International Journal of Advanced Science and Technology
Vol. 29, No.4, (2020), pp. 3782 – 3793

HIC: Health Immunity Certificate Using NFC Technology for Controlling and Monitoring of COVID-19 Patient Movement during and after MCO Period

Mustafa Man[1], Mohd Kamir Yusof[2], Wan Aezwani Wan Abu Bakar[3] and Lim Chee Hwa[4]

[1]Faculty of Ocean Engineering Technology and Informatics,
University Malaysia Terengganu (UMT),
21030 Kuala Nerus, Terengganu, Malaysia.
mustafaman@umt.edu.my
[2,3]Faculty of Informaticsand Computing,
Universiti Sultan Zainal Abidin (UniSZA), Besut Campus,
22200 Besut, Terengganu, Malaysia.
kamir2020@gmail.com, wanaezwani@unisza.edu.my
[4]One Team Networks Sdn. Bhd.
1-1B, Block 6, Jalan Pahat 15/H, Section 15,
40200 Shah Alam, Selangor, Malaysia.
limcheehwa@gmail.com

Abstract

Coronavirus disease (Covid-19) is an infectious disease caused by a newly first discovered coronavirus in Wuhan, China. Statistics reveals more than 3 million of total cases with more than 900K recovery and more than 200K deaths around the world as to date. Those recovered Covid-19 patients already have Covid-19 immunity in their body system. Movement Control Order (MCO) is the government enforcement policy during and after lockdown period for controlling the person's movement from red, yellow and green zone in combating the disease. During MCO period, it is vital to control and monitorthose recovered Covid-19 patient movement so that when they pass each security road blocks, they just show their health immunityid without having further explanation and clarification regarding their current status to the authority party. In response to Covid-19 issues, we propose a Health Immunity Certificate (HIC) with Near Field Communication (NFC) tag that acts as recovered patient's immunity passports or Patient Identification (PID). This certificate allows those Covid-19 recovered patient to be exempted from any movement restrictions from or to red, yellow or green zone to perform their daily activity. Our HIC offers a high security with 2 way encryption-decryption id. Prior to simulation done, resultsindicate that HIC system is executed at average of 0.001245 seconds of each HIC scans at each particular roadblock. This shows that our proposed HIC may contribute to significant usage to those Covid-19 frontliners such as Majlis Keselamatan Nasional (MKN), security agencies or even medical practitioners.

Keywords: *Health Immunity Certificate (HIC), Covid-19, Near Field Communication (NFC) Technology, Movement Control Order (MCO), Patient Control and Monitoring*

1.0 Introduction

Coronavirus Disease 2019 (Covid-19) is a global health emergency issues ever since its outbreak in late 2019. According to [1], it can quickly spread from one city to the entire country in immediately 30 days. Medical researchers are still working on some specific and effectivepharmacological treatment as Covid-19 vaccine. As to date, few researchers and scientist from several countries claim to have found the treatments but still in investigation and testing process that takes time to prove as facts. Studies have suggested that *chloroquine*, an *immunomodulant* drug that refers to medications used to help regulate or normalize the human body immune system. This drug is used as an additional therapy in treating asthma, malaria as well as the SARS-associated coronavirus (CoV) and MERS-CoV [2–4].The Covid-19 virus propagatesthrough droplets of saliva or discharge from the nose when an infected person coughs or sneezes. Infected individuals may have sore throat, or diarrhea or even vomiting for mild cases. It urgently affects patient's respiratory system for severe cases.To certain extend, a requirement is needed to those already an immune Covid-19 patient may need an immunity certificates to track for his/her movement for some security and caution purposes.According to [5], immunity certificates will guarantee those immune patients may lead normal life and help to support others around the word to revive while finding treatments solution or appropriate vaccine. United Kingdom government is looking into issuing "immunity certificates" to recovered Covid-19 patients andreturn back to their normal life.Germany researchers are studied on the pandemic extension by testing coronavirus antibodies to 100,000 volunteers. They called it as the *immunity passports*[6] that applies to those who are immune could be issued with vaccination pass that would allow them to be exempted from restrictions on their activity.

2.0 NFC Technology

Near Field Communication (NFC)is a trending wireless technology in contactless application [7]. NFCoffers a shortrange wireless communication technology that facilitates mobile phone usage. It provides diverse services ranging from payment applications to offices and houses accessibility [8].For optimum usage, it requires NFC compatible devices to be put very close to each other approximately less than 4cm in distance to communicate. NFC operates at 13.56 MHz with maximum transmission rate of 424 Kb per second [9]. This technology requires two devices i.e. first is called the *initiator* which is an active device and it is responsible for sorting communication. Second device is called the *target* and responds to the initiator's requests. The target device may be active or passive. The communication begins when the active device gets close to the target and generates a 13.56 MHz magnetic field and power the target device. The NFC technology also works via magnetic field induction and operates on an unlicensed radio frequency band. It also includes an embedded energy source component whereas the target can be RFID card, tag or an NFC device which gives the reply to initiator's request [10]. NFC provides easy connections, quick transactions, and simple data sharing. NFC complements many wireless technologies, in a way that it utilizes the key parameters and elements in the existing standards for contactless card technology [11].NFC applications are primarily used in money payment and personal information that demands for high level of security.

3.0 HIC Development Methodology

Development of an application for HIC is based on open source technology related to a secure algorithm included with NFC tag as a device for detection using mobile based apps. The development process comprises of several stepsi.e. first, to setup an Algorithm for NFC Tag and Reader. Second, to develop an apps for NFC Tag data readerand tracking and third, to test and evaluate the proposed apps prototype.

3.1 Setup an algorithm for NFC Tag and Reader Using Cryptographyapproach

Three (3) methods involve in encryptions i.e. hashing, symmetric methods, and asymmetric methods. Hashing function is defined on a domain of values which includes the possible key-values of the items to be processed [12-13]. The range of a hashing is some given segment of integers, 0, 1… n - 1. Each key-value is unique to a specific message, so minor changes to that message would be easy to track. Once data is encrypted using hashing, it cannot be reversed or deciphered. To the baseline, hashing is not an encryption methodtechnically, only it is used for providing data that yet to be tempered. Symmetric encryption is also known as private-key cryptography, because they are using a key to encrypt and decrypt the message [14]. In this method, the sender encrypts the data with one key, sends the data (the cipher text) and then the receiver uses the key to decrypt the data. Asymmetric key is known as a public key [15]. Key pairs (public, private) used in asymmetric cryptography where public distributed public and private key used on the decryption side to convert the cipher text in plain text. This encryption method is used widely in most of organization for security purposes during exchange of communication on the internet. In this paper we are going to use the combination of unique key value and symmetric encryption algorithms.

We used three (3)algorithms in this process which areunique key value generation algorithm, encryption algorithm and decryption algorithm.

Algorithm 1: Unique key value generation

1.1: Initialize the variable of index, x = 5, y = {012...abcABCD...}, z and key.
1.2: Assign value of i = 0
1.3: IF i < x: compute index = rand (0, strlen(y)); z = z.y[index]
Repeat step 3 until i more than x
1.4: Write a unique key value, z = z + key

Algorithm 2: Encryption algorithm

2.1: Initialize the variable of z, size, iv, crypt and key = "013FT~!6"
2.2: Set the encoded size = mcrypt_get_iv(MCRYPT_BLOWFISH, MCRYPT_MODE_CBC)
2.3: Set the encode iv = mcrypt_create_iv(size, MCRYPT_RAND)
2.4: Set the encode crypt = mcrypt_encrypt(MCRYPT_BLOWFISH, key, z, MCRYPT_MODE_CBC, iv)
2.5: Write a result, R in encryption data format

Algorithm 3: Decryption algorithm

3.1: Initialize variable of a, b, z, R and key = "013FT~!6"
3.2: Set the encoded a = pack("H", substr(R, 0, 16))*
3.3: Set the encoded b = pack("H", substr(R, 16))*
3.4: Set the encoded z = mcrypt_decrypt(MCRYPT_BLOWFISH, key, b, MCRYPT_MODE_CBC, a)
3.5: Write a unique key value, z

3.2 Develop an apps for NFC Tag Data reader and Tracking

A secure channel isinitialized before NFC transactions. In the secure channel, authentication and encryption process is implemented to ensure all NFC data in encrypted format. Unauthorized users or attackers cannot easily view or get NFC data because the NFC data in encryption format. Figure 1 shows a secure channel established between sender and receiver in the 2 steps of authentication and encryption process involved.

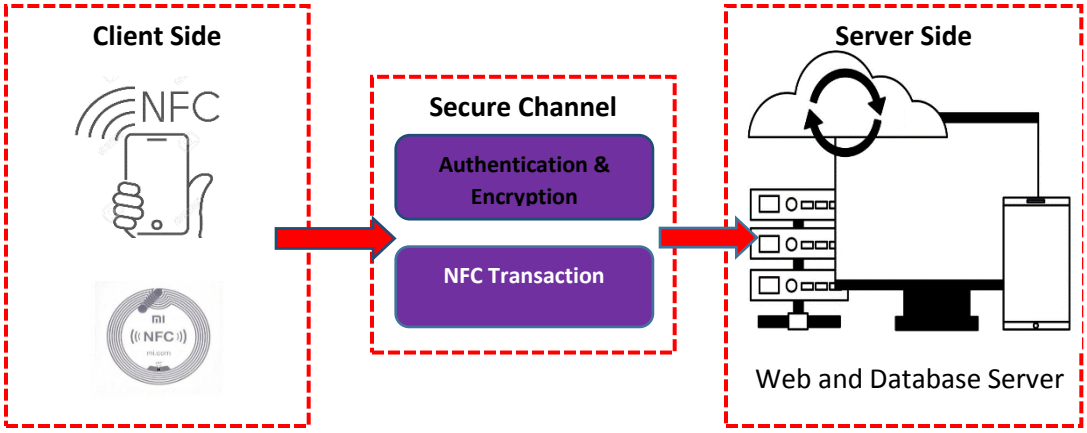


Figure 1. A secure channel for NFC transactionsArchitecture

We developed NFC secure channel using 2-way encryption and decryption process. The first step is to generate a unique key value. Then, combine the unique key value with NFC tag serial number of unique ID for each NFC tag. Combination between unique key value and NFC tag serial number will produce a plain text. Then the plain text valueis encrypted using blowfish algorithm [16].The blowfish specifies a cryptographic algorithm that can be used to protect electronic data. The blowfish is basically a symmetric block cipher. The algorithm of blowfish encryption depends on variable length key 32 bits to 448 bits, the algorithm takes 64 data blocks as input. The algorithm also dependent on the round in its process. Detail steps are as follows:

Algorithm 4: NFC Encryption Process

4.1: Generate a unique key value
4.2: Get a unique ID for each NFC tag and combine this value and a unique key value
4.3: Produce a plain text based on combine a unique key value and NFC ID
4.3: Encrypt plain text into encrypted data format by using a secret key.

Algorithm 5: NFC Decryption Process

5.1: *Decrypt an encrypted data format into plain text using a secret key.*
5.2: Produce an original data or plain text.

3.3 Testing and Evaluate the proposed Apps Prototype

We have developed the Health Immunity Certificates application based on the proposed methodologyintracking the movement of COVID-19 patient during or after Movement Control Order (MCO) period. Figure 2illustrates the communication between NFC device or reader and NFC tag. In this transaction, the NFC reader reads the information from the NFC tag that has been embedded to the NFC Button/Card. A secure channel is required to encrypt the data in encryption format in order to avoid unauthorized users read the original data.

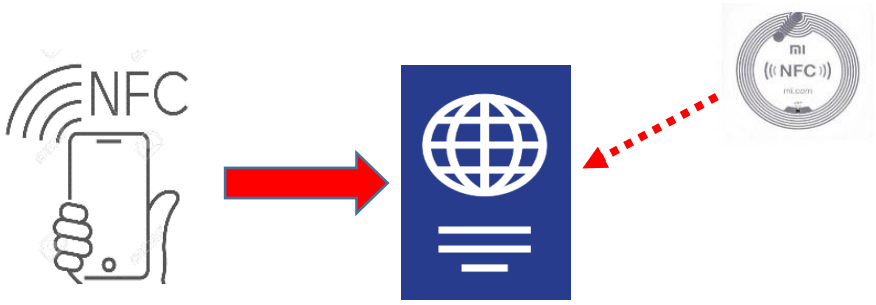


Figure 2. NFC Transaction using Special HIC/Passport/Card with NFC Tag.

HIC development focuses on generate a unique key value, encryption of data and decryption of data using a secret key.First step is to detect and acquire an NFC tag serial number. Figure 3 illustrates the process of detecting and acquiring a NFC serial number.

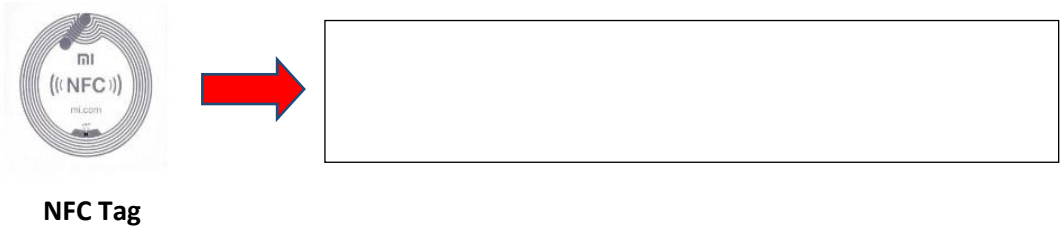


Figure 3. Detect and Get a NFC Serial Number

The second step is to generate a unique key value. Algorithm 1 will be used in order to generate the unique key value. Figure 4 shows a unique key value based on NFC serial number detected.

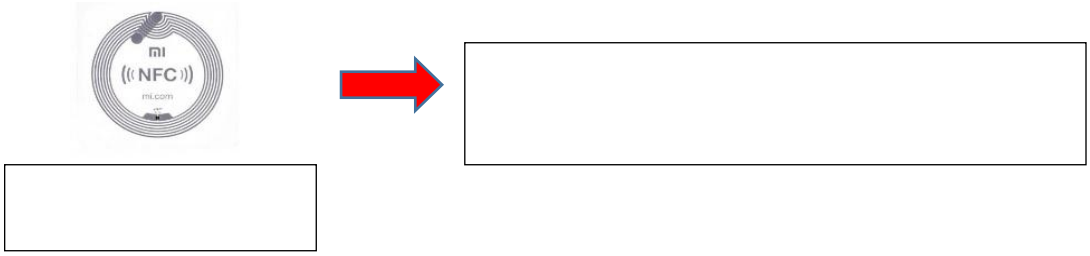


Figure 4. A Unique Key Value for the NFC Serial Number

Next step is to encrypt a unique key value into encryption format. This encryption format is also stored into database. Figure 5and 6shows an encryption and ion process and this encryption data format will be stored in the database. After that we can decryptback the data in encrypted format into a unique key value. A decryption process using the same secret key during the encryption process.

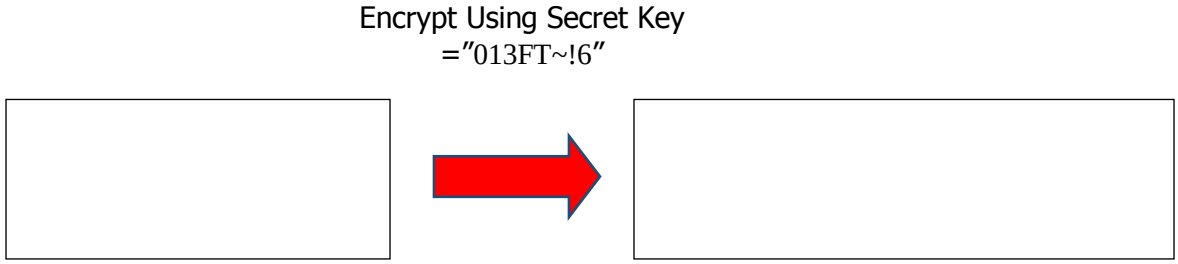


Figure 5. Data Encryption Process

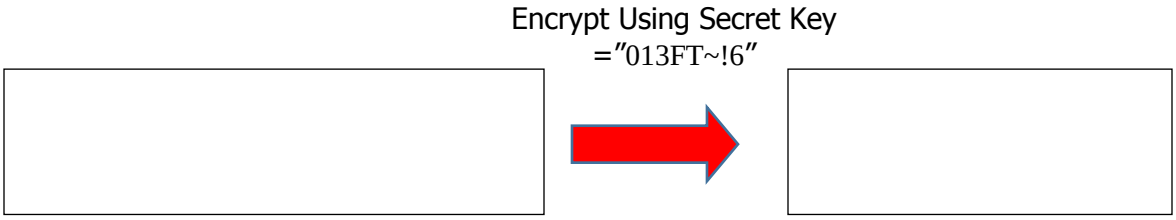


Figure 6. Data Decryption Process

Implementation of a unique key value and encryption algorithm provides a secure channel for any NFC transactions. This secure channel can prevent any threats such as data modification, data corruption, and man in the middle attack and relay attack.

4. HIC implementation in real environment

Real HIC implementation will include several agencies or government authorities that directly involved in the monitoring and tracking on Covid-19 patient from one area to another area of their movements. Following is the example scenario for our HIC apps. First, doctors in Public Health office need to setting up the Patient Identification (PID) with NFC tag for each recovered Covid-19 patient. This process is called as “Health Immunity Certificate (HIC)” with NFC Tagging by Doctor in that particular hospital or quarantine units. Each patient must have this NFC Tag for their movement around all the areas. Then, the authority party such as policemen, army and special task force will use HIC apps as a reader for checking and tracking the movement of each patients via the road block inside their mobile phone. These scenarios are needed during and after the MCO period. Figure 7 shows the first process for the setting up the PID for each recovered Covid-19 patients.

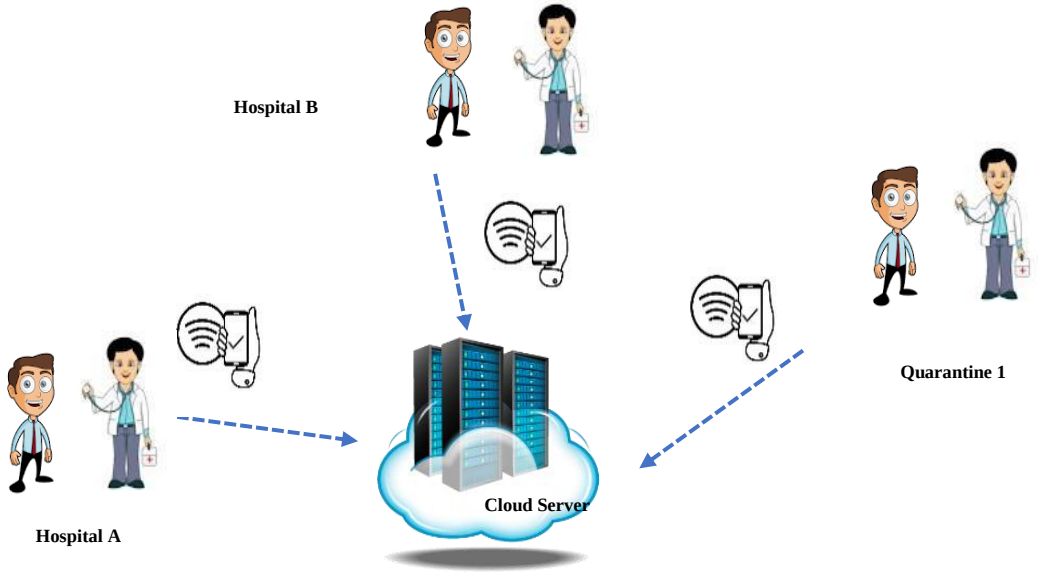


Figure 7. Setting up the NFC Tag for PID by Authorized Doctor in Different Places

Figure 8 depicts the scenarios that this apps can be tested and giving the information related to movement during or after MCO. This scenario was based on the road block via several location to detect and keep tracks of the patient's movement with NFC tag.

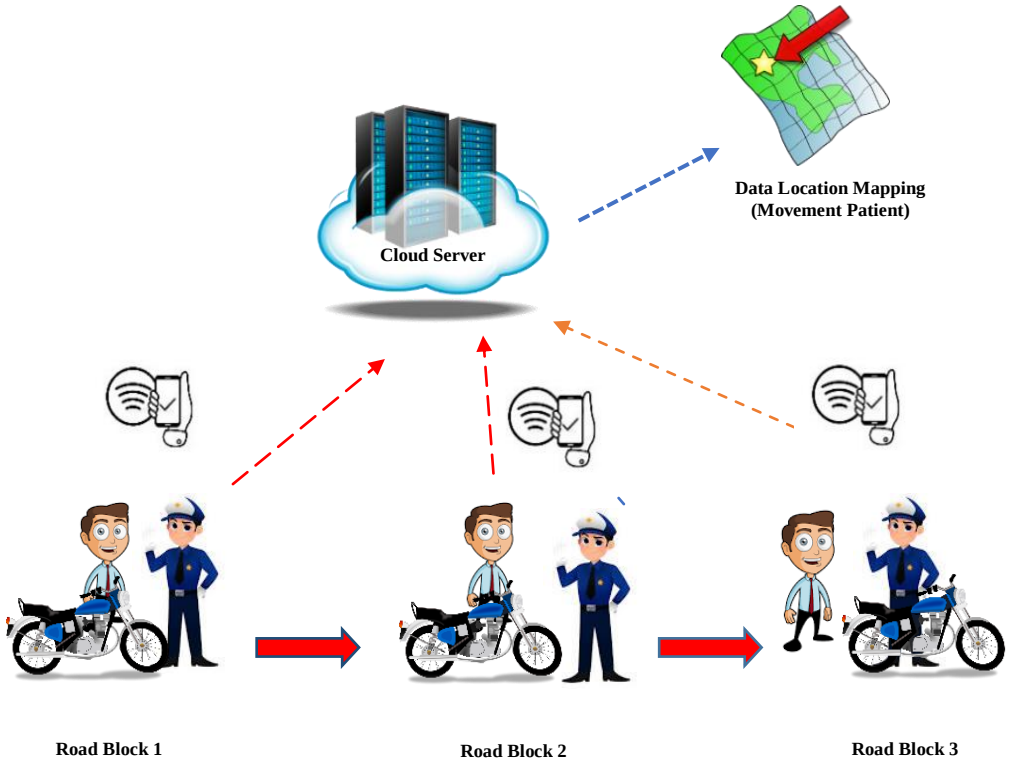
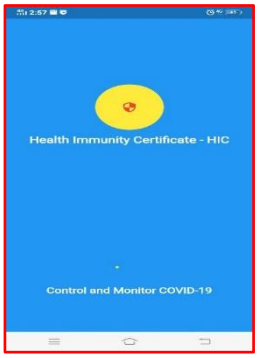


Figure 8. Scenarios of the Covid-19 Patient Movement Tracking and Monitoring

Using our HIC apps with NFC technology, we can keep track the movement of Covid-19 patients by visualizing PID data through Google or mapping system. Based on this, we can identify the movement of the patient when each patient has passed through the road block location. Using HIC apps, data is collected and activated directly to the cloud server/database via mobile internet access once the NFC Tag of each PID is read and recognizedby each of the authorized person.Data that includes date, time and also person who scan the PID Passport/Card with NFC Tag will be automatically recorded at each of the road block areas.

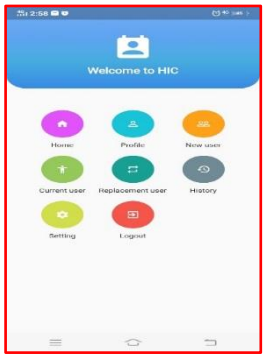
4.1 User Interface for HIC Mobile Apps

HIC system have several modules including multiple user access included *a. Administrator b. Doctors c. Authorized person for road block (such as policemen, army and others authorized person by the authorities)*. HIC user interfaces are shown in Figure 9.



Starting Apps

Login & Password

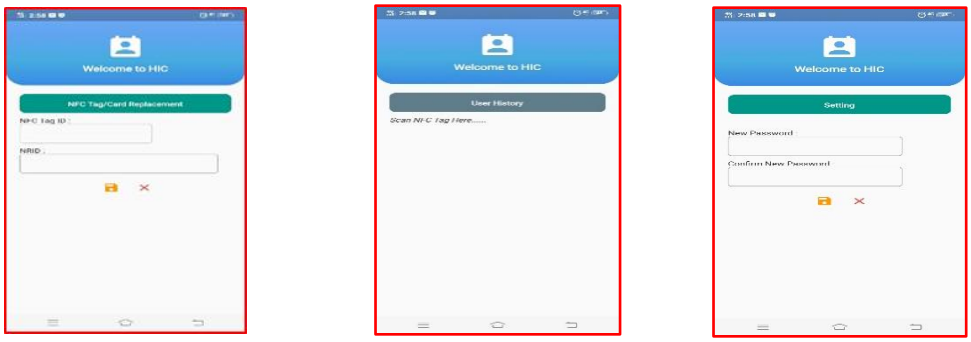


Menu Function

User Profile

Register NFC Tag

Patient Register with NFC Tag



Changing NFC Tag for Patient Patient Tracking Data Log User Password Setting

Figure 9. User Interface for HIC mobile apps

4.2 Database Design and data Collection

HIC database comprises of nine (9) tables namely *hic_user*, *hic_level*, *hic_official*, *hic_kkm*, *hic_publicmove*, *hic_publichealth*, *hic_public*, *hic gender* and *hic_tag*. All 8 tables from hic_user to hic_gender are interrelated with its relationships except for hic_tag, that it is put as an independent. This is done prior to security concerns where the NFC tagging is randomly generated during encryption and decryption process. Thus it could not be linked to other tables for matching due to security purposes. As such intruder could not simply hacked to our HIC system. Figure 10 to Figure 11 shows our HIC Entity-Relationship-Diagram (ERD) and Data Structure for NFC Tag ID respectively.

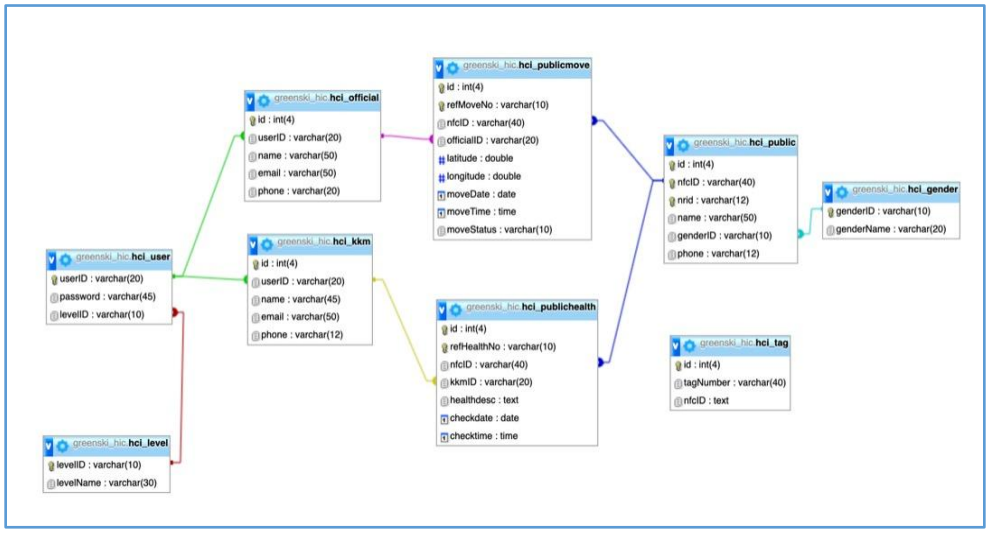


Figure 10.HIC Entity-Relationship-Diagram (ERD)

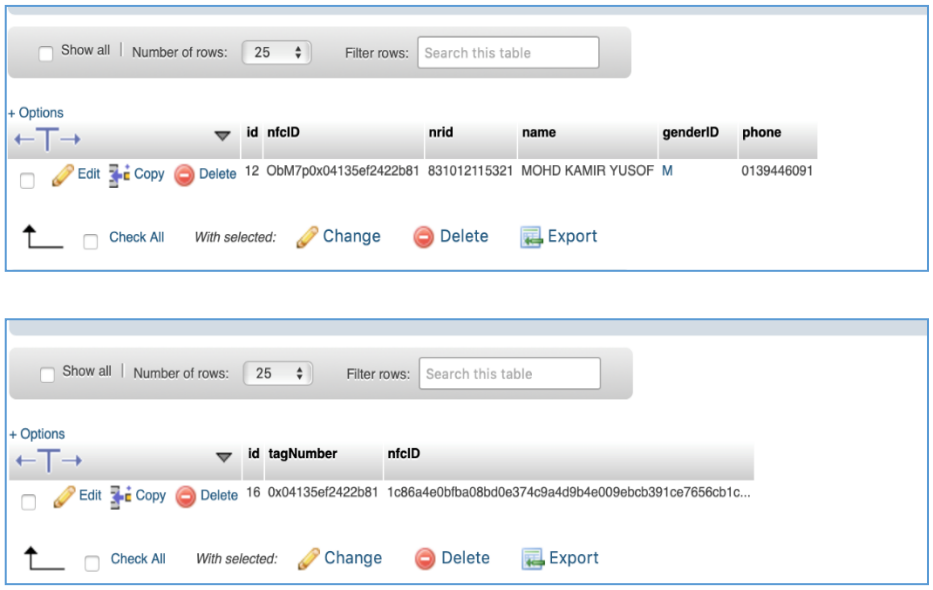
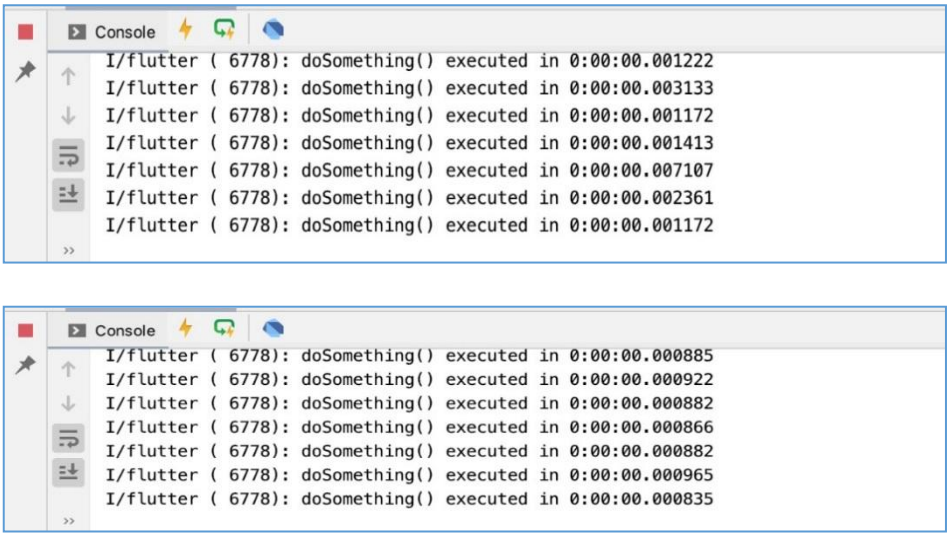


Figure 11. Data Structure for NFC Tag ID

4.3 Experimentation Results of HIC apps

We simulate our HIC apps prior to given scenario. Each HIC process at each particular roadblock requires averagely less than 1 second. Below results illustrate for the authorized user id 6778, he/she has done 14 HIC process that took average execution or interval time of 0.001245 seconds.



5.0 Conclusions and Recommendations

A secure NFC transaction is important to prevent unauthorized users or attackers get the information between sender and receiver. A unique key value and encryption algorithm have been implemented to encrypt message into 32-bit during NFC transactions. Implementation of this method is proven secured which is the attacker's needs to decrypt the message in encryption format using by using a correct secret key. But in this case, the attackers don't know the correct secret key. However, NFC transactions have a potential to improve the security level by extent the encryption message into 64-bit, 128-bit or more. But, the problem is time consuming during encryption and decryption process, which is 32-bit is faster compared to 64-bit and 128-bit. In this paper, we have introduced 32-bit encryption message for NFC transactions, and proven secured by establishing a secure channel between sender and receiver with a significant execution time in less than a second. We recommend to use NFC technology as a solution alternative in tracking Covid-19 patient movements so that people would notice he/she already has a Covid-19 immunity system. The importance for this Health Immunity Certificate is to care for each person's pride and dignity since this Covid-19 outbreaks.

References

[1] Wu Z, McGoogan JM. Characteristics of and important lessons from the coronavirus disease 2019 (COVID-19) outbreak in China: summary of a report of 72 314 cases from the Chinese Center for Disease Control and Prevention. Jama 2020. https://doi.org/10.1001/jama.2020.2648.

[2] Savarino A, Boelaert JR, Cassone A, Majori G, Cauda R. Effects of chloroquine on viral infections: an old drug against today's diseases? Lancet Infect Dis 2003; 3:722–7.

[3] Lai, C. C., Liu, Y. H., Wang, C. Y., Wang, Y. H., Hsueh, S. C., Yen, M. Y., ... & Hsueh, P. R. (2020). Asymptomatic carrier state, acute respiratory disease, and pneumonia due to severe acute respiratory syndrome coronavirus 2 (SARSCoV-2): Facts and myths. *Journal of Microbiology, Immunology and Infection*.

[4] Gupta, N., Agrawal, S., & Ish, P. (2020). Chloroquine in COVID-19: the evidence. *Monaldi Archives for Chest Disease*, *90*(1).

[5] [5] Henry T. Greely, APRIL 10, 2020. Covid-19 'immunity certificates': practical and ethical conundrums retrieved from https://www.statnews.com/2020/04/10/immunity-certificates-Covid-19-practical-ethical-conundrums/

[6] Ronald Bailey, 4.2.2020 5:00 PM. COVID-19 'Immunity Passports' Could Be a Good Idea. Why not let recovered coronavirus patients out of lockdown? Retrieved from https://reason.com/2020/04/02/Covid-19-immunity-passports/

[7] Anusha Rahul, Gokul Krishnan H, Sethuraman Rao, (2015). *Near Field Communication (NFC) Technology: A Survey*. International Journal on Cybernetics & Informatics (IJCI), Vol. 4, No. 2, April 2015.

[8] Coskun, V., Ozdenizci, B., & Ok, K. (2013). A survey on near field communication (NFC) technology. *Wireless personal communications*, *71*(3), 2259-2294.

[9] NFC-Forum, Available: http://www.nfc-forum.org

[10] Esko Strommer, JuhaParkka, ArtoYlisaukko-Oja, 2006. *Application of Near Field Communication for Health Monitoring in Daily Life*. Proceedings of the 28th IEEE EMBS Annual International Conference, February 2006.

[11] Lu, Y. F., Shu, I. C., Tseng, H. W., & Chou, S. C. (2014, April). An NFC-phone mutual authentication scheme for smart-living applications. In *2014 International Conference on Information Science, Electronics and Electrical Engineering* (Vol. 2, pp. 1053-1057). IEEE.

[12] Heon June Kim, (2016). *A Study on the Cryptographic Algorithm for NFC*. Indian Journal of Science and Technology.Vol. 9(37), pp: 1 - 5.

[13] Gary Knott, (1975). *Hashing Functions*. The Computer Journal. Vol. 18, No. 3, March 1975, pp: 265 - 278.

[14] [14] Samar Lofty, Abdel Nasser H. Zaied, (2017). *Survey of Compression and Cryptography Techniques of Data Security in E-Commerce*. Int. Journal on Innovative Research in Information Security. Vol. 4, Issue 8, August 2017, pp: 1 - 8.

[15] Abdul Ghaffar Khan, Sana Basharat, Muhammad Usama Riaz, (2018). *Analysis of asymmetric cryptography in information security based on computational study to ensure confidentiality during information exchange*. Int. Journal of Scientific & Engineering Research, Vol. 9, Issue. 10, October 2018, pp: 992 - 999.

[16] Manku, S., & Vasanth, K. (2015). Blowfish encryption algorithm for information security. *ARPN journal of engineering and applied sciences*, *10*(10), 4717-4719.

Authors

Mustafa Man is an Associate Professor in Faculty of Ocean Engineering Technology & Informatics and also as a Deputy Director at Research Management Innovation Centre (RMIC), UMT. He started his PhD studies in July 2009 and finished his studies in Computer Science from UTM in 2012. He has received Computer Science Diploma, Computer Science Degree, Master's Degree from UPM. In 2012, he has been awarded a "MIMOS Prestigious Awards" for his PhD by MIMOS Berhad. His research is focused on the development of multiple types of databases integration model and also in Augmented Reality (AR), android based, and IT related into across domain platform.

Mohd Kamir Yusof obtained her Master of Computer Science from Faculty of Computer Science and Information System, UniversitiTeknologi Malaysia in 2008. Currently, he is a Lecturer at Department of Computer Science, Faculty of Infomatics and Computing, Universiti Sultan Zainal Abidin (UniSZA), Terengganu, Malaysia. His research is focused on development of mobile application, web-based application and data integration.

Wan Aezwani Bt Wan Abu Bakar received her PhD in Computer Science at Universiti Malaysia Terengganu (UMT) Terengganu in Nov, 2016. Her focus area is in association rule in frequent itemset mining. She received her master's degree in Master of Science (Computer Science) from Universiti Teknologi Malaysia (UTM) Skudai, Johor in 2000 prior to finishing her study in Bachelor's degree also in the same stream from Universiti Putra Malaysia (UPM) Serdang, Selangor in 1998. Her master's research was formerly on Fingerprint Image Segmentation in the stream of Image Processing. Now she's pursuing her research towards association relationship in infrequent itemset mining which is more downstream to educational data setting.

Lim Chee Hwa is a Founder and Managing Director of One Team Network Sdn. Bhd. since 2010 until recent. He has commercialized an innovative & creative product – AedesTech Mosquito Home System. He also has commercialized an innovative & creative product – 4 corner mini aerosol mosquito killer X'MOS & MOZONE. He was the Team leader of the R&D team collaborated with IMR – winning a prestigious award "Dengue Tech Challenge 2016". Currently as a Vice President of working committee of National Dengue Video Competition 2019 and acts as a Sub-Committee member for Federation of Malaysian Manufacturers (FMM) Selangor Industry 4.0.