

Near Field Communications (NFC) as Halal Detection Application

Siti Salwa Md. Sawari¹

Mohd Al'Ikhsan Ghazali²

Siti Mariam Abu Bakar Yap³

Faculty of Islamic Civilization, Universiti Teknologi Malaysia

Email:¹ salwa.sawari@gmail.com, alikhsan@ic.utm.my, nuruldinulislam@gmail.com

Doi:10.5901/mjss.2015.v6n5s2p547

Abstract

The objective of this study is to discover the advantages and disadvantages uses of Near Field Communications (NFC) as halal certificate detection. NFC is a type of wireless connectivity protocols, in which it allows reliable communications within devices in short range. Consumers can easily detect the halal status of the nearby restaurants as their phones will vibrates if the restaurants have the legal halal certificates in 500 meter distance. In addition, consumers can easily report to authorities about the fake halal logos of the restaurants using this system, with that an immediate action will be taken. However, it also discovers that NFC could bring several disadvantage such data loss and tag damage, technical limitations in the implementations of software card emulation and loss in security.

Keywords: Near Field Communications (NFC), Halal Certification,

1. Introduction

Besides E-halal system, The Malaysian Islamic Development Department (JAKIM) also introduced Near Field Communication (NFC) system. According to Najmuddin (2013), Near Field Communication (NFC) system can be used with 'Halal Square' and 'Halal Inside' application. Using this technology, Muslim consumers can easily detect the halal certificates of the nearby restaurants by only using their smartphones. Through this application, consumers can easily detect the halal status of the nearby restaurants in 500 meter estimation. In addition, by using these applications, consumers can easily track the fake halal logos used by the restaurants using only their smartphones or any other technological gadgets. The consumers of the local markets can easily detect the halal status of the nearby restaurants as their phones will vibrates if the restaurants have the legal halal certificates from JAKIM in 500 meter distance. In addition, consumers can easily report to JAKIM about the fake halal logos of the restaurants using this system and JAKIM can immediately take any necessary actions. According to Najmuddin (2013), with the existence of this kind of technology, it is hoped that the halal industry in Malaysia can have a better future.

2. Near Field Communications (NFC)

Basically, Near Field Communications (NFC) is a type of wireless connectivity protocols, in which it allows reliable communications within devices in short range. NFC which is based on a technology called Radio-Frequency Identification (RFID), an electromagnetic wireless, is standardized in ISO/IEC 18092. According to Cavoukian (2011), NFC can be described as "a short-range wireless technology that allows mobile devices to actively interact with passive physical objects and other active mobile devices, connecting the physical world to mobile services in ways that empower and benefit users" (p. 1). Additionally, Mohamed Mostafa (2011) claims that NFC is "a technology for high frequency wireless short distance point-to-point communication" (p. 51). Meanwhile, Curran, Millar, and Garvey explain that NFC is a "specification for contactless communication between two devices", in which it helps the interaction with a maximum distance of around 20 cm, or less (p. 371).

According to Hussein and Mohammad (2012), there are two modes of NFC which are; (1) communication; and (2) operation. In term of communication, there are three modes defined by NFC that can be identified as; (a) read and write mode, in which this mode can read and write to the tag, as an example of this mode is smart poster; (b) tag emulation mode, which this mode is supported by contactless communication, while it enables the NFC devices to act like a smart

card, where the mobile phones, for instance, can be used as an electronic platform for several purposes; (c) peer-to-peer mode, which "link level communication is established between two NFC phones" (Hussein & Mohammad, 2012, p. 94). Exchanging business cards is an example of peer-to-peer mode. Meanwhile, in term of operation, NFC can function in both active and passive mode, according to defined requirements. In active mode, both devices elicit radio frequency (RF) field to transfer all data. In contrast, in passive mode, only one device triggers the RF field while the other one uses load transition to either transfer or exchange the data or files.

In addition, there are four ways of how the NFC works, in which they can be classified into four categories: (1) from phone to phone; (2) from phone to device, (3) from phone to tag; and (4) from phone to reader. In brief, firstly, from phone to phone, two devices that are equipped with NFC can exchange information with each other, such as transferring data, music, files or images, by touching each other. Secondly, from phone to device, a device that is equipped with NFC can communicate with any device by touching. For example, a printer that is fitted with NFC can print the images stored in a mobile phone by touching it (Hussein & Mohammad, 2012). Thirdly, from phone to tag, the users can transfer the data to a device by touching, in which the tag itself keeps the data. Normally, the tag is embedded on posters for marketing purposes can. For instance, a device can transfer the details of a bus departure by touching the tag on the bus terminal. Last but not least, from phone to reader, the users can purchase and accumulate electronic tickets on their devices. Basically, "cell phone can communicate with external reader by just touching it with reader. So one can purchase ticket easily instead of standing and waiting in a long queue" (Hussein & Mohammad, 2012, p. 96). It is evident that NFC is reliable and easily accessible as ECMA (2004) claims that NFC is "as easy as a touch" (p. 2).

According to Hussein and Mohammad (2012), NFC is a very crucial technique because the "integration of technology in mobile phones to make people's lives much easier" (p. 93). Regarding this statement, it can be concluded that NFC brings many advantages to the world. PHILIPS (2004) mentions that NFC is advantageous as it enables smart key access, enhances personal mobility and enables m-commerce. On the other hand, ECMA (2004) convinces that NFC helps people to work much easier than usual as it is easily accessible and reliable. In addition, HCL (2013) explores that NFC nowadays is very beneficial since it is more secure than other wireless connectivity protocols, more intuitive and suitable for transactions, and consumes less battery. More than that, Baker (2011) insists that NFC is beneficial due to its convenience on the devices.

3. Smart Key Access

"NFC is fully compatible with both Philips' MIFARE® and Sony's Felica contactless smart card platforms. These proven systems provide a solid foundation for the introduction of NFC-enabled devices" (PHILIPS, 2004, par. 7). Regarding this, devices that are equipped with NFC, such as mobile phone or tablets, are authorized to act as a key to the users' access. This allows the users to get accessed to their home, office, as well as transportations tickets. NFC devices can read and detect the data from contactless cards. This makes the smart cards become the primary choice for expanding information and electronic coupons into the NFC world. Hence, it makes users' lives much easier (Hussein & Mohammad, 2012).

4. Personal Mobility

A smartphone is one of very few personal items which people are always carrying around. NFC eases the stress of traveling by ensuring the user always has the right cards and documents at hand (PHILIPS, 2004). "Online reservation systems already exist that work with a booking code or form that the user needs to print or receive through the mail. With NFC, the codes can be stored on the user's phone, PDA or credit card" (PHILIPS, 2004, par. 18). On the other hand, the users can also get easily accessed to their online banking to do any transactions such as paying the bills, by getting all sources or information of their accounts by bringing their NFC-enabled device up to a similarly enabled computer. This is really beneficial to the users as they can securely get accessed to at any time they need to, without authorizing their user names and passwords for logging in as NFC freeing the user from having to memorize a host of user names and passwords.

5. M-Commerce

Mobile commerce or m-commerce involves any commerce activity such as ticketing, banking or purchasing goods and services, using mobile devices (Vazquez-Briseno et al., 2012). M-Commerce is an extensive and huge area of activities, covering any transactions that involves financial issues. PHILIPS (2004) claims that "offering consumers the possibility to make any sort of electronic payment wirelessly, NFC-enabled mobile devices are well placed to become the heart of

mCommerce" (par. 8). NFC offers the users to interact within electronic environment over their devices. As reported in Analysys Mason Limited (2008), NFC technology has huge potential for different business and marketing models, as a medium for the users to maximize the use of NFC. Nowadays, there are few businesses that are currently using NFC as a base for their purchasing and marketing system (Analysys Mason Limited, 2008).

6. Accessible and Reliable

ECMA (2014) claims that NFC is helpful as it is easily accessible and reliable to the users, as is as simple as a touch. It is evident that NFC is accessible as Jaring, Törmänen, Siira, and Matinmikko (2007) explains that NFC has the ability to "decrease or eliminate duplicate work" and help "decreasing the amount of user made errors" (p. 365). There is a correlation as Jaring, Törmänen, Siira, and Matinmikko (2007) state that "decreasing the amount of duplicate work decreased the user made errors, because the amount of opportunities to make errors was diminished" (p. 365). This method benefits the users to transfer larger data or continuing the communication session if devices go away after touching each other (Hussein & Mohammad, 2012). Besides, with NFC, the users can get access to their favorite music and listen to their music whenever and wherever they want. This makes things easier as they no longer need to copy their CDs or wait for tracks to download from the Internet. They just need to download the digital rights to a track to stream the music directly to their music system.

6.1 Secure

According to HCL (2013), NFC is more secure compared to other wireless connectivity protocols such as Bluetooth, Wi-Fi and others. In NFC policy, a connection can be enabled only if the two devices are brought close to one another. This property makes a transaction or data exchange "less prone to hacking by a third party (HCL, 2013, p. 6). Additionally, Jaring, Törmänen, Siira, and Matinmikko (2007) claim that NFC help to increase the capability of the system to verify user actions. This helps the system to identify the accurate location and time where an account is accessed. Hence, there are high possibilities to avoid hacking or data stealing as the system will report accurately (Hussein and Mohammad, 2012). Pertaining to these issues, NFC as a wireless standard will be more acceptable to companies involved in money transactions than other wireless technologies.

7. Intuitive and Suitable

NFC is more intuitive and suitable for transactions such as ticketing and money transfers (HCL, 2013). For instance, by using NFC, "the eTicket purchasing process takes just a matter of seconds and is extremely simple and convenient for consumers" (PHILIPS, 2004, par 15). It just needs the card and the reader to be brought close to one another. That is more convenient and easy to understand than swiping, choosing from a menu or entering a password. Since it is also based on universally followed standards like the ISO and European Telecommunication Standard Institute (ETSI), "interoperability with other existing wireless technologies is not a problem. In fact, NFC, which is inherently more secure, can be used as the identification and authentication procedure for a Wi-Fi or Bluetooth connection to be established for higher data transfer speeds" (HCL, 2013, p. 6). Additionally, Ankey (2011) also claims that NFC eases people in making any payment or for identification purpose. Pertaining to this issue, NFC technology has a great potential for different business and marketing models (Analysys Mason Limited, 2008).

8. Less Battery

HCL (2013) claims that NFC is advantageous as it was "purposefully built with lower transfer speeds of 106 kbps to 424 kbps so it consumes less battery" (p. 6). Analysys Mason Limited (2008) reports that NFC can prepare the users with battery power that is significantly for long period, since the NFC system provides the users with significant processing power and memory for NFC applications. Hence, this is much more practical for devices for which power consumption is an overriding priority. For example, NFC can be a natural choice for an implantable medical device which needs to communicate to an outside device. Basically, the time taken to establish a connection through NFC is on the order of 100 milliseconds, which is much better than other competing technologies which take a few seconds to establish a connection. Additionally, NFC protocol can be used as an authentication procedure before other wireless standards take over the function of actual data transmission at higher transfer speeds (HCL, 2013).

8.1 Convenience

According to Baker (2011), NFC is superior to other wireless connectivity protocols due to its convenience, where the users can rapidly become familiar with and enthusiastic about the technology. In addition, the ability of the NFC to smoothly and rapidly run on the devices does also contribute to the advantages to the users. ACUTA (2013), NFC is very convenient as it can be a very helpful application in education, in which it can be used for attendance monitoring that can save time which can be dragged into teaching and learning process. Other than that, "when linked up to back-office systems, the data that NFC generates can trigger early warning signals about students in trouble, helping the college to take action and retain as many students as possible" (ACUTA, 2013, p. 17). Last but not least, NFC also helps students to get on with their studies, as well as to run their business as "NFC makes it easy for them to pay for the things they need across campus, from libraries and photocopying to cafes, shops, and even transportation" (ACUTA, 2013, p. 17).

However, HCL (2013) does also mention that NFC somehow has several disadvantages that users may face. The drawbacks include hacking and roadblocks. On the other hand, Kaur, Sandhu, Mohan and Sandhu (2011) justify that NFC also brings disadvantages to the users as it include data loss and tag damage. Additionally, Roland (2012) claims that technical limitations in the implementations of software card emulation is also an advantage of NFC, in which it has significant loss in security.

9. Hacking

Although NFC is more secure than other wireless connectivity protocols, still, attacks and treats are possible (Mohammad Umair & Umair, 2012). This is because the attackers can "program tags to direct to their website which may contain harmful content or steal vulnerable information stored on the phone's NFC tag" (Mohammad Umair & Umair, 2012, p.15). Similarly, HCL (2013) also states that the possibility to be hacked appears even though the security is there. This is because NFC security is not foolproof, in which the hackers are able to gain full control of the target device and run malicious codes. According to HCL (2013), "it has been demonstrated that smartphones with NFC can be hacked into. Hackers were able to gain full control of Android-based smartphones and run malicious code on them" (p. 8). Besides, Lefebvre, Simonova and Girdharry (2013) suggest that "NFC is vulnerable to 'data corruption' and 'eavesdropping' hacking methods and may potentially present a serious threat to personal and finance information although there are passwords protecting the account" (p. 1).

10. Roadblocks

According to HCL (2013), NFC can be disadvantageous because of the passive tags that are used. This is because it needs to be powered by "an external reader which can lead to higher power consumption than Bluetooth Low Energy" (HCL, 2013, p. 8). In term of medic, his kind of disadvantages can be potential roadblocks for adoption of NFC in implantable medical devices where security is paramount, and communication has to reliable over longer distances, particularly if the implanted devices are placed deep in the body, implantable defibrillators, for instance. These problems will limit users' usage as the passive tags consume higher power, although the NFC was built with lower transfer speed (HCL, 2013).

11. Data Loss

Kaur, Sandhu, Mohan and Sandhu (2011) explore that the risk of losing the data is possible. This may be resulted from users' attempt of reading several tags at the same time. In fact, this kind of attempt will result on signal collision, in which it ultimately expose the users to data loss. Although this problem can be prevented by applying anti-collision algorithm, it somehow burdens the users as the application of the "cure" cost users with high price. Additionally, Lefebvre, Simonova and Girdharry (2013) also explain that opening several tags at the same time exposes the users' account to be hacked as the system cannot fully protect the tags when they are opened and accessed simultaneously. Hence, the possibility for the tags to be broken is great and this will lead to the loss of confidential and personal data. For example, transactions such as payment receipts may be lost, and this is kind of troublesome to the users.

12. Tag Damage

Basically, tags have the possibility to get damaged or broken during the usage (Kaur, Sandhu, Mohan & Sandhu, 2011).

"A wide range of application challenges can be answered by the multitude of suitable tags, yet none of them is completely invulnerable and the causes of damage may vary from type to type" (Kaur, Sandhu, Mohan & Sandhu, 2011, p. 154). Hence, Kaur, Sandhu, Mohan and Sandhu (2011) define that read failure, which the tags will encounter difficulties to identify data, is a result due to this issue. This will create another issue, which appearing a problem when the devices cannot identify a payment details due to the damaged tag, for instance. Indirectly, tag damage gives the hackers an opportunity to attack the users' account (Kaur, Sandhu, Mohan & Sandhu, 2011).

13. Software Card Emulation

According to Roland (2012), technical limitations in implementations of software card emulation also contributes to drawback of NFC. It is difficult for card emulation application to store sensitive data without secure storage. In addition, it is also harmful to users' privacy even though the devices are with software card emulation because security critical applications are possible to some extent. This is due to the capability of software card emulation, in which the software-emulated smartcards are only allowed to use a certain set of UIDs with NXP's NFC controllers. Some devices that are not compatible with these kind of UIDs have major risk to be attacked. Hence, users have great potential to lose their valuable data, either by hijacking or stealing by the hackers (Roland, 2012). This is a very worrying issue as mobile phones are now used as a platform for the hackers to attack the users' software card emulation even though all data are encrypted.

14. Conclusion

NFC is a very crucial technique because the integration of technology in mobile phones to make people's lives much easier. The consumers of the local markets can easily detect the halal status of the nearby restaurants as their phones will vibrate if the restaurants have the legal halal certificates from JAKIM in 500 meter distance. In addition, consumers can easily report to JAKIM about the fake halal logos of the restaurants using this system and JAKIM can immediately take any necessary actions. According to Najmuddin (2013), with the existence of this kind of technology, it is hoped that the halal industry in Malaysia can have a better future. Regarding this statement, it can be concluded that NFC brings many advantages to the world. However, it also discovers that NFC could bring several disadvantage such data loss and tag damage, technical limitations in the implementations of software card emulation and loss in security.

References

- ACUTA. (2013). Near Field Communication Brings Convenience to Campus Coming soon to a Device near You: NFC, the Enabling Technology. Retrieved on March 11, 2015, from <http://www.campusm.com/wp-content/uploads/2013/07/ACUTA-Summer13-Pg.16-18.pdf>
- Analysys Mason Limited. (2008). Mobile proximity payments: scenarios for market development. Retrieved on March 9, 2015, from Analysys Mason: http://www.analysismason.com/PageFiles/4588/Mobile_proximity_payments_sample_pages.pdf
- Hab Halal Division. (2014). The Recognized Foreign Halal Certification Bodies & Authorities. Department of Islamic Development (JAKIM).
- Ankeny, J. (2011). The New Smart Money. Retrieved on March 10, 2015, from Entrepreneur: <http://www.entrepreneur.com/article/218100>
- Baker, J. (2011). Strong growth expected for NFC-enabled smartphones, pyramid finds. Retrieved on March 9, 2015, from PR Newswire: <http://www.prnewswire.com/news-releases/stronggrowth-expected-for-nfc-enabled-smartphones-pyramid-finds-120111709.html>
- Cavoukian, A. (2011). Mobile Near Field Communications (NFC) "Tap 'n Go" Keep it Secure & Private. Toronto: Ontario, pp. 1-18.
- Curran, K., Millar, A. & Garvey, C. M. (2012). Near Field Communication. *International Journal of Electrical and Computer Engineering (IJECE)*, 2(3), pp. 371-382.
- ECMA. (2014). Near Field Communications (NFC). Retrieved on March 11, 2015, from <http://www.ecma-international.org/activities/Communications/2004ga-067.pdf>
- HCL. (2013). Near Field Communication in Medical Devices. Retrieved on March 11, 2015, from www.hcltech.com/.../near_field_communication_in_medical_devices.pdf
- Hussein Ahmad Al-Ofeishat & Mohammad A.A. Al Rababah. (2012). Near Field Communication (NFC). *International Journal of Computer Science and Network Security*, 12(2), pp. 93-99.
- Jaring, P., Törmänen, V., Siira, E. & Matinmikko, T. (2007). Improving Mobile Solution Workflows and Usability Using Near Field Communication Technology. VTT Technical Research Center of Finland. Finland: Oulu, pp. 358-373.
- Kaur, M., Sandhu, M., Mohan, N. & Sandhu P. S. (2011). RFID Technology Principles, Advantages, Limitations & Its Applications. *International Journal of Computer and Electrical Engineering*, 3(1), pp. 151-157.

- Lefebvre, R., Simonova, E. & Girdharry, K. (2013). Mobile Payments in Canada – The Demand Side of the Equation. Retrieved on March 12, 2015, from http://www.cga-canada.org/en-ca/ResearchReports/ca_rep_2013-03_informed-view.pdf
- Mohamed Mostafa Abd Allah. (2011). Strengths and Weaknesses of Near Field Communication (NFC) Technology. *Global Journal of Computer Science and Technology*, 11(3), pp. 51-56.
- Mohammad Umair Yaqub & Umair Ahmad Shaikh. (2012). Near Field Communication. Retrieved on March 9, 2015, from http://www4.kfupm.edu.sa/ssc/4845_MohammedUmair_Yaqub.pdf
- PHILIPS. (2004). Near Field Communications. Retrieved on March 10, 2015, from <http://www.sacg.com.tw/sacweb/marcom/epaper/images/NFC.pdf>
- Roland, M. (2012). Software Card Emulation in NFC-enabled Mobile Phones: Great Advantage or Security Nightmare? UK: Newcastle. Retrieved on March 11, 2015, from <http://www.medien.ifi.lmu.de/iwssi2012/papers/iwssi-spmu2012-roland.pdf>
- Najmuddin. (2013). Pelancaran Global Pelaksanaan Sistem Pengesanan Pensijilan Halal Malaysia. Portal Rasmi Halal Malaysia. (Online) Retrieved on March 10, 2015, from <http://www.halal.gov.my/v3/index.php/ms/mengenai-pensijilan-halal/takrifan-halal>
- Vazquez-Briseno, M., Hirata, F. I., Sanchez-Lopez, J. D., Jimenez-Garcia, E., Navarro-Cota, C. & Nieto-Hipolito, J. I. (2012). Using RFID/NFC and QR-Code in Mobile Phones to Link the Physical and the Digital World. Retrieved on March 11, 2015, from <http://cdn.intechopen.com/pdfs-wm/31056.pdf>