Enhanced IoT-Based Online Access Control System for Vehicles in Truck-Loading Fuels Terminals

Moatz M. Bahgat
Communication and Electronics Department
Faculty of Engineering, Alexandria University
Alexandria, Egypt
e-mail: moatz.bahgat@gmail.com

***Abstract*—The emergence of the Internet of Things (IoT) as a new Future Internet concept has led to a new wave of application potential which could play an important role in our daily life. Not only does the IoT connect the Cyber and Physical worlds together, but it may also improve the performance of existing applications greatly by efficiently applying IoT-enabling technologies. In the case of Access Control Systems for granting the entry and exit of vehicles in Truck-Loading Fuels Terminals, the IoT may be used to overcome the several system performance issues. This paper presents a developed IoT-based access control system for vehicles passing through the entry and exit gates in Truck-Loading Fuels Terminals. The developed system follows a new design approach utilizing one of the most prominent IoT technologies, the Radio Frequency Identification (RFID), with its write capabilities. The novel design approach followed in developing the presented topic aims at offering enhanced system performance with regard to speed, security and allocated resources.**

***Keywords*-IoT, RFID, Web, Server, HTTP, HTML5, Access Control, Embedded, Gate**

I. Introduction

An Access Control System (ACS) for vehicles in Truck-Loading Fuels Terminals is used to permit the entry or exit of authorized vehicles [1]. There exists various access control systems which use different techniques, mechanisms and communications protocols; however, the most common method in controlling the terminal access is to use access cards [2]. Although they are commonly used in Truck-Loading Fuels Terminals, traditional Card-based Access Control Systems (ACS) have several performance issues regarding the speed, the security and the utilized resources consumed during their operation.

Many Access Control Card Readers are still based on the Wiegand Protocol that became popular due to the discovery of the Wiegand effect which is a nonlinear magnetic effect, named after its German discoverer John R. Wiegand in 1974 [3]. Wiegand discovered that a certain ferromagnetic alloy metal which was made of cobalt, iron and vanadium can be used to transfer a signal based on applying a magnetic field on the Wiegand alloy metal, also known as Wiegand Wire [2], [3]. Due to the physical size limitations of the access card, a maximum of 37 Wiegand wires may be used, which in turn limited the maximum length of Wiegand Cards Identifiers to less than 37 bits [1], [4].

Moreover, most Access Control Card Readers communicate through serial RS-485 cables. Despite the fact that serial RS-485 cables provide distances up to 1200 meters, however; they can only communicate with baud rates up to 1 Megabits per second i.e. slower speed when compared to Ethernet cables which may provide higher data rates [1], [4], [5].

Another issue with the majority of Access Control Systems, including systems with intelligent card readers, is that they use Read-Only access cards without any capabilities of writing application-specific data. Those Read-Only cards are also prone to the card cloning security attacks [6], [7].

Finally, and in case the Access Control Card Reader was connected to a communications server that keeps polling the Access Control Card Reader for data periodically, a lot of the server processing power and the available network resources are wasted which result in degraded system performance [5].

This paper presents a novel design approach followed in implementing a Card-based Access Control System (ACS) for controlling and monitoring the entry and exit of vehicles in Truck-Loading Fuels Terminals. The aim of the new system design is to overcome the aforementioned system issues and enhance the system performance with regard to:

- Speed
- Security
- Allocated Resources

The developed system uses the Internet of Things (IoT) concepts [8], [9] applying one of the key IoT-enabling technologies which is the Radio Frequency Identification (RFID) [10], [11]. The RFID technology belongs to the automatic identification and data capture (AIDC) technologies [2] and offers many advantages including:

- Line-Of-Sight (LOS) is not required
- Large data storage capacity
- Read and Write abilities

RFID offers these advantages because it relies on radio frequencies to transmit information between the tag, also

978-1-7281-0851-3/19/$31.00 ©2019 IEEE

known as the transponder, and the reader, also known as the interrogator, rather than light, which is required for optical AIDC technologies such as barcodes [2]. Regarding the use of the RFID technology in access control applications, there are two general types of access control systems: online and offline. Online access control systems have RFID readers which are networked to a central computer in contrast to offline systems which are not networked [12].

The architecture of the developed access control system and its components are discussed in more detail in the next section.

II. System Architecture And Components

The developed system follows a server-client model [5] with the gates card readers acting as the clients which communicate with a web server. In a 3-layer IoT architecture, the developed system may be divided into three parts as shown in Fig. 1:

1) Identification Layer
2) Network Layer
3) Service Layer

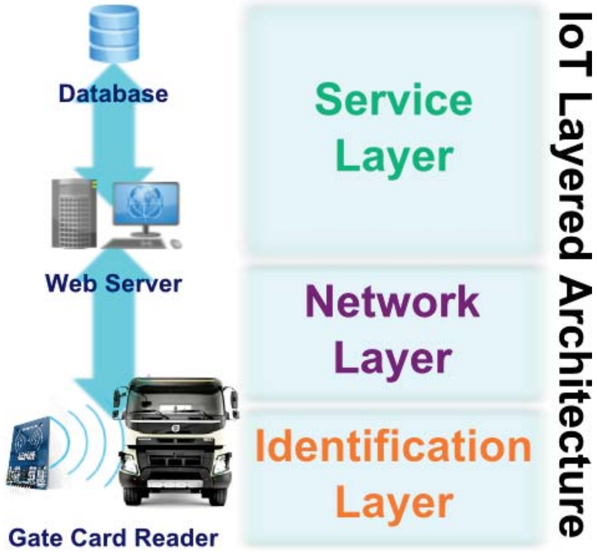


Figure 1. Developed IoT-based Access Control System architecture.

A. Identification Layer

In the developed IoT-based Online Access Control System, the RFID technology is used at the Identification layer, also known as the Perception layer, of the IoT layered architecture [8]. A RFID reader installed at the terminal gate detects a RFID card and reads its unique identifier and data stored on it. Each entry or exit gate is equipped with a card reader which consists of an ATmega AVR microcontroller, an Ethernet module, a RFID proximity card reader module and a SD card reader module. As an enhancement, and in order to simplify the configuration process of the Gate Card Reader, the SD card reader module is used to store the Gate Card Reader configuration parameters required to uniquely identify the gate when communicating with the web server through HyperText Transfer Protocol (HTTP) [5], [13] in the developed IoT-based Online Access Control System. The embedded system components use Serial Peripheral Interface (SPI) [4], [5], [14] for communications with the AVR microcontroller as shown in Fig. 2.

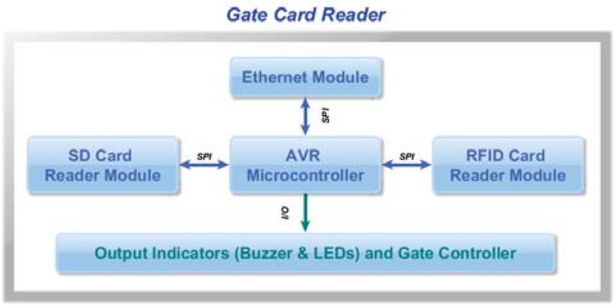


Figure 2. Block diagram of the Gate Card Reader components.

B. Network Layer

In the Network layer, also called as the Transport layer, of the IoT layered architecture, the data read is transferred between the RFID reader and a web server through an Ethernet cable, which is connected to the Gate Card Reader embedded Ethernet module, using HyperText Transfer Protocol (HTTP) [5], [13].

C. Service Layer

The Service layer, also known as the Application layer, of the IoT layered architecture is the layer at which the data collected at the Identification layer and transmitted through the network is processed and managed [8], [9]. There are two main components which provide these services in the developed IoT-based Online Access Control System:

1) Database Management Server
2) Web Server

1) Database Management Server: This is an Object-Oriented Relational Database Management Server, ORDBMS, [15] used for storing all the terminal-specific data including orders, vehicles, products, customers and destinations.

2) Web Server: The web server is part of the client-server model which is responsible for interfacing the client gates card readers using HyperText Transfer Protocol (HTTP) [5], [13]. It is the only component allowed to interact with the back-end database and its sole purpose is for serving database-related clients requests. In an Online Access Control System, the web server may be installed in a different location other than the Truck-Loading Terminal [12].

RFID Card Writer

An additional and very important step is to write application-specific data on the RFID card prior to the entry of the vehicle. This additional step enhances the system security. Fig. 3 shows the RFID Card Writer along with its embedded components connected to a host workstation through the Universal Serial Bus (USB) cable [4], [14]. The host workstation transmits the encoded order-specific data to the RFID Card Writer which in turns writes it to the RFID proximity card.

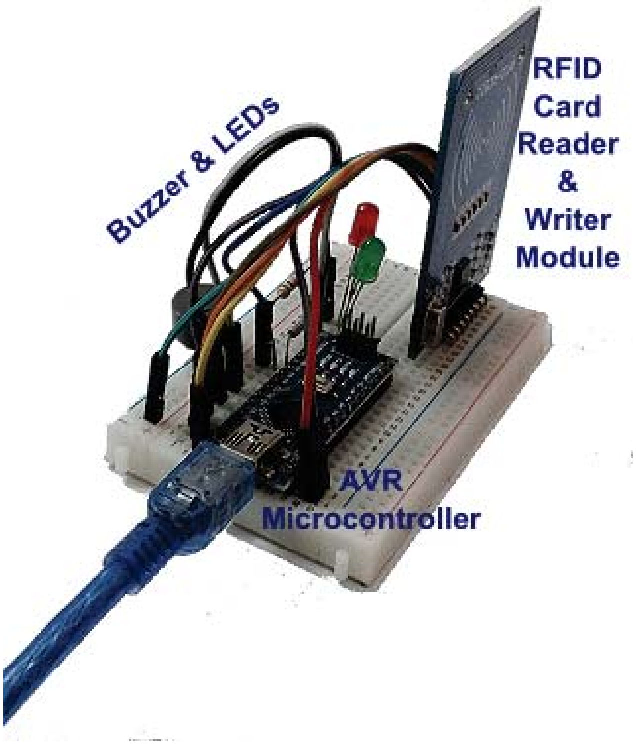
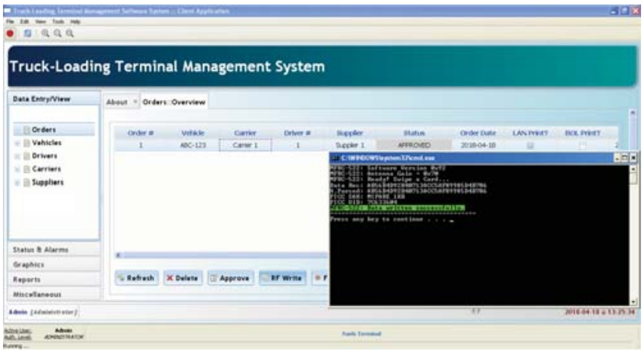


Figure 3. Prototype of RFID Card Writer embedded system.

The main purpose of the RFID Card Writer, as mentioned before, is for writing encoded order-specific data to the RFID card to be used at the entry and exit gates of the terminal. A vehicle is to be allowed entry or exit by the developed Access Control System only if the unique data stored in the RFID card, in addition to the RFID Card unique identifier, match those stored in the database, thus adding a new layer of security to the system. This is done once a new order was created through a developed Web-based software system. The developed software uses the latest web technologies including HyperText Markup Language version 5, HTML5, Cascading Style Sheets version 3, CSS3, and Javascript, JS [16], [17], [18] as shown in Fig. 4.



Order #	Vehicle	Carrier	Driver #	Supplier	Status	Order Date	LAN PRINT	BOL PRINT
1	ABC-123	Carrier 1	1	Supplier 1	APPROVED	2018-04-18	□	□

```
MFRC-522: Software Version 0x92
MFRC-522: Antenna Gain = 0x70
MFRC-522: Ready! Swipe a Card...
Data Rec: [illegible]
H_Parsed: [illegible]
PICC SAK: MIFARE 1KB
PICC UID: [illegible]
MFRC-522: Data written successfully.
--------------------------------------------
Press any key to continue . . .
```

2018-04-18 @ 13:25:34

Figure 4. Writing encoded order-specific data using the developed Web-based software system.

III. System Checks and Validations Procedures

This section describes the validations procedures which are performed by the developed access control system in order to control the movement of vehicles through the entry and exit gates. Fig. 5 shows a flow chart for all system validations checks. Validations are carried out through the HTTP communication between the Gate Card Reader and the Web Server.

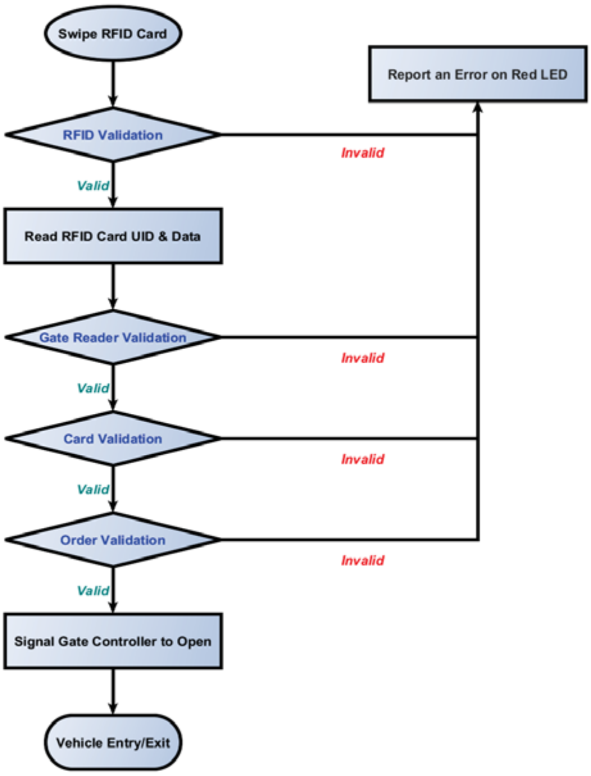


Figure 5. Access Control System Validations Flow Chart.

A. RFID Communications Validation

The developed access control system initially performs validation of RFID wireless communications by checking that:

- Is RFID Card Detected?
- Is RFID Card Authenticated?

Once a valid RFID card is detected and authenticated by the Gate RFID Card Reader, subsequent validations steps are performed.

B. Gate Card Reader Validation

Validation of the Gate RFID Card Reader includes checking that:

- The gate exists in the system database
- The gate identification parameters match those stored in the system database
- The gate status permits entry or exit of the vehicle

C. RFID Card Validation

For RFID Card validation, two main checks are performed by the developed access control system:

- Card Unique Identification (UID) number Validation
- Card Data Validation

D. Order Validation

The developed system allows a vehicle to enter or exit the site only after order validation which is carried out by checking that:

- The order number exists in the system database
- The order status permits entry or exit of the vehicle
- Additionally, for a vehicle to exit the site, the system checks that there are no remaining quantities for this vehicle

IV. Practical Results and Comparisons

This section sheds some light on the performance enhancements provided by the new design approach followed in the developed IoT-based Online Access Control System along with comparisons with traditional Access Control Systems too.

A. Speed Performance

Regarding the communications between the web server and the gates card readers, Ethernet cables are used rather than using Serial cables. Ethernet cables provide significant speed performance compared to serial RS-232 or RS-485 cables [1], [4] as shown in Table I.

Table I
Comparison between Serial RS-232, RS-485 and Ethernet communication cables

Point of Comparison	RS-232	RS-485	Ethernet
Maximum cable length (m)	15	1200	100
Maximum data rate	115.2 kbps	1 Mbps	1000 Mbps
Maximum number of nodes	1	32	65535

In addition, the system follows an interrupt-driven design approach in which the communications between a gate card reader and the web server only takes place once a card is detected instead of repeated continuous communications [11], [13]. This reduces the amount of network traffic and thus no noticeable delays would occur, and hence improving the system performance. Those enhancements are not found in other Card-based Access Control Systems.

B. Security Performance

Security of the access control system implies the protection of the terminal data against unauthorized access. This is enforced by the following design considerations:

- All the data is stored in a password-protected database server residing on the server
- No entity from outside the server is allowed to access the database directly
- The application-specific data written to the RFID card is encoded using one-way hash functions

The new design approach followed in developing the Card-based Access Control System makes the system immune to the tag cloning security attack [6] due to the fact that the data encoded on the RFID card is valid only once.

Moreover, the RFID ISO/IEC 14443 standard used, which is a unique enhancement, enforces authentication of RFID cards using secret keys before data reading or writing [2], hence increasing the level of security of the Access Control System [16].

C. Allocated Resources Performance

The resources utilized by an Online Access Control System mainly include the central processing unit (CPU) usage of the server machine and the amount of traffic i.e. the number of packets transmitted and received through the network. In other Access Control Systems, the server keeps polling the gate card readers for data periodically. This wastes a lot of the server CPU cycles and also keeps the network busy which may lead to noticeable delays in the system response. On the other hand, in the developed access control system, the performance is enhanced drastically. The server no longer polls the gate card reader for data, but instead, the IoT-based gate RFID card reader sends the RFID card data only when an authenticated card is detected. This interrupt-driven i.e. event-driven approach is more efficient with regard to the CPU usage and the network utilization [16]. Table II shows the results of a practical experiment to compare the performance of an access control system with a polling server and the developed access control system. The experiment was carried out on matching platforms for a duration of one hour and the same number of access cards i.e. trucks. Monitoring a server polling the gate card reader repeatedly every second showed that it utilized an average of around 10% of the CPU usage, whereas for the event-driven system, the average CPU usage was around 2%. In addition, the network utilization was decreased greatly due to adopting this interrupt-driven IoT communications approach.

Table II
COMPARISON BETWEEN ACS WITH POLLING SERVER AND THE DEVELOPED INTERRUPT-DRIVEN IOT-BASED ACS

Point of Comparison	Polling ACS	Developed ACS
Average CPU Usage	~ 10%	~ 2%
Average number of network packets	~ 15600	~ 250

V. CONCLUSION

In this paper, the developed online access control system was presented. The advantages of the system design were stated with practical results. The Internet of Things concept not only connects the Cyber and Physical worlds, but also may enhance the performance of existing systems in various fields. It should be noted that the work done in this paper, and to the extent of the author's knowledge, applied a new approach in developing and studying the presented topic.

ACKNOWLEDGMENT

Warm thanks are due to the Department of Communications and Electronics, the Faculty of Engineering of Alexandria University for the great input and support.

REFERENCES

[1] Zurawski, R., *Industrial Communication Technology Handbook, Second Edition*, ser. Industrial Information Technology. Taylor & Francis, 2014.

[2] Klaus Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd ed. John Wiley & Sons, 2003.

[3] William H. Hayt, Jr. and John A. Buck, *Engineering Electromagnetics*, 6th ed. Tata McGraw-Hill, 2001.

[4] Reynders, D. and Mackay, S. and Wright, E., *Practical Industrial Data Communications: Best Practice Techniques*, ser. Practical professional books from Elsevier. Elsevier Science, 2004.

[5] William Stallings, *Data and Computer Communications*, 7th ed. Pearson Prentice Hall, 2004.

[6] Ahmed Khattab, Zahra Jeddi, Esmaeil Amini and Magdy Bayoumi, *RFID Security: A Lightweight Paradigm*, ser. Analog Circuits and Signal Processing. Springer International Publishing AG, 2017.

[7] Steven Arms, Alan Bensky, Tony Bradley, Praphul Chandra, Chris Hurley, Steve Rackley, James F. Ransome, John Rittinghouse, Timothy Stapko, George L. Stefanek, Frank Thornton, Chris Townsend and Jon Wilson, *Wireless Security: Know it all*. Elsevier Inc., 2009.

[8] Greengard, S., *The Internet of Things*, ser. The MIT Press Essential Knowledge series. MIT Press, 2015.

[9] Slama, D. and Puhlmann, F. and Morrish, J. and Bhatnagar, R.M., *Enterprise IoT: Strategies and Best Practices for Connected Products and Services*. O'Reilly Media, 2015.

[10] Kai Hwang, Geoffrey C. Fox and Jack Dongarra, *Distributed and Cloud Computing: From Parallel Processing to the Internet of Things*. Elsevier Inc., 2012.

[11] Holler, J. and Tsiatsis, V. and Mulligan, C. and Avesand, S. and Karnouskos, S. and Boyle, D., *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*. Elsevier Science, 2014.

[12] NIST, Computer Security Division, "Guidance for Securing Radio Frequency Identification (RFID) Systems," NIST Special Publication, April 2007, recommendations of the National Institute of Standards and Technology.

[13] McEwen, A. and Cassimally, H., *Designing the Internet of Things*. Wiley, 2013.

[14] Strauss, C., *Practical Electrical Network Automation and Communication Systems*, ser. Electronics & Electrical. Newnes, 2003.

[15] Sumathi, S. and Esakkirajan, S., *Fundamentals of Relational Database Management Systems*, ser. Studies in Computational Intelligence. Springer Berlin Heidelberg, 2007.

[16] Moatz M. Bahgat, "Enhanced terminal automation software system for truck-loading fuels terminals," in *IEEE 28th International Conference on Microelectronics (ICM)*. IEEE, December 2016.

[17] Pilgrim, M., *HTML5: Up and Running*. O'Reilly Media, 2010.

[18] MacDonald, M., *HTML5: The Missing Manual*, ser. EBSCOhost ebooks online. O'Reilly Media, 2013.