IOP Conf. Series: Materials Science and Engineering **433** (2018) 012088 doi:10.1088/1757-899X/433/1/012088

Design and Implementation of an Anonymous Vehicle Identification System Based on the IoT

M S Nasr and W Y Y Alebady

Department of electrical engineering, University of Babylon, Hilla, Iraq.

Email: mahmoud111957@yahoo.com; wallaa.alebady@yahoo.com

Abstract. Security has become an important issue that needs to be addressed in all cities of the world. Simultaneously, information technology is undergoing a period of great development, and it is important to exploit this development in the service of society, particularly in terms of urban security. An Anonymous Vehicle Identification (AVI) system design is thus presented in this research. Much previous research has dealt with the development and implementation of systems to identify anonymous vehicles, and all previously proposed systems appear to work efficiently; however, some are very expensive and others require the installation of many devices within a city. Further, some of them do not transfer information to a control centre in the city using the internet.

The proposed AVI system presented in this paper is thus based on Internet of Things (IoT) and consists of two main parts: a handheld device used by officers, and a web application. The handheld device is used to send car licence plate number to a website which is controlled by an authorised person. The authorised person receives the data and requests information relating to the car (car number, owner's name and mobile number, registered address, etc.) from the Central Traffic Police Directorate, before sending these to the officer's handheld device to allow the officer to take action based on the information and instructions from the central office. The design of web application is based on several techniques and multiple programming languages including HTML, PHP, and Java Script. These languages are compatible with each other and have thus been combined to form the desired application.

The proposed system was implemented practically and tested for about 50 cases; the results obtained during testing were very satisfactory and reflect good reliability within the system.

***Keywords*:** Security System, vehicle identification, AVI, IoT applications.

Abbreviations.

AVI: Anonymous Vehicle Identification.
AJAX: Asynchronous JavaScript and XML.
HTML: Hypertext Mark-up Language.
IoT: Internet of Things.
GSM: Global System for Mobile communication.
GPRS: Global Packet Radio Service.
GPS: Global Positioning System.
PHP: Hypertext Processor.

1. Introduction.

The security situation has posed a crucial challenge for all Iraqi cities since 2003 to the current day. Explosions and congestion have caused multiple security problems, especially with regard to anonymous vehicles.
Several researchers have presented varying systems for anonymous vehicle identification. The core point of the research of Stephen G. Ritchie [1] was an algorithm for signalized intersections based on inductive vehicles that used laser techniques and GPS tracking; for Oh. Cheol, et. al. [2], vehicle reidentification utilised the same traffic sensors (conventional square inductive loops) and detectors (high-speed scanning detector cards) at both locations; while for Magdy Kozman, et al [3], Bluetooth technology was used to detect a given car, and a huge number of Bluetooth enabled phones, about 1,123, were installed along the road from Houston to Dallas.

Internet of Things (IoTs) is a smart technology that connects the world as if it were a small region. All required sensors and objects can be connected with each other to share and handle obtained information from multiple different places to coordinate multiple applications such as telemedicine, industry, and traffic [4][5].
The IoT revolution has changed the course of technologies in several fields, especially in recent years [6]. General Packet Radio Service (GPRS) is one such technology, and it now plays a major role in systems such as that proposed in this work (AVI), in addition to its use in Global System for Mobile Communication (GSM) technology. GPRS technology is an excellent method for transferring data to the web, as it is characterized by its low cost and fast response times [7][8].
The Anonymous Vehicle Identification (AVI) system proposed in this paper could be one of the leading systems in Iraq and other countries if given appropriate care and development in the coming years, as the designed system is an initial step towards an integrated IoT AVI system. Research institutions and firms predict that 100 billion devices will be connected to the IoT cloud by 2025, and IoT offers a tremendous ability to connect a wide range of devices via various techniques and protocols [6]. Conventional applications such as control systems, wireless sensor networks, and home automation are likely to become more intelligent and efficient due to the IoT revolution, and IoT has a wide range of applications in different fields and specialties such as smart cities, intelligent traffic systems, telemedicine, and wearable instrumentations. Media applications enabling exchange and advertising worldwide are also one of the current vital applications of IoT [6] [9].

2. Proposed Anonymous Vehicle Identification system (AVI)

The proposed system is comprised of two main parts: a handheld device and a web application. If an officer or security personnel have any doubt about a parked vehicle, they can send its plate number

to the Monitor Center Station (MCS) via the handheld device. In the Monitor Center Station, an authorised person monitors the web application of the AVI continuously; once the officer's request has been received, the user, as an authorized person within the MCS, re-sends the information on the vehicle to the officer through the officer's handheld device. Based on the received data, along with any accompanying instructions, the officer can act in a proper manner.

3. System Design.

The structure of the proposed AVI system consists of two parts, as depicted in figure 1. The first is the officer handheld device which remains with an officer, and the second is the web application and database. The web application is the interactive part of the system through which the whole system can be monitored and controlled, while the database is the storage unit.

A special Android application installed on a smart Android phone can replace the OHD, but this is vulnerable to hacking than the OHD. In the following sections, further details are presented.

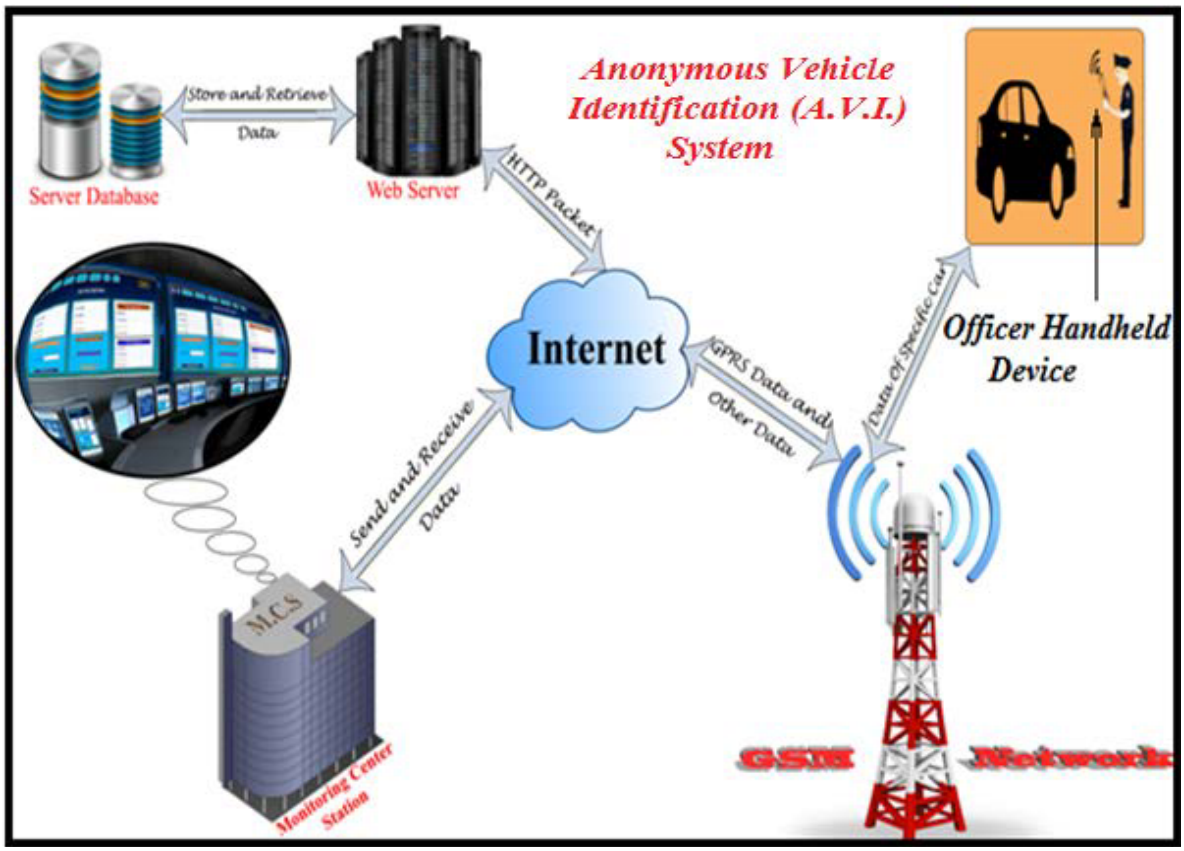


Figure 1: Structure of proposed Anonymous Vehicle Identification system.

3.1. Officer Handheld Device (OHD)

The officer handheld device is the portable part of the AVI system, with both hardware and software components.

3.1.1. Hardware Structure. The hardware structure of the officer handheld device has several elements specialised tasks such as input, output, and processing:

a. Keypad. This element is utilised to input required data such as the officer's password, the car plate number, and other details.

The keypad uses a 4x4 matrix as depicted in figure 2 that is programmed to allow entry of several symbols, letters, and numbers.

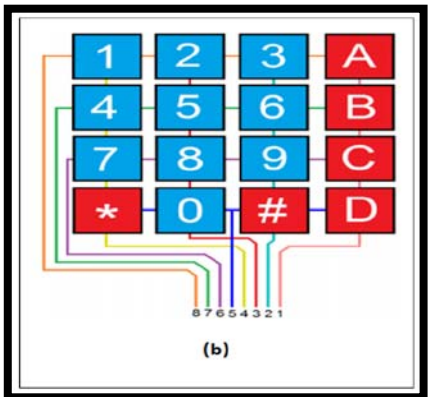


Figure 2: 4x4 keypad.

b. Character Liquid Crystal Display (LCD). This device is used to output unit. A 20x4 I2C-LCD is used in the officer handheld device to display the entered and received data.

This basic format is used to reduce the number of required GPIO pins on the microcontroller and to prevent a large number of connections that complicate the electrical circuit. An I2C interface LCD module requires only two lines (SDA and SCL) to display the required data as shown in Figure 3. To support this module, a potential-meter is used to adjust the display contrast.

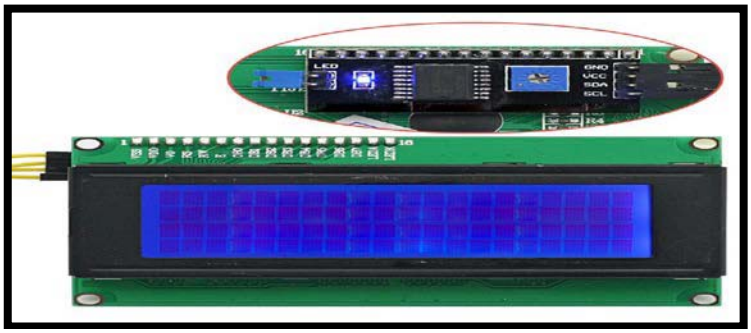


Figure 3: 20x4 I2C-LCD.

c. Processing unit. The processing unit is the device's "brain", tasked with control and processing. In the proposed device, an ATmega2560 microcontroller is used as the processing unit as a result of its programming flexibility, low energy consumption, high durability, open source

software and hardware, and low cost [10]. The ATmega2560 is connected with all hardware elements of the device to form the inner architecture of the device, as depicted in figure 4.

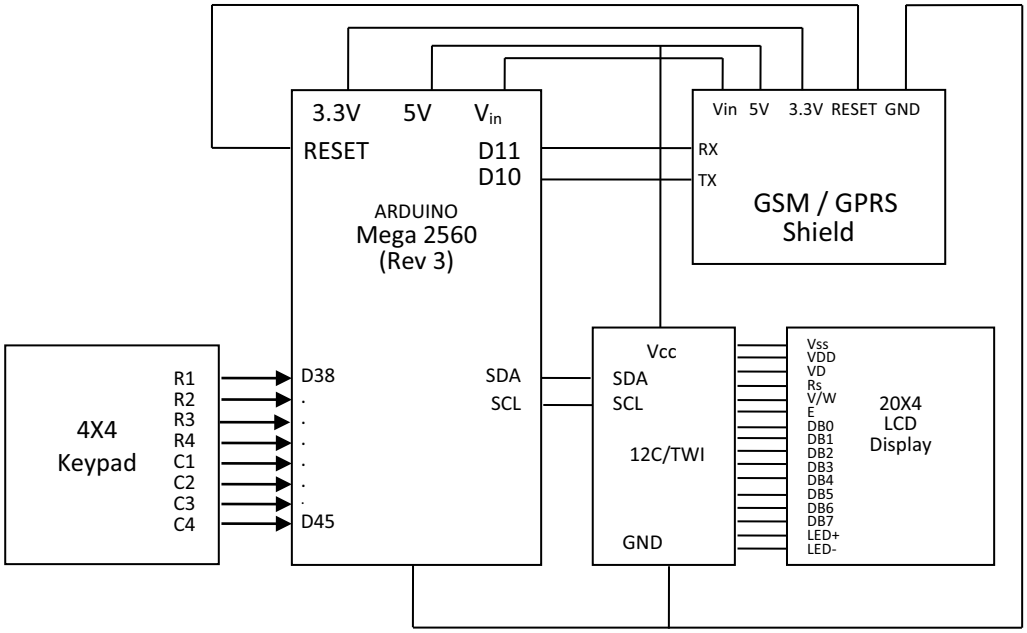


Figure 4: The inner structure of an officer handheld device.

d. SIM900 Quad-band GSM GPRS Shield. The officer handheld device is a type of communication device, and the communication unit is thus an essential part. This unit is used to send and receive data from and to the device. The SIM900 Quad-band GSM GPRS Shield, shown in figure 5, is used as a communication unit within the officer handheld device. The Quad-band GSM/GPRS Shield relies on a SIM900 module from SIMCOM. This module can be controlled via AT commands and is compatible with the Arduino platform. The GSM/GPRS shield requires an unlocked SIM card in addition to the power conditions listed in table (1) to connect with the GSM network [11].

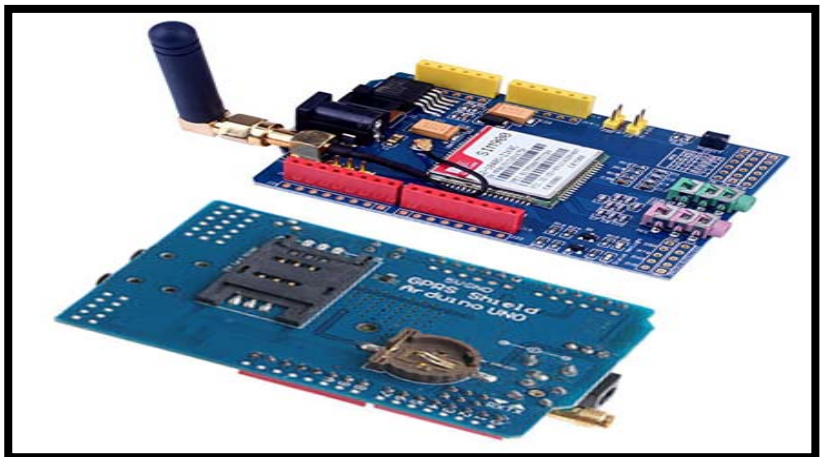


Figure 5: SIM900 Quad-band GSM/GPRS Shield [11].

Table 1. Power conditions for GSM/GPRS operation.

Parameter	Condition	Min.	Max.	Units
Vin		5	12	V
Current	Sleep mode		1.5	mA
	Voice call		250	
	GPRS Data Mode	76	440	
	During TX Burst		2	A

e. *Power unit.* The power unit is a critical part in all portable devices such as phones and GPS devices. The officer handheld device has two separate power sources, one for the microcontroller and the other for the SIM900 Quad-Band GPRS shield. A 9-v lithium-polymer battery with 350 mAh is used to drive the microcontroller; however, the SIM900 Quad-Band GPRS shield requires another source because it draws a higher current during data transmission of up to A. Thus, two 3.7 V/2.2 AH lithium batteries connected in series are used to solve the problem of the current requirements; however, 7.4 V is a large potential to drive the shield. Thus, the LM2596S step up down power converter module is used to regulate the voltage to 5 V. In addition, the SIM900 Quad-Band GPRS shield can be driven from an external source.

Two power supplies are used rather than a single power supply because a reliable power supply of this type was not available.

Figure 6 shows the implemented device details and a photo of the final form of the device.

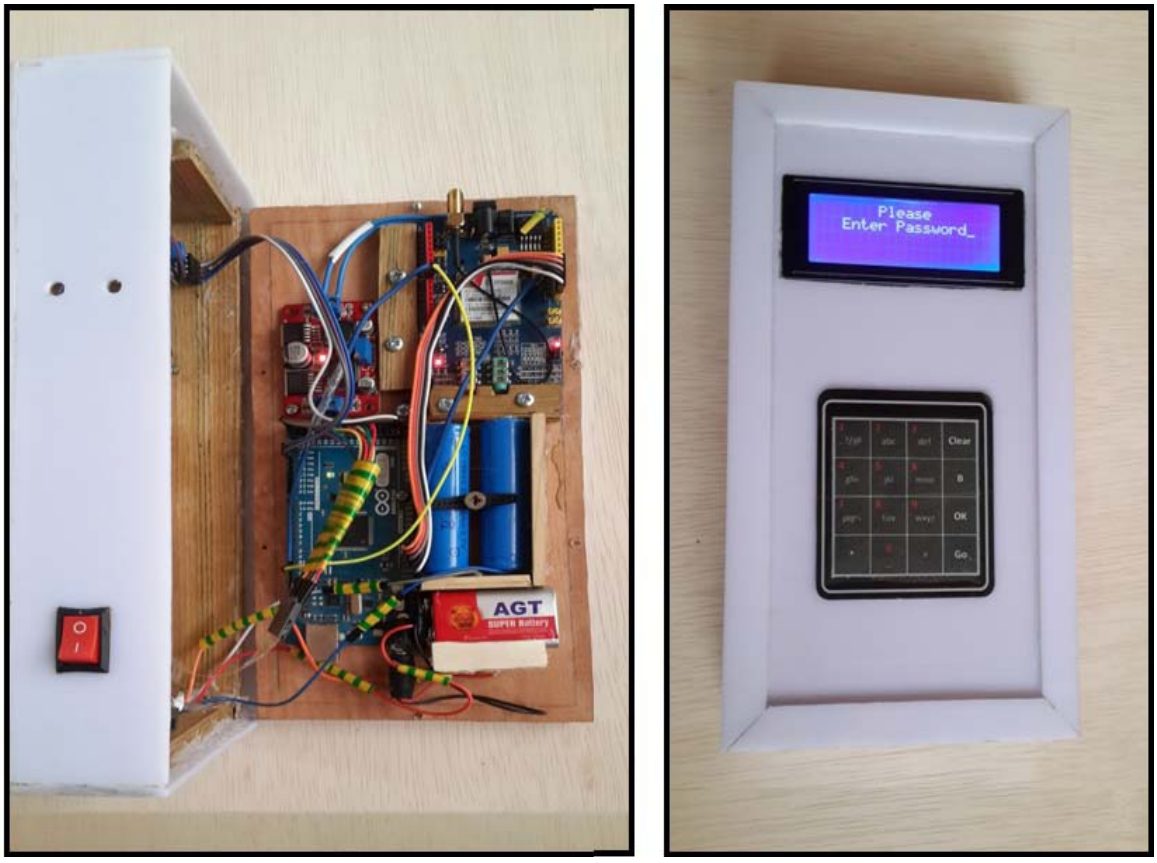


Figure 6: Final form of the officer handheld device.

3.1.2. Software. The software program for the officer handheld device is comprised of several steps, as illustrated in figure 7.

3.2. Database and Web Application

The AVI requires a smart web application to enable it to be an intelligent system that relies on IoT technology. Thus, modern programming languages and techniques have been used to design a smart application to provide the connection between elements of the system that include the Monitoring Center Station (MCS), the OHD, the officer device, and the Traffic Center (TC).

The proposed web application is designed to perform sending, receiving, controlling, and monitoring. The web app has been designed using HTML, CSS, JavaScript, PHP, and MYSQL database. These languages and database are compatible with each other and were thus collected to form a modern application. The database is a significant part of the application, and the MYSQL database is used to store system information that includes data on vehicles, devices, users, supervisors, and officers. This database is part of main server.

As shown in figure 8, the main page of the web app has several parts, each responsible for a specific function.

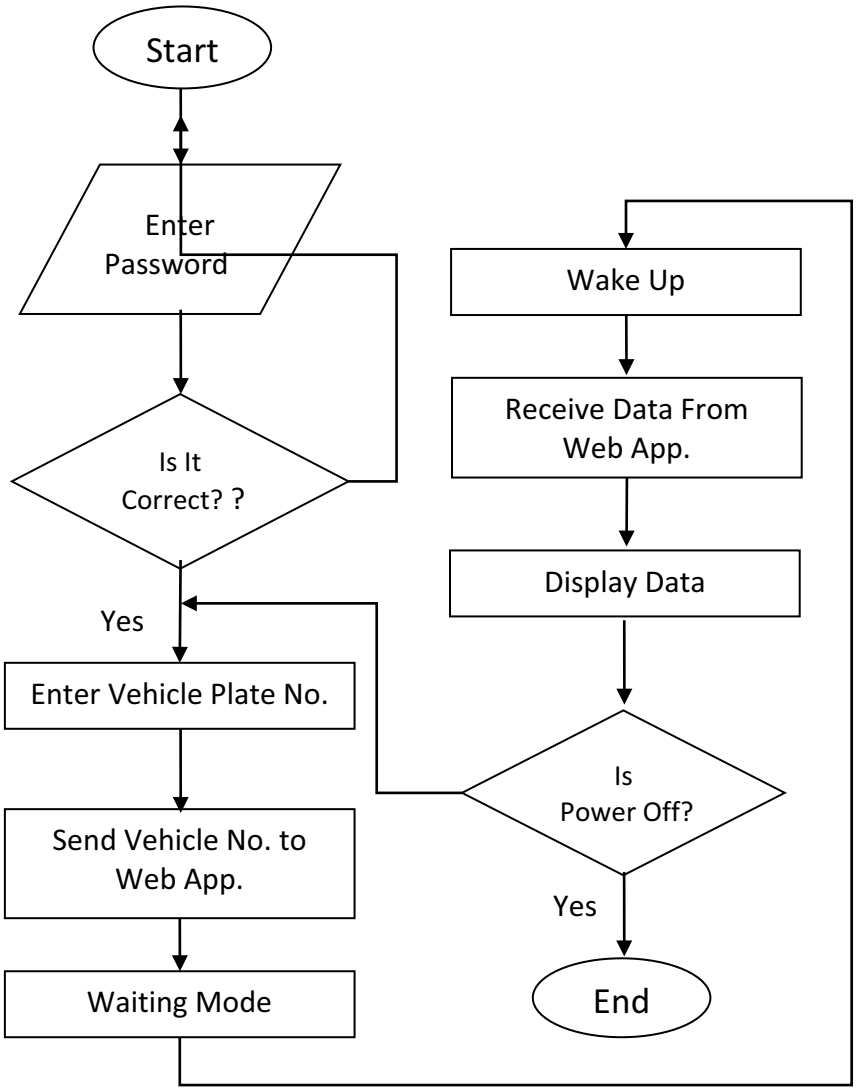


Figure 7: Software flowchart for the officer handheld device.

4. System Features

The proposed system has the following features:

- Relatively low cost compared to similar systems.
- Bidirectional transmission system with machine-to-machine communications between the officer and the monitoring centre station.
- Friendly, clear GUI, and simple-to-use system.
- Secure system: the OHD and the pages of the web application are protected by a password and login pages, respectively, to prevent use by unauthorized persons.

- Robust against adverse climatic conditions: using the GPRS technique makes the system less affected by climatic conditions.
- Ubiquitous: the web app can be accessed by an authorized user at any place and any time.

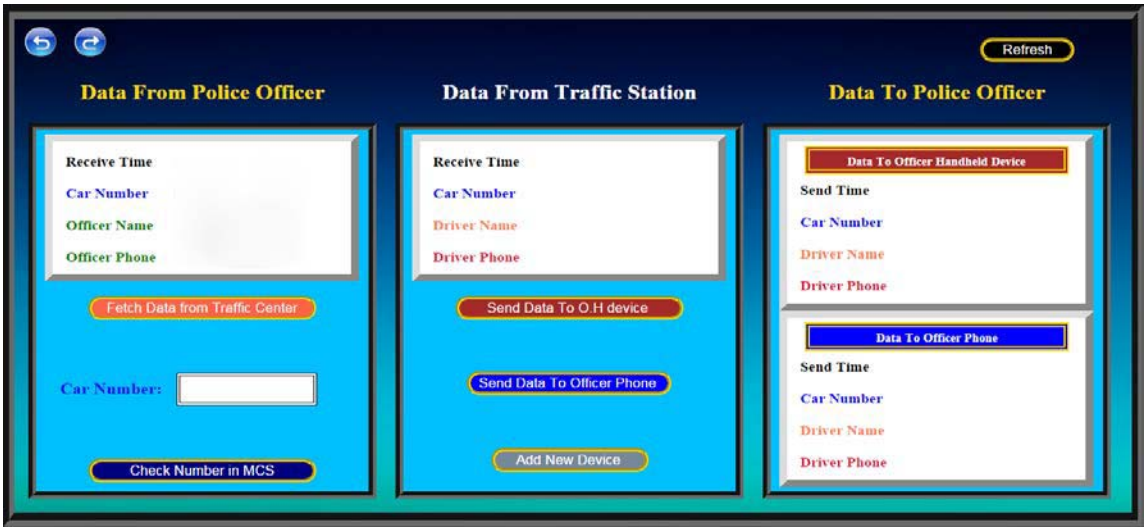


Figure 8: Main page of the system's web application.

5. System operation.

In terms of operation, the proposed Anonymous Vehicle Identification system is divided into two sections: the handheld device side and the web side. The operation of the system begins at the handheld device side and en there, with the web side acting as a middleware layer. The system operation can be explained in the following steps:

Handheld device side: (see figure 6)

a. An officer or any person authorised to use the device turns on the device and unlocks it with the password.
b. The anonymous car number is entered and the "GO" button pressed to send the information to the web application.
c. The user then awaits data from the web application.

Web side: (see figure 8)

d. The employee managing the web application receives the new data.
e. The employee copies the car number and pastes it in the "Car Number" field, then presses the "Check Number in MCS" button. If any results ensue, go to step **g**; else, go to step **f**.
f. Press the "Fetch Data from Traffic Center" button.
g. After receiving any data/confirmation of no data, press the "Send Data To Device" button.
h. If there is any problem sending the data to the officer handheld device, press the "Send Data To Officer Phone" button.

Handheld device side:

i. Data arrives at the device from the web application.

j. After fifteen second, the data disappears from the screen for security, and a window appears telling the officer to press **"*"** to retrieve the data or to press the "**GO**" button twice to send another car number.

6. Results and Discussion.

In order to examine the reliability of the proposed system, it was tested in more than 50 cases. After a vehicle's plate number was sent via the handheld device to the web application (as shown in figure 9), the officer's and vehicle's data (car number, officer's name, officer's phone number) appeared on the main page of the application as shown in figure 10. There are two options for calling up vehicle-related data: The first option is to retrieve fetch them from the monitoring centre station and the second option is to retrieve them from the Traffic Police Directorate.

After retrieving vehicle-related data, these can be sent from the web application to the handheld device or to the officer's phone. Figure 11 shows the process of sending the data to the OHD, while Figure 12 shows the process of sending the data to the officer's phone.

According to the test results, the proposed system offers high security with a reliable, real time response.

Figure 9: Sending the car plate number to the web application

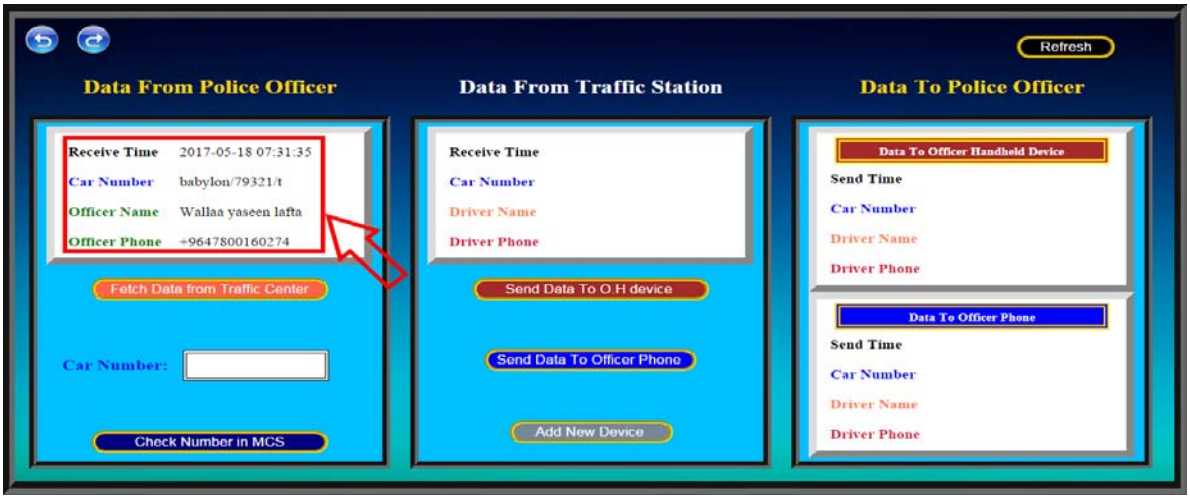
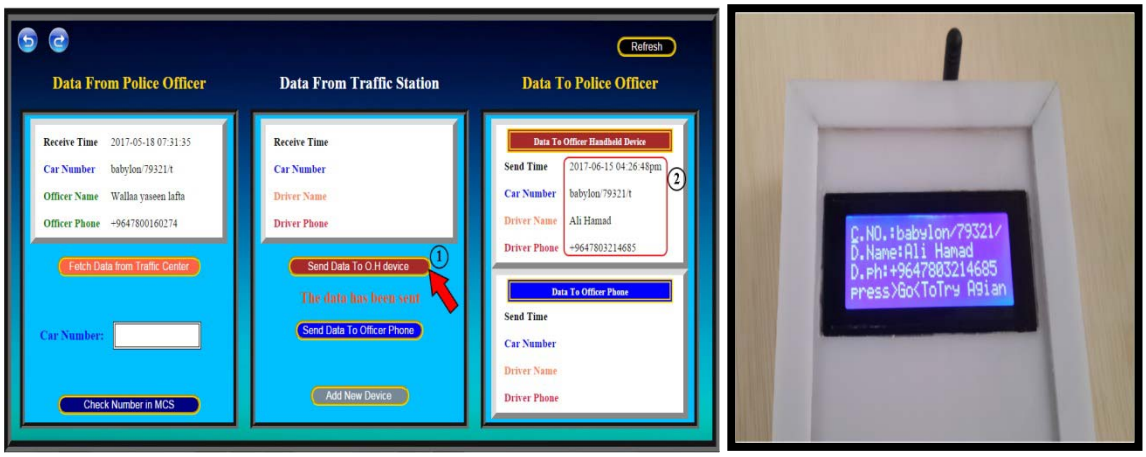
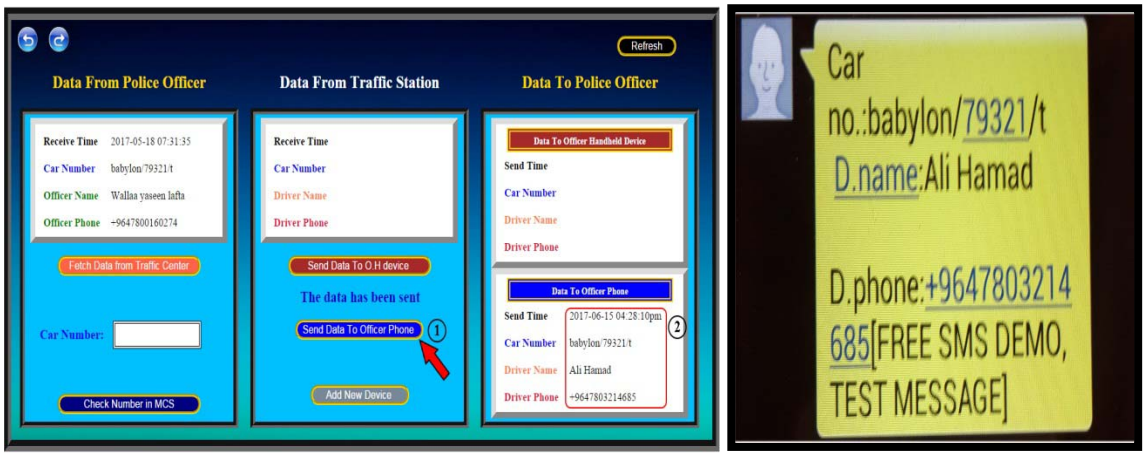


Figure 10: Receiving the data from the handheld device.



(a) (b)

Figure 11: (a) Sending the vehicle-related data to OHD. (b) Receiving the vehicle-related data from OHD.



(a) (b)

Figure 12: (a) Sending the vehicle-related data to a phone device. (b) Receiving the vehicle-related data on a phone device.

7. Conclusions.

The proposed system was designed to contribute to resolving several modern security problems with a solution based on IoT technology. GSM and GPRS form the backbone of the system, though other technologies have been used in the system's design.

The GPRS technology used offers a low-cost option in addition to providing a reliable and fast system. In case of internet failure, the system can be operated using the GSM service. The presented system can also be added to other related systems, as it is characterised by low cost and available technology.

It is worth noting that human intervention does not generally exists in public systems that use internet technology, and this is was indeed implemented in the first version of the presented system; however, due to the seriousness of the security situation, experience suggested that it is necessary to have control over information transmission in the form of an employee.

In terms of future work, the handheld device could be remanufactured using modern micro components to simulate a modern portable device, and the manual entry process for the car plate

number could be replaced by taking a picture of the car registration plate and using image processing technology.

References

[1] Stephen G and Cheol O 2003 *Anonymous Vehicle Tracking for real time surveillance performance on signalized arterial*, TPR paper number 03-4347 presented to the 82nd annual meeting of the transportation research, Washington DC, January.
[2] Cheol O, Jeng, Shin-Ting, Ritchie, Stephen G 2007 *Anonymous vehicle reidentification using heterogeneous detection systems,* IEEE Transactions on Intelligent Transportation Systems, No.3 September.
[3] Magdy Kozman P E 2015 *Automatic Vehicle Identification (AVI) Versus Anonymous Wireless Address Matching (AWAM) also known as Bluetooth,* Texas Department of Transportation Operation Engineer.
[4] Dave E 2011 *The Internet of Things; How the Next Evolution of the Internet is Changing Everything* (USA: *Cisco IBSG*).
[5] Ajay R M 2007 *Advanced Cellular Network Planning and Optimisation 2G/2.5G/3G ... Evolution 4G,* (England: John Wiley & Sons Ltd).
[6] Karen R, Scott E and Lyman C 2015 *The Internet of Things (IoT): An Overview, Understanding the Issues and Challenges of a More Connected World* (USA: *Internet Society (ISOC) organization*).
[7] Geoff S, Lionel T, Manfred R, Oliver R and Stefan D 2003 *GPRS Networks,* (England: John Wiley & Sons Ltd).
[8] Jörg E, Hans-Jörg V, Christian B and Christian H 2009 *GSM – Architecture, Protocols and Services,* (UK: John Wiley & Sons Ltd).
[9] Kondamudi S S R and Gupta A N P S 2016 IoT based Data Logger System for weather monitoring using Wireless sensor networks *Int. Journal of Engineering Trends and Technology* (IJETT) **32** India 71-75.
[10] https://www.arduino.cc/en/Main/ArduinoBoardMega2560/
[11] http://linksprite.com/wiki/index.php5?title=SIM900_GPRS/GSM_Shield.