World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:17, No:10, 2023

Developing a Smart Card Using Internet of Things: Uni-C

Shatha S. Alshehri, Enji E. Alzamzami, Roaa H. Alansari, Rahaf J. Alwafi, Kholod A. Almwallad, Aeshah A. Alsiyami

Open Science Index, Computer and Information Engineering Vol:17, No:10, 2023 publications.waset.org/10013284.pdf

***Abstract*—**This paper demonstrates a system that helps solve the congestion problem at the entrance gates and limits the spread of viruses among people in crowded environments, such as COVID-19, using the IoT (Internet of Things). Uni-C system may assist in organizing the campus entry process efficiently by developing a smart card application supported by NFC (Near Field Communication) technology through which users' information could be sent to a reader to share it with the server and allow the server to perform its tasks and send a confirmation response for the request either by acceptance or rejection.

***Keywords*—**COVID-19, IoT, NFC technology, Uni-C.

I. Introduction

CORONAVIRUS (COVID-19) has been an ongoing pandemic since 2019, which has affected people's lifestyles. Due to this, technical support took place to limit the spread of this virus by using different smartphone applications. The pandemic brought extraordinary disruption to public places such as malls, schools, mosques, and public services offered by the government. Thus, technology has recently played a more significant role in government services.

The Kingdom of Saudi Arabia has provided citizens with many governmental applications and mobile services that helped in different ways. One of the most valuable applications that have a big hand to contribute the management of relief efforts by electronically granting permits during the "Curfew Period" is Tawakkalna.

To reduce the spread of the coronavirus, the government has limited entry to public places, to only fully vaccinated visitors. The security guards, at gateways, are committed to checking the health status through the colored QR codes in the Tawakkalna application to see if the visitor is vaccinated. All these processes take much time and always cause conjunction and crowd at the gates. Therefore, it is good to work on an application that will help the security guards and make their work easier and more efficient.

The security guards at the university, for example, face huge crowds in queues due to the verification process. They have to check on the Tawakkalna app and do other authentication methods for all the entrants which take more time and effort.

This paper will propose a solution by merging these apps with the help of NFC technology to solve this problem which will make the checking process much easier and faster to achieve a safe return in the country where it is crucial to deliver safer and more efficient services to the society of the Kingdom of Saudi Arabia and support the digital health vision that has a significant role in the Kingdom's 2030 vision [1].

A. Motivation

One of the most essential purposes of technology is to solve problems faced in life and optimize the lifestyle. Moreover, nowadays, smartphones can include members of the community with an endless range of ages, and these devices serve as a critical technique for easing people's daily life. It is evident that the pandemic COVID-19 has changed social life and made it hard, especially when people have to get into some places where the security system has to check the health status of each one. Therefore, improving the checking process using NFC technology can make the process faster and easier and eliminate the problem of congestion and long line queues. The basis of the study is to highlight this use of NFC technology.

II. Related Work

NFC technology requires little power and can be easily integrated into several devices, such as smartphones and sensors. There are three basic modes of operation of NFC, and the existing systems differ according to them, which are (a) reader/writer mode, (b) peer-to-peer (P2P) mode, and (c) Host Card Emulation (HCE) mode. NFC reader/writer mode is used for one-way communication between NFC readers and writers, such as contactless payment mechanisms, device pairing, smart posters, and sharing of short messages with users of NFC-enabled smartphones. [2] The P2P mode is used for Bluetooth or Wi-Fi connections or small data transfers, such as sending a URL to another smartphone. The researchers also discussed using P2P mode for payment services such as IDA-Pay [3] and secure credit transfer between smartphones [4]. Reference [3] proposes a mobile micropayment module for Point of Sale (POS) transactions.

NFC technology is an upgrade of Radio Frequency Identification (RFID) technology and can be considered an RFID evolution. Contrary, RFID technology operates at a long-range distance, and it is not used to exchange sensitive information because it can be vulnerable to a wide range of malicious attacks since RFID tags can be read without authorization. For example, in Item tracking, the contents of a handbag or a shopping cart can become visible to intruders

Roaa Hasan Al Ansari, Shatha Salem Al Shehri, Rahaf Jamil Al Wafi, Kholood Ali Al Mwallad, Enji Essam Al Zamzami, and Aeshah Abdulkarim Al Siyami are with the Department of Computer Science and Informatics, Umm Al Qura University, Mecca, Saudi Arabia (e-mail: roaahasan18@gmail.com, shathasalem.cs@gmail.com, rahafalwafi19933@gmail.com, kholood056046@gmail.com, Enjizamzami20@gmail.com, aasiyami@uqu.edu.sa).

Open Science Index, Computer and Information Engineering Vol:17, No:10, 2023 publications.waset.org/10013284.pdf

without leaving a trace [5]. In Uni-C system, users bring their devices to the reader, which reads the E-Card data from the user's device in a short range and transmits it to the server for authentication. So, in this way we ensure that the user's data are not readable by any other readers the user is unaware of.

The comparison between the two technologies NFC and RFID is shown in Table I.

TABLE I
COMPARISON BETWEEN NFC AND RFID TECHNOLOGIES

	NFC	RFID
Set-Up Time	< 0.1 ms	< 0.1 ms
Range	Up to 10 cm	Up to 3 m
Usability	Human-centric, easy, intuitive, fast	Item centric, easy
Selectivity	High, given, security	Partly given
Use Cases	Pay, get access, share, intuitive service, easy setup	Item tracking
Consumer Experience	Touch, simply content	Get Information

In [4], the authors discussed the potential use of NFC in payment mechanisms and proposed an application for credit transfer from mobile to mobile. In this field of mobile banking, commercial applications such as Swing-Pay, Samsung Pay, Apple Pay use a) Reader\Writer NFC mode and b) HCE NFC mode for payment so that a smartphone application can emulate the smart card and communicate directly with the NFC reader for payment or identity verification process. As it is noted that those applications above are on mobile phones, the Uni-C system also requires users to use their smartphones to pass checkpoints and complete the verification process, and it is on Reader\Writer mode.

As we mentioned, NFC is currently mainly intended to be used with mobile phones. The most visible use case of NFC technology is in contactless payment systems [6] such as mobile wallet apps, which are a lot safer than carrying around a physical card due to the security and protection in the device itself, and data encryption. In this way NFC-based transactions are inherently secure against unauthorized access by hackers.

A smartphone-based Physical Access Control System (PACS) uses the phone's connectivity to employ the same technology to authorize a user access request online by a central access server, another related work that addresses our problem domain [7]. Although the access points are not directly connected to the authorization server, [7] outlines a system based on a microSD secure element. HCE mode allows the access points to connect to it. There are many examples, like modern, more real-life applications, such as tracking tuna fish and agricultural products via blockchain such as in [8], is in Peer-to-Peer mode.

All of these alternatives/applications above are due to the rapid extension of mobile handsets, as we use our mobile phones for mobile payment, for mobile ticketing (bus, parking) and soon it will replace all the cards (passport, identity card) we carry in our wallets. The smartphone has become the central gadget in our life and an ideal alternative to a handheld wallet, making our wallets increasingly redundant over time, which are reflected in most of the proposed systems in this era.

Uni-C offers a smart alternative to the process that requires a security employee for several security reasons to verify both the user ID card and the vaccination status manually. Also, the E-card in the UQU app and the vaccination status in the Tawakkalna app have QR codes that could be used. However, they do not offer the speed of time to check the data as the user still has to show both QR codes separately. With the help of NFC technology, the verification process should be faster and more secure. The reader only reads the E-Card data, and the verification is on a database server which provides security for user information and efficiency in verifying the data to control access to the University campus.

III. PROJECT SCOPE

The project targets all check-needed entry gateways places. It helps visitors to enter quickly and safely, reducing the congestion problem that may lead to the spread of the ongoing infection of the COVID-19 virus.

It can be used in places such as central malls, hospitals, cinemas, universities, and airports, as they are the most crowded. However, the proposed solution will be implemented in the university community as a use case, and consequently, it can be implemented in other likewise places.

A. Project Description

Due to the current situation of the COVID-19 pandemic and the process of returning to the everyday lifestyle, people need help getting in through the university gates. The large number of students and faculties makes entering more difficult, as they must show the electronic university card and Tawakkalna to show their health status. So, entering the campus takes too much time and leads to clutter at the front doors that cause a crowd and could increase the spread of the coronavirus despite all the efforts by the security guards.

The proposed solution for this problem is to convert all these processes to an electronic verification process using NFC technology, which is an extension of RFID technology, and a wireless connection as data are transferred between two technology-enabled devices or between the device and an NFC chip without any rely on Wi-Fi and 3G [9].

The system consists of the user's mobile application, the Server, and the NFC reader. The academic information of the university community, including the health status file, will be stored in a database. The NFC reader will be located at different entrance gates and linked to a server.

The reader terminal will receive the user's E-Card information from his mobile and give back the response light in which the user knows if he\she can access or not (If the verification is valid, a green light will appear; if it is not, a red light will appear).

The user brings the NFC mobile device into close proximity to the reader and acts as a trigger for the verification process. The reader will receive the user information and send it to the backend server to check the user's information in the database. The Server will take the user ID number from the reader to check the database to see if the ID number exists. Secondly, the Server can check the vaccination data, such as number of doses, dose expiration date, etc.

Open Science Index, Computer and Information Engineering Vol:17, No:10, 2023 publications.waset.org/10013284.pdf

If the user ID is active, the Server will check the user's vaccination status approval; if all information is valid, the Server will send true to the reader to show the user a green light. Otherwise, it will show a red light. If the user ID is inactive, the Server will not have to check the user's vaccination status, and a false reply will be sent back to the reader to show a red light to the user.

The proposed system will make the checking process at the gates fast and accurate, which reduce the crowding and allow reaching the campus in a short time.

B. Expected Outcome

Programming a mobile application that sends the user ID (ID is taken from the electronic card) using an NFC signal to the reader might help in this situation. The reader should be programmed to take the data and connect to the server database to verify the information.

This system will save time and verify every data with no possible error. It also will not allow using the same ID for entering by different users, which will help the security guards at the entry points and facilitate their work to serve the university visitors.

IV. Method / Approach

The university has different gates, and for implementing the proposed system, each gate should have one or more NFC readers to communicate with the server. Therefore, the Client-Server (Agent-based) approach has been chosen for this work to allow for communicating in a request–response messaging pattern.

- The different benefit of the client-server method is much more convenient to the proposed system.
- The server hosts all required data, facilitating easy protection and managing authorization and authentication.
- NFC readers as clients can be added to the system without any interruptions.
- Data can be checked without requiring the reader and server to be nearby.
- All readers are independent and can contact the server anytime through the Internet.

A. Use Case Implementation

The university community was chosen as a use case for applying the proposed idea to make daily entry easy and efficient, which will reduce the mistakes that might happen through checking in the crowd. It also can help the university's vision of achieving digital transformation and make the checking process faster and more efficient, where the NFC reader will respond if a student can pass by contacting the server using the information in the student E-card.

The application contains three main parts, the server, the user application, and the reader side. Since the server side refers to the administrator who has the authorization to access the database and the card data verification process, but the user application displays the main service, for example, the electronic card. The entry process starts by passing the card through the reader to send data to the server and get the response.

- The Arduino IDE has been chosen for implementing the reader because it is inexpensive and simple to learn.
- The server side simulated the university database, which already has all the user's data (personal information, academic information, and vaccination information).
- The app, written in Kotlin, established a connection between the user and the server. Card information that supports NFC technology will be displayed and sent to the reader.
- Verifying the data stored on the server is quick and efficient.
- The entry process requires user information to be verified, the user must have an active file, the vaccination status is valid, and the user must be outside the campus (still needs to sign in).

The final step in the entry process is receiving the response status from the server, which is either rejected or accepted if the conditions are met. The green light and acceptance voice will be on. Otherwise, if one of the conditions is unmet, it will be rejected, and a red light with a rejection voice will be on.

B. Feasibility Study and Future Enhancement

All proposed solutions have an impact. We have to conduct a feasibility study for that solution. Our findings are as follows:

- The user's mobile phone must support NFC technology.
- The NFC reader sends and receives data quickly and easily, and there are several options for selecting the reader. Its prices are low, and the implementation process is simple as D-logic uFR Classic.
- The entity must provide a strong internet network to connect with the reader to ensure that data is sent and received in less than one second.
- The reader's components are inexpensive and easily obtained, as each portal requires more than one reader.
- The entity must provide one security guard for each gate to monitor the movement of users entering from the administration system and a reader that can respond with a confirmation message.

The process can be improved by different future works to have easy-to-use services and reduce congestion among these improvements such as:

- Electronic gates can allow entry according to the acceptance or rejection status automatically.
- Facial recognition technology could be used to identify a person's identity.
- Application can be implemented in many areas, such as health, entertainment, and transportation.
- The application can be used as part of another system.
- The application can be developed to fit into many operating systems.

V. Conclusion

The pandemic of COVID-19 has brought extraordinary disruption to public places such as malls, cinemas, universities and hospitals, and all visitors have to show their health and vaccination status to check at the entry gates. Therefore, this

paper presents a solution to the problem of long queues and conjunction at the entry point caused by the traditional checking process.

The proposed system will develop a mobile smart card application that is supported by NFC technology through which users' information can be sent to the reader to share it with the server and allow the server to perform its checking tasks and send back the status of the request either valid or invalid and accordingly pass or not.

The system will reduce the pressure on the security guards and provide a safer and more efficient checking mechanism that can be used at any entry gate.

REFERENCES

[1] Health Care," GOV.SA, (Online). Available: https://www.my.gov.sa/wps/portal/snp/aboutksa/HealthCareInKSA.
[2] InfoWorld., "6 Cool Uses of Near-Field Communication," (Online). Available: https://www.infoworld.com/article/2607039/mobile-technology/mobile-technology-6-cool-uses-of-near-field-communication.html. (Accessed 2018).
[3] L. Mainetti, L. Patrono and R. Vergallo, "IDA-Pay: a secure and efficient micro-payment system based on Peer-to-Peer NFC technology for Android mobile devices," Journal of Communications Software and Systems, vol. 8, no. 4, p. 117–125, 2012.
[4] J. Rodrigues and J. Lloret, " A secure NFC application for credit transfer among mobile phone," in Computer, Information and Telecommunication Systems (CITS), 2012.
[5] A. Mitrokotsa, M. R. Rieback and A. S. Tanenbaum, "Classifying RFID attacks and defenses," Information Systems Frontiers, vol. 12, no. 5, pp. 491-505, 2009.
[6] C. Navarro, E. Jimenez-Garcia, F. I. Hirata, J. d. D. S. Lopez, J. I. Nieto and M. Vazquez, "Interactive Multimedia," in Using RFID/NFC and QR-Code in Mobile Phones to Link the Physical and the Digital World, 2012, pp. 219-249.
[7] C. Arnosti, D. Gruntz and M. Hauri, "Secure Physical Access with NFC-enabled Smartphone," New York, NY, USA, 2015.
[8] M. P. Caro, M. S. Ali, M. Vecchio and R. Giaffreda, "Blockchain-based traceability in agri-food supply chain management: A practical implementation," 2021.
[9] B. Ozdenizci, K. OK and V. Coskun, Near Field Communication (NFC), John wiley & sons, 2012.

Open Science Index, Computer and Information Engineering Vol:17, No:10, 2023 publications.waset.org/10013284.pdf