SMART VEHICLE IDENTIFICATION SYSTEM: AUTOMATIC PLATE NUMBER RECOGNITION BASED ON IOT FOR RESIDENTIAL ACCESS CONTROL

Ammar Aizat Khalil, Nazhatul Hafizah Kamarudin

Faculty of Information Science & Technology
Universiti Kebangsaan Malaysia
43600 Bangi, Selangor

Abstrak

Sistem Pengenalan Kenderaan Pintar adalah sistem pengurusan akses kediaman pintar yang direka untuk meningkatkan keselamatan dan kemudahan di kawasan perumahan berpagar. Projek ini menangani masalah biasa berkaitan kemasukan kenderaan yang tidak sah dan pengurusan tetamu yang tidak cekap, yang boleh mengganggu keselamatan dan menyebabkan ketidakselesaan bagi penduduk dan pentadbir. Masalah utama adalah kekurangan penyelesaian bersepadu dan automatik untuk menguruskan kenderaan penduduk, akses tetamu, dan pemantauan kemasukan masa nyata. Sistem tradisional sering bergantung pada penyimpanan rekod manual atau penyelesaian RFID/kod bar asas, yang mudah terjejas dengan kesilapan, kelewatan, dan ancaman keselamatan. Untuk menyelesaikan masalah ini, *smart vehicle identification system* mengintegrasikan aplikasi mudah alih (Android) dengan peranti IoT berasaskan ESP32-CAM untuk pengecaman plat nombor kenderaan automatik (ANPR) di pintu masuk. Sistem ini menggunakan Firebase sebagai backend awan untuk pengesahan, penyimpanan data, dan penyegerakan masa nyata. Penduduk dan pentadbir boleh mendaftarkan kenderaan dan pas tetamu melalui aplikasi, manakala ESP32-CAM mengimbas plat lesen di pintu gerbang dan menyemak dengan senarai putih yang disegerakkan awan. Sistem ini menguatkuasakan had pendaftaran untuk mencegah penyalahgunaan dan menyediakan log kemasukan masa nyata. Projek ini dibangunkan menggunakan senibina *Model-View-ViewModel* (MVVM) untuk aplikasi Android, Firebase untuk perkhidmatan *backend*, dan C++/Arduino untuk *firmware* ESP32-CAM. Pembangunan berulang dan maklum balas pengguna membimbing reka bentuk dan pelaksanaan. Hasil akhir adalah sistem yang teguh dan mesra pengguna yang mengautomasi akses kenderaan dan tetamu, meningkatkan keselamatan, dan memperlancarkan pengurusan untuk kedua-dua penduduk dan pentadbir. *Smart vehicle identification system* menunjukkan integrasi berkesan teknologi mudah alih, awan, dan IoT untuk menangani cabaran keselamatan sebenar di komuniti perumahan.

Abstract

Smart Vehicle Identification System is a smart residential access management system designed to enhance security and convenience in gated communities. The project addresses the common problem of unauthorized vehicle entry and inefficient manual guest management, which can compromise safety and cause inconvenience for residents and administrators. The core problem is the lack of an integrated, automated solution for managing resident vehicles, guest access, and real-time entry monitoring. Traditional systems often rely on manual record-keeping or basic RFID/barcode solutions, which are prone to errors, delays, and security breaches. To solve this, smart vehicle identification system integrates a mobile application (Android) with an IoT-based ESP32-CAM device for automatic number plate recognition (ANPR) at the entry gate. The system uses Firebase as a cloud backend for authentication, data storage, and real-time synchronization. Residents and administrators can register vehicles and guest passes through the app, while the ESP32-CAM scans license plates at the gate and checks them against a cloud-synced whitelist. The system enforces registration limits to prevent abuse and provides real-time logs of all entry attempts. The project was developed using the Model-View-ViewModel (MVVM) architecture for the Android app, Firebase for backend services, and C++/Arduino for the ESP32-CAM firmware. Iterative development and user feedback guided the design and implementation. The final outcome is a robust, user-friendly system that automates vehicle and guest access, improves security, and streamlines management for both residents and administrators. Smart vehicle identification system demonstrates the effective integration of mobile, cloud, and IoT technologies to address real-world security challenges in residential communities.

1.0 INTRODUCTION

As our world becomes increasingly connected, the rise of the Internet of Vehicles (IoV) has ushered in a new era of transportation, one brimming with the promise of enhanced safety, efficiency, and convenience. It is within this dynamic landscape that the development of the Smart Vehicle Identification System takes center stage. This innovative system is poised to revolutionize the way we manage and interact with our vehicles, leveraging the power of cutting-edge technologies to create a truly transformative experience.

At the heart of this system lies the seamless integration of Automatic Number Plate Recognition (ANPR) and Internet of Things (IoT) technologies. Imagine a world where your vehicle is effortlessly identified, and the availability of parking slots is monitored in real-time, right at your fingertips. This dynamic duo not only streamlines the parking management process but also provides invaluable data to administrators, empowering them to optimize the transportation infrastructure and address the evolving needs of the community.

But the Smart Vehicle Identification System goes beyond mere functionality, it seeks to engage and inspire. By incorporating gamification elements, such as points, badges and leaderboards, the system taps into our innate desire for a sense of achievement and belonging. Much like how educational institutions have harnessed the power of gamification to boost student motivation and academic success, this system aims to foster a similar sense of participation and investment among its users, ultimately transforming the way we experience and interact with transportation services.

As we stand on the cusp of a new era in IoT, the development of the Smart Vehicle Identification System represents a significant milestone. By seamlessly blending cutting-edge technologies and innovative gamification principles, this system promises to redefine the way we navigate our transportation landscape, delivering a truly transformative impact on our daily lives.

2.0 LITERATURE REVIEW

Smart Vehicle Identifcation System

This study discusses the access management system designed to enhance security and convenience in gated communities. With rapid advancements in communication and transportation technologies, IoT has emerged as a promising field to enhance safety, efficiency, and convenience in transportation systems. Effective detection of unauthorized vehicles has become a critical requirement to protect these systems from various threats that can compromise user safety. In this study, we will examine the various contemporary approaches and technologies used in access management system within IoT, as well as the challenges and opportunities in this field.

The study explores the use of Blockchain-based Secure Vehicle Communication, Federated Learning for Collaborative Intrusion Detection, and Secure V2X Communication using Quantum Cryptography. It also introduces a Smart Parking Management System (SPMS) that integrates Automatic Number Plate Recognition (ANPR) and Internet of Things (IoT) technologies. The SPMS system utilizes ANPR algorithms and AI Cloud to detect and extract

vehicle number plates with high accuracy, as well as IoT sensors to monitor parking slot availability in real-time. The system also includes automated data management and billing, and an Administrative Dashboard for efficient management and remote monitoring.

The study highlights the effectiveness of approaches like ANPR, machine learning, and blockchain in improving the accuracy and security of access management within IoT. However, it also identifies limitations such as imbalanced data, high computational resource requirements, and the feasibility of the system in real-world situations.

The key gaps in the research include a lack of studies on the integration of multiple technologies (such as deep learning and quantum cryptography) in IoV systems, and the limited exploration of the impact of attack detection on road safety and user experience. This study aims to fill these gaps by combining various technologies to develop a more efficient vehicle number plate detection system.

The study also suggests innovative solutions, such as utilizing more advanced ANPR techniques, integrating multiple security technologies, implementing online registration for visitor number plates, and ensuring access verification through the ANPR system. These approaches can enhance the overall security and efficiency of the IoT system, addressing the challenges identified in previous research.

3.0 METHODOLOGY

This study includes requirements analysis, conceptual model design, application development, usability testing and results. The methodology describes the methods to overcome the identified problems and explains the research process carried out.

3.1 Needs Analysis

The Needs Analysis looks at the important issues of vehicle identification and safety in the digital era, which is becoming more important with the rise of the Internet of Vehicles (IoV). At the core of this investigation is the main goal of the Smart Vehicle Identification System, which is to use automated number plate recognition to expedite the vehicle identification

procedure. Through the use of cameras and Automatic Number Plate Recognition (ANPR) technology, the system is able to recognise and record vehicle number plates, store the data in an organised manner, and display it to users.

According to a detailed description, ANPR technology is a specialised method created to automatically recognise license plates from pictures or videos. Optical Character Recognition (OCR) is used to turn the number plate picture into machine-readable text once the number plate has been carefully extracted from the backdrop using image processing methods. By overcoming the inherent limits of human recognition methods, the ANPR feature enables the system to recognise vehicle number plates with exceptional precision and lightning-fast processing rates.

By offering a digital platform that automates the vehicle identification procedure, the system primarily seeks to improve the effectiveness and security of entrance and exit management within a facility or residential area. By meeting the increasing need for automated and dependable vehicle access control systems, our contribution is well-positioned to give the target institution a more orderly and secure environment. The technology can reduce the burden for security staff, speed up reaction times, and reduce the possibility of human mistake or illegal vehicle access by automating the vehicle identification procedure.

3.2 Conceptual Model Design

The conceptual model design section outlines the functional requirements (FR) of the number plate recognition system, which represent the services provided to the users. These requirements serve as a guide for the system development, ensuring that the user needs are met and the problem is effectively addressed. The system has two (2) types of actors (users and admin) with specific requirements, including user registration, login, vehicle number plate verification, vehicle information storage, vehicle information display, and error message handling.

The system specifications are then detailed, covering the functional and non-functional requirements. The functional requirements align with the user requirements to ensure the system operates efficiently. These include a database connection, vehicle image registration,

number plate recognition, vehicle information storage, vehicle information display, and failure handling mechanisms. The non-functional requirements, on the other hand, address aspects such as restricted system access and a user-friendly interface, which contribute to the overall quality and usability of the system.

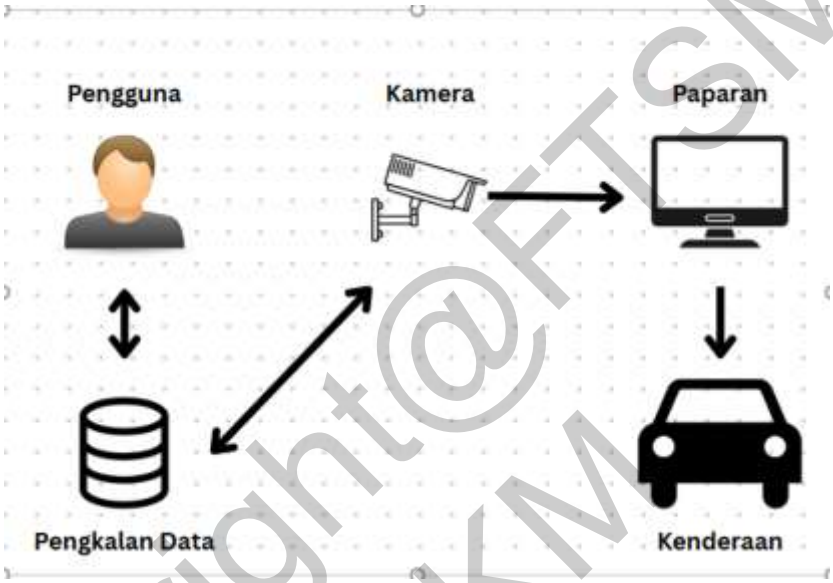

Figure 1 Conceptual Model Design

The overall system architecture is illustrated in Figure 1, which shows the workflow of the "GuardianGate" system. Users register their vehicles in the application, and the data is stored in the database. The camera then captures the vehicle's number plate and checks it against the database. Finally, the verification result is displayed on the screen. This architectural diagram provides a high-level overview of the system's components and their interactions, setting the stage for the detailed design and implementation phases.

4.0 RESULTS

4.1 System Development

The system was developed using an iterative and modular approach, integrating modern Android application development with IoT programming to enhance security and convenience within a housing community. The development utilized Kotlin, Jetpack Compose, and the MVVM architecture for the Android application, while the IoT components were programmed using C++/Arduino for the ESP32-CAM. The backend of the system leverages Firebase for authentication, real-time database management, and cloud storage solutions.

In the development phase, a smart residential access management solution was created that integrates an Android application with IoT technology. The implementation of the system is based on the requirements and design outlined in the project proposal, requirement specification, and design specification. The scope of this document includes an analysis of the development process, an explanation of critical code segments, and the system architecture that supports the interaction between the application and IoT devices. By focusing on these aspects, it provides clear guidance on how the system is developed and functions in the context of daily operations. This document is also related to several other documents that provide the necessary background and context for a better understanding of this system. For example, the project proposal provides an overview of the project's vision and goals, while the requirement and design specifications offer more detailed guidance on the functions and features that need to be incorporated into the system. The documents resulting from D6 include the user interface, source code, test plan, and user manual, all of which will support the utilization and maintenance of the "GuardianGate" system.

Key technologies used in the GuardianGate system include Android development with Kotlin and Jetpack Compose, Firebase for authentication, Firestore, and Realtime Database, as well as IoT programming with C++/Arduino for the ESP32-CAM and a cloud-based ANPR API by CircuitDigest.

4.2 System Testing

For the testing phase for the system, ensuring that the software and hardware components meet the specified requirements and function as expected. GuardianGate serves as a vehicle access management system that utilizes automatic number plate recognition technology to enhance security and convenience. The scope includes the planning, design, implementation, and reporting of tests for the Android application and the ESP32-CAM IoT device, covering both functional and non-functional requirements. Additionally, several key terms used in this document include UAT (User Acceptance Testing), ANPR (Automatic Number Plate Recognition), IoT (Internet of Things), and MVP (Minimum Viable Product).

i. Functional Testing

This table outlines the functional test cases conducted for the GuardianGate system. Each test case includes a unique ID, a description of the test, the steps to execute it, the test data used, the expected results, and the criteria for pass/fail status. These tests are designed to ensure that the system functions correctly and meets the specified requirements.

Table 1: Tested Function

Test Case ID	Description	Steps	Test Data	Expected Result	Pass/Fail Criteria
TC-01	User Login	1. Open the application 2. Enter email, password, and admin code (if needed) 3. Tap login	Email, Password	User is authenticated and directed to the dashboard	User logs in and the dashboard loads
TC-02	Add Vehicle	1. Log in as a resident 2. Navigate to Vehicle Management 3. Add new vehicle details 4. Save	License Plate, Model, Color	Vehicle appears in the list and is added to the whitelist	Vehicle is listed and recognized by ESP32
TC-03	Create Guest Pass	1. Log in as a resident 2. Create a guest pass 3. Enter guest details 4. Save	Guest Name, License Plate	Guest pass is created and added to the system	Guest pass is listed and recognized by ESP32
TC-04	Unauthorized Vehicle Entry	1. ESP32 scans an unregistered plate	License Plate	Access denied, red LED flashes, log created	Access denied, log recorded in Firebase
TC-05	Whitelist Synchronization	1. Add/remove vehicle/guest pass 2. Check ESP32 whitelist	-	ESP32 whitelist updates in real-time	ESP32 allows/denies access based on current data
TC-06	Vehicle Registration Limit	1. Register vehicles up to the limit 2. Try to register one more	User ID, Vehicle Data	System prevents registration, shows error	Error displayed, vehicle not added
TC-07	Guest Pass Registration Limit	1. Register guest passes up to the limit 2. Try to register one more	User ID, Guest Data	System prevents registration, shows error	Error displayed, guest pass not added

In test case 1, verifies the user login functionality of the GuardianGate application. The process begins with the user opening the app, followed by entering their email, password, and an optional admin code if required. Upon tapping the login button, the system should authenticate the user. The expected outcome is that the user successfully logs in and is redirected to the dashboard, confirming that the authentication mechanism works correctly and that users can access their accounts seamlessly.

In test case 2, the functionality for adding a vehicle to the system is evaluated. After logging in as a resident, the user navigates to the Vehicle Management section and inputs the details of a new vehicle, including its license plate, model, and color. Once the information is saved, the vehicle should appear in the list and be added to the whitelist. This ensures that the system correctly processes new vehicle entries and that the ESP32 device can recognize them, thereby enhancing the overall vehicle management capability.

This test case 3 focuses on the creation of guest passes within the GuardianGate system. The resident logs in and initiates the guest pass creation process by entering the relevant guest details. After saving the information, the system should generate a guest pass and include it in the list for recognition. This test confirms that the application can effectively manage guest access and that the ESP32 device recognizes the guest pass, thereby facilitating temporary access for visitors.

For test case 4, assesses the system's response to unauthorized vehicle entries. The ESP32 device scans a license plate that is not registered in the system. The expected result is that access is denied, indicated by a flashing red LED, and a log entry is created for security purposes. This test ensures that the system effectively prevents unauthorized access and maintains a record of such attempts, thereby enhancing security measures.

In this test case 5, evaluates the real-time synchronization of the whitelist between the GuardianGate application and the ESP32 device. The user can add or remove vehicles and guest passes, and the system must reflect these changes immediately in the ESP32 whitelist. The expected outcome is that the ESP32 updates its whitelist in real-time, allowing it to grant or deny access based on the most current data. This functionality is crucial for maintaining accurate access control.

In this test case 6, the system's handling of vehicle registration limits is tested. The user registers vehicles up to the predefined limit and then attempts to register one additional vehicle. The system should prevent this registration and display an error message, confirming that it enforces the registration limit correctly. This test ensures that the application adheres to the specified constraints, preventing potential overload or misuse.

Similar to the vehicle registration limit test case, this test case 7 evaluates the system's management of guest pass registrations. The resident registers guest passes up to the allowed limit and then tries to register one more. The system should block this attempt and show an error message, confirming that it correctly enforces the guest pass limit. This functionality is essential for maintaining control over temporary access rights and ensuring that the system operates within its defined parameters.

ii. Usability Testing

Unit testing is conducted using the built-in tools available in Android Studio, which allows developers to test individual components or modules of the application in isolation. For the ESP32, manual code review is performed to ensure that the firmware operates correctly. This phase focuses on verifying that each unit of code functions as intended, identifying any bugs or issues at an early stage, and ensuring that the smallest parts of the application are reliable before moving on to more complex testing.

Integration testing simulates real-world scenarios to evaluate how different modules of the system work together. For instance, it tests scenarios such as vehicle entry and the use of guest passes to ensure that all components interact correctly. This phase is crucial for identifying issues that may arise when combining various parts of the system, ensuring that data flows seamlessly between modules and that the overall functionality meets the specified requirements.

System testing involves end-to-end testing of the entire application, from user login to door access. This comprehensive testing phase ensures that all components of the system work together as expected in a real-world environment. It verifies that the application meets its functional and non-functional requirements, including performance, security, and usability. By simulating user interactions, this phase helps to identify any potential issues that could affect the user experience or system performance.

UAT is conducted with a group of target users, including residents and administrators, to validate that the system meets their needs and expectations. This testing phase is essential for gathering feedback from actual users, ensuring that the application is user-friendly and functions as intended in real-life scenarios. UAT helps to identify any remaining issues before the system goes live and provides an opportunity for users to influence the final adjustments to the system.

4.3 Testing Result

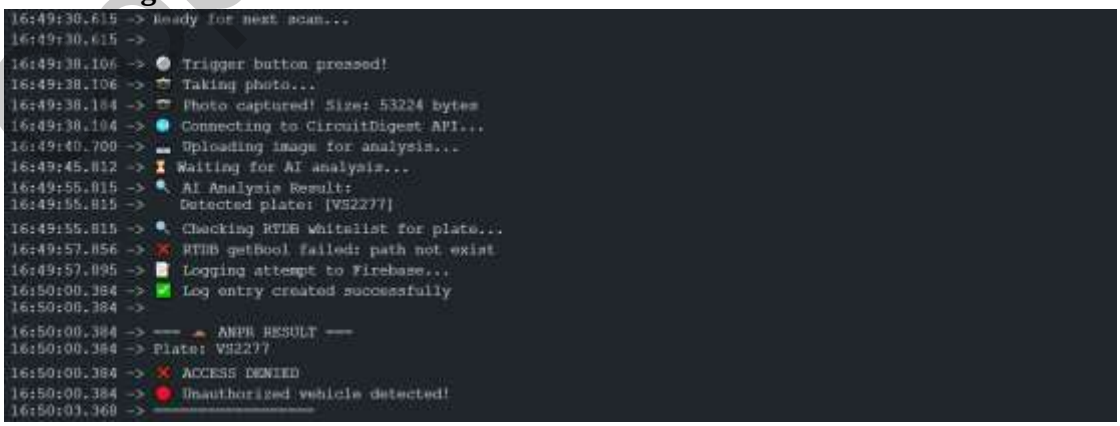

Figure 2: Model Performance Metrics

a. Unregistered Vehicle

Result: ACCESS DENIED, Unauthorized vehicle detected!

Figure 2 shows that the system functions correctly by detecting unregistered vehicles and denying access. This aligns with the security and access management requirements set for this system.

Figure 3: Model Performance Metrics

b. Registered Vehicle

Result:

ANPR RESULT, Plate: VS2277

ACCESS GRANTED, Welcome! Gate opening...

Figure 3 demonstrates that the system successfully detects and verifies the license plate number of a registered vehicle through the ANPR (Automatic Number Plate Recognition) process. Once the registered vehicle is verified, the system grants access by opening the gate.

Overall, the test results show that the **GuardianGate** system can effectively detect and control vehicle access, regardless of whether the vehicle is registered or not. This meets the system's primary objective of enhancing security and ease of access management.
For registered vehicles, the system performs well in detecting license plates, verifying presence in the whitelist, and automatically opening the gate. This indicates good integration between the ANPR module, database, and gate control mechanism.
In summary, the testing results confirm that the GuardianGate system operates effectively and

fulfills the specified requirements. No significant issues were encountered, and the system can be implemented successfully.

Table 2: Testing Results

Test Case	Result	Remarks
TC-01	Pass	Successful login for authorized user
TC-02	Pass	Vehicle added and recognized by ESP32
TC-03	Pass	Guest pass functions as expected
TC-04	Pass	Unauthorized vehicle denied access
TC-05	Pass	Real-time whitelist synchronization
TC-06	Pass	System correctly blocks registration of a 3rd vehicle
TC-07	Pass	System correctly blocks registration of a 2nd guest pass

5.0 CONCLUSION

Overall, this project has successfully developed GuardianGate, an integrated access management system for residential communities. This system combines a modern Android application, cloud-based backend, and IoT-based camera devices to automate and secure vehicle and visitor entry.

The key strengths of the GuardianGate system include real-time and automated vehicle and visitor access control using ANPR technology, cloud-based management and synchronization

through Firebase, user-friendly interfaces for both residents and administrators, enforced registration limits to prevent system abuse, and comprehensive entry logs for security auditing.

However, the system also has some limitations, such as ANPR accuracy depending on camera quality and lighting conditions, support for only one type of IoT device (ESP32-CAM), the requirement for internet connectivity for real-time operation, and static registration limits that may not suit all community needs.

For future improvements, suggestions include enhancing ANPR accuracy, supporting multiple IoT device types, allowing customizable registration limits, adding offline functionality, and integrating additional security features like facial recognition. Overall, GuardianGate demonstrates the potential of integrating mobile, cloud, and IoT technologies to address real-world security and management challenges in residential environments.

This project has gone through a comprehensive software development process, covering the planning, requirements analysis, design, implementation, and testing phases. The thorough requirements analysis and design process have enabled the development of a system that meets user needs. However, the usability testing results indicate that there are some aspects that require improvement, such as adding clearer instructions for functionalities perceived as complex by users.

In conclusion, this project has successfully produced an integrated, automated, and secure residential access management system. GuardianGate demonstrates the potential of using mobile, cloud, and IoT technologies to address security and management challenges in residential communities. The development and testing experience gained from this project will be a valuable guide for future similar projects.

6.0 APPRECIATION

Faculty of Technology and Information Science Grant FTSM 1 and Mutiara Grant A193256.

7.0 REFERENCES

Seo. 2024, June 21. Menavigasi Masa Depan: Peningkatan Teknologi Internet

Kenderaan (IoV) - Penyelesaian Peranti Penjejakan GPS Tersuai .

Internet of Vehicles (IoV): Revolutionizing Transportation of Tomorrow Riding on 5G and Edge AI - Wipro.

Rani, P., et al. 2023. Federated Learning-Based Misbehaviour Detection for the 5G

Enabled Internet of Vehicles. IEEE Transactions on Consumer Electronics.

Shi, Z., et al. 2019. DeepWindow: An Efficient Method for Online Network Traffic Anomaly Detection. IEEE Transactions on Consumer Electronics.

Kang, B., Kim, D., & Choo, H. 2016. Internet of Vehicles: Applications, Services, and Challenges. *International Journal of Distributed Sensor Networks, 12*(9):1-13.

Sharma, V., You, I., Palmieri, F., Jayaraman, R., & Qiu, Y. 2019. Secure and Efficient Protocol for Internet of Vehicles (IoV) with Blockchained Data and Certified Public Keys. *IEEE Access, 7*, 100384-100401.

Yin, C., Zhu, Y., Fei, J., & He, X. 2017. A Deep Learning Approach for Intrusion Detection

Using Recurrent Neural Networks. *IEEE Access, 5*, 21954-21961.

Porambage, P., Okwuibe, J., Liyanage, M., Ylianttila, M., & Taleb, T.2018. Survey on

Multi-Access Edge Computing for Internet of Things Realization. *IEEE Communications*

Surveys & Tutorials, 20(4), 2961-2991.

Zeng, Y., Zhao, R., & Chen, W.2019. Quantum-Secure Communication for the Internet of Vehicles. *IEEE Network, 33*(5): 136-141.

Jawale, M., William, P., Pawar, A., & Marriwala, N. 2023. Implementation of number plate detection system for vehicle registration using IOT and recognition using CNN. *Measurement Sensors, 27*, 100761.

Ditta, A., Ahmed, M. M., Mazhar, T., Shahzad, T., Alahmed, Y., & Hamam, H. (2024). Number plate recognition Smart Parking Management System using IoT. *Measurement Sensors*, 101409.

Larman, C. 2012. Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development (3rd ed.). Prentice Hall.

AraNaldinho. (n.d.). Applying-uml-and-patterns-3rd-editiom/Applying UML and Patterns 3rd

Edition.pdf at master ·AraNaldinho/Applying-uml-and-patterns-3rd-editiom. GitHub.

Ditta, A., Ahmed, M. M., Mazhar, T., Shahzad, T., Alahmed, Y., & Hamam, H. 2024. Number plate recognition Smart Parking Management System using IoT. *Measurement Sensors*, 101409.

Krisna, R. 2025, June 27. *How to use ESP32 CAM for Automatic Number Plate Recognition (ANPR)*. CircuitDigest.

Muhd Ammar Aizat Khalil (A193256)
Dr. Nazhatul Hafizah Kamarudin
Faculty of Information Technology & Science
National University of Malaysia