MPAES: A Multiple-Privileges Access E-Door System based on Passive RFID Technology

Conference Paper · May 2017

CITATIONS
0

READS
54

3 authors:

Mohammed I. Younis
University of Baghdad
48 PUBLICATIONS **351** CITATIONS
SEE PROFILE

Maad Issa Al-Tameemi
3 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Maysam Sameer Hussein
2 PUBLICATIONS **4** CITATIONS
SEE PROFILE

MPAES: A Multiple-Privileges Access E-Door System based on Passive RFID Technology

Mohammed Issam Younis, Maad Issa Al-Tameemi
Computer Engineering Department, College of Engineering,
University of Baghdad,
Baghdad, Iraq
younismi@gmail.com, maadesaa@yahoo.com

Maysam Sameer Hussein
Computer Engineering Department,
Al-Isra'a University College,
Baghdad, Iraq
emaysamsamir@yahoo.com

***Abstract*—Many techniques have been used in achieving secure door systems, with the development of Internet of Things (IoT) and technologies, Access control systems grow differentially and rapidly. This paper proposes a novel reconfigurable embedded system called multiple-privileges access E-Door system (MPAES). Unlike existing E-Door systems, MPAES is developed in such a way that enables the administrator to set multiple access rules to the users. Moreover, a single e-door can be configured to be accessed by a single person or multiple people identification based on passive Radio Frequency Identification (RFID) technology. In addition, unlike the physical keys, the passive tags (keys) can be used to open or participate in opening multiple e-doors. Furthermore, The administrator could control and monitor the access events. In doing so, this paper gives the hardware and software components selection; the architectural design; and the concrete hardware prototyping and dynamic software implementation of the proposed MPAES. Finally, this paper gives the future direction in developing E-door systems.**

Keywords*— *Access control; e-door; automatic lock; RFID; Raspberry Pi; IoT

I. INTRODUCTION

The Internet of Things (IoT) is about connecting the unconnected. It allows for things to be accessible from the Internet that historically have not been. With 50 billion devices to be connected by 2020, the globe itself will be "growing a nervous system" and have the ability to sense and respond to ever-increasing amounts of data. The Internet of Everything (IoE) is able to improve the quality of life for people everywhere by taking advantage of these connected things and the data produced. The IoE also incorporates new processes that enable people to make better decisions and offerings [1]. This transition requires digitizing the physical world. In 2012, the number of connected devices on the Internet exceeded the world population. This includes traditional computing devices and mobile devices, as well as new industrial and consumer devices that we think of as "things" [2]. Although this may seem like a lot of devices on the Internet, it represents less than 1% of the objects that could be connected [1,2].

Sensors are one way to collect data from non-computers. They convert physical aspects of our environment into electrical signals that can be processed by computers. Some examples are soil moisture sensors, air temperature sensors, radiation sensors, and motion sensors. Sensors of all types will play an important role in connecting what has traditionally been unconnected in the IoE. On the other hand, actuators reverse the role of sensors (i.e., take the commands from computers and produce electrical signals convertible to physical aspects). Sensors and actuators are connected to the main device called the controller. Controllers may have the ability to make immediate decisions or they may send data to a more powerful computer for analysis [3]. This paper deals with digitizing the door locks, keys, and prototyping a solution as depicted in Fig 1.

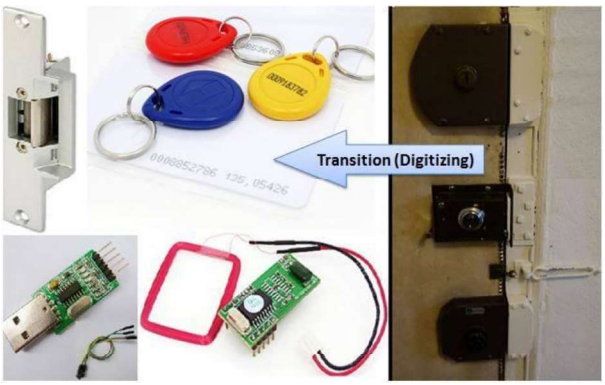

Fig. 1. Digitizing the physical locks and keys.

A popular type of sensor uses radio frequency identification (RFID). RFID uses radio frequency electromagnetic fields to communicate information between small coded tags (RFID tags) and an RFID reader [4]. Usually, RFID tags are used to identify and track what they are embedded into, such as a pet, an identification card. Because the tags are small, they can be attached to virtually anything including clothing identity card, and cash. Some RFID tags carry no batteries called passive tags [5, 6]. The energy required by the tag to transmit information is obtained from the electromagnetic signals that are sent by the RFID tag reader. The tag receives this signal and uses part of its energy to power the response. Because of their flexibility and low power requirements, RFID tags are a great way to connect a non-computer device to a network by providing information to an RFID reader device [4, 5, 6]. Typically, the RFID reader is connected to a host that contains a database as shown in Fig. 2. Fortunately, there are many actuators based e-doors

ISBN: 978-1-5386-0802-9/17/$31.00 ©2017 IEEE

available for developing and commercialized use. The main goal of constructing an automated door lock is the security feature. Security is growing need throughout the world and lack of security can result in a great damage. Many solutions are available for access control depending on the technologies available and the level of restriction [7].

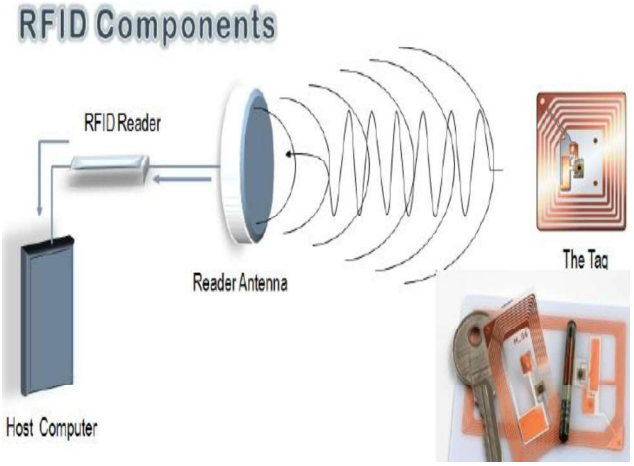

Fig. 2. The parts of passive RFID System and data communication [4].

There are some situations (e.g., examination committee, safe, etc) require multiple privilege access. For instance, a single e-door requires two persons to present their identities to open the lock. In addition, the same key could be used to open (or participate in the opening) more than on door. This paper proposes a multiple-privileges access E-Door system (MPAES). The reminder of this paper is organized as follows. Section II highlights related works. Section III gives the architectural design of the MPAES. Section IV gives a clarifying example. Section V gives the selection of hardware and software components of the MPAES and the reasons for choosing these components and the hardware prototyping. Section VI gives the dynamic software implementation of the MPAES. Finally, conclusion and recommendation for future work are stated in Section VII.

II. Related Works

In order to justify the desired features in practice, the following subsections contain a brief description and features of these systems.

Verma and Tripathi (2010) proposed a security system containing door locking system using RFID, authenticate, and validate the user and unlock the door in real time for secure access, with a central controller manages transaction and operation task. When the user put his tag in contact with a reader the door the door open quickly. The system also makes a log containing check-in and check-out for each user with basic information of that user [8].

Mahdi (2013) proposed a PC-based access control system, using LEDs, electronic circuit, magnetic lock, relays, sensors and some mechanical system to build the hardware parts which is connected and controlled by the PC via PC parallel port; the operation relies on a time schedule, so that the door opened and closed according to the specified day and time [7].

Ogri et al. (2013) proposed a prototype security door that uses a GSM phone set dual tone multi-frequency (DTMF) connected to the door motor interfaced with microcontroller unit via DTMF decoder and remotely controlled by a GSM phone set acting as the transmitter [9].

Mishra et al. (2014) proposed control door system that opens the door according to the entered combination via a keypad which is controlled by a microcontroller, the microcontroller manages and control the system by signaling the motor to open door [10].

Ha (2015) proposed a digital door lock system based on the Internet of Things (IoT), digital door lock detects the physical impact of an invalid visitor. Controlled by Arduino, the system checks the image of the visitor if it is valid, open the door, otherwise notifies the user's mobile device. If an incorrect pass-code is repeated more than a certain number of times, the lock captures an image of the invalid user and transfers it to the mobile device [11].

Summing up, most of the researchers are focused on a single-tag e-doors. A little bit attention is given to buildings that have multiple authorization rules to access the e-doors. Fixing and building from earlier works, this paper proposed MPAES, which be discussed in the following sections.

III. The Architectural Design of MPAES

The MPAES consist of three modules: A Computing, Storage, and Control Unit (CSCU), A Passive RFID Reader Unit (PRRU), and A Door Lock and Alarm Unit (DLAU). The PRRU and DLAU are connected to the CSCU as depicted in Fig. 3. There are two actors in the MPAES: the administrator(s) and user(s). The MPAES works as follows.

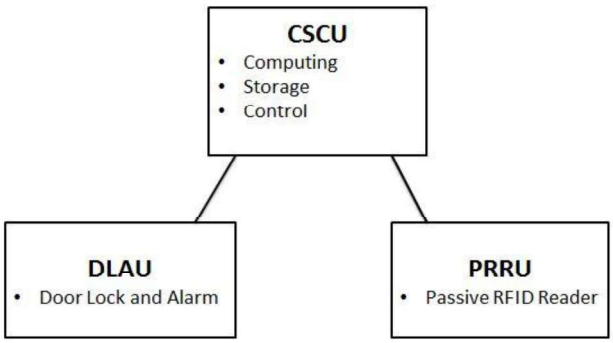

Fig. 3. The MPAES block diagram.

The administrator is responsible for setting the privilege rules for the authorized keys (i.e., passive RFID tags) to open the lock, and storing these rules into a database. In addition, when the authorization rules require more than one tag to be presented to open the lock the administrator set the time period for authorization. The keys stored in the database are considered legal, otherwise, they are illegal. Also, the

ISBN: 978-1-5386-0802-9/17/$31.00 ©2017 IEEE

administrator is responsible for setting up the time period for opening the lock.

The users present their tags to PRRU. Next, the PRRU sends the identification (i.e, tag-id or key) to the CSCU. The CSCU filters the repetitive tags during the authorization period. In addition, the CSCU checks whether/or not one of the authorization rules is satisfied. If an authorization rule is satisfied during the authorization period the CSCU signals the DLAU to open the lock for a pre-defined period; next, the lock will be closed automatically. If an opening attempt occurred without a tag reading or with a reading of an unauthorized tag read identified by the PRRU, the CSCU signals the DLAU such that the alarm circuit to raise the alarm so that a break in is notified.

IV. Illustrative Example

In order to clarify the operation of the proposed MPAES, let's consider the following example. The administrator makes the setting of three doors as tabulated in Table I.

According to Table I, Door_1 will be opened for six seconds whenever K1 holder presents his/her tag or (K2 and K3) or (K2 and K4) (regardless the order) are presented during three seconds. Similarly, Door_2 will be opened for three seconds whenever K1 or K2 is presented. Door_3 will be opened for five seconds if K1, K2, and K3 are presented during four seconds. In addition, all doors are locked and MPAES go to alarm state whenever an attempt to open the door without tags or when reading unauthorized tags. Notice that K1 can open door_1, door_2 and participates in opening door_3. Similarly, K2 participates in the rules to open door_1, can open door_2 and participates in opening door_3. From these scenarios, the key has multiple privileges access and can be used to access multiple looks according to the administrator setting.

The period of authorization is important and acts as a watchdog timer. In order for opening a lock for multiple users, it is required to identify the tags within a period of time to prevent undesired function. For instance, consider door_1 in Table I; K2 is tagged, after 1 hours K3 is tagged, without the watch-dog timer the door_1 will be opened. With the aid of watch-dog timer when K3 is tagged, K2 is required to be tagged within three seconds. Finally, the last column in Table I represents the time period to keep the door open, after that time the CSCU signals the DLAU to close the door.

TABLE I. The Administrative Setting for E-Doors

Door_id (Reader-id)	Authorization Rules	Period of Authorization (ms)	Time period for keeping the lock open (ms)
1	{K1}, {K2,K3}, {K2,K4}	3000	6000
2	{K1}, {K2}	-	3000
3	{K1, K2, K3}	4000	5000

V. MPAES Components and Interfacing

Before going to the implementation details, it is necessary to plan the design and selection of modules to be involved in the development. As secure door system runs the software over the hardware components, MPAES consists of hardware and software prerequisites can be stated as follows.

A. Hardware Components

- Raspberry Pi 3.
- GPIO interface sockets.
- Automatic door-lock and its interface circuit.
- A micro switch is a simple sensor to sense whether the door is opened or closed.
- Passive RFID reader and tags.

B. Software Components

- Raspbian Linux operating system for the Raspberry Pi 3[12].
- Netbeans IDE 8.1 and Java Development Kit (JDK) 8 enterprise edition for coding.
- Derby database.

The relational behind selection for these components is described as follows. The benefits of using Raspberry Pi and GPIO socket:

1. Expendability: the available ports in the raspberry pi make it easy to add more hardware and features [13].
2. Portability: raspberry pi has a small size and light weight which makes its setup easy anywhere.
3. Inexpensive compared with other electronic cards.
4. Ease of use and maintain: java programming performed regularly and easily [14].
5. Full computer quality (acts as mini PC) [13,15,16] used as a server to control several doors.
6. Could be connected to another raspberry pi or PC to make a network that controls entire building doors.
7. Raspberry Pi is shipped with free open source Raspbian Linux operating system
8. Raspberry Pi 3 has quad core CPU [16]. As such, it can run multiple threads and processes without affecting the overall performance of the system (e.g., run the main application, the database, networking, watch-dog and observable threads, etc).

Raspberry Pi 3 is shown in Fig. 4.

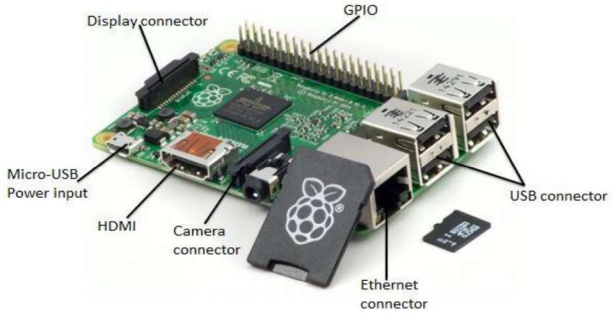

Fig. 4. Raspberry Pi 3 interface.

ISBN: 978-1-5386-0802-9/17/$31.00 ©2017 IEEE

Java programming language is chosen because of its cross-platform functionality [5]. Moreover, Java is fully supported by Raspberry Pi [15]. Furthermore, Derby database is a small footprint database that suitable to be embedded into the Rasperian operating system, Derby is also embedded within JDK. It should be mentioned that these software components are available free for development purposes.

There are many available solutions for the automatic door lock, passive RFID reader, and tags. For automatic door lock, we select a product called UHPPOTE [17]. UHPPOTE provides fail secure(i.e., Locked when power is removed); suitable for any door materials; made of stainless steel, and has built-in voltage spike suppressor for safety. The UHPPOTE is connected to the Raspberry Pi 3 interfaced via the GPIO port. A simple alarm circuit consists of a buzzer and red LED is also connected to the Raspberry Pi 3 interfaced via the GPIO port. The RDM630 RFID reader module is selected due to its low-power consumption; low-cost module and tags; and maximum effective distance up to 50mm[18]. As such, RDM630 can be applied in office/home security, personal identification, and access control. Hence the PRRU consists of the RDM630, RFID antenna, and Serial–USB converter (PL2303HX), Fig. 5 shows interfacing of the passive RFID reader with Raspberry Pi 3.

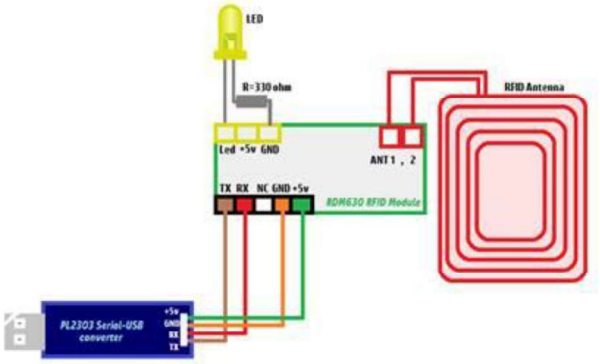

Fig.5. RDM630 interfacing circuit.

The challenge in interfacing the hardware circuit with the Raspberry Pi 3 is auto lock circuit (i.e., for UHPPOTE module) operates on 12-volts, while Raspberry Pi 3 can only provide 3 and 5 volts. To compromise this situation, a relay circuit added, so that the Raspberry Pi 3 turn on the relay circuit, that operates the auto lock circuit which is supplied by the 12-volts battery, as shown in Fig. 6. Notice from Fig. 6, a LED is connected to the normally opened part of the relay indicates that lock circuit is off or on. If the LED is on this means that the lock circuit is open, therefore the lock circuit is off. The lock circuit is connected to the normally opened part of the relay, while the coil of the relay is connected to the GPIO of the raspberry pi, hence, if the raspberry sends a signal, the coil will switch the relay from normally closed to normally opened, which closes the lock circuit. Putting all together, Fig. 7 shows the detailed design of the proposed MPAES. After the hardware components connected to the Raspberry Pi 3, the hardware implementation (prototyping) can be achieved as shown in Fig. 8. It should be mentioned also, that other selection (i.e., variant) of the above-mentioned components could be made without the loss of generality.

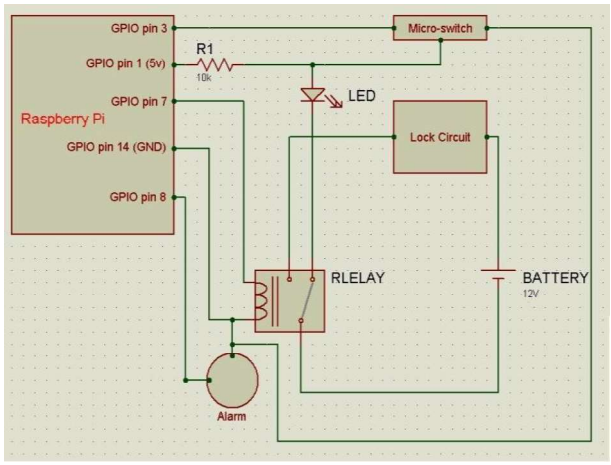

Fig.6. The hardware circuit for interfacing UHPPOTE with GPIO.

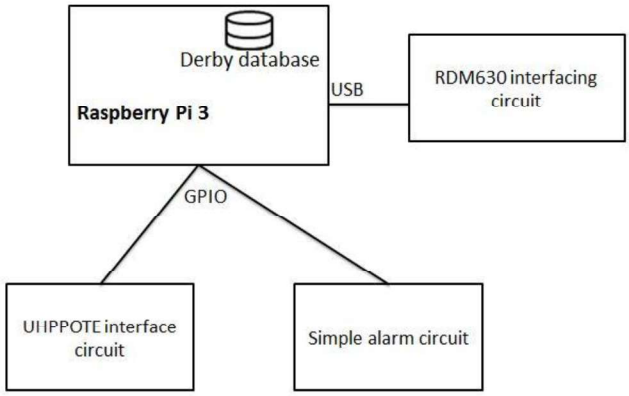

Fig.7. The MPAES detailed design.

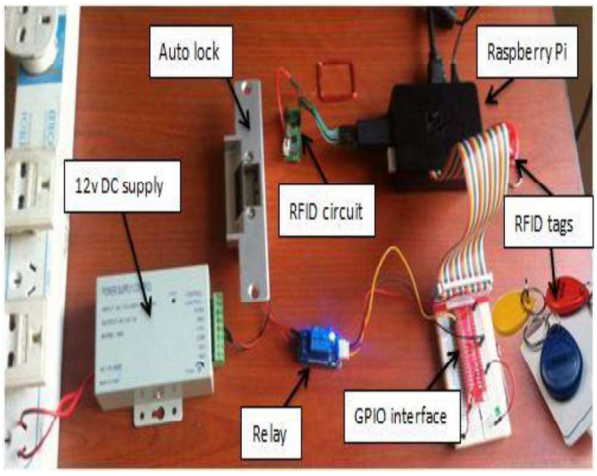

Fig.8. The MPAES prototyping.

ISBN: 978-1-5386-0802-9/17/$31.00 ©2017 IEEE

VI. MPAES SOFTWARE

In IoE development, whenever possible, hardware logic is replaced by software programs, because software is easy to upgrade and software is not wear out. The MPAES software consists of the administrative setting package and the working package. These packages are implemented using Java programming language.

A. Administrative Setting Package

The administrative setting package deals with the Derby database and consists of five sub-packages, these sub-packages are developed using Model-View-Control (MVC) model. The view is a GUI class, the model is the object representation of database entity, and finally, the control is used to facilitates the interaction between the view and the model. As such, the database consists of five tables. In addition, each sub-package consists of three classes. These sub-packages are described as follows:

- Person package: this package is an MVC classes to enter/store/edit the personal information of the users and their roles (users and/or administrator).
- Administrator package: this package is an MVC classes to enter/store/edit the administrator user's name and password.
- User package: this package is an MVC classes to assign the users their corresponding key (i.e., the tag_id).
- Administrative Setting package: this package is an MVC classes used to enter/store/edit the e-door-id, USB port identifier, authorization rules, period of authorization (PA), Time period for keeping the lock open (TK), and the GPIO setting. The GPIO setting consists of five columns; namely, VCC (V), GND (G), OPEN (O), ALARM (A), MICROSWITCH (M); The entry under these columns are the PINs used in the GPIO interface. Table II shows an example of typical entries. According to the business needs, the PINs could be shared or separated. For instance, refer to Table II, V and G are shared among the three e-doors. In addition, A is shared between e-door_1 and e-door_2. Finally, e_door_3 has neither A nor M interfaces.
- Event Monitoring package: this package is an MVC classes used to store/retrieve events to/from the database table. A typical entry includes the door_id, key(s) caused the event, the event (O, Invalid_Tag, Break-in), date, and time. In addition, the GUI (view) contains some reporting query to take the attendance/ departure of individuals, tracking and tracing person functionality.

B. System Package

The System package contains the main class called System and dynamic thread classes. The System class starts after the administrator logged-in. Next, the System class reads the entries from the Administrative-Setting-Table. After that, for each entry, the System class creates an e-door working thread with parameters: e-door-id, USB_port identifier, authorization rules, PA, TK, V, G, O, A, M, and the name of Event-Monitoring-Table. The System runner can reset the system, restart any working thread by GUI.

The e-door working thread starts with the e-door in the initialization state. The initialization state involves sending True to V Pin. False to G and A PINS (when A is not null). When M is not null, the e-door working thread Reads M PIN and checks its value. If the value is true (i.e., the door is closed) the initialization checking is done and the e-door in CLOSED state, otherwise, display a message indicates the door is already opened (i.e., Break in) and send true to the A PIN (i.e., Alarm Signal is True when the M-value is false) and the e-door in ALARM state, and makes an entry to the Event-Monitoring-Table. Next, the working thread enters in an infinite loop (i.e., pooling). The loop starts with creating observable_M_thread that caused the Event door_open whenever the door is opened and the e-door state is CLOSED; whenever receiving this event, the e-door go to ALARM state and makes an entry to the Event-Monitoring-Table. After that, the working thread creates the Authorization_Thread.

The Authorization_Thread starts by continues reading of passive RFID tags from the USB_PORT. After reading the first tag, the thread starts a watch-dog-timer thread for PA value. The reading tags are stored in tags linked list. During PA, the Authorization_Thread checks the authorization rules. If one the authorization rules is satisfied, the Authorization_Thread sends Open Signal (i.e., O=True), and enter in OPENING State and makes an entry to the Event-Monitoring-Table, sleeps for TK, then sends Close Signal (i.e., O=False), clear the tags linked list, and return to the CLOSED State in the pooling loop. If a tag is unauthorized the e-door thread go to ALARM state (by sending A=True), makes an entry to the Event-Monitoring-Table, and clear the tags linked list. If the PA is elapsed, an entry will be made to the Event-Monitoring-Table with null O column value to indicate unsuccessful attempt, and clear the tags linked list.

It should be mentioned that the e-door could go to normal state either by the System class by the administrator or by legitimate users by presenting their tags. The reason behind this is to prevent the denial of service attack when the system reads an unauthorized tag.

VII. CONCLUSION AND FUTURE WORK

This paper proposed a novel embedded system called multiple-privileges access E-Door system. The proposed system can be reconfigured dynamically by the administrator without any change the software code. Moreover, Unlike existing E-Door systems, MPAES is developed in such a way that enables the administrator to set multiple access rules to the users. Unlike the physical keys, the passive RFID tags (keys) can be used to open or participate in opening multiple e-doors.

There are multiple avenues for future work. One avenue is to connect the MPAES to cloud environment in the case of a large-scale system for configuration and monitoring purposes.

ISBN: 978-1-5386-0802-9/17/$31.00 ©2017 IEEE

TABLE II. THE ADMINISTRATIVE SETTING DATABASE TABLE FOR E-DOORS

Door_id	USB_Port	Authorization Rules	PA (ms)	TK (ms)	V	G	O	A	M
1	0	{K1}, {K2,K3}, {K2,K4}	3000	6000	1	14	7	8	9
2	1	{K2,K3}	3000	6000	1	14	2	8	3
3	2	{K1,K4}	3000	5000	1	14	5	-	-

Another avenue is to make a horizontal extension to the functionality of the MPAES by adding other devices like a camera or another biometric identification like face recognition, take a snapshot in the case of an Alarm state. Another avenue is to develop more complex authorization rules (e.g., makes active time for the keys). Another direction in the future work is to derive more secure rules (e.g., put the sequence of entering the keys into account). Finally, the IoE is still developing, there are still unknown tasks to discover. For this reason, more and more digitization of physical world is in the forthcoming research stream.

ACKNOWLEDGMENT

The authors desire to express their gratitude and thanks to AL-Tameer Company for Trading, Transportation and Electromechanical Services and system solutions/Raban Al Safina Companies, Cisco Networking Academy and the Computer Engineering Department, College of Engineering, University of Baghdad for their support to do this research work.

REFERENCES

[1] Cisco Networking Academy, "Introduction to the Internet of everything," Cisco Press, June 2016.

[2] M. Schatten, J. Seva, and I. Tomicic, "A roadmap for acalable agent organizations in the Internet of everything," Journal of Systems and Software, vol. 115, no. C, pp. 31–41, May 2016.

[3] C. Prazeres and M. Serrano, "SOFT-IoT: self-organizing FOG of things," 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Crans-Montana, pp. 803-808, May 2016.

[4] B. M. R. Mahmood, M. I. Younis, and H. M. Ali, "Construction of a general-purpose infrastructure for RFID–based applications," Journal of Engineering, vol. 19, no. 11, November 2013.

[5] M. F. M. Ali, M. I. Younis, K. Z. Zamli, and W. Ismail, "Development of Java based RFID application programmable interface for heterogeneous RFID system", Journal of Systems and Software (JSS), vol. 83, no. 11, pp. 2322-2331, November 2010.

[6] M.I. Younis, Z. F. A. Al-Tameemi, W. Ismail, and K. Z. Zamli, "Design and implementation of a scalable RFID-based attendance system with an intelligent scheduling technique," Wireless Personal Communication, Springer, vol. 71, no. 3, pp 2161-2179, August 2013.

[7] S. A. Mahdi, "Development of anti-theft door system for security room," Academic Research International, vol. 4, no. 3, pp. 237-242, May 2013.

[8] G. K. Verma, and P. Tripathi, "A digital security system with door lock system using RFID technology," International Journal of Computer Applications, vol. 5, no.11, pp. 6-8, August 2010.

[9] U. J. Ogri, D. Enang, B. Okwong, and A. Etim, "Design and construction of door locking security system using GSM," International Journal Of Engineering and Computer Science, vol. 2, no. 7, pp. 2235-2257, July 2013.

[10] A. Mishra, S. Sharma, S. Dubey, and S. K. Dubey, "Password based security lock system," International Journal of Advanced Technology in Engineering and Science, vol. 2, no. 5, pp. 100-103, May 2014.

[11] I. Ha, "Security and usability improvement on a digital door lock system based on Internet of things," International Journal of Security and Its Applications, vol.9, no.8, pp.45-54, August 2015.

[12] W.W. Gay, "Raspberry Pi system software reference," Apress, November 2014.

[13] V. Vujovic, and M. Maksimovic, "Raspberry Pi as a sensor web node for home automation," International Journal of Computers and Electrical Engineering, Elsevier, vol. 44, pp. 153-171, February 2015.

[14] W. W. Gay, "Raspberry Pi hardware reference", Apress, November 2014.

[15] S. Chin, and James L. Weaver, "Raspberry Pi with Java: programming the Internet of things (IoT) ", Oracle Press, 2016.

[16] Raspberry pi official website, https://www.raspberrypi.org/products/raspberry-pi-3-model-b.

[17] https://www.amazon.com/UHPPOTE-Electric-Strike-Secure-Control/dp/B00V45GWTI.

[18] http://wiki.seeedstudio.com/wiki/125Khz _RFID_module_-_UART.

ISBN: 978-1-5386-0802-9/17/$31.00 ©2017 IEEE