Crypt-Tag Authentication in NFC Implementation for Medicine Data Management

Z. Zainal Abidin[1], N. A. Zakaria[2], N. Harum[3], M. R. Baharon[4], Ee-Song Hong[5]
Information Security Forensics and Computer Networking
Universiti Teknikal Malaysia Melaka (UTeM)
Melaka, Malaysia

Z. Abal Abas[6]
Optimization Modelling Analytic and Simulation
Universiti Teknikal Malaysia Melaka (UTeM)
Melaka, Malaysia

Z. Ayop[7], N. A. Mat Ariff[8]
Information Security Forensics and Computer Networking
Universiti Teknikal Malaysia Melaka (UTeM)
Melaka, Malaysia

***Abstract*—This study focus on the implementation of expiry date detection for medicine using RFID in the health care industry. The motivation for doing this research is the process of searching for the expired medicine is a time consuming and lack of security features included in current NFC implementation. Therefore, the objective of this research is to study the RFID technology used for detecting medicine expiry product and to develop a new system that integrated NFC with authentication feature. Moreover, the problem of current data management for medicine still using manual or barcode system that lead to inconsistency, easy duplication and human error. Here, the NFC is chosen, due to smaller distance of signal coverage, since less interference and the time spending for sniffing activity by the hacker can be reduced. The system is developed using C#, SQLite, Visual Studio, NFC Tag and NFC reader (ACR122U-A9). Experiments have shown that the proposed system has produced medicine expiry date system and only authorized person in charge can monitor the medicine. The impact of the proposed system produces safer, greener and easier environment for better medicine data management. The significance of this study gives a medicine expiry date detection system for health care.**

Keywords*—Expiry date notification; Radio-Frequency Identification (RFID); Near-Field Communication (NFC); internet of things insider threats; health care

I. Introduction

Radio-Frequency Identification (RFID) has been introduced to improve the supply chain process and increase the productivity in various fields. The importance of RFID gives a better solution in terms of lightweight device and remote detection to the industry since it is a small electronic device, that consist of a small chip and an antenna. In fact, RFID increases traceability of product through assembly line or warehouses which provides a unique identifier for an object based on magnetic circuit that must be scanned to get the information. However, current RFID based systems have no data privacy features and there is some limitation to access the RFID devices. Assuming a person has the same radar, they might have access to receive all the data capture and there is a limitation in the frequency length which makes the connection slow. Therefore, the proposed tracking system with security features is developed by using RFID. Nevertheless, a short-range frequency of RFID is used for the prototype development due to its small coverage of data signal that permits data transmission within the respective distance. In fact, the use of short-range frequency features is to prevent the interference in frequencies which another RFID reader captures information from another RFID reader data of a product or values due to its characteristics of long distance range. On the other hand, most of the manufacturer still using manual operations, such as Barcode, QR code [1] and RFID [2]. In the field of Information Security, access control is one of the method to protect or control the systems and infrastructure for physical security implementation such as accessing the building or premises, monitoring and surveillance systems and physical access infrastructure for instance door and window. Thus, in the access control method consists of smart card, biometrics, bar code, QR code and RFID. Each of these technology has its own specialty and limitation. The NFC is a short range type of RFID that provide a smaller distance of frequency coverage and performs basic tasks of scanning and tagging. The theoretical taxonomy of the existing systems is illustrated as in Figure 1 and explained in sections of A, B, C and D.

A Special thanks to Malaysia Research Assessment (MYRA) and Universiti Teknikal Malaysia Melaka (UTeM) for giving a sponsor.

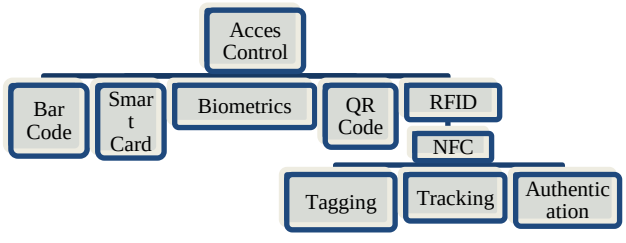

Fig. 1. Taxonomy of Theoretical in Access Control.

A. Barcode

The barcode system is available in various fields for example healthcare, transportation, manufacturing and retail stores. In fact, the barcode is useful for users to keep track of inventory easily which can make time spent doing inventory checks are minimized and at the same time reduces rates of human error [3].

In medical industry is not the only industry that uses barcodes. Other industry that using barcode includes food, transportation, manufacturing and industrial [4]. A bar code (often seen as a single word, barcode) is the small image of lines (bars) and spaces that is affixed to retail store items, identification cards, and postal mail to identify a particular product number, person, or location. The code uses a sequence of vertical bars and spaces to represent numbers and other symbols. A bar code symbol typically consists of five parts: a quiet zone, a start character, data characters (including an optional check character), a stop character, and another quiet zone as shown in Figure 2.

By using barcode scanners, it helps users to keep track of inventory easily which can shorten the time of work as well as reduces rates of human error. Furthermore, some of the features can allow users to set up alerts for items that are out of stock so orders can be filled promptly [6].

The disadvantages of barcode scanners are it needs a direct line of sight and need to close to the barcode for doing scan or read. Besides that, barcodes have no read or write capabilities. In fact, barcodes have a weak security element as they can be more easily reproduced or forged, it can easily damage which means if a barcode is ripped or damaged there is no way to scan the product. Although barcode scanner is cheaper, but in the long run it requires a lot of money for manually entering information into the system that must be scanned continuously from one product to another till to the end of line.

On the other hand, Quick Response code (QR code) is a two-dimensional barcode that can be read via QR barcode reader or camera and is able to transmit data both in vertical and horizontal track, which is why it is named a 2D barcode. The most significant objective of using QR code is the traceability or monitoring the system [1]. As stated by [4], one of the advantages of the QR Code is that it eliminates the need to type WEB addresses which it is only necessary to launch the application and point the cell phone at a QR Code for the additional content to be displayed in the reader or Web browser.

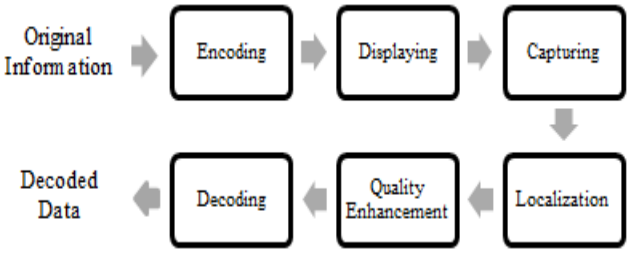

Fig. 2. Barcode Process Diagram [5].

Fig. 3. Left is the Correct Version, Right is the Spammed [8].

However, QR code has a problem that can easily duplicate and manipulate the accurate data, the physical spaces are the most vulnerable to spamming pointing to unsolicited content over the internet [7]. However, the first kind malicious detected by Kaspersky lab which is the attack method used in the QR code was that when a user scans the code, he is directed towards a website and then a malicious file downloads in the user's device without the knowledge of the user [8]. Figure 3 shows how file is modified without being noticed by a user.

B. Radio-Frequency Identification (FRID)

RFID consist of a tag attached to a product which classifies and tracks the product via radio waves. Besides, tags can carry up to 2000 bytes of records per second. The basic components of an RFID system are a tag, scanner, antenna, writer, control equipment and software [9]. RFID able to capture any added information such as expiry date but RFID contains a limitation space to store information especially about the manufacturer and product.

However, RFID is highly used instead of barcode because it cannot be easily duplicated based on circuit based chip, which represents unique identification number and address [2]. For example, an Italian Food Company Barilla had launched an RFID-enabled product which exploring the use of both passive and active radio frequency identification technology to help track ingredients at the same time maintaining the quality and food safety [10], which the topology of RFID block diagram is illustrates in Figure 4. In fact, RFID technology can avoid or decrease sources of errors, decrease of labor costs and the saving of inventory inaccuracies. [11]. Moreover, the use of RFID prevents sniffing or Eavesdropping, Spoofing, Cloning, Replay, Relay and Denial of Service Attacks are some of the security threats [12].

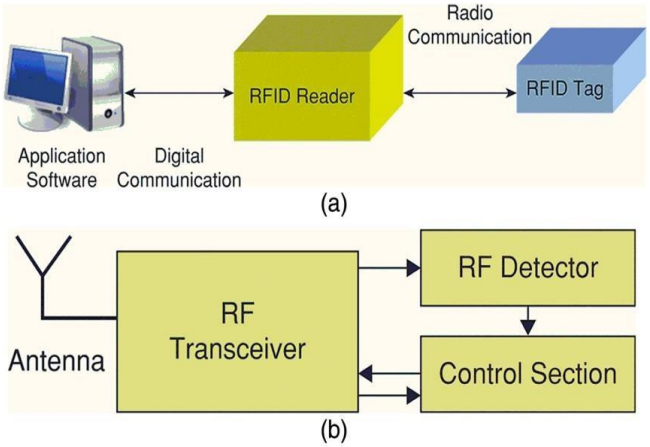

Fig. 4. RFID Reader Block Diagram [10].

However, most organizations control the supplies movement, effective inventory management and maintain productivity, demand higher safety and security checks monitoring [13]. Since the messages are transmitted by using radio waves, RFID systems and protocols are still directly using the real tags' identity, thus, for these reasons, RFID users can be affected by broadcasting the content of the RFID tags because any malicious RFID reader can track the location or obtain the identification and private information [14].

Based on previous studies [15] discussed on the security as the main problem in RFID system since the communication between RFID components is wireless which is still demand a better solution for authentication and detection. Furthermore, RFID is lack of authentication feature of security [16] and vulnerabilities have been found in RFID tagging phase [17], which lead to Man-in-the-middle attack.

A major criticism work in [18] explains that most companies are protecting critical products or items and supplies moving, manage inventory level effectively, maintain productivity, improve safety and security, in order to confirm or agreed requirements and keep emergency transport costs in check. This inconsistency may be due to improve inventory organization at the retail store and together with the supply chain. However, Sun [19] points out that the prime asset for an inventory system is an automatic identification technology system. One of the best examples is the Auto-ID based on RFID technology. This asset is on behalf of two reasons. First, the perceptibility provided by this technology allows a precise information of inventory level by removing the difference between inventory record and physical inventory. Second, RFID technology can avoid or decrease sources of errors. A reasonable approach to tackle this issue could be to decrease of labor costs, the popularization of business processes and the saving of inventory inaccuracies.

It seems that a change of high social concern and high contribution services such as services with banks as opposite to groceries stores [20] have more impact on user's privacy issues when they use QR codes to access the business web sites. Moreover, results suggest that privacy issues when using QR code and [21] describes sniffing or Eavesdropping, Spoofing, Cloning, Replay, Relay and Denial of Service Attacks are some of the security threats to RFID technology. One possible methods being used as countermeasures to the security threats presented against RFID technology.

Park and Lee [22] holds the view that there are many kind of authentication technologies that are developed to protect personal information. However, if the NFC-based services are being used widely, the efficiency and payment information protection of these technologies must be ensured. Initial observations suggest that there may be a link between protection of a user and service provider in NFC-based. Alqarni finds an accurate authentication protocols between the tag and the back-end server is the crucial issue [23]. Since the messages are transmitted by using radio waves through the air in RFID systems and those protocols are still directly using the real tags' identity such as tag identifier and secret key in the authentication phase. For these reasons, RFID users can be affected by broadcasting the content of their RFID tags because any malicious RFID reader can track their location or obtain their identification and private information. The data reported here appear to support the assumption that solving RFID authentication issues that go a long way to persuade people that using these tags are not expose their secret data.

Recent research [24] has suggest that there are many types of applications that can be run using NFC technology. The fact that the lower layer of NFC includes no communication security primitives makes this technology exposed to a wide range of vulnerabilities and attacks. A possible explanation for this might be that NFC security issues.

However, previous method suffers from serious drawbacks and time taken for the valuable information is extracted from the RFID data that is too long [25]. Meanwhile, the object moves within the distance of a RFID reader, it reads the tag attached on that object. It seems possible that these results are due to reading the same tag so the duplicated data or information has been generated. In fact, based on survey conducted [26], respondents agree that human interactions with smart devices makes people feel more confident as the technology becomes an inseparable part of human life.

C. Near Field Communication (NFC)

The technology involved is deceptively simple: evolved from radio frequency identification (RFID), an NFC chip operates as one part of a wireless link. Once the NFC chip is activated by another chip, small amounts of data between the two devices can be transferred when held a few centimeters from each other during recent years. Mobile phones with NFC enabled has become widely used and most common itinerant computing devices, playing an important role socially, emotionally and recreationally. The innovations in communication networks particularly in mobile phones technology have made it prone for a broad range of applications. Thus, Near Field Communication (NFC) service, as one of the most recent technologies in telecommunication area, is going to be developed around the world through transformation from initial testing to full scale deployment. In fact, Near Field Communication (NFC) is a type of passive 13.56 MHz RFID technology that enables short-range wireless data transmissions at 4 centimeters (1.6 inches) or less [27] and it lets consumers use NFC enabled mobile devices to interact with RFID tags or other NFC-enabled devices and products.

The number of applications in which NFC technology is widely used including application which is new secure system should be proposed for managing security in complex mobile and variable conditions such as secure payment tools, access management and retailing industry among others. Keeping smartphone secure is a very fundamental nonetheless, to ensure security for the valuable data that may be found stored in the hand phone is another issue. Users would dislike to waste even a few more seconds of their time to unlock a phone, however, the entire process produce a lot easier with the introduction of technologies like NFC, which faster data transmission and better accessibility with the security feature and based on the standards of communication.

The focus of this research is general security specifications, which should serve as guidelines that cover most of the basic

security requirements within the system [28]. Starting with the initial connection to the system, which is done via NFC, the user is required to provide an identity for optimal protection. As a user taps his or her smartphone next to the tag, then the reader captures that tag's unique ID number [29] which is prompting the phone to access webpage. Although this technology is increasingly becoming main stream, there are issues that need to be addressed mainly regarding on security concerns with Secure Element (SE) personalization, management, ownership and architecture that can be useable by attackers to interval the alteration of NFC within societies. Figure 5 illustrates how the attacker captured data from access control reader through the use of the card emulator in a specific distance. On the hand, hacker injects the malicious codes to the NFC reader to obtain crucial information at the receiver or sender sides yet depending on the frequency range of the NFC device and features available in the hardware and firmware.

In order to protect the NFC device, a lightweight authentication method and a secure way need to be developed in response to these attacks. Thus, adding an authentication element to the NFC provide a better security solution to the user.

The motivation to implement authentication in NFC also inspired by the study done by Jung [30] that stated that with the combination of authentication feature in the NFC contributes a better protection for data management. Figure 6 illustrated Jung case diagram of solution.

Therefore, the proposed study is to develop a system of NFC implementation with authentication for medicine data management using cryptography, named as Crypt-Tag Medicine Data Management. The methodology of the proposed system is explained in section II. Moreover, section III illustrates the results and discussion and section IV concludes the study.

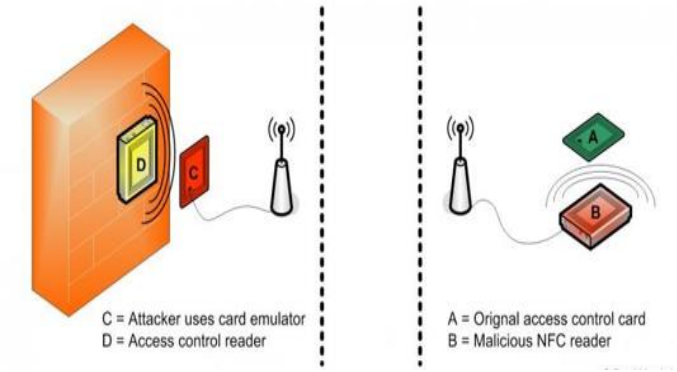

Fig. 5. NFC Attack.

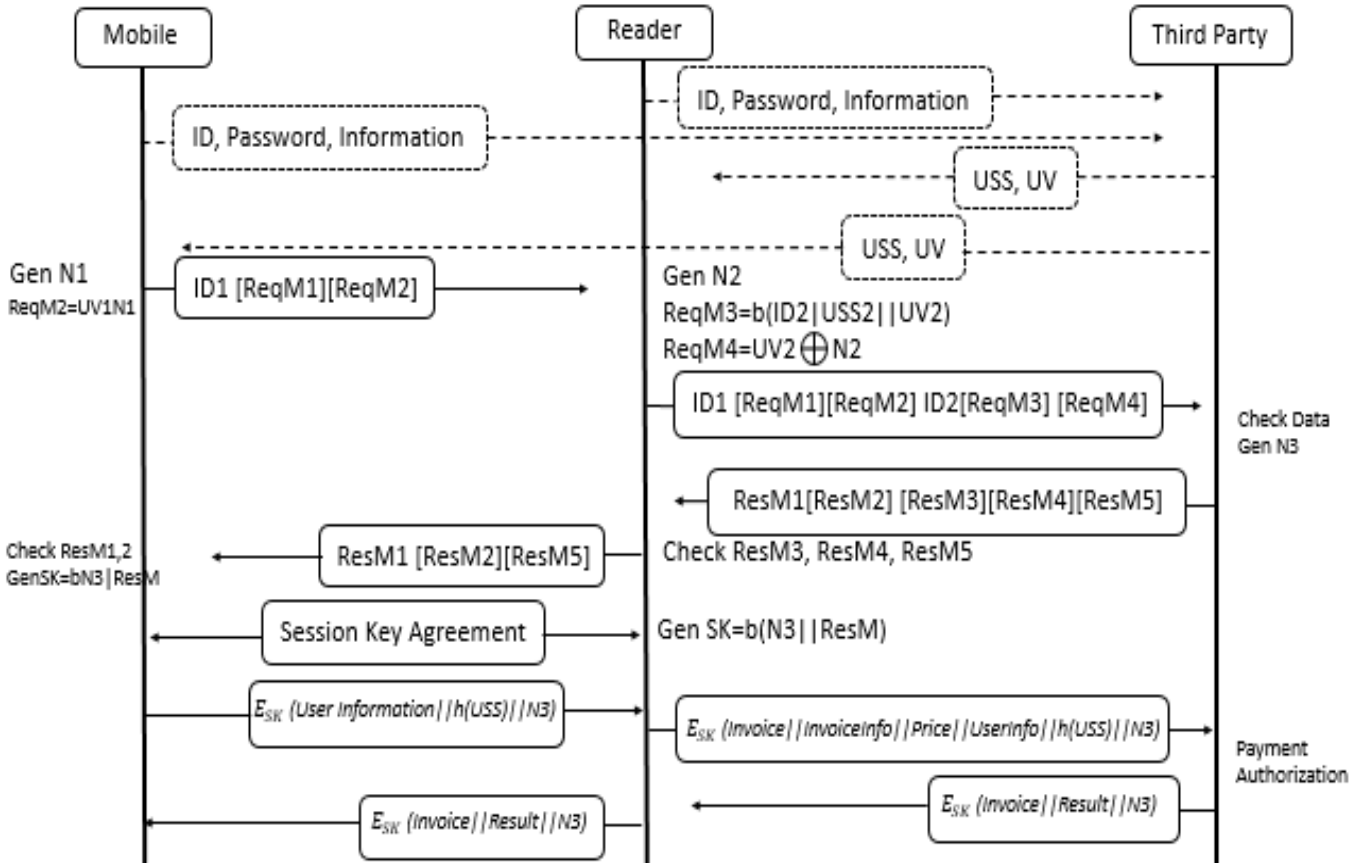

Fig. 6. Case Diagram for Authentication in NFC [30].

II. METHODOLOGY

The implementation of the Crypt-Tag Medicine Data Management system is using waterfall model as shown in Figure 7 that consists of six phases.

A. Project Planning and Feasibility Study

In phase 1, the purpose of the project planning and feasibility study needs to gather all information and requirement such as to determine the objectives, to identify the current technology used in health care and to find the suitable software and hardware to be used in the execution of the project. In this phase, research needs to include the implementation idea that involves NFC, how it works and the system requirement to fulfil the study needs.

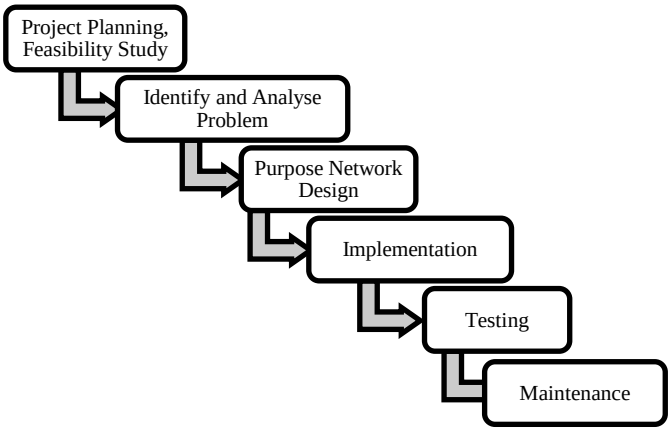

Fig. 7. Waterfall Model Life Cycle.

B. Identify and Analyze Problem

In phase 2, identify and analyze problem is a process to collect data, to identify the problem and to recommend suggestions in improving the existing system. This phase involves gathering data, finding solution for overcome the limitation of the current system and identify the target users in developing NFC technology. The main objective of this phase is to find out the solution on what, who, when and how the system been and there is a certain technique used to gather data about this study.

C. Propose Network Design

In phase 3, a new system for the proposed network is designed based on the requirement and analysis such as architecture design, software and hardware selection. Moreover, the user interface for authentication is designed at the beginning of the system using AES cryptography and integrates with the NFC Tag development that called as Crypt-Tag. The AES algorithm is encoded into the authentication system using C# and generates the password into encrypted version. The encrypted password is represented in a series of hexadecimal numbers and alphabets which hacker or intruder is unable to read the real password. The outcome of the proposed system shows that Justin's password is bac363ad53ee1 as shown in Figure 14, which is not his real password.

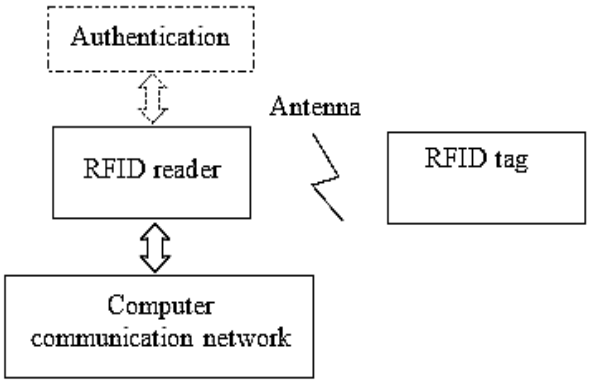

Fig. 8. Proposed Network Design Architecture of Proposed System.

This new design shows the solution to the current network design problem that the existing system of NFC do not has the authentication and cryptography encoded with. All information regarding NFC and detection system are needed to be analyzed in this phase which includes interfaces, NFC reader and NFC tag. The architecture of the network design is created as in Figure 8.

D. Implementation

Phase 4 shows the installation and configuration of the system development using NFC conducted in the real environment. The hardware and software are required to fully execute the system; and the database with security is setup. This system is using C# for interfaces and SQLite for the database. Sample of system development is provided as in Figure 9.

```
private void staff_id_TextChanged(object sender, TextChangedEventArgs e)
{
    SQLiteConnection sqliteCon = new SQLiteConnection(dbConnectionString);

    try
    {
        sqliteCon.Open();
        string Query = "select * from staff where staff_id = '" + staff_id.Text + "'";
        SQLiteCommand createCommand = new SQLiteCommand(Query, sqliteCon);
        createCommand.ExecuteNonQuery();
        SQLiteDataReader dr = createCommand.ExecuteReader();

        while (dr.Read())
        {

            string sstaffname = dr.GetString(1);
            string sphonenumber = dr.GetString(2);
            string semail = dr.GetString(3);
            string ssusername = dr.GetString(4);
            string sspassword = dr.GetString(5);

            staffname.Text = sstaffname;
            phonenumber.Text = sphonenumber;
            email.Text = semail;
            susername.Text = ssusername;
            spassword.Password = sspassword;
        }

        sqliteCon.Close();
    }

    catch (Exception ex)
    {
        MessageBox.Show(ex.Message);
    }
```

Fig. 9. Data Retrieval from Database.

E. Testing

In phase 5, unit testing, integration testing, system testing and user acceptance testing are conducted to ensure the system working well. All units developed in the implementation phase are integrated into a system after being tested by each unit to ensure the system is working completely.

F. Maintenance

In phase 6, researchers need to ensure the requirement statements are fulfilled. This phase dealing with any changes that needed to be done. All recorded data are collected and with the collected results, to determine the effectiveness of the research application. The hardware and software is set up as shown in Figure 10.

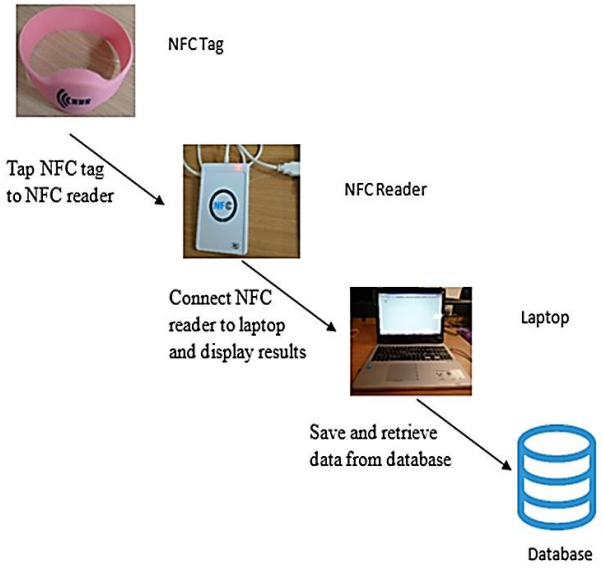

Fig. 10. Hardware and Software Setup of the Proposed System.

III. Results and Discussion

In this paper, two experiments were conducted during the proposed system development, which is the (a) authentication and (b) detection of medical staff who in charge of the medicine data and medicine records. The first experiment is to develop the authentication feature with AES algorithm, meanwhile the second experiment is to integrate the NFC-Tag Staff Data Management System with authentication.

Figure 11 illustrates the introduction page and Figure 12 shows the authentication using NFC Tag that is scanned by the NFC Reader to access to the proposed system. For this study, user need to click at the "Log in with ID" button for the number from the NFC Tag to display the ID number of the NFC Tag. A user need to key in username and password at the log in page. If the authentication is successful and access is granted, as shown in Figure 13, then only the user able to get to the Crypt-Tag Data Management Page, shown in the main page at Figure 14. If the user is an administrator, then the administrator needs to register to the medical staff who is currently working in the department to avoid misconduct of theft activities in the organization.

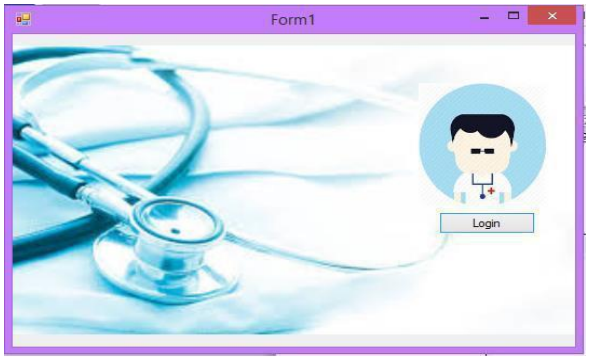

Fig. 11. Introduction to Log in Page.

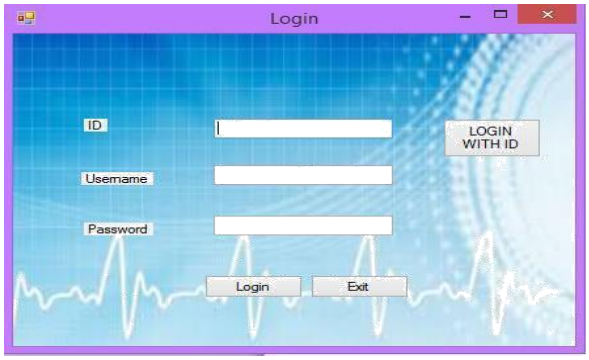

Fig. 12. Authentication using Crypt-Tag for Admin and User.

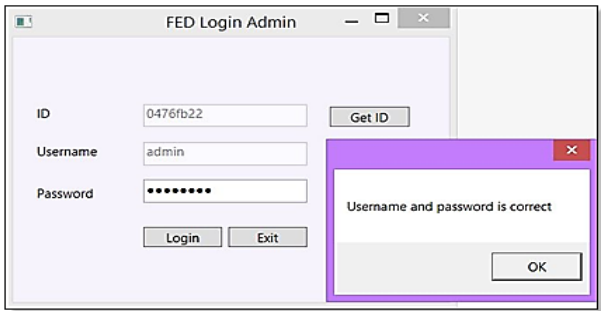

Fig. 13. Administrator Authentication.

The registration of medical staff is done by tapping the staff's identification card (ID) at the NFC Reader and key in the details of the employee; and click the button "Save" to store information into the database as shown in Figure 15. The admin could click the "Exit" button to end the session.

Fig. 14. Crypt-Tag Data Management Page.

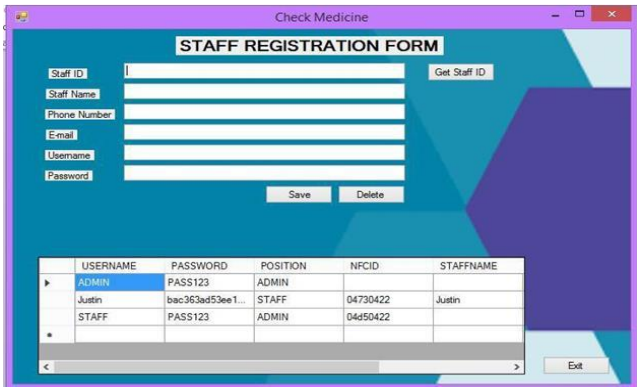

Fig. 15. Integration of NFC Tag Staff Information with Database.

The result indicates that, the staff who has logged-in to the proposed system using his ID (by tapping his ID at the NFC Reader) was Justin. Then, as the NFC Tag of the product is tapped at the NFC Reader, the expiry date and remaining days of the medicine is listed.

Based on our findings, staff can print expired or not expired data, which this process does not only display the item information but also the name of the staff who access the expiry date about the medicine from the proposed system. For future development, the name of the staff no need to be displayed only the medicine name is important.

Another finding that has been encountered is the user interface of this proposed system displayed the process data from receiving and retrieving, which are the list of items tag information with time remaining and current medicine status. This can be improved with an automatically read and save data in database or cloud-based database, which allow the system to be faster and convenience system.

The current system tends to get data leak from several sources such as human being and social media. For example, intruder finds the vulnerability to achieve his or her goal to do malicious activities such as explore or public personnel confidential data or information.

The unauthenticated person easily gain access to an operational process in an organization. For example, attacks will use social engineering such as tailgating or piggybacked to retrieve certain data.

In addition, the current devices used were no security features implemented on it. In fact, there is a lack of security element especially to identify the person who obtain medicine information due to the current devise that not apply encryption technology. Thus, the data or information an easily to achieve by an attacker.

The advantage of this proposed system is it integrates authentication to the proposed system. The authentication features reduce the time taken for sniffing activity by the hacker and able to delay the hacking process before the administrator able to be notified by the system.

IV. Conclusion

In this paper, the implementation of an expiry date detection using RFID that is NFC (short range) in health care industry. The combination of NFC with medicine data management, helps the health care industry to be more effective and efficient in management. The experimental results have shown the development of authentication and the detection of medicine expiry date. Nevertheless, the proposed system needs to be improved to have a smooth execution, which the information from the NFC Tag appeared instantly without clicking at the "Get Staff ID" button. In future, our proposed system should be able to execute better and able to be applied in other industries that are aligned with the Industrial Revolution.

The future implementation is to automatically get UID tag and save to database. The NFC reader should be able to automatically read NFC tag once the tag is tap to the reader. Suggestion for future work, once the NFC tag is detected by NFC reader, the data will be automatically read and save in the database. For future work, once staff login, they only need to tap medical tag to get data and their name are automatically saved in report. Every user can change their own password. In this project, staff is given a default password which based on their UID and they cannot change it. Suggestion of future work, all staffs can be able to change their own password which make the system more interactive. The system should be able to use cloud or wireless which make it easier to be used by all the user.

Acknowledgment

High appreciation to the Center of Applied Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi (FTMK) and Universiti Teknikal Malaysia Melaka (UTeM).

References

[1] I. Tzoulis, and Z. Andreopoulou, "Emerging Traceability Technologies as a Tool for Quality Wood Trade", Procedia Technology, vol. 8, pp. 606–611, 2013.

[2] A. Yewatkar, F. Inamdar, R. Singh, R. Ayushya and A. Bandal "Smart Cart with Automatic Billing, Product Information, Product Recommendation Using RFID and Zigbee with Anti-Theft", Procedia Computer Science, vol. 79, pp. 793–800, 2016.

[3] N.M.Z. Hashim, N.A. Ibrahim, N.M. Saad, F. Sakaguchi and Z. Zakaria, "Barcode Recognition System", International Journal of Emerging Trends & Technology in Computer Science vol. 2 no. 4, pp. 278–283, 2013.

[4] Hashim, N. M. Z., Ibrahim, N. a, Saad, N. M., Sakaguchi, F., & Zakaria, Z. (2013). Barcode Recognition System. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2(4), pp. 278–283.

[5] Changsheng Chena, Alex C. Kota, Huijuan Yang, "A two-stage quality measure for mobile phone captured 2D barcode images", Pattern Recognition, vol 46, pp. 2588-2598, 2013.

[6] R.F. Dos Santos and F.A.S Marins, "Integrated model for reverse logistics management of electronic products and components", Procedia Computer Science, vol. 55, pp. 575–585, 2015.

[7] F. Razzak, "Spamming the Internet of Things: A possibility and its probable solution.", Procedia Computer Science, vol. 10, pp. 658–665, 2012.

[8] A.S. Narayanan, "QR Codes and Security Solutions", International Journal of Computer Science and Telecommunications, vol. 3, no. 7, pp. 1–4, 2012.

[9] E. Ginters, and J. Martin-Gutierrez, "Low cost augmented reality and RFID application for logistics items visualization", Procedia Computer Science, vol. 26, pp. 3–13, 2013.

[10] M. Forouzandeh anf N.C. Karmakar, "Chipless RFID tags and sensors: a review on time-domain techniques", Wireless Power Transfer, vol 2, no. 2, pp. 62-77, 2013.

[11] C. Swedberg. (2016). NFC Tags Take to the Slopes on Ski Jackets NFC Tags Take to the Slopes on Ski Jackets [Online]. Available FTP: http://www.rfidjournal.com/articles/view?15408, C. Sun. (2012). Application of RFID Technology for Logistics on Internet of Things. [Online]. Available FTP: https://doi.org/10.1016/j.aasri.2012.06.019

[12] A. Williamson, L-S. Tsay, I.A. Kateeb and L. Burton, "Solutions for RFID Smart Tagged Card Security Vulnerabilities", AASRI Procedia, vol. 4, pp. 282–287, 2013.

[13] M. Attaran, "Critical success factors and challenges of implementing RFID in supply chain management", Journal of Supply Chain and Operations Management, vol. 10, no. 1, pp. 144–167, 2012.

[14] S.A. Joseph, and N.J. Joby, "Analyzing RFID Tags in a Distributed Environment", Procedia Technology, vol. 24, pp. 1483–1490, 2016.

[15] A. Zavvari, M. Shakiba, M.T. Islam, E. Sundararajan and M.J. Singh, "Computational Cost Analysis on Securing RFID Protocols Conforming to EPC Class-1 Generation-2 Standard", Procedia Technology, vol. 11, pp. 778–784, 2013.

[16] A. Alqarni, M. Alabdulhafith and S. Sampalli, "A Proposed RFID Authentication Protocol based on Two Stages of Authentication", Procedia Computer Science, vol. 37, pp. 503–510, 2014.

[17] T. Feng, M. Hwang and L. Syu, "An Authentication Protocol for Lightweight NFC Mobile Sensors Payment", INFORMATICA, vol. 27, no. 4, pp. 723–732, 2016.

[18] M. Attaran. Critical success factors and challenges of implementing RFID in supply chain management. Journal of Supply Chain and Operations Management, vol 10, no. 1, pp. 144–167, 2012.

[19] Sun, C. Application of RFID Technology for Logistics on Internet of Things. AASRI Procedia, vol. 1, pp. 106–111, 2012.

[20] A. Wilson, T. Hainey, and T. Connolly, Evaluation of Computer Games Developed by Primary School Children to Gauge Understanding of Programming Concepts. Proceedings of the European Conference on Games Based Learning, 2013, pp. 549–558.

[21] Williamson, "Avery, Tsay, L.-S., Kateeb, I. A., & Burton", L. (2013). "Solutions for RFID Smart Tagged Card Security Vulnerabilities." AASRI Procedia, 4, 282–287.

[22] Park, S., & Lee, K. (2014). Advanced Approach to Information Security Management System Model for Industrial Control System. The Scientific World Journal, 2014.

[23] Alqarni, A., Alabdulhafith, M., & Sampalli, S. (2014). A Proposed RFID Authentication Protocol based on Two Stages of Authentication. Procedia Computer Science, 37, 503–510.

[24] Badra, M., & Badra, R. B. (2016). A Lightweight Security Protocol for NFC-based Mobile Payments. Procedia Computer Science, 83(Ant), 705–711.

[25] Joseph, S. A., & Joby, N. J. (2016). Analyzing RFID Tags in a Distributed Environment. Procedia Technology, 24, 1483–1490

[26] Priporas, C.-V., Stylos, N., & Fotiadis, A. K. (2017). Generation Z consumers' expectations of interactions in smart retailing: A future agenda. Computers in Human Behavior.

[27] Mary, B., & Connor, C. O. (2015). New NFC Security Feature Tightens Controls on Tag Data New NFC Security Feature Tightens Controls on Tag Data, 1–2.

[28] Persson, M., & Håkansson, A. (2015). A communication protocol for different communication technologies in cyber-physical systems. Procedia Computer Science, 60(1), 1697–1706

[29] Swedberg, C. (2016). NFC Tags Take to the Slopes on Ski Jackets NFC Tags Take to the Slopes on Ski Jackets, 1–2.

[30] Jung, M. S. (2015). A study on electronic-money technology using near field communication. Symmetry, 7(1), 1–14.