American Journal of Smart Technology and Solutions (AJSTS)

ISSN: 2837-0295 (ONLINE)

VOLUME 4 ISSUE 2 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Smart Technology and Solutions (AJSTS)

Volume 4 Issue 2, Year 2025
ISSN: 2837-0295 (Online)
DOI: https://doi.org/10.54536/ajsts.v4i2.4717
https://journals.e-palli.com/home/index.php/ajsts

Parking Occupant Management System Using QR Code Solutions With AES Algorithm

Albert I. Luzuriaga[1], Gawain Destiny A. De Groot[1], Jerold E. Cortez[1], Nathaniel U. Babanto[1], Meridel C. Ejusa[1*]

Article Information

Received: March 12, 2025

Accepted: April 17, 2025

Published: August 28, 2025

Keywords

AES Encryption, Data Security, Parking Management System, QR Code, Vehicle Cataloging

ABSTRACT

This study presents a Parking Occupant Management System utilizing QR Code Solutions integrated with Advanced Encryption Standard (AES) technology to address inefficiencies in manual vehicle cataloging within educational institutions. Automating this process improves accuracy, efficiency, and security while ensuring adaptability across diverse school parking environments. QR codes facilitate seamless logging of vehicle entries and exits, embedding contact information that enables security guards to communicate directly with vehicle owners in case of issues. The incorporation of AES encryption provides robust protection for sensitive data, safeguarding it against unauthorized access. Designed as a mobile application for Android devices, the system empowers security guards to scan QR codes in real time, effectively recording vehicle activity. Focusing on educational institutions in General Santos City, this study demonstrates significant enhancements in parking management through automation and improved data protection. The system establishes a new standard for secure data management in parking operations and holds promise for application in sectors such as commercial and residential complexes. By offering a scalable solution that enhances efficiency while ensuring data security, it contributes to better resource management. Future developments may explore security enhancements and expansion to platforms beyond Android, increasing accessibility and catering to a wider range of parking management needs. Ultimately, this system serves as a blueprint for modernizing parking management, paving the way for smarter, more secure urban environments.

INTRODUCTION

The increasing vehicle populations and urbanization pose challenges in managing parking operations on college and university campuses (Dokania *et al.,* 2020). This growing demand highlights the urgent need for efficient parking solutions. Traditional manual cataloging methods fall short—they are slow, prone to mistakes, and lack strong security measures, resulting in operational hiccups and safety risks. To tackle this, this research proposes a QR-based vehicle management system paired with the Advanced Encryption Standard (AES) encryption algorithm to enhance the handling of vehicle entries and exits in university parking areas securely and efficiently.

This QR-based system with AES encryption offers a major improvement over outdated methods, delivering benefits to both campus parking facilities and vehicle owners. It strengthens security by encrypting QR codes with AES, safeguarding parking occupants' data from unauthorized access or tampering—only a decryption key can unlock intercepted details. The system also optimizes vehicle entry and exit through quick QR scanning, cutting down wait times, improving traffic flow, and boosting overall parking efficiency by reducing human errors. While urban parking systems have embraced technological upgrades, campus parking has lagged, often sticking to manual processes with little use of QR technology. This gap has weakened communication between parking users and attendants, increasing risks like theft, vandalism, accidents, and legal issues.

The main goal of this work is to create a secure, efficient, and user-friendly parking management system for educational institutions using QR code technology and AES encryption. By adopting automation and focusing on user needs, this research improves parking operations, enhances security, and fosters better communication, overcoming the drawbacks of manual methods. The author's key contribution is showing how these technologies can modernize campus parking, ensuring lasting efficiency, safety, and convenience as campuses adapt to rising vehicle numbers and urban growth.

LITERATURE REVIEW

Improving vehicle management systems on university campuses has become increasingly important in our rapidly changing environment. This literature review examines how Quick Response (QR) codes and the Advanced Encryption Standard (AES) encryption algorithm can enhance the security and efficiency of campus parking management. By leveraging these advanced technologies, the review draws on significant contributions from prior studies to justify their integration into parking systems, highlighting their potential to streamline operations and bolster data security.

QR Codes in Vehicle Management

As urban environments evolve, integrating QR codes

[1] College of Engineering and Technology Education, Holy Trinity College, General Santos City, Philippines
[*] Corresponding author's e-mail: htc_ejusam@online.htcgsc.edu.ph

into vehicle management systems significantly enhances user convenience by enabling faster queuing processes and minimizing waiting times. Lin, Rivano, and Le Mouël (2017) classify smart parking ecosystems, identifying essential components and usage trends that underscore the effectiveness of QR-based systems in optimizing parking operations. Their findings suggest that QR codes improve user experience and operational efficiency by streamlining data collection and vehicle tracking. Similarly, Barriga *et al.* (2019) explore the primary components and usage patterns of smart parking systems, emphasizing how QR codes, alongside sensors and software, enhance functionality and urban mobility. Kadu *et al.* (2014) further address urban parking challenges by introducing a QR code-based smart parking system that identifies users, provides real-time parking information, reduces traffic congestion, and increases user satisfaction. These studies collectively highlight QR codes as a key variable in improving parking management efficiency.

Encryption and Security

The combination of QR codes with AES encryption addresses crucial security concerns in vehicle management systems. Chai *et al.* (2023) stress the necessity of incorporating AES encryption into QR codes to protect sensitive information, preventing data leakage and unauthorized access while preserving system integrity. Ajini Asok and Arun (2016) explore the use of AES-128 encryption to secure private data within QR codes, mitigating risks like eavesdropping due to their visual nature. Their approach ensures safe verification without delays, enhancing security in data exchange. Additionally, Agarwal and Malik (2022) investigate steganography with QR codes and AES encryption, emphasizing the preservation of image quality to conceal data effectively. These contributions justify AES as a robust cryptographic mechanism for securing QR-based systems, supporting its adoption in campus parking contexts.

Performance and Efficiency

The efficiency of AES encryption is vital for its practical implementation in parking systems, particularly on resource-constrained devices. Doomun, Doma, and Tengur (2008) assess AES in Cipher Block Chaining (CBC) mode, finding that optimized implementations improve encryption speed by 12% to 30%, though with increased memory demands. Almuhammadi and Al-Hejri (2017) analyze AES block cipher modes like Electronic Codebook (ECB) and CBC, evaluating encryption time and throughput to guide mode selection. Vaidehi and Rabi (2014) highlight ECB's vulnerabilities and advocate for CBC to enhance security and effectiveness. These studies provide a foundation for optimizing AES performance, a critical variable for real-time parking applications.

Applications and Case Studies

Insights from related fields reinforce the applicability of QR codes and AES encryption in parking management. Ferdiansyah, Hadiana, and Rakhmat (2021) demonstrate their integration in healthcare administration, where encrypted QR codes secure sensitive data, offering a model for parking systems. Agun, Rabie, and Satoquia (2022) showcase a QR-based automated ticketing system for traffic violations, improving data collection and transaction efficiency—principles applicable to parking operations. Gangurde *et al.* (2022) further emphasize the broader implications of these technologies, noting their benefits in security and user experience across contexts. These case studies support the hypothesis that QR codes and AES can transform campus parking management.

Hardware Implementations

Efficient hardware implementations enhance AES applicability in parking systems. Rachh *et al.* (2012) propose two AES architectures using composite field arithmetic, optimizing S-boxes and operations like MixColumns for encryption and decryption. Their designs improve processing efficiency, making them suitable for mobile and embedded systems in parking management. This hardware focus complements software-based security measures, reinforcing AES as a versatile solution.

In conclusion, the literature underscores the critical role of QR codes and AES encryption in modernizing parking management systems on university campuses. These technologies address security, efficiency, and user experience challenges, justifying their adoption and suggesting hypotheses for further research, such as their impact on reducing parking delays and enhancing data protection.

MATERIALS AND METHODS

This section outlines the materials, tools, and methodologies employed to develop and evaluate the Parking Occupant Management System Using QR Code Solutions with AES Algorithm. The system was designed to automate vehicle cataloging, enhance data security, and improve parking management efficiency in educational institutions within General Santos City. The approach is detailed below, structured into subsections for clarity, providing sufficient information to replicate the study while maintaining a concise narrative.

System Development Methodology

In developing the parking occupant management system using QR code solutions with AES algorithm, the researchers used the Iterative Waterfall Model. The f low of this model takes you through system level requirements, requirement analysis, design, implementation, testing, integration deployment, and maintenance in a structured way. This is different from the traditional waterfall project management model, where each stage is fed feedback from all stages behind it, as opposed to the classic model comparison which just checks for similarities or differences between aspects of project management in practice.

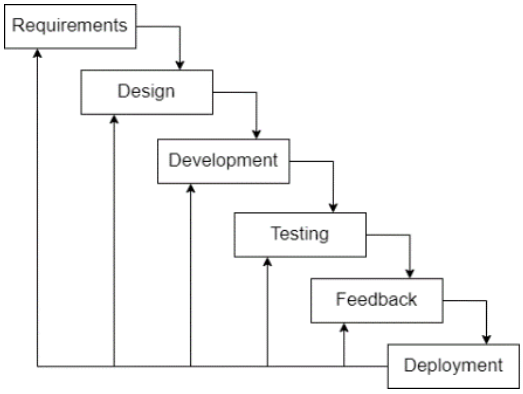

Figure 1: Iterative Waterfall Model of Software Development Life Cycle

Requirement Analysis

The initial phase involved analyzing the existing manual parking management processes in educational institutions to identify inefficiencies and define system requirements. Data were collected through interviews conducted with stakeholders, such as security guards and administrative personnel, from institutions like General Santos Doctors' Medical School Foundation Inc. For instance, interviews revealed that parking management relied on manual steps: occupants completed registration forms, administrators processed permits, and guards logged vehicle entries and exits manually. These processes were prone to errors and delays, necessitating automation.

The collected data included occupant details (full name, contact number, address) and vehicle information (license plate number, type, color, brand, model), which were critical for system functionality and security verification. This information was securely stored in a MySQL database, forming the basis for QR code generation and access control.

System Design and Architecture

The system was designed as a multi-component architecture integrating web and mobile platforms. Key components included:

Frontend Technologies

- Vue.js with Vuetify: Used for the web interface, providing reactive data binding and pre-designed UI elements (e.g., buttons, text fields) for a consistent and intuitive user experience.
- Flutter with Material.dart: Employed for the Android mobile app, ensuring a clean and intuitive design aligned with Google's Material Design guidelines.

Backend Technologies

- PHP Native via RESTful APIs: Managed backend logic, such as form processing and database interactions, using HTTP methods (GET, POST) with Axios for communication.
- MySQL: Stored structured data, including occupant profiles, vehicle details, and parking logs.
- XAMPP: Provided a local development environment with Apache, MySQL, PHP, and Perl.

Cryptographic and QR Code Tools

- Crypto-JS: A JavaScript library implementing AES encryption in Cipher Block Chaining (CBC) mode with PKCS7 padding, used to encrypt occupant and vehicle IDs.

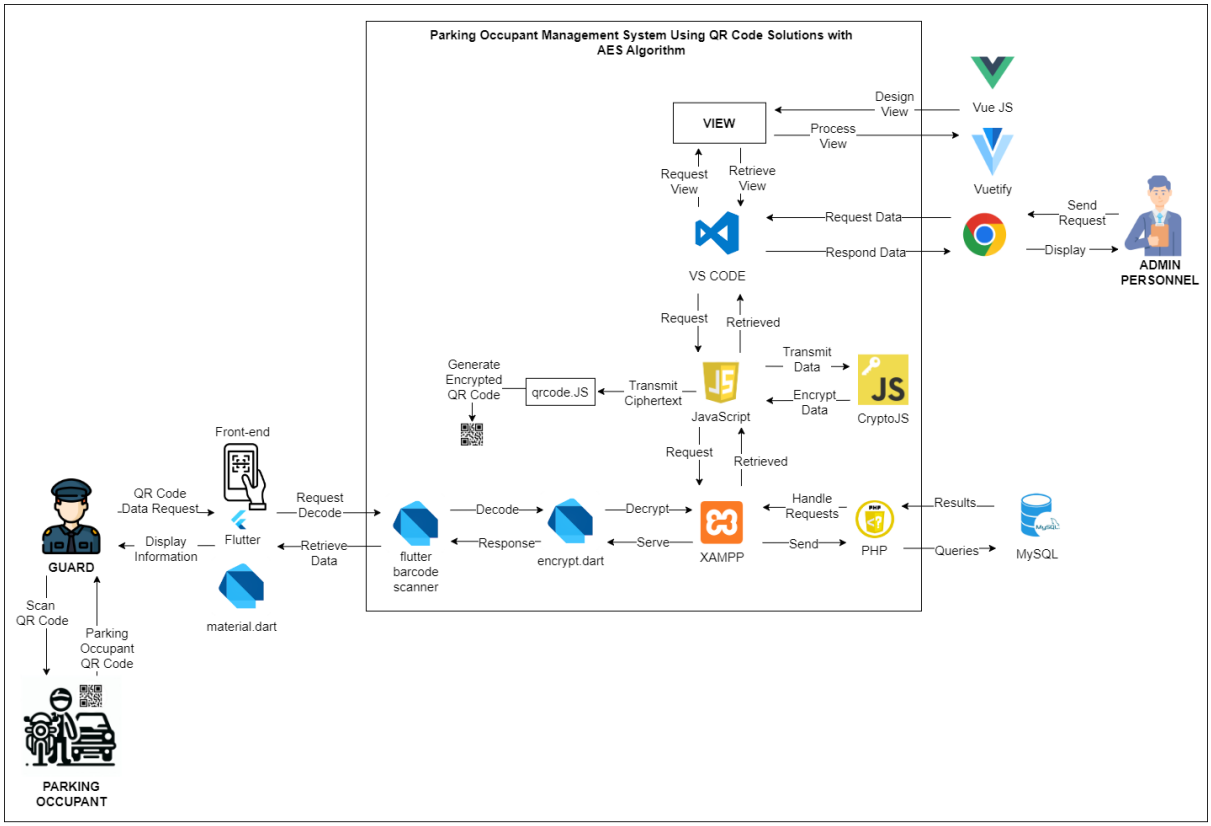

Figure 2: System Architecture

- Encrypt.dart: A Dart library for AES decryption in CBC mode with PKCS7 padding, used in the mobile app to decode encrypted QR code data.
- QRCode.js: Generated QR codes embedding encrypted data.
- Flutter_barcode_scanner: A Flutter plugin for scanning QR codes on Android devices

The system architecture supported secure data flow, with encrypted occupant and vehicle IDs embedded in QR codes, scanned by guards to log entries and exits.

The Entity Relationship Diagram detailed the database structure, comprising ten interconnected tables to manage

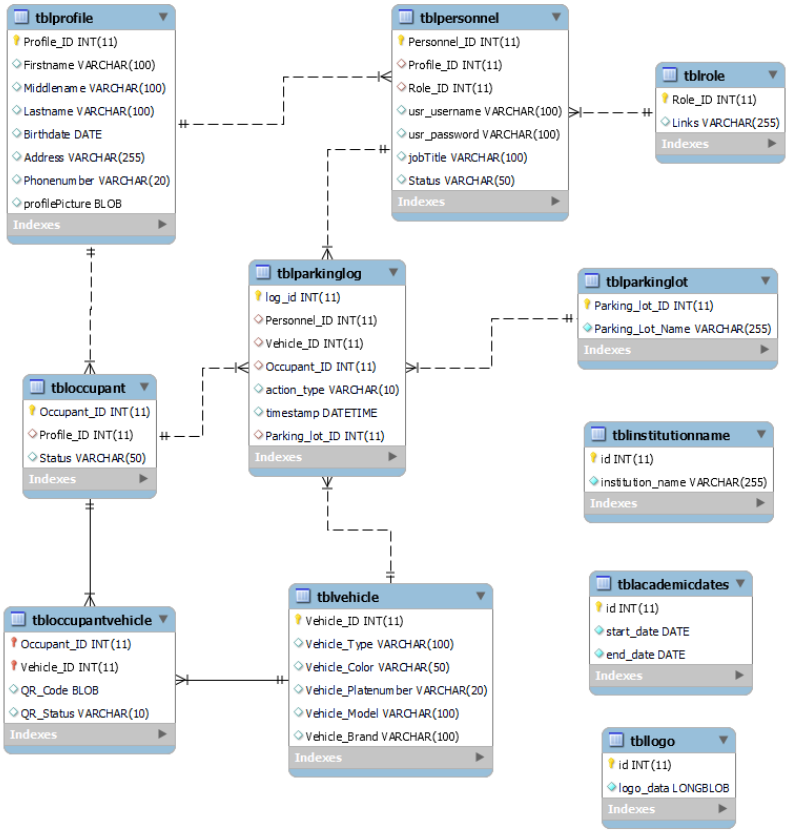

Figure 3: Entity Relationship Diagram of the Database

occupant profiles, vehicle data, and parking logs efficiently.

Implementation Details

Data Collection and Encryption

Occupants registered via a web interface, providing personal and vehicle details. These data were encoded into a JSON string (e.g., {"vehicleId": 65, "occupantId": 126}; encrypted using the AES-CBC algorithm implemented in Crypto-JS. The encryption process, detailed, involved:

1. Generating a random 16-byte Initialization Vector (IV).
2. Encrypting the JSON string with a predefined AES key (stored as an environment variable) in CBC mode with PKCS7 padding.
3. Outputting a Base64-encoded string combining the IV and ciphertext (e.g., MM/sbt5xTvvBUVWv16nslg==:1tr4ZmBEInxw+FoRO7mAgeSa5mOthdrlpI6Dy9nkFr5xs81s/9ii5RNsXiSOLu+J; Appendix E, p. 77). This encrypted data was embedded into QR codes using QRCode.js, printed, and affixed to vehicles for scanning.

QR Code Generation and Scanning

The QR code generation process linked encrypted Occupant ID and Vehicle ID to each vehicle, ensuring secure identification. The mobile app, developed in Dart using Flutter, utilized flutter_barcode_scanner to decode QR codes. Upon scanning, the app extracted the Base64-encoded data, decrypted it using encrypt.dart, and retrieved the original JSON string via the AES key and IV, enabling guards to log vehicle actions.

AES Algorithm Implementation

The AES encryption adhered to the standard outlined by the National Institute of Standards and Technology (NIST) in [FIPS 197], implemented in Cipher Block Chaining (CBC) mode as described by Doomun *et al.* (2008). Modifications to the standard included the use of a fixed AES key in Base16 format and a randomly generated IV for each encryption to bolster security.

In CBC mode, each plaintext block is XORed with the previous ciphertext block before encryption, with the IV serving as the initial vector for the first block. The encryption process for each block i is defined as:

$C_i = E_k (P_i \oplus C_{(i-1)})$, with $C_0 = IV$

The decryption process reverses this operation to recover the original plaintext, expressed as:

$P_i = D_K (Ci) \oplus C_{(i-1)}$, with $C_0 = IV$

This implementation ensured both data integrity and confidentiality. The use of a random IV per encryption guaranteed that identical plaintext blocks produced distinct ciphertexts, significantly enhancing the system's security.

Testing and Evaluation

The system underwent thorough testing to assess accuracy, efficiency, and security:

- Unit Testing: Verified individual components (e.g., encryption, QR code scanning) using Microsoft Visual Studio Code as the primary IDE for debugging.
- Integration Testing: Ensured seamless interaction between web, mobile, and backend components.
- Security Testing: Confirmed that encrypted QR codes were unreadable by third-party scanners (e.g., Google Lens), validating AES effectiveness.
- User Testing: Conducted with five respondents from educational institutions on October 18, 2024, using a survey. Respondents rated interface, functionality, usability, experience, and security on a 1-5 scale, yielding a mean score of 5.0 (Very Satisfied) across all categories.

Testing focused on real-time logging accuracy, QR code scanning speed, and data protection, with results indicating high reliability and user satisfaction.

Deployment

The system was deployed in educational institutions in General Santos City, operating within the institution's WLAN for enhanced security. The deployment phase involved:

1. Installing the mobile app on institution-provided Android devices.
2. Configuring the MySQL database on a local XAMPP server to store parking data.
3. Distributing QR codes to registered occupants (faculty, staff, students).

Deployment ensured that guards could scan QR codes to log vehicle entries and exits, with logs stored securely and accessible only within the institution's network.

Data Analysis

Data collected included parking logs (e.g., Log ID, Vehicle ID, timestamp, action type; and user feedback. Logs were analyzed to evaluate system performance, such as entry/exit frequency and error rates. Survey responses were quantified to assess user satisfaction and security perceptions. The AES encryption's effectiveness was validated by its inability to be decrypted by unauthorized tools, ensuring data confidentiality.

RESULTS AND DISCUSSION

This section presents the outcomes of the evaluation of the Parking Occupant Management System Using QR Code Solutions with AES Algorithm, conducted within educational institutions in General Santos City, and discusses their significance in the context of modern parking management challenges. The evaluation, based on a survey of five respondents, assessed the system across five key dimensions: Interface, Functionality, Usability, Experience, and Security. The results indicate exceptional user satisfaction, with a consistent mean score of 5.0 (on a 1–5 scale, where 5 denotes "Very Satisfied") across all evaluated criteria, highlighting the system's effectiveness in automating vehicle cataloging and enhancing data security through AES encryption.

Summary of Key Findings

The survey results demonstrate that the Parking Occupant Management System excels in delivering a user-friendly, functional, and secure solution for parking management. Respondents universally praised the system's consistent interface design across web and mobile platforms, noting its intuitive layout and clear feedback mechanisms, such as pop-up messages, which enhance usability. The system's functionality, particularly its ability to accurately process QR codes and update parking occupancy in real time, was rated highly, indicating seamless integration of essential parking management features. Usability was a standout feature, with first-time users finding navigation effortless and QR code scanning smooth and efficient. In terms of overall experience, respondents reported significant improvements in convenience and time savings, attributing these benefits to the system's reliable performance and the unobtrusive integration of AES encryption, which operates without compromising speed. Most notably, the security dimension received unanimous approval, with users expressing strong confidence in the AES encryption's ability to protect sensitive data, such as personal and vehicle information, during QR code scanning and transmission.

As shown in Table 1, the system achieved a total mean score of 5.0 across all sections, reflecting its exceptional performance in meeting user expectations.

Table 1 : Summary of Survey Results

Section	Mean Score	Verbal Description
Interface	5.0	Very Satisfied
Functionality	5.0	Very Satisfied
Usability	5.0	Very Satisfied
Experience	5.0	Very Satisfied
Security	5.0	Very Satisfied

Significance of the Results

The uniformly high satisfaction scores underscore the system's success in addressing key challenges in parking management, particularly within educational settings. The flawless mean score of 5.0 across all dimensions suggests that the system not only automates the manual cataloging process effectively but also elevates user trust through robust security measures. A critical factor in this success is the implementation of AES encryption, which ensures that sensitive data—such as occupant and vehicle IDs embedded in QR codes—remains protected against unauthorized access. This is particularly significant in

an era where data breaches and privacy concerns are escalating, especially in digital systems managing personal information. The respondents' confidence in the system's security, as evidenced by their approval of features like the prevention of QR code decoding by third-party tools (e.g., Google Lens), highlights AES encryption as a cornerstone of the system's value proposition.

Beyond security, the system's ability to improve parking operations through QR code technology offers practical benefits. The real-time logging of vehicle entries and exits, facilitated by efficient QR code scanning, reduces human error and administrative overhead compared to traditional manual methods. This efficiency is vital for educational institutions, where parking facilities often face high demand and limited resources. The seamless user experience, from intuitive navigation to time savings, further positions the system as a user-centric solution that enhances operational flow without sacrificing security.

Comparison with Recent Developments and Novelty

In the context of recent advancements in parking management and IoT-based systems, the integration of AES encryption with QR code technology distinguishes this work from existing solutions. Recent literature emphasizes the growing importance of data security in smart systems, with studies noting that many parking management platforms lack robust encryption, leaving them vulnerable to unauthorized access (e.g., Chai *et al.,* 2023, on secure QR-based systems). Unlike these systems, the Parking Occupant Management System leverages AES encryption to safeguard data at rest and during transmission, addressing a critical challenge in the field. This focus on security aligns with current trends toward privacy-centric design in digital infrastructure, particularly as urban environments increasingly adopt smart technologies.

Moreover, the system's adaptability to educational institutions—a setting often overlooked in favor of commercial or municipal parking solutions—adds to its novelty. While some smart parking systems prioritize features like space allocation or payment processing (Lin *et al.,* 2017), this system emphasizes secure communication between parking attendants and vehicle owners via encrypted QR codes. This capability fills a gap in campus parking management, where manual processes have historically limited efficiency and responsiveness to incidents like unauthorized parking or emergencies.

Supporting Visuals

The system's automated workflow and security features are captured in three key figures, providing a clear visual overview of its operational efficiency and data protection capabilities. These visuals highlight the interactions within the system and the encryption-decryption processes that safeguard sensitive information.

Figure 4 shows the automated workflow of the system. Parking occupants submit personal information to generate QR codes, guards scan these codes to manage parking logs, and admin personnel oversee operations, making the entire process more organized and efficient.

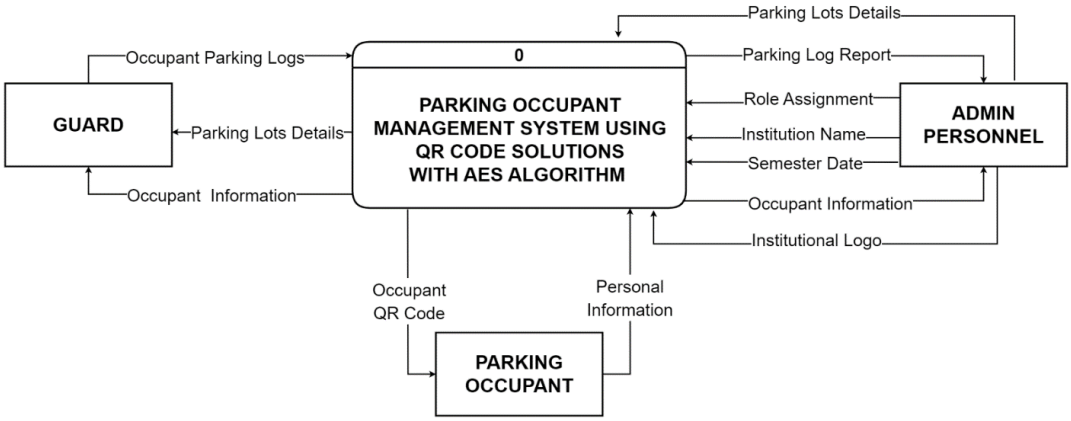

Figure 4: Context Diagram

Figure 5 illustrates the AES encryption process, where plaintext data is transformed into secure ciphertext. This encrypted data is embedded into QR codes, ensuring that access remains protected and confidential.

Figure 6 shows the AES decryption process, reversing the encryption to retrieve the original data from the QR codes. This step ensures that only authorized personnel can access the information, maintaining data integrity and security.

Together, these figures demonstrate how the system enhances parking management efficiency while employing robust security measures. The inclusion of both the AES Encryption Flow (Figure 5) and AES Decryption Flow (Figure 6) emphasizes the complete cycle of data protection, from securing information to safely retrieving it, making the system a notable advancement in secure parking management.

CONCLUSION

The Parking Occupant Management System using QR Code Solutions with AES Algorithm was successfully

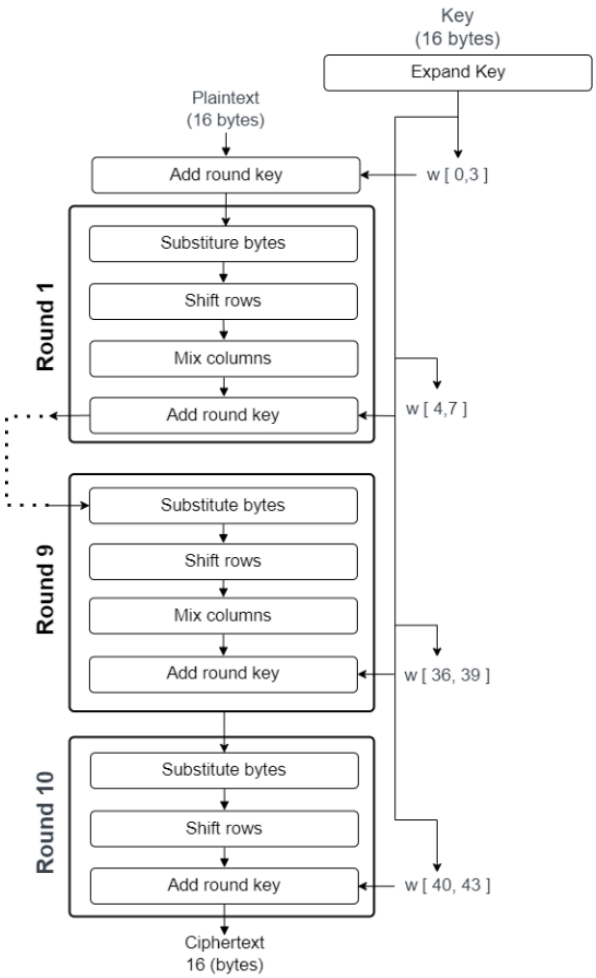

Figure 5: AES Encryption Flow

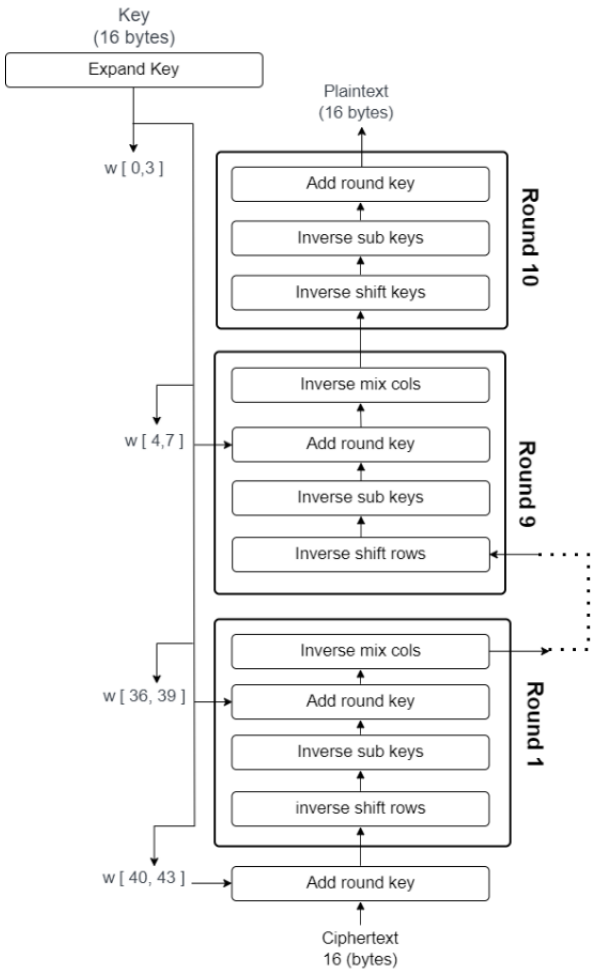

Figure 6: AES Decryption Flow

developed and evaluated, demonstrating high levels of user satisfaction across various aspects including interface design, functionality, usability, user experience, and security. This system addresses critical inefficiencies in manual vehicle cataloging processes within educational institutions by automating vehicle tracking and enhancing data security through AES encryption, significantly improving accuracy, efficiency, and security in parking management. Its importance lies in providing a modern, automated solution that reduces human error, improves overall workflow, and ensures robust protection of sensitive data, making it a valuable advancement for campus parking facilities. Despite its strengths, the study faces some limitations: it is specifically tailored for educational institutions in General Santos City, does not extend beyond campus boundaries, restricts QR code generation to faculty, staff, and students, relies on internet connectivity for logging, is designed exclusively for Android devices, and lacks the capability to monitor parking space occupancy. Despite these constraints, the system holds substantial relevance for educational institutions aiming to upgrade their parking management practices, offering a secure and efficient framework that could potentially be adapted for broader use in commercial and residential parking facilities. The application of QR code technology paired with AES encryption sets a new standard for secure parking operations, with scalability that promises wider implementation beyond its current scope. To enhance its future potential, it is recommended that the system incorporate advancements in encryption technologies to sustain its security edge, expand its functionality to include features like predictive parking availability and real-time notifications, and develop versions for additional mobile platforms to broaden accessibility and user adoption. This comprehensive approach ensures the system not only meets current needs but also paves the way for smarter, more secure parking management solutions.

REFERENCES

Agarwal, A., & Malik, S. (2022). An AES-based efficient and valid QR code for message sharing framework for steganography. In *Lecture notes in networks and systems* (pp. 581–598). https://doi.org/10.1007/978-981-19-2500-9_44

Agun, J. E. C., Rabie, M. A., & Satoquia, R. V. P. (2022). *Portable vehicle ticketing device using QR code technology and Android application.* https://ejournals.ph/article.php?id=19020

Ahmed, A. A., Al-Sanjary, O. I., & Kaeswaren, S. (2020). Reserve parking and authentication of guest using QR code. In *2020 IEEE International Conference on Automatic*

Control and Intelligent Systems (I2CACIS) (pp. 103–106). https://doi.org/10.1109/i2cacis49202.2020.9140192

Ajini, A., Arun G. (2016). QR code-based data transmission in mobile devices using AES encryption. *International Journal of Science and Research, 5*(6), 1116–1120. https://doi.org/10.21275/v5i6.nov164419

Almuhammadi, S., & Al-Hejri, I. (2017). A comparative analysis of AES common modes of operation. In *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)* (pp. 1–4). https://ieeexplore.ieee.org/abstract/document/7946655

Asok, A. (2016). QR code based data transmission in mobile devices using AES encryption. *International Journal of Science and Research (IJSR), 5*(6), 1116–1120. https://doi.org/10.21275/v5i6.nov164419

Awan, I. A., Shiraz, M., Hashmi, M. U., Shaheen, Q., Akhtar, R., & Ditta, A. (2020). Secure framework enhancing AES algorithm in cloud computing. *Security and Communication Networks, 2020*, 1–16. https://doi.org/10.1155/2020/8863345

Barriga, J. J., Sulca, J., León, J. L., Ulloa, A., Portero, D., Andrade, R., & Yoo, S. G. (2019). *Smart parking: A literature review from the technological perspective.* https://scholar.google.com/citations?view_op=view_citation&hl=en&user=nVqXOvsAAAAJ&citation_for_view=nVqXOvsAAAAJ:Y0pCki6q_DkC

Bhatia, S. (2023, June 22). *QR codes for vehicle verification: A detailed guide.* QR Batch Blog. https://qrbatch.io/blog/qr-code-for-vehicle-verification/

Chai, S., Chong, L., Chong, S., & Goh, P. M. Y. (2023). Bus ticket booking system using QR code with AES encryption. *International Journal of Membrane Science and Technology, 10*(3), 1854–1871. https://doi.org/10.15379/ijmst.v10i3.1846

Dokania, V. D., Sevak, M. M., Patel, D. D., & Barve, P. S. (2020). QR code based smart parking system. *Journal of Emerging Technologies and Innovative Research.* https://www.jetir.org/papers/JETIR2310482.pdf

Doomun, R., Doma, J., & Tengur, S. (2008). AES-CBC software execution optimization. In *2008 International Symposium on Information Technology* (pp. 1–8). https://doi.org/10.1109/ITSIM.2008.4631586

Ferdian, F., Id, A. I. H. A., & Rakhmat, F. R. U. F. (2021). Penggunaan QR code berbasis kriptografi algoritma AES (Advanced Encryption Standard) untuk administrasi rekam medis. *Joint (Journal of Information Technology), 3*(2), 20–27. https://doi.org/10.47292/joint.v3i2.64

Gangurde, N., Ghosh, S., Giri, A., & Gharat, S. (2022). Ticketing system using AES encryption based QR code. In *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT).* https://doi.org/10.1109/icssit53264.2022.9716234

GeeksforGeeks. (2023, May 9). *Block cipher modes of operation.* https://www.geeksforgeeks.org/block-cipher-modes-of-operation/

Hurbungs, V., Bassoo, V., & Fowdur, T. P. (2021). Fog and edge computing: Concepts, tools and focus areas. *International Journal of Information Technology, 13*(2), 511–522. https://doi.org/10.1007/s41870-020-00588-5

Inderscience Publishers. (n.d.). L*inking academia, business and industry through research.* https://inderscience.com/offers.php?id=132421

Ingole, M., Patle, C., Gahane, S., Atkare, A., Bante, A.(2023). QR based car parking system. *International Research Journal of Modernization in Engineering Technology and Science.* https://doi.org/10.56726/irjmets47293

Kadu, A., & Kadu, A. (2014). QR code-based smart parking system. *Journal of Emerging Technologies and Innovative Research.* https://www.jetir.org/papers/JETIR2310482.pdf

Lin, T., Rivano, H., & Le Mouël, F. (2017). A survey of smart parking solutions. *IEEE Journals & Magazine.* https://ieeexplore.ieee.org/document/7895130

Lu, Z., & Mohamed, H. (2021). A complex encryption system design implemented by AES. *Journal of Information Security, 12*(2), 177–187. https://doi.org/10.4236/jis.2021.122009

Rachh, R., Mohan, P. V. A., & Anami, B. S. (2012). Efficient implementations for AES encryption and decryption. *Circuits, Systems, and Signal Processing, 31*(5), 1765–1785. https://doi.org/10.1007/s00034-012-9395-0

Singh, S. (2024, January 23). *Encrypted QR code: A complete guide with best 6 advantages.* Scanova Blog. https://scanova.io/blog/encrypted-qr-code/

Vaidehi, M., & Rabi, B. J. (2014). Design and analysis of AES-CBC mode for high security applications. In *Second International Conference on Current Trends In Engineering and Technology - ICCTET 2014* (pp. 499–502). https://ieeexplore.ieee.org/abstract/document/6966347

Wahsheh, H. A., & Luccio, F. L. (2020). Security and privacy of QR code applications: A comprehensive study, general guidelines and solutions. *Information, 11*(4), 217. https://doi.org/10.3390/info11040217