Integration of Hash Function and Salted Algorithms in enhancing Security of QR Code Gate System

Erman Hamid *, Lim Chong Gee, Nazrulazhar Bahaman, Mohd Zaki Mas'ud

Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

*Corresponding e-mail: erman@utem.edu.my

Keywords: QR Code; Hash Function; Salted Algorithms

ABSTRACT – Our project deals with a QR Code Gate System that uses the integration of Hash Function and Salted Algorithms in enhancing the security aspects. This type of a gate system can be used in many type of organization, where the salted algorithm is implemented to protect the hashing value and minimal the possibility from any attack. It implemented in a system that using a valid staffs' QR code pass card to activate the gate. The system is based on VB.NET, PIR motion sensor, servo motor, Arduino microcontroller, Piezo buzzer and camera.

1. INTRODUCTION

Security System is a defence system that designed to prevent any unauthorized entry/intrusion to a building or a company [1]. It is widely used in housing area, company, and military properties for protection against the burglary. A good security system is very important as it can help the owner to take the immediate action to minimize the loss.

The front line of security system for a building or premise is Gate System [2]. It is a mechanical system that are mainly used to manage a gate; and to prevent any unauthorized person from entering the area of the company [3]. There are many types of Gate System being introduced in the market. The most common and famous are Biometric Gate System [4][5][6], Password/RFID Automatic Gate System [3][7][8], Vehicle License Plate Recognition Automatic Gate System [9][10], and QR Code System [11][12].

In this project, the research on QR code Gate System will be carry out focusing to the implementation of Hash Function with Salted Algorithms; due to the chances to enhance it security features.

2. DATA COLLECTION AND ANALYSIS

2.1 QR Code

QR (Quick Response) code is the two-dimensional barcode that used to scan components at high speeds. Once the Denso Wave hold the patent of this technology, he granted this technology as a free license and publish on internet allowing everyone to use it [13].

The consumer product is usually used to the one-dimensional barcodes to store the information such as price and name [14]. The information will be viewed if they are mechanically scanned. The barcode has been read by physically bouncing a narrow beam of light onto the code which can be interpreted using the pattern of light reflected off the white gaps between the lines [12]. QR codes as the improvement of the barcode which can hold the more data than barcode and it also can be detected by any digital scanner [14].

2.2 Security Features in QR Code

The security level for a normal QR code is very low because it can easily decode by any QR code decoder [15] and can be easily read by anyone. Hence, if a normal QR code is applied to the security application, it is not suitable as some of people might steal the information to make a copy to pass through the security system without alert the security department [15][14]. Thus, in this research, some Salted Hashing Algorithm is add into the QR code to make it become the secure QR code.

A hash is simply a one-way function, that will take a string or data source and create an encrypted looking string. It will randomly generating a string that used to add in the hash value. Anyway, the main purpose of the salted algorithm (as shown in Figure1) is to protect the hashing value and minimal the possibility from any attack for example dictionary attack. To increase the security level, it is implemented with the combination of salted algorithm and hashing algorithm [16]. This makes this coordination as a double protection in term of security.

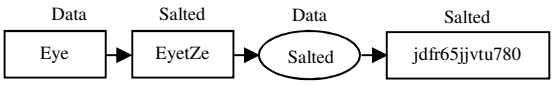

Figure 1: Salted hashing technique

3. PROPOSED SOLUTION

In this project, a software system will be created to monitor the gate system. It will notify the security department for any unauthorized scanning detected and the alarm will be triggered at the same time. A new QR code can be send at any time by the security department if it's lost and the previous one will be deactivate immediately. This immediate action can prevent the unauthorized person with holding the QR code to enter the company. A security camera will be recording the activities of the gate. The serial port technology will be implemented as a medium to provide the communication between Arduino Uno and VB.NET.

The product design is conceptualized of how the flow of the product. Figure 2 below shows the System Architecture of the Intelligent Automated Gate System and the overall flow of the product.

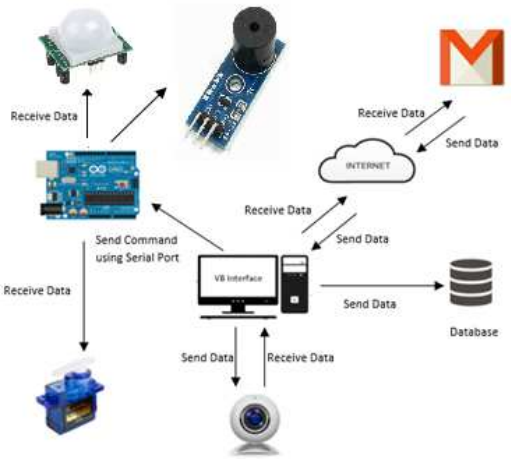

Figure 2: The architecture

4. RESULTS

The Salted Hash Algorithms QR Code Gate System is successfully developed, well implemented and tested. It shows that from 100 number of detection, only 1 considered as error detection, making the efficiency value reach 99%.

5. CONCLUSION

This QR Code Gate System with the integration of Hash Function and Salted Algorithms is aim to provide a gate system with security features. It is responsible to prevent any unauthorized person to enter the company area and prevent any break-in happen.

This project is unique among the current gate system as it is developed with comprehensive security functions. The QR code used in IAGS is encrypted by salted hashing algorithm to provide the integrity of data. The system is support with the internet connection which are able to sending out the alert via email immediately if any unauthorized activity is detected. Besides that, a picture in front of the gate will also be taken and sending to security department to take an immediate action.

This QR Code Gate System with the integration of Hash Function and Salted Algorithms can also be used as an attendance system which record down check in and check out time of staff. The staff who are late can be easily trace and fine them according to the regulations of the company. This is more efficient and systematic way than paper work and reduce the workload of the administrator.

ACKNOWLEDGEMENT

The authors would like to thank C-ACT and INSFORNET Research Group of Universiti Teknikal Malaysia Melaka (UTeM) for providing facilities and financial support under the university Short Term Grant with Project No. PJP/2018/FTMK(4B)/S01631.

REFERENCES

[1] J. A. Enokela and M. N. Tyowuah, "An electronically controlled automatic security access gate," *Leonardo J. Sci.*, no. 25, pp. 85–96, 2014.

[2] P. Sighila, V. Valsan, and C. Preethibha, "IoT Based RFID Gate Automation System," vol. 36, no. 9, pp. 471–473, 2016.

[3] P. D. K, R. R. D, P. K. C, and H. M. A, "Automatic Gate Opening System for Vehicles With Rfid or Password," vol. 2, no. 2, pp. 35–41, 2014.

[4] J. Sanchez del Rio, D. Moctezuma, C. Conde, I. Martin de Diego, and E. Cabello, "Automated border control e-gates and facial recognition systems," *Comput. Secur.*, vol. 62, pp. 49–72, 2016.

[5] R. G. Cooper, "Stage-gate systems: A new tool for managing new products," *Bus. Horiz.*, vol. 33, no. 3, pp. 44–54, 1990.

[6] A. K. Jain and K. Nandakumar, "Biometric authentication: System security and user privacy," *Computer (Long. Beach. Calif).*, vol. 45, no. 11, pp. 87–92, 2012.

[7] M. S. Jian, K. S. Yang, and C. L. Lee, "Modular RFID parking management system based on existed gate system integration," *WSEAS Trans. Syst.*, vol. 7, no. 6, pp. 706–716, 2008.

[8] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," in *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, 2012, pp. 1282–1285.

[9] I. S. Eltoum and Z. Xue, "Automatic Gate Control System Based On Vehicle License Plate Recognition," *Int. J. Eng. Res. Technol.*, vol. 3, no. 8, pp. 79–83, 2014.

[10] S. Chang and L. Chen, "Automatic license plate recognition," *... , IEEE Trans.*, vol. 5, no. 1, pp. 42–53, 2004.

[11] W. Hogpracha and S. Vongpradhip, "Recognition system for QR code on moving car," in *10th International Conference on Computer Science and Education, ICCSE 2015*, 2015, pp. 14–18.

[12] R. M. Bani-Hani, Y. A. Wahsheh, and M. B. Al-Sarhan, "Secure QR code system," in *2014 10th International Conference on Innovations in Information Technology, IIT 2014*, 2014, pp. 1–6.

[13] T. J. Soon, "QR code," *Synth. J. 2008*, pp. 59–78, 2008.

[14] P. Kieseberg *et al.*, "QR code security," in *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia - MoMM '10*, 2010, p. 430.

[15] A. S. Narayanan, "QR Codes and Security Solutions," *Int. J. Comput. Sci. Telecommun.*, vol. 3, no. 7, pp. 1–4, 2012.

[16] R. Morris and K. Thompson, "Password security: a case history," *Commun. ACM*, vol. 22, no. 11, pp. 594–597, 1979.