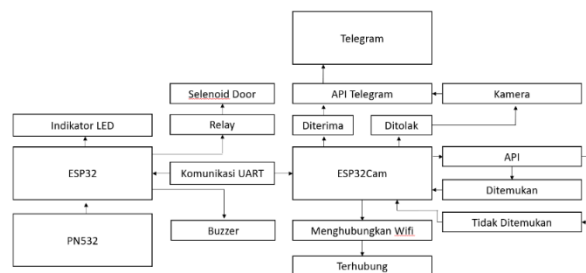
Gambar 4 menunjukkan diagram blok sistem yang mengintegrasikan beberapa komponen utama untuk mendukung fungsionalitas perangkat berbasis IoT.

Sistem ini menggunakan ESP32-CAM sebagai modul utama untuk pengambilan gambar dan komunikasi dengan perangkat lain, yang dihubungkan ke sumber daya 12V melalui regulator untuk menyesuaikan kebutuhan daya komponen. Selain itu, terdapat modul relay yang berfungsi sebagai saklar elektronik untuk mengontrol perangkat tertentu, serta modul RFID untuk proses identifikasi berbasis tag. Seluruh komponen dirancang untuk saling terhubung melalui kabel dan pin-pinnya dengan pengaturan yang memastikan aliran data dan daya berjalan sesuai dengan kebutuhan sistem.



Gambar 5. Desain Internal

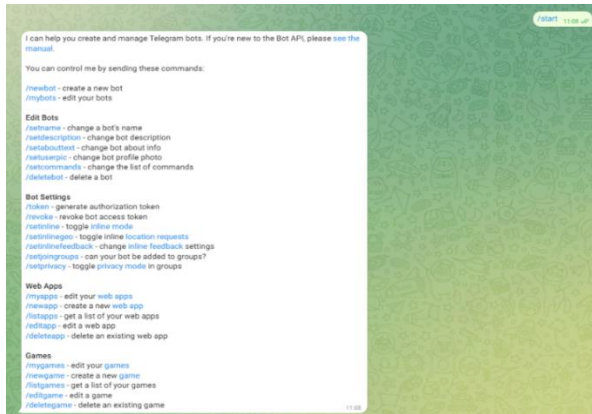
Gambar 5 memperlihatkan desain internal sistem yang dirancang untuk mendukung pengoperasian perangkat berbasis IoT. Desain ini mencakup modul ESP32-CAM yang bertugas sebagai komponen utama untuk pengambilan gambar, ditempatkan di bagian atas bersama power step down 5V untuk mengatur tegangan sesuai kebutuhan sistem. Sensor RFID/NFC PN532 diletakkan di bagian bawah untuk keperluan identifikasi berbasis frekuensi radio, sementara relay 5V digunakan untuk mengontrol perangkat lain yang terhubung. Komponen lain seperti buzzer, LED box, dan mini switch ditempatkan secara terorganisir untuk mempermudah integrasi. Bagian luar sistem dilengkapi dengan power jack input dan output, switch on/off, serta indikator LED untuk memberikan informasi status perangkat secara visual. Desain ini tidak hanya mengutamakan fungsionalitas tetapi juga mempertimbangkan kemudahan dalam pemasangan dan pemeliharaan.



Gambar 6. Desain Internal

Gambar 6 menampilkan desain eksternal sistem yang menggambarkan alur kerja perangkat berbasis IoT untuk mendukung fungsionalitasnya. ESP32 terhubung dengan PN532 sebagai modul RFID/NFC untuk membaca tag, yang kemudian memicu relay untuk mengontrol solenoid door jika akses diterima. Indikator LED dan buzzer digunakan sebagai alat notifikasi visual dan audio, memberikan umpan balik kepada pengguna

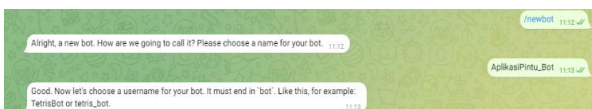
mengenai status sistem. ESP32-CAM berperan untuk menangkap gambar yang dikirim melalui API Telegram, di mana sistem menentukan apakah akses diterima atau ditolak berdasarkan data yang ditemukan atau tidak. Koneksi ESP32-CAM ke jaringan WiFi memastikan komunikasi real-time dengan Telegram untuk pengiriman data, termasuk informasi visual dari kamera. Desain ini dirancang untuk integrasi yang seamless antara komponen perangkat keras dan platform Telegram guna memastikan keamanan dan efisiensi dalam pengoperasian.



Gambar 7. Respon Perintah /start

Gambar 7 menunjukkan langkah awal dalam pembuatan bot Telegram yang memerlukan bantuan dari bot resmi bernama BotFather dengan username @BotFather. Proses ini dimulai dengan mengirimkan perintah /start kepada BotFather untuk memulai interaksi dan mendapatkan akses dalam membuat bot baru. BotFather kemudian akan memberikan panduan dan token API yang diperlukan untuk mengonfigurasi dan mengoperasikan bot yang dibuat.

Gambar 8 menunjukkan langkah berikutnya dalam pembuatan bot Telegram, yaitu mengirimkan perintah /newbot kepada BotFather. Setelah perintah dikirim, pengguna diminta untuk memberikan nama bot yang akan dibuat, seperti "AplikasiPintu.Bot." Setelah nama berhasil dimasukkan, BotFather akan memberikan token API yang digunakan untuk mengintegrasikan bot dengan sistem yang akan dikembangkan.

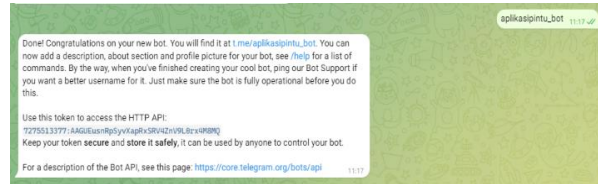


Gambar 8. Pembuatan Nama Bot

Gambar 9 menunjukkan bahwa Pintu_Bot telah berhasil dibuat, sehingga proses selanjutnya adalah menentukan username untuk bot tersebut. Username yang dipilih, seperti "aplikasipintu_bot," akan digunakan sebagai identitas unik untuk bot dalam sistem Telegram.

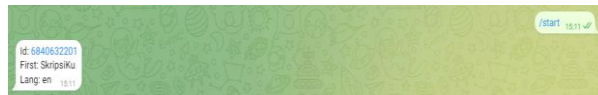
Proses pembuatan bot Telegram telah selesai, namun bot belum dapat digunakan secara langsung. Untuk membuka jendela obrolan dengan AplikasiPintu_Bot, pengguna dapat mengklik tautan t.me/aplikasipintu_bot

yang diberikan oleh BotFather pada langkah sebelumnya. Agar bot dapat merespons perintah, diperlukan langkah tambahan berupa pengaturan komponen penting seperti API dan chat_id. API untuk AplikasiPintu_Bot sudah diperoleh dari proses sebelumnya, dengan token berupa 7275513377:AAGUEusnRpSyvXapRxSRV4ZnV9L0r x4M8MQ.



Gambar 9. Penamaan Username Bot

Gambar 10 menunjukkan proses mendapatkan chat_id, yang dilakukan dengan bantuan bot pihak ketiga bernama userinfobot dengan username @userinfobot. Proses ini dimulai dengan mengirimkan perintah sederhana seperti /start kepada userinfobot. Setelah itu, bot akan merespons dengan memberikan chat_id yang diperlukan untuk mengintegrasikan bot dengan sistem dan memungkinkan interaksi yang sesuai.



Gambar 10. Mendapatkan Chat_id

Perancangan Aplikasi memiliki berbagai tahapan yang cukup panjang, dalam proses ini hal yang dilakukan adalah dengan menyiapkan framework yang diperlukan seperti Laravel yang digunakan sebagai backend untuk penyimpanan data pengguna terdaftar. Tahapan utama tersebut dapat dilihat sebagai berikut :

Fungsi tampil data sebagai berikut :

```

Fungsi tampil data
public function index()
{
    $datakartu = DataKartu::all();
    return DataKartuResource::collection($datakartu);
}
    
```

fungsi data spesifik sebagai berikut :

```

Fungsi tampil data spesifik
public function show(string $UID)
{
    $datakartu = DataKartu::find($UID);
    if (!$datakartu) {
        return response()->json(['message' => 'Data tidak ditemukan'], 404);
    } else {
        return new DataKartuResource($datakartu);
    }
}
    
```

Fungsi simpan data sebagai berikut :

```

Fungsi simpanan data
public function store(Request $request)
{
    $data = $request->validate([
    
```

```

        'UID' =>
'required|unique:datakartu,UID',
        'NamaPegguna' =>
'required|max:100',
        'Jeniskelamin' =>
'required|max:100',
        'Nohp' => 'required|max:100',
    ];
return new DataKartuResource(DataKartu::create($data));
    
```

Fungsi program model sebagai berikut:

```

Program model
use HasFactory;
public $incrementing = false;
protected $table = "datakartu";
protected $keyType = 'string';
protected $primaryKey = "UID";

protected $fillable = [
    'UID',
    'NamaPegguna',
    'Jeniskelamin',
    'Nohp',
];
    
```

Fungsi program resource sebagai berikut:

```

Program resource
public function toArray(Request $request):
array
{
    return [
        'UID' => $this->UID,
        'NamaPegguna' => $this->NamaPegguna,
        'Jeniskelamin' => $this->Jeniskelamin,
        'Nohp' => $this->Nohp,
    ];
}
    
```

Gambar 10 menggambarkan langkah pembukaan obrolan dengan BotFather untuk memodifikasi AplikasiPintu_Bot. Proses ini dilakukan dengan mengirimkan perintah /mybot kepada BotFather untuk mengakses opsi pengaturan dan konfigurasi bot tersebut.



Gambar 10. Memodifikasi Bot

Gambar 11 menunjukkan proses pemilihan bot yang ingin dimodifikasi, yang kemudian akan menampilkan menu baru dengan berbagai opsi pengaturan.



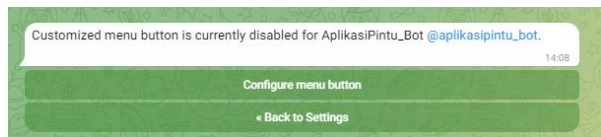
Gambar 11. Opsi Modifikasi Bot

Gambar 12 menunjukkan langkah memilih Bot Settings dari menu yang telah ditampilkan sebelumnya untuk melanjutkan pengaturan bot.



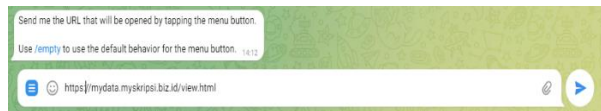
Gambar 12. Pembuatan Button

Gambar 13 menunjukkan langkah memilih opsi Menu Button dari menu pengaturan yang tersedia untuk AplikasiPintu_Bot.



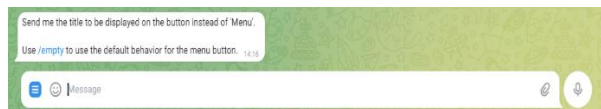
Gambar 13. Pembuatan Menu Button

Gambar 14 menunjukkan langkah memilih opsi Configure Menu Button, diikuti dengan memasukkan URL tampilan aplikasi yang telah dibuat sebelumnya. URL tersebut digunakan untuk menghubungkan bot dengan halaman aplikasi.



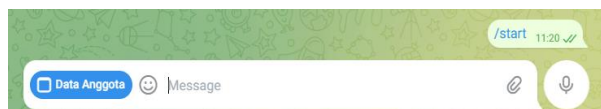
Gambar 14. Input URL

Setelah mengirimkan URL dari aplikasi, tahap selanjutnya adalah menetapkan nama yang akan ditampilkan pada tombol, seperti "Data Anggota". Ini ditunjukkan pada Gambar 15.



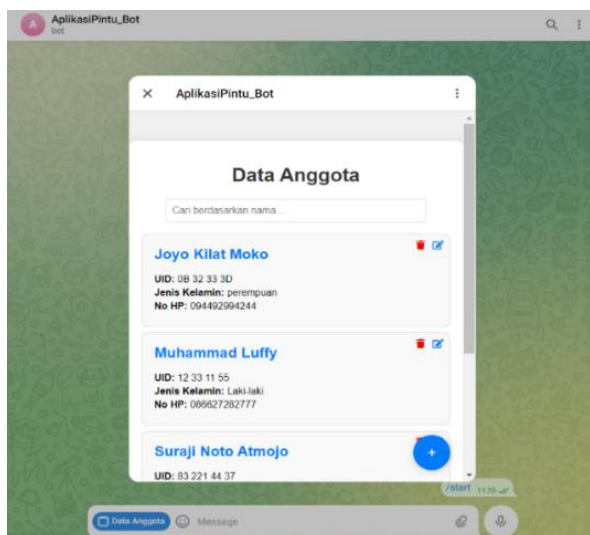
Gambar 15. Input Display Name

Setelah nama tombol dikirimkan, menu button berhasil dibuat dan dapat dilihat pada obrolan AplikasiPintu_Bot, seperti yang ditampilkan pada Gambar 16.



Gambar 16. Hasil Pembuatan Menu Button

Untuk mengakses aplikasi yang telah dibuat, pengguna cukup mengklik tombol Data Anggota. Hal ini ditampilkan pada Gambar 17 sebagai tampilan aplikasi pengolahan data.



Gambar 17. Tampilan Aplikasi Pengolah Data

4. Kesimpulan

Sistem keamanan berbasis IoT yang menggunakan sensor RFID dan kamera ESP32 telah terbukti efektif dalam meningkatkan keamanan akses di Madrasah Ibtidaiyah Wathoniyah Sumber Makmur. Sistem ini dirancang untuk mengatasi masalah utama berupa ketiadaan bukti visual, yang sering menyebabkan penyalahgunaan kartu akses dan ketidakmampuan mengidentifikasi pelaku yang menggunakan kartu palsu. Dengan penerapan teknologi ini, risiko penyalahgunaan kartu akses oleh pihak yang tidak sah dapat dikurangi secara signifikan, sementara kamera ESP32 memberikan lapisan keamanan tambahan melalui bukti visual yang dikirimkan secara otomatis melalui Telegram.

Prototipe sistem ini dikembangkan menggunakan metode prototyping yang melibatkan kolaborasi aktif antara perancang dan pengguna akhir untuk memastikan solusi yang dihasilkan sesuai kebutuhan. Pengujian perangkat keras, termasuk ESP32, ESP32-CAM, dan sensor PN532, serta perangkat lunak seperti Arduino IDE, Telegram, dan Visual Studio Code, menunjukkan bahwa sistem ini efektif dalam melakukan verifikasi otomatis dan memberikan notifikasi visual. Sistem ini juga mampu mendeteksi upaya akses ilegal secara akurat, termasuk penggunaan kartu palsu yang bersifat spam, sekaligus memberikan data visual yang dapat membantu mengidentifikasi pelaku.

Hasil penelitian menunjukkan bahwa sistem ini secara signifikan meningkatkan keamanan dan pengelolaan akses di lingkungan madrasah. Dengan memanfaatkan bukti visual dan notifikasi real-time, sistem ini tidak hanya mengurangi risiko ancaman keamanan tetapi juga memberikan transparansi dan kemudahan dalam proses identifikasi. Solusi ini dapat menjadi model untuk pengembangan sistem keamanan di institusi pendidikan lainnya.

Daftar Rujukan

- [1] K. Hamdi, "ANALISA KEPUASAN SISWA TERHADAP SARANA PRASARANA SEKOLAH MENGGUNAKAN FUZZY LOGIC," *J. Ipteks Terap.*, vol. 11, no. 3, p. 208, Oct. 2017.
- [2] M. Gawlik-Kobylińska and P. Maciejewski, "New Technologies in Education for Security and Safety," in *Proceedings of the 2019 8th International Conference on Educational and Information Technology*, 2019, pp. 198–202.
- [3] I. Gunawan, S. Kom, and M. Kom, "SISTEM INFORMASI ABSENSI SISWA BAGI ORANG TUABERBASIS WEB DAN SMS SEBAGAI UPAYA MENINGKATKAN KONTROL ORANG TUA TERHADAP ANAK (STUDI KASUS: SMK NASIONAL PADANG)," *J-Click*, vol. 3, no. 2, 2017.
- [4] N. Novinaldi, I. Gunawan, D. A. Rahayu, D. E. Subroto, and I. Ikhsan, "Workshop Routing dan Server bagi Guru-guru Anggota IGMP TIK/Informatika," *J. Pustaka Mitra (Pusat Akses Kaji. Mengabdikan Terhadap Masyarakat)*, vol. 3, no. 2, pp. 106–109, Mar. 2023.
- [5] Arnita, B. Sunaryo, P. R. Daulay, F. Hasnul, and Hidayat, "Gate-apps Number Plate Recognition untuk Sistem Akses Parkir Berbasis Internet of Things," *Pros. SISFOTEK*, vol. 5, no. 1, pp. 270–276, 2021.
- [6] H. Setiawan, T. Tasmii, and D. Dhamayanti, "Design of Additional Safety Locks for Motor Vehicles Using RFID," *J. Inf. Syst. Informatics*, vol. 5, no. 4, pp. 1691–1704, Dec. 2023.
- [7] Arpan, Mohammad Yusup, and Aidil Ahmad, "Peningkatan Efisiensi dan Akurasi Kehadiran Sekolah: Sistem Berbasis IoT dengan Teknologi RFID di SMK Putra Anda Binjai," *J. MAHAJANA Inf.*, vol. 9, no. 1, pp. 7–18, Jun. 2024.
- [8] V. V. Jituri, "RADIO FREQUENCY IDENTIFICATION (RFID) AND EASE OF LIFE," *Int. J. Res. - GRANTHAALAYAH*, vol. 8, no. 8, pp. 49–55, Aug. 2020.
- [9] J. S. Brisbane, "Enhancing School Security System Using RFID: A Comprehensive Approach," *Int. Sci. J. Eng. Manag.*, vol. 03, no. 03, pp. 1–9, Mar. 2024.
- [10] B. Kaliski, "RFID Privacy: Challenges and Progress," in *ISSE 2004 — Securing Electronic Business Processes*, Wiesbaden: Vieweg+Teubner Verlag, 2004, pp. 108–116.
- [11] W. Huang *et al.*, "An efficient visualization method of RFID indoor positioning data," in *The 2014 2nd International Conference on Systems and Informatics (ICSAI 2014)*, 2014, no. Icsai, pp. 497–504.
- [12] A. Li, J. Li, Y. Zhang, D. Han, T. Li, and Y. Zhang, "Secure UHF RFID Authentication With Smart Devices," *IEEE Trans. Wirel. Commun.*, vol. 22, no. 7, pp. 4520–4533, Jul. 2023.
- [13] Y. Wang, J. Shen, X. Guo, and W. Dong, "Research on RFID attack methods," in *2020 IEEE 3rd International Conference on Automation, Electronics and Electrical Engineering (AUTEEE)*, 2020, pp. 433–437.
- [14] D. R. Tisna, T. Maharani, and K. T. Nugroho, "PEMANFAATAN CHATBOT TELEGRAM UNTUK MONITORING DAN KONTROL KUALITAS AIR MENGGUNAKAN ESP32," *JUPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.)*, vol. 9, no. 3, pp. 1292–1306, Aug. 2024.
- [15] R. T. Prabu, J. T., and G. Ramkumar, "A Real-Time Internet of Things based Systematic Toll Plaza Controlling System using Logical RFID," in *2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICES)*, 2023, pp. 1–8.
- [16] P. Samuda, K. Sivachandar, N. G. Praveena, C. Nithiya, D. Kamalesh, and C. Lokesh, "Low-cost Prototype for IoT-based Smart Monitoring through Telegram," in *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 2023, pp. 1–5.
- [17] G. S. A. R. P. B., K. A. V. V. A., and L. K., "Design and Development of IoT Camera with CHATBOT for Domestic Surveillance," in *2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS)*, 2023, pp. 1–5.
- [18] Z. Muslimin, M. A. Wicaksono, M. F. Fadlurachman, and I. Ramli, "Rancang Bangun Sistem Keamanan dan Pemantau Tamu pada Pintu Rumah Pintar Berbasis Raspberry Pi dan Chat

- Bot Telegram,” *J. Penelit. Enj.*, vol. 23, no. 2, pp. 121–128, Nov. 2019.
- [19] R. Ganpatrao Sabale, “Comparative Study of Prototype Model For Software Engineering With System Development Life Cycle,” *IOSR J. Eng.*, vol. 02, no. 07, pp. 21–24, Jul. 2012.
- [20] F. Oura, T. Ainoya, A. Eibo, and K. Kasamatsu, “Prototyping Process Analyzed from Dialogue and Behavior in Collaborative Design,” H. Mori and Y. Asahi, Eds. Cham: Springer Nature Switzerland, 2023, pp. 545–556.