

## Comparative Study on Preventing Security Attacks in Automated Gate System

*Erman Hamid<sup>1</sup>, Hani Maisarah Zainal Subari<sup>2</sup>, Norharyati Harum<sup>3</sup>, Robiah Yusof<sup>4</sup>*

erman@utem.edu.my

<sup>1,2,3,4</sup>Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka

### Abstract

This study is conducted to identify the current approach to preventing security attacks in one of the Internet of Things – the Automated Gate System. The question of vulnerability of the Automated Gate System is a critical issue as this system acts as a front line that protects an organization from any security intrusion. A sound security system leads to the cyber and physical security of the organization, enabling the organization to move forward in achieving management goals. The focus is specifically on methods and techniques for security elements used in previous studies, prompting answers to questions on security mechanisms to Automated Gate Systems that are practical and reliable. The literature review shows various studies conducted on this issue, focusing on how an IoT system for automated gates operates, how it works logically and physically, the security level, and the extent to which a gate system is immune from hacking. This study employed the Content Analysis technique, meaning the previous research data were analyzed and summarized scientifically. It continued with interviews conducted with experts and owners of the Automated Gate System. It is a series of activities analyzing and summarizing the scientific 'data' produced by previous research and interviews. The 'data' refers to spoken, written, or visual pictures, words, symbols, meanings, ideas, diagrams, or any message that can be analyzed. The study then focused on a final comparison involving three security techniques on the IoT Gate System: a QR Code System, RFID System, and Vehicle License Plate Recognition System, which is a reliable but practical technique for an IoT Automated Gate System. This study ultimately offers future work to analyze the three selected Automated Gate Systems with a selected security testing technique, with the objective of security but with practical financial capabilities.

### Keywords:

Automated Gate System, Security Attacks, Security Tools

### Introduction

The security of an organization's premises or a private house, both physical security and network security, is essential in ensuring that the organization's affairs run smoothly without any security disturbances such as intrusion and theft (Kim et al., 2009). In a situation where the crime rate is increasing day by day, premises owners should take the correct initiative to ensure the security of their respective premises (A et al., 2017).

Internet of Things (IoT) Automated Gate System are one of the very first options that the premises owner can integrate by ensuring that the entrance to each premise is equipped with an intact and guaranteed security system, preventing the intrusion of unwanted individuals into the premises of an organization or private premises (Baek et al., 2021). It is done by providing the entrance door or gate to the premises with IoT functionality that allows the system to verify the validity of the identity of each individual who enters the premises. In other words, inappropriate

Erman Hamid, Hani Maisarah Zainal Subari,  
Norharyati Harum, and Robiah Yusof

individuals will not be allowed to enter by the IoT system installed at each entrance of the premises, making it the first security measure integrated into the series of premises security controls (UI Rehman & Manickam, 2016).

However, before installing IoT functionality on the entrance system of each premise, consideration should be given to the security elements of the IoT Gate System (Jian et al., 2008)(Cooper, 1990). The Intrusion of the Automated Gate System is the issue, and this is the basis for the development of this study. Various types of automated gate systems are available on the market, but how effective are each of these systems in preventing security intrusions? How complete is the security protection of each automated gate system used, and which network security technique is the most optimal and, at the same time, affordable so that this system can be used by most people with adequate security impact.

Security tools integrated into the automated gate system need to be given special attention to ensure that only authorized individuals are allowed to pass through the Automated Gate System while restricting access to unauthorized people (Cooper, 1990). Authorization activity performed at the automated gate needs to be sent using a wired or wireless computer network to the security server for validation and exposing the data to various concepts of intrusion and hacking. It is a gate system that facilitates owners and individuals entering the premises with automated access and the adaptation of accurate and efficient security tools. Starting from this, the study is driven to the objective of the study as outlined in Table 1 below:

**Table 1. Research Direction**

| No | Management   |
|----|--|
| 1  | Highlights of the security mechanism for an automated gate system            |
| 2  | A survey of the practicality of an automated gate system for premises owners |

## Literature Review

Consideration of security techniques for a security system at the entrance of the premises is intended to ensure adequate property protection from unauthorized access. According to Shoewu (2023) a microprocessor monitors the entrance by installing sensors to detect authority on vehicles entering the premises. The gates will automatically open after sensing and authorizing each vehicle entry and open for a while before closing again. The automated gate system developed by Shoewu & Baruwa (2006) is an example of an Automated Gate System that does not include security elements in its operation simultaneously. It can be seen that these gates need to provide appropriate security methods since any vehicle can enter the property.

A study by Asha et al. (2018) refers to the security element of the automated gate system as the most fundamental issue that must be addressed without delay considering that it is used by government organizations, businesses and knowing the security methods that need to be implemented will directly strengthen the security element. This awareness shows that implementing an automated gate system is widespread in the community, but most come with high development and installation costs. Some are aware of the risk of using an Automated Gate System without security elements but preferably taking risks not installing the gate system as they cannot afford the fee (Hamid et al., 2018)(Primus et al., 2015). This strongly encourages the study of producing a safe but low-cost automated gate system.

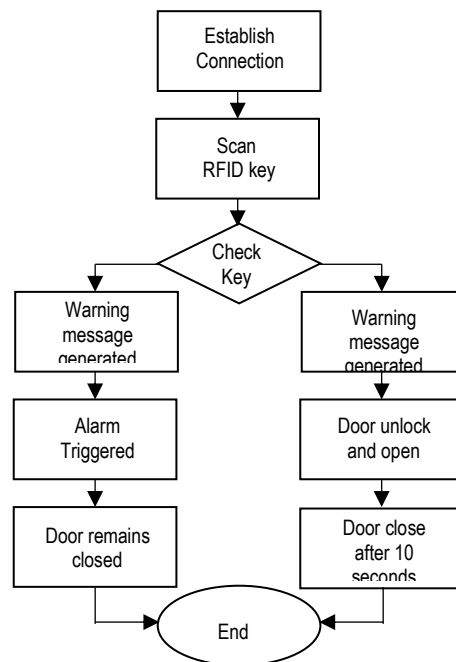
The following review highlights the automated gate system available in the market with different security techniques, prompting a comparative study for a safe and low-cost automated gate system (Jian et al., 2008)(Eltoum & Xue, 2014a). Among the security techniques that are widely used include Radio Frequency Identification (RFID) technology (Eltoum & Xue, 2014b)(Choi & Park, 2006), biometric identification techniques (Sanchez del Rio et al., 2016), license plate recognition technique (Tham, Mau-Luen, 2021) and QR Code technique (Hamid et al., 2018).

Erman Hamid, Hani Maisarah Zainal Subari,  
Norharyati Harum, and Robiah Yusof

**1. RFID**

Choi & Park (2006) show the use of RFID technology as a security method for the automated gate system. This study critically reviews the use of bar code and video identification technology. It classifies this technique as inappropriate due to the physical characteristics of bar code cards that are easily damaged, causing difficulty in the reading information process. Video identification, although admittedly offers better security than the bar code, requires higher installation costs and a high possibility of being affected by external environments. The use of RFID technology was chosen due to a better level of operational efficiency.

The study by Asha et al. (2018) also explains the implementation of RFID in the automated gate system with details of administration, controlling, exchange activity and keeping up records. It starts with a new user registering with the system, and the new user's information will burn into the RFID tag accessible through the system. Then, whoever owns the RFID tag can enter the property after the tag is put into the reader, and the system admits the user as registered. The information that is in the RFID tag matches the information that is stored in the system (K et al., 2014)(Choi & Park, 2006). The warning alarm will be triggered if the system recognizes it as an imposter. Figure 1 shows the process of RFID in an Automated Gate System.



**Figure 1.** Flowchart of The System (Asha et al., 2018)

**2. License Plate Recognition System**

According to Eltoum & Xue (2014b), vehicle license plate recognition is another option for the automated gate system. The system is based on a PIC microcontroller and regular PC with a video camera to catch video frames that include a vehicle license plate and process them. They have used MATLAB software, Proteus and Micro C to implement the algorithm. For the system's flow, the car will stand in front of the barrier first, and then the IR sensor will send a signal to the microcontroller to send a message to

Erman Hamid, Hani Maisarah Zainal Subari,  
Norharyati Harum, and Robiah Yusof

MATLAB. A welcome note will then be displayed on the LCD. The image of the license plate from the camera will be analyzed in MATLAB, where most of the data analysis parts were done. Then, the analyzed image of the license plate will be compared with the information stored in the database. If it matched, MATLAB would send a message to the microcontroller to open the gate, and it will be closed again after some time. But, if the information does not match, the alarm will be triggered, and a "you are not allowed to enter, please go back." message will be displayed on the LCD. Figure 2 shows the process.

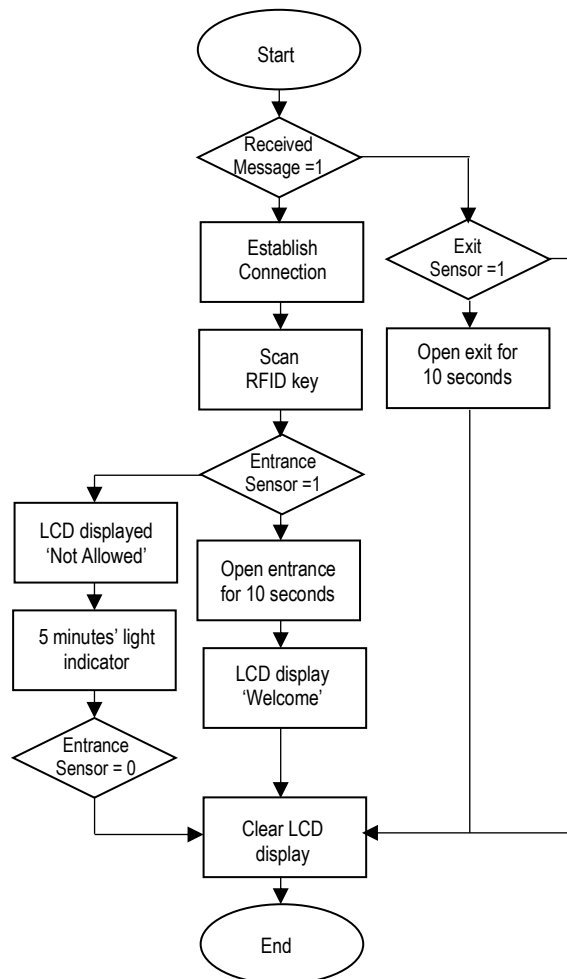


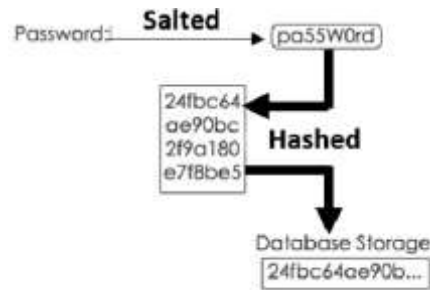
Figure Error! No text of specified style in document.. Flowchart of The Process (Eltoum & Xue, 2014b)

### 3. QR Code with Salted Algorithms

QR Code is one of the most current security methods that started to be used in the automated gate system (Ganesh et al., 2018)(Hogpracha & Vongpradhip, 2015)(Patil et al., 2018). QR code-based automated gate system is an implementation of medium-level security gate systems mainly for small companies that cannot afford to install expensive auto gate systems (Hamid et al., 2018). The QR code generator is used to store individual data that crosses the automated gate into a QR code, and salted algorithms are used as a security element to protect the data and the QR code system from being

Erman Hamid, Hani Maisarah Zainal Subari,  
Norharyati Harum, and Robiah Yusof

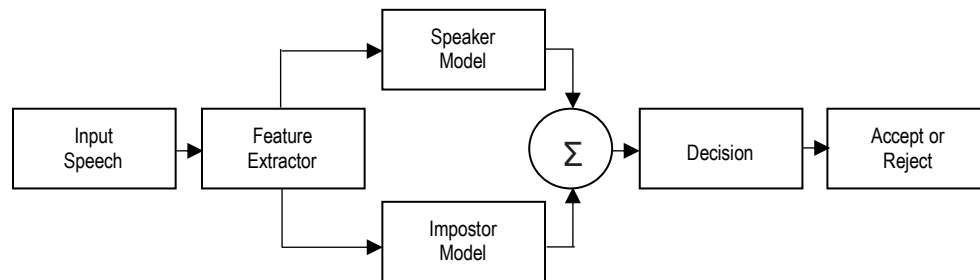
penetrated. This encoded data through a process decoded by scanning the QR code symbol with a mobile device that is equipped with a camera and a QR code reading software. (Hamid et al. (2018) further described that they implemented a salted algorithm and hashing algorithm to increase the security level of the QR code and make it hard to crack. Figure 3 shows an example of the salted hashing algorithm.



**Figure 2.** Example of The Salted Hashing Algorithm (Hamid et al., 2018)

#### 4. Voice Recognition System

Voice Recognition System is also another good option. It is classified as a safe study as this technology uses the user features parameter as the password, and it is unique for everyone (Hairol Nizam Mohd. Shah et al., 2014). Voice biometric technology is more convenient and accurate for authentication as the user has nothing to carry or remember any password and is afraid the ID card might be stolen or hacked. The voice recognition system has two main modules, which are feature extraction and feature matching, while the speech signal and its characteristics can be represented in two different domains, which are the time and frequency domains. They implemented this system by using MATLAB (SIMULINK). Users must speak their names and save them in the .wav file form. Severable variables such as pitch, dynamics and waveform are included and executed to recognize the user's voice using the function block available in SIMULINK. Figure 4 shows the speaker verification process involved in the Voice Recognition System.



**Figure 4. Speaker Verification** (Hairol Nizam Mohd. Shah et al., 2014)

#### Research Methods

This study combines Content Analysis and Interview techniques, which means the data from the previous research were analyzed and summarized scientifically (Berger, 1998), which was followed by a questionnaire session conducted with ten selected respondents. It is a series of activities in analyzing and summarizing the scientific data produced by previous research (Neuendorf, 2002). The 'data' refers to verbal, written or visual forms of pictures, words, symbols, meanings, ideas, diagrams, or any message that can be analyzed (Neuman, 2003). The findings from the content analysis were then compared with the findings from the interview session, and Erman Hamid, Hani Maisarah Zainal Subari, Norharyati Harum, and Robiah Yusof

conclusions were drawn from the comparison results. Figure 1 shows the coordination of Content Analysis and questionnaire techniques used as a methodology in extracting the best methods for the implementation of a safe and low-cost IOT Automated Gate System.



**Figure 5.** Steps Taken in Analyzing Problem

This paper gathered, reviewed and analyzed data from ten major selected papers and twenty more related references. It started with a review of research that was being carried out regarding the automated gate system. Analysis began by constructing a corpus of papers on intrusion and security techniques in gate systems by searching the term "Automated Gate System", "Intrusion", and "Security Technique". Each selected paper was examined and evaluated to see whether it suited the topics discussed.

The interview session was then conducted, and it was divided into two parts. Part I involves ten selected respondents consisting of premises owners who use automated gate systems, while Part II involves ten selected respondents who are experts in network security, consisting of 10 experts in information technology and network security (5 from industry and five from academic institutions). The questions in Part I revolve around awareness of the importance of network security elements in a gate system, while the questions in Part II consist of (1) important factors in implementing gate systems and (2) security tools that are trusted in automated gate systems, and (3) security testing tools that are suitable for use in the gate system.

The questions of the interview session were formed from the conclusions obtained from the literature review carried out previously. The results of the Content Analysis and the Interview session were then concluded to fulfil the objectives of the research by including (1) the Security method implemented in Automated Gate System and (2) Tools used to test and analyze the Automated Gates System. The purpose of the study is represented in Fig. 6 below.



**Figure 6.** Research Direction

## Results and Discussion

As discussed earlier, an automated gate system has been implemented with many security methods. There are most recent and standard security methods, and a lot of research has been carried out for these security methods: RFID Technology, QR code, Biometric Recognition and Vehicle License Plate Recognition.

Firstly, regarding expenses and fees, RFID technology can offer tight security with high efficiency. However, based on (Elechi P., Ahiakwo C., 2021), RFID technology is not affordable and requires high cost. Despite the cost, according to (Asha et al., 2018), RFID can be effortlessly accessible and more helpful to utilize. Although RFID technology has been known to be quite expensive, there are also low-cost RFID tags. However, based on (Juels, 2006), they are computationally weak devices that cannot perform basic symmetric-key cryptographic operations. Unlike RFID, QR code is a low-cost implementation for automated gate systems. According to (Hamid et al. (2018) and Marthasari et al. (2022), medium-level security can be developed with minimum cost. This is because the technology and RFID offer higher protection than QR codes. Hence, the installation and maintenance fees will be higher. The Vehicle License Plate Recognition system is cheaper than RFID technology and Biometric

Recognition, which needs higher installation and maintenance fees. For the cost, the QR code offers the lowest price in total and is affordable for any clients who have a tight budget.

Although these security methods offer tight security and have many security benefits, it is also exposed to many privacy and security threats and risks. Based on (Suárez-Albela et al., 2017), RFID is exposed to security and privacy risks. For security risks, the most common attacks are tag isolation, which blocks tag communications to avoid sending data to the reader. Next is tag cloning. Tag cloning is the unique identifier, and the content of the RFID tag is extracted and inserted into another title to access restricted areas. For privacy risks, personal tracking is dangerous as the attacker can know the routes, purchases and habits of the owner of the RFID tag. The information may even be used for marketing purposes.

For QR Codes, it is widely known that it is easy to crack and decode. However, the security of QR codes can be higher when security features are added (Marthasari et al., 2022). But still, the risks of getting attacks are there, and one of them is phishing. Phishing using a QR code is easy as they only need to put a sticker with the QR code that leads them to the malicious websites. Most people need to be aware of the threats, and there is little awareness about phishing using QR codes. This is crucial as people out there scan the QR code without even knowing the context of the QR code. For biometric and license plate recognition, data breaches can happen. Because the data are collected and stored to do the recognition process, this can be constant threats from hackers, and many security precautions need to be taken to protect clients' sensitive data.

Next, in the scanning process, only RFID technology and QR code support 360° of reading, making the scanning process faster and easier. It is efficient when there are a lot of scanning processes to be done at the same time. Meanwhile, for the range, RFID and Vehicle License Plate Recognition allow a more extended range compared to Biometrics as the data type for Biometric is either eyes, face or hand palm that needs a shorter field to be identified. Thus, using Biometrics, Vehicle License Plate Recognition and QR codes, they can be read and scanned one by one simultaneously, while RFID can be scanned and read many times at a time. Table 2 will show the comparison of the security methods.

**Table 2. The Comparison of The Security Methods**

|              | Biometric Recognition System (Voice Recognition System)        | RFID technology  | Vehicle License Plate Recognition  | QR code                               |
|--------------|--|--|--|---------------------------------------|
| Cost         | Expensive  | Expensive  | Cheaper than RFID  | Cheapest                              |
| Efficiency   | Can only scan and read once at a time                          | Can read and scan many times at once   | Can only scan and read once at a time  | Can only scan and read once at a time |
| Scan Range   | Short  | Longest  | Long   | Short                                 |
| Advantage    | Offers the best security level and accurate most of the times. | Efficient and tight security.  | Real time detection and recognition process.   | Low in cost and flexible              |
| Disadvantage | Too expensive.   | Cannot be used if the card or RFID tag is lost and it is expensive to setup and install. | Bad weather or lighting can affect the system and the system will not be completely effective. | Can be decoded easily                 |

Furthermore, to analyze the security methods, some of them have not identified specific tools that can help them to know how secure the security methods can be. It is important as clients need to know how secure each security method can be, in order to protect their properties from unauthorized access. Plus, clients need to know what security method to choose to invest for a better security. Based on Irfan Yaqoob et al. (2017), security testing is important as it can discover and evaluate potential vulnerabilities in a system so that attacks can be faced and the system does not stop working or be exploited. It also aids in the detection of any potential security concerns in the system, as well as assisting developers in the resolution of issues through code. According to Choi et al. (2006), before the security method can get evaluated, the vulnerabilities need to be discovered first. Choi et al. (2006) also mentioned that find the vulnerabilities, determine the risks of exploiting these vulnerabilities, and do a risk analysis for each potential threat. This adds a layer of protection. Its security posture may be assessed based on how threats are resolved (accept, mitigate, transfer). Security is always relative, and any compliance standards might act as a guideline. The content analysis conducted concludes 5 security testing techniques (refer to Figure 5) that can be carried out against the autogate system to evaluate the security effectiveness of each system.

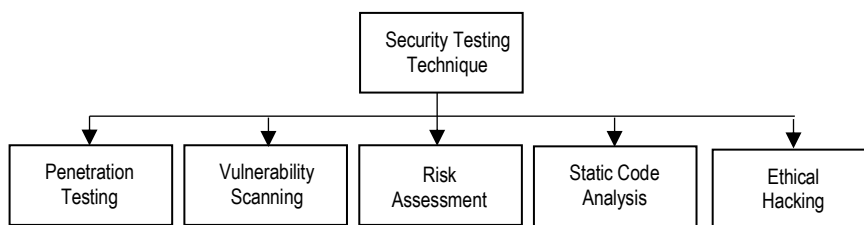


Figure 7. Testing Methods

Interviews with ten respondents also gave the same content analysis, with most automated gate system users seen as needing to be more sensitive to the security aspects of their respective automated systems. Although many security methods are implemented on the automated gate system, most clients need to learn the importance of having a secured gate system protecting their property. Most clients need to see the importance of a secured gate system to protect their property (refer to Figure 8). The expert interview showed (refer to Figure 9) 37.2% of respondents agreed that QR Code is the most secure technique implemented in the automated gate system, better than Voice Recognition System and RFID system. 40% of the experts also agreed to choose Penetration Testing as the best technique to test and analyze the degree of penetration that occurs against an automated gate system (refer to Figure 10).

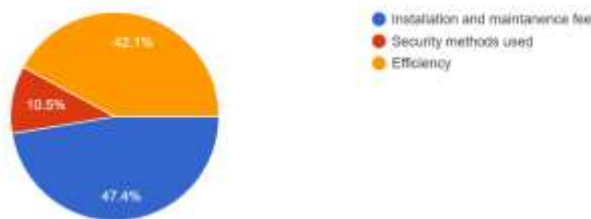
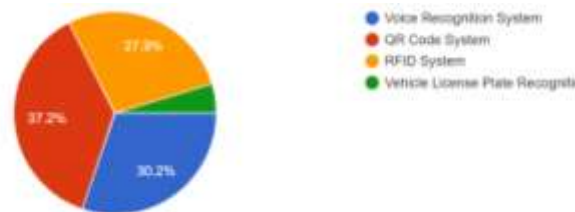
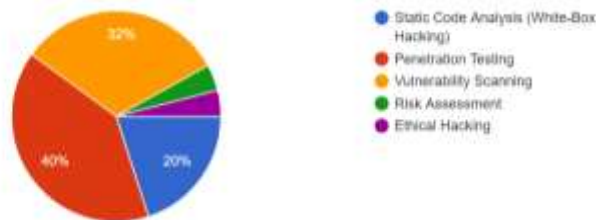


Figure 8. The Importance of Having A Secured Gate System





**Figure 9.** The Technique to be Implemented in Automated Gate System



**Figure 10.** The Penetration Testing Technique in Automated Gate System

## Conclusions

Continuing from Content Analysis and Interview techniques, future studies will be conducted to choose which security technique is best implemented in the Automated Gate System. Based on secured and economic objectives, this comparative study has succeeded in shortlisting selected techniques from the many techniques used in the market. The security methods that have been chosen to be analyzed are RFID technology, QR code and Voice Recognition System, as it is accurate in scanning and has many advantages in the security aspect. Static code analysis, penetration testing and vulnerability testing will be carried out for the Automated Gate System with the three techniques proposed with the objective of choosing the best security method to be implemented in the Automated Gate System.

## Acknowledgement

The authors are grateful to Universiti Teknikal Malaysia Melaka for the financial support through PJP/2021/FTMK/S01826.

## References

- A, J. C., Nagarajan, R., Satheeshkumar, K., Ajithkumar, N., Gopinath, P. A., & Ranjithkumar, S. (2017). Intelligent Smart Home Automation and Security System Using Arduino and Wi-fi. *International Journal Of Engineering And Computer Science*, March. <https://doi.org/10.18535/ijecs/v6i3.53>
- Asha, N., Syed Navaz, A. S., Jayashree, J., & Vijayashree, J. (2018). Rfid based automated gate security system. *ARPJ Journal of Engineering and Applied Sciences*, 13(22), 8901–8906.
- Baek, J., Kanampiu, M. W., & Kim, C. (2021). A secure internet of things smart home network: Design and configuration. *Applied Sciences (Switzerland)*, 11(14). <https://doi.org/10.3390/app11146280>
- Berger. (1998). *Media Research Technique*.
- Choi, H. R., & Park, N. K. (2006). An Automated Gate System Based on RFID Technology in a Container Terminal. *Ocean Policy Research*, 21(1), 83–108.
- Choi, H. R., Park, N. K., Yoo, D., & Kwon, H. K. (2006). A Study on the Technology Development for Non Stop Automated Gate System. *Proceedings of the Second International Intelligent Logistics Systems Conference 2006*, 1–9.

Erman Hamid, Hani Maisarah Zainal Subari,  
Norharyati Harum, and Robiah Yusof

- Cooper, R. G. (1990). Stage-gate systems: A new tool for managing new products. *Business Horizons*, 33(3), 44–54. [https://doi.org/10.1016/0007-6813\(90\)90040-I](https://doi.org/10.1016/0007-6813(90)90040-I)
- Elechi P., Ahiakwo C., S. S. T. (2021). Design and Implementation of an Automated Security Gate System using Global System for Mobile Communication Network Fraud Detection Systems in Nigeria View project Improved Lightning Protection on 132kV Transmission Lines and Probability of strike View pr. In *Article in Journal of Network and Computer Applications* (Issue March). [www.matjournals.com](http://www.matjournals.com)
- Eltoum, I. S., & Xue, Z. (2014a). Automatic Gate Control System Based On Vehicle License Plate Recognition. *Internation Journal of Engineering Research & Technology*, 3(8), 79–83.
- Eltoum, I. S., & Xue, Z. (2014b). Automatic Gate Control System Based On Vehicle License Plate Recognition. *Internation Journal of Engineering Research & Technology*, 3(8), 79–83.
- Ganesh, S. J., Avenash, A., Prakashreddy, A., Baarathi, C., & Sudhan, S. H. H. (2018). *Electronic toll collection system using QR code and RFID registration*. 10, 5–10.
- Hairol Nizam Mohd. Shah, Mohd. Zamzuri Ab Rashid, Mohd. Fairus Abdollah, Muhammad Nizam Kamarudin, C. K. L. and Z. K. (2014). V Oice R Ecognition B Ased S Echure a Ndroid M Odel. *Indian Journal of Science and Technology*, 6(3), 344–351.
- Hamid, E., Gee, L. C., Anawar, S., & Ayob, Z. (2018). Implementation of Intelligent Automated Gate System with QR Code - An IOT System to Help Gate Management. *International Journal of Advanced Computer Science and Applications*, 9(10), 359–363.
- Hogpracha, W., & Vongpradhip, S. (2015). Recognition system for QR code on moving car. *10th International Conference on Computer Science and Education, ICCSE 2015*, 14–18. <https://doi.org/10.1109/ICCSE.2015.7250210>
- Irfan Yaqoob, Syed Adil Hussain, Saqib Mamoon, N. N., & Akram, Jazeb, A. ur R. (2017). Penetration Testing and Vulnerability Assessments. *Journal of Network Communications and Emerging Technologies (JNCET)*, 7(August 2017), 10–18.
- Jian, M. S., Yang, K. S., & Lee, C. L. (2008). Modular RFID parking management system based on existed gate system integration. *WSEAS Transactions on Systems*, 7(6), 706–716. <https://doi.org/10.1023/B:WINE.0000044028.20424.85>
- Juels, A. (2006). RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications*, 24(2), 381–394. <https://doi.org/10.1109/JSAC.2005.861395>
- K, P. D., D, R. R., C, P. K., & A, H. M. (2014). Automatic Gate Opening System for Vehicles With Rfid or Password. *International Journal of Electrical and Electronics Research*, 2(2), 35–41.
- Kim, G. W., Lee, D. G., Han, J. W., Lee, S. H., & Kim, S. W. (2009). Security technologies based on a home gateway for making smart homes secure. *Internet Research*, 19(2), 209–226. <https://doi.org/10.1108/10662240910952355>
- Marthasari, G. I., Sari, Z., & Prasetyoko, H. (2022). Rancang Bangun Pintu Portal Otomatis Berbasis IoT (Studi Kasus: Perumahan Mutiara Jingga). *Jurnal Repositor*, 4(2), 195–202. <https://doi.org/10.22219/repositor.v4i2.1338>
- Neuendorf, K. A. (2002). A Flowchart for the Typical Process of Content Analysis Research. In *The Content Analysis Guidebook* (p. 320). <http://academic.csuohio.edu/kneuendorf/content/resources/flowc.htm>
- Neuman, W. L. (2003). Social Research Methods: Qualitative and Quantitative Approaches. In *Relevance of social research* (Vol. 8). <http://books.google.fr/books?id=nObtAAAAMAAJ>
- Patil, K., Patil, P., Rane, S., Redkar, R., & Salunkhe, P. G. (2018). Intelligent Car Parking System commanded by Android Application. *International Research Journal of Engineering and Technology (IRJET)*, 5–8.
- Primus, C. K., Yahya, N. S., Arba, A., N. A. N.Dandang, & O.AFI, N. (2015). Design and Development of Low Cost Erman Hamid, Hani Maisarah Zainal Subari, Norharyati Harum, and Robiah Yusof

- Auto Gate System for House , Part 4. *2nd Integrated Design Project Conference (IDPC) 2015, January*, 0–11. <https://doi.org/10.13140/RG.2.1.2686.9844>
- Sanchez del Rio, J., Moctezuma, D., Conde, C., Martin de Diego, I., & Cabello, E. (2016). Automated border control e-gates and facial recognition systems. *Computers and Security*, 62, 49–72. <https://doi.org/10.1016/j.cose.2016.07.001>
- Shoewu, O. (2023). Design and Implementation of a Microcontroller Based Automatic Changeover Switch. *International Research Journal of Modernization in Engineering Technology and Science*, 6(1), 21–32. <https://doi.org/10.56726/irjmets32878>
- Shoewu, O., & Baruwa, O. T. (2006). Design of a Microprocessor Based Automatic Gate. *The Pacific Journal of Science and Technology*, 7(1).
- Suárez-Albela, M., Fernández-Caramés, T. M., Fraga-Lamas, P., & Castedo, L. (2017). A practical evaluation of a high-security energy-efficient gateway for IoT fog computing applications. *Sensors (Switzerland)*, 17(9). <https://doi.org/10.3390/s17091978>
- Tham, Mau-Luen, and W. K. T. (2021). IoT based license plate recognition system using deep learning and OpenVINO. *2021 4th International Conference on Sensors, Signal and Image Processing*, 7–14.
- Ul Rehman, S., & Manickam, S. (2016). A Study of Smart Home Environment and its Security Threats. *International Journal of Reliability, Quality and Safety Engineering*, 23(3). <https://doi.org/10.1142/S0218539316400052>