VOL. 16, NO. 2, 2017, 39-43
www.fke.utm.my/elektrika
ISSN 0128-4428

ELEKTRIKA
Journal of Electrical Engineering

GuardExpert PRO: Application-centric IoT solution for Guard Touring System

Amirul Hazeim Faizul and **Rozeha A. Rashid***

[1]Faculty of Electrical Engineering, Universiti Teknologi Malaysia, 81310 UTM Skudai, Johor, Malaysia.

*Corresponding author: rozeha@utm.my, Tel: 607-5535218, Fax: 607-5566272

Abstract: Internet of Things (IoT) technology promotes remote data acquisition and device control across wireless network infrastructure and is a catalyst for increasing internet-connected applications. This paper presents the development of an IoT based application for a guard touring system (GTS). A traditional GTS lacks real-time functionalities such as data upload, multitasking, summon features as well as competitive pricing. It is proven that the developed IoT based GTS, which consists of an Android application, web browser and cloud database, enables easy deployment and monitoring of guard's patrolling activities. The performance analysis shows that the accuracy for Global Positioning System (GPS) location tracking has by default a 68% confidence level within a set geo-fencing radius of 25 meters while the end-to-end delay is about one minute over cellular and Wi-Fi networks from a test run within UTM campus.

Keywords: Internet of Things (IoT), Near Field Communication (NFC), Graphical User Interface (GUI), Guard Touring System (GTS), Radio Frequency Identification (RFID).

1. INTRODUCTION

Internet of Things (IoT) is a technology where all the devices, appliances, sensors, vehicles and wireless enabled systems can be controlled by finger tips or remotely due to their connectivity to the internet. It is a network of physical objects that can interact with each other to share information and make a decision [1]. Many traditional devices which have evolved to become IoT based devices can collect and transmit data as well as enabling control via smartphones because of the network connectivity. Some examples of these devices or systems are smart home monitoring system, smart car park barrier, smart door access, smart bird house and also smart guard touring system. IoT applications measures real world analog phenomena that will be digitized by IoT devices that contain processors, memory and sensors. These sensors need to connect to a network to send the digital data to the cloud. There are many options of networking to serve the gateway to choose from, such as 2G/3G/4G/LTE as well as the upcoming 5G, Wi-Fi, Zig-Bee, Satellite, Bluetooth, Ethernet, and local broadband options. Furthermore, utilization of mobile information and communication technologies in home monitoring applications are becoming more and more common [2].

The conventional GTS lacks features for real-time deployment. Useful functions such as software application for monitoring purposes, summon features, image reporting, direct editable text interaction with management and automatic database updates are not present. Subsequently, there is no real-time evidence or records the guards had done the rounds or patrol their daily assigned area. The process of manual updating of database in the existing system is also error-prone in cases of excessive of touring tasks assigned. Thus, the conventional GTS requires more operational expenditure (OPEX) as more resources is needed in man power and time to manage some of its manual processes. In addition, the capital expenditure (CAPEX) for conventional GTS device is also too expensive given the provided features.

Therefore, in this project, the development of application-centric IoT solution for a Guard Touring System (GTS), named GuardExpert PRO, that provides audio and image communication, cloud database management and Global Positioning System (GPS) technology is proposed. The NFC reader in the smartphone will be used as the medium for collecting data while patrolling. A web browser will also be designed for easy and user-friendly access. The system performance will be investigated in term of network delay and GPS accuracy to guarantee it is within acceptable time limit and distance limit.

This paper is organized as follows. In section II, we discuss the modules of the developed system. Subsequently in section III, the proposed architecture for the IoT based GTS is introduced. Section IV presents the results and discussion. Finally the conclusion is drawn in the last section.

2. RELATED WORKS

Due to the rapid growth of mobile technology for the past centuries, network planning and optimization are major issues [6]. It is noted that when there are simultaneous multiple calls or activities on the carrier network, the network will be overloaded thus leading to system failure.

The use of smartphones as gateways has brought some challenges due to the lack of continuous network connectivity [7]. The tradeoffs of delay tolerant networks in energy, latency, and storage while improving technology are addressed in [7].

The proposed GPS tracking system in [8] uses a differential GPS (DGPS) for improved accuracy of GPS tracking. It requires operating a GPS receiver around familiar location. The receiver is used to compute satellite pseudo range correction data using stored knowledge of the correct satellite pseudo ranges, which is then broadcast to users around the same geographic area. The pseudo range corrections are integrated into the navigation solution of another GPS receiver to correct the observed satellite pseudo range measurements, thereby improving the accuracy of the position determination.

The proposed IoT based Smart GTS in [9] deploys a NFC reader to obtain the identification of the guards and Wi-Fi Access Point to upload the collected data to the cloud database. However, it has high cost to benefit ratio.

IoT based Home Intercom System proposed a system with notification and video which is developed to provide a solution for issues of remote home control and security by identifying people at the front door via a smart phone [10]. However, the graphical user interface lacks features as well as no server and database involved [18].

3. SYSTEM MODULES

The main modules of the proposed system are presented in the proceeding section.

3.1 Guard Touring System

Guard touring system (GTS) is basically a system that records and manages guard patrolling activities. With IoT, it can be transformed into a platform that optimizes security sites or patrol route coverage. There is normally a monitoring page for administrator to capture all of the data generated by patrol guards from their daily security operations. This is used to ensure the guards perform their daily touring routine and records are uploaded real time and kept as evidence.

3.2 NFC System

Near Field Communication (NFC) is a short-range wireless communication protocol which was adapted from Radio Frequency Identification (RFID) technology [7]. It uses standards ISO 14443 and the operating frequency is 13.56MHz. Its operation is quite similar too except the distance required is much closer to its target (approximately 10cm) compared to RFID. NFC reader can be operated in any of these three modes, which are card emulation mode, reader/writer mode and peer-to-peer mode because it supports two-way communication. Reader/writer mode allows NFC tags to read information or write into embedded chips and is adopted into this project as this function is used in the embedded NFC reader from smartphone.

3.3 Java Integrated Development Environment (IDE)

An IDE is basically a programming environment that has been integrated as an application program, typically consisting of a code editor, compiler, debugger, and graphical user interface (GUI) builder [4]. Android Studio is an IDE framework using a common set of APIs to connect code editors, compilers, debuggers, and other build in Android Studio compatible tools. Although it is optimized for Java, Android Studio can work with APIs that hook into other languages such as XML. This Java-based framework is made up of two components: The Android SDK Platform, a runtime library that provides the basic IDE elements such as an application's data presentation, configuration, and template coding that are mainstream to be used by users or programmers and user interface; and the IDE itself, which provides controls, such as editing and version control, for the platform's functionality [5].

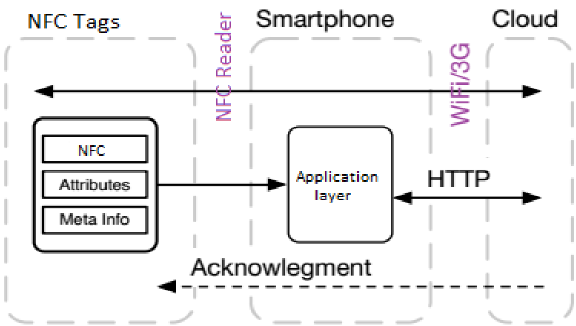

Figure 1. NFC Work Frame

3.4 GSM Based Network Operators

The fundamental services offered by these GSM network operators are significant as the enabling platform for nearly 80% of the application's functionalities developed for the proposed system. Among those functionalities are sending text messages as well as sending notification in terms of email and GPS map location tracking. Thus, a reliable internet and voice call in and out services provided by these network operators are key requirements.

4. SYSTEM ARCHITECTURE

This section discusses in detail about the methodological approach in design and development of the IoT based guard touring system and an Android-based application. The methodology includes the overall system and the programming flowchart.

4.1 Methodology

The guard touring system will be used by the guard or employee and it is connected to the internet via GSM/3G/3G network from the smartphone. It also can be connected via Wi-Fi network as an alternative to send and receive data. In order to make the network connection, User Datagram Protocol (UDP) is used to send data. In this system, the embedded NFC reader in the smartphone acts as the data collector, while a webpage is designed for cloud database management and for real-time monitoring by the authorized personnel. The data collected by the NFC reader then will be uploaded to cloud server through the internet to be retrieved by the administrator.

4.2 System Flowchart

Figure 2 and Figure 3 show the flowcharts for the IoT based guard touring system. In this section, the guard is referred to as the user.

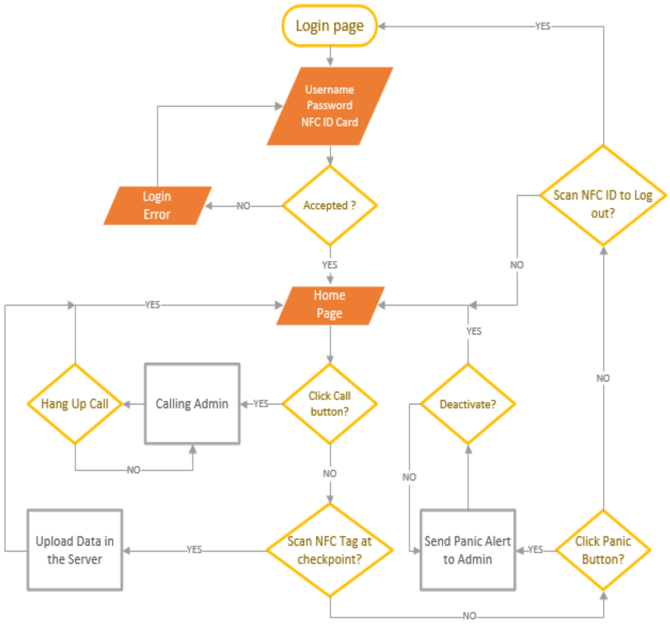

Figure 2. Flowchart of the NFC Reading, Panic Button and Call part of the system

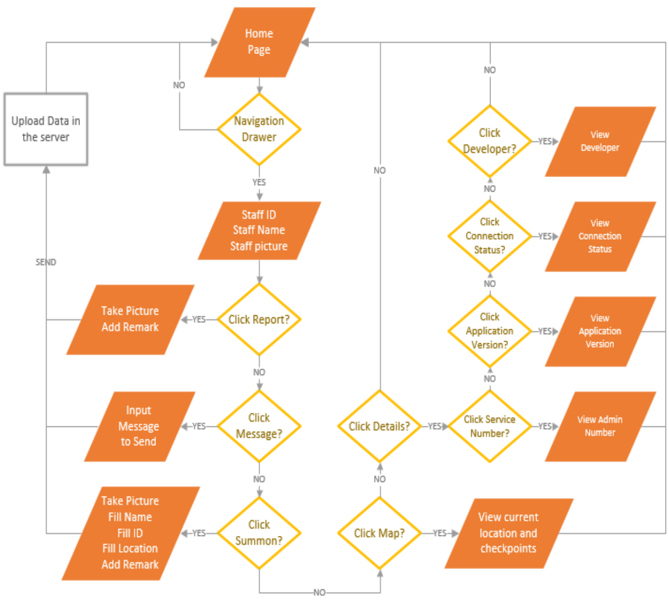

Figure 3. Flowchart of the Camera, Summons, message and Map part of the system

The functionality of the administrator's monitoring web page is shown in Figure 4. Only an authorized personnel will be given the account to log into this facility. Upon logging in, the administrator will have full control on the communication and monitoring of the guards.

4.3 Hardware Modules

The hardware modules involved are NFC embedded Android smartphone, a network operator SIM Card and NFC tags to be placed at respective checkpoints for scanning purposes.

The NFC reader on the smartphone is used for checkpoint scan and real time upload to the cloud server. The NFC tags are assigned and set to a location via its NFC tag ID. The tags are scanned for their ID and their ID is then designated to the desired locations along the patrol route.

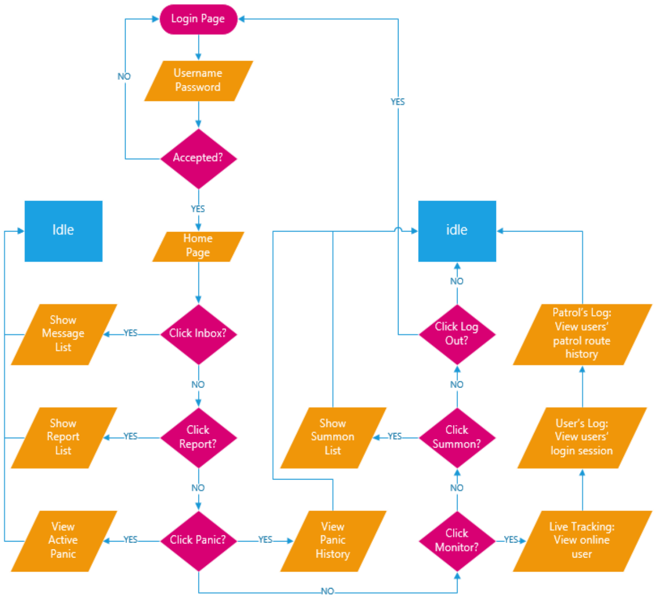

Figure 4. Flowchart of the Monitoring Web Page

4.4 Software Development

The software development for this project is divided into two parts which are the development of the Android Application and secondly, developing the webpage monitoring for management. Java language is the main programming language in order to establish the function activity for the Android App while HTML, PHP, JavaScript, *json* and *.css* are the main languages to develop the webpage monitoring for management.

There are three parts in Android Studio that need to be programmed to create and design the application's interface which are *java* part to configure the function, *xml* part to configure GUI and *android manifest* to configure permission for the android system within the smartphone. Every languages used in Adobe Dreamweaver also have their own task handlers. HTML is to handle the basic content of the web page. PHP is to handle the communication between web page and server. JavaScript is to handle the dynamic activity command in the web page. *.css* is to handle the design and styling of web page content. *json* is to handle the flow of data from web page to the server and database.

5. RESULTS AND DISCUSSION

This chapter presents the results achieved from the testing of the completed work. Finally, analysis is made on the data collected to investigate on the determining factors that influence the GPS accuracy and delay tolerance.

5.1 GPS Location Tracking

The reliability of the system's GPS location tracking in this project is investigated through outdoor experiments. Indoor experiment is not viable as obstacles such as walls and roof will contribute to poor reception of GPS signal. The investigation is run with a geo-fencing limit set at 25 meter in radius as shown in Figure 5. This limit is the decision threshold whether a new reading on location positioning should be taken or otherwise. Too many readings taken can lead to false or redundant location positioning while too few readings might give less accuracy. If the limit is set at a lower value with the intention of obtaining a more accurate location positioning, in the event when the GPS signal is poor, the Android application might not be able to give any respond, which results in lesser obtained data. The technical specification for an Android device indicates that by default, it should have 68% confidence level for location accuracy. This means that for every location reported by the Android device, there is a 68% probability that the location is correct within the set limit. In terms of transmitting data, the application should transmit a location update as one data when the user exceeds 25-meter radius from the previous uploaded location. The calculation is explained further by equations (1) – (3):

$$A \div B = C \quad (1)$$

$$0.32 \times C = D \quad (2)$$

$$C + D = E \quad (3)$$

A is the total distance travelled during the patrol; *B* is the radius interval set; *C* is the number of data that the system is 68% confident is true; 0.32 is the 32% remaining of the confident level; *D* is the number of extra data sent; *E* is the maximum average data acquired in the database. So, implying this algorithm to the tested patrol:

$$2200 \div 25 = 88$$

$$0.32 \times 88 \approx 28$$

$$88 + 28 = 116$$

Thus, average point sent, X is in between $88 \leq X \leq 116$.

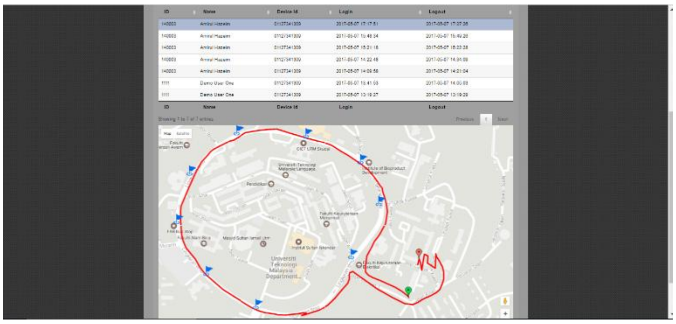

Figure 5. Complete Patrol route for testing GPS location

Thus, theoretically, the average number of location data sent should be within the range of 88-116.

5.2 Network Latency

The investigation for the end-to-end network latency involves three different cellular network operators inside UTM campus. Figure 6 shows the resulted delay for sending messages over Digi, Celcom and U-mobile cellular networks at several locations. The results are within acceptable limit as on average, the end-to-end delay is around one minute. Transmitting and receiving messages over Wi-Fi also registered almost similar results. The delay is observed to be longer for transmitting and receiving messages with image as presented in Figure 7. Over the cellular network, it can take up to two-minute for sending image data. The delay is reduced by 30 seconds on average for sending image data over the Wi-Fi network. Note that for practical usage, this end-to-end delay depends heavily on the network coverage of the network operators and the signal strength of the Wi-Fi connection at a specific location.

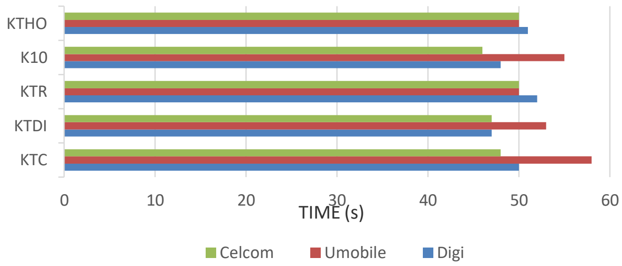

Figure 6. Results for sending message using three different cellular networks latency around UTM

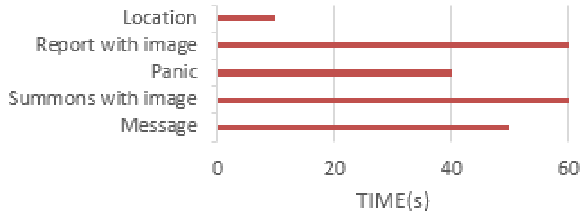

Figure 7. Results of sending data using cellular network (CELCOM) latency around checkpoints location

6. CONCLUSION

A IoT based Smart GTS, named GuardExpert PRO, is successfully developed using an Android application that can connect wirelessly, upload data in real-time and equipped with many attractive features such as audio and image incident reporting, GPS location tracking, panic button, call in and out, as well as low cost to benefit ratio among others. This application provides autonomous and easy deployment for the guards as their patrolling activities can be managed via a smartphone by using the NFC reader on their smartphones for checkpoint scan and real time upload to the cloud server. The designed web browser enables real-time, ubiquitous and remote information services via an integrated monitoring web page for administrator using cloud (iotwave.utm.my). It also provides complete visibility into scanned or missed checkpoints in real time. Instant activities reports and history logs are also included in the features. The investigated GPS accuracy for location tracking has by default a 68% confidence level at a set geo-fencing radius of 25 meters while the end-to-end delay is about 1 minute on average over cellular and Wi-Fi networks from a test run within UTM campus.

ACKNOWLEDGMENT

The authors wish to express their gratitude to Ministry of Higher Education (MOHE), Malaysia and Research Management Center (RMC), Universiti Teknologi Malaysia for the financial support of this project under GUP research grant no: Q.J130000.2523.14H35.

REFERENCES

[1] V.Sandeep, K.Lalith Gopal, S.Naveen, A.Amudhan, L. S. Kumar. Globally Accessible Machine Automation Using Raspberry Pi. International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2015. p.p 1144 – 1147.

[2] T.-L. Chen, T.-C. Hsiao, S.-C. Chen, Y.-F. Chung, Y.-M. Huang, and T.-S. Chen, “Patrol management system applying RFID to petrochemical industry,” 2013 IEEE International Conference of IEEE Region 10 (TENCON 2013).

[3] M. Mareli, S. Rimer, B. Paul, K. Ouahada, and A. Pitsillides, “Experimental evaluation of NFC reliability between an RFID tag and a smartphone,” 2013 Africon.

[4] Steven J. Vaughan-Nichols. The Battle over the Universal Java IDE. Technology News. April 2003.

[5] Neil Symth. Android Studio 2.2 Development Essentials - Android 7 Edition. July 2016.

[6] Ajay R. Mishra. Fundamentals of Cellular Network Planning and Optimization: 2G/2.5G/3G/4G. April 2004.

[7] Thomas Zachariah. The Internet of Things has a Gateway Problem. February 2015.

[8] Alison K. Brown. GPS tracking system. January 3, 1995.

[9] Toh Jun Hau, Rozeha A. Rashid and et al, ‘IoT based Smart Guard Touring System (T-REC System)’, Proceedings of 2016 Electrical Engineering Symposium, December 2016.

[10] Nur Zafirah Azman, Rozeha A. Rashid and et al, ‘IoT based Home Intercom System’ Proceedings of 2016 Electrical Engineering Symposium, December 2016.