EPiC Series in Computing

Volume 81, 2022, Pages 165–176

Proceedings of 11th International Congress on Advanced Applied Informatics

The Survey of Data Stealing on Virtual School Based on NFC

Andrew Martin Tan[1], Filip Beniah Anggara[1], Jennifer Goldwin[1], Ford Lumban Gaol[1], Tanty Oktavia[1], Chew Fong Peng[2], and Suzanna[1]

[1] Bina Nusantara University, Indonesia

[2] Malaya University, Kuala Lumpur, Malaysia

andrewmartintan@gmail.com, Filipanggara123@gmail.com, jennifer.goldwin@gmail.com, fgaol@binus.edu, toktavia@binus.edu, fpchew@um.edu.my, suzanna@binus.ac.id

Abstract

In this Digital Era, we are facing a lot of threats to protect our data. One of the latest technology on the short raneg communication is Near-Field Communication (NFC) with so many implications of technology that ranging from Non-physical access control to digital payments. These applications are frequently proclaimed as being more secure, as they require near physical vicinity and don't include Wi-Fi or versatile systems. In any case, these frameworks are still defenseless to security assaults at the time of the exchange, as they require small to no extra confirmation from the user's end. The problem that is the main concern of our paper is about NFC Data Stealing. Not everyone realized that their data get stolen by the Cyber Criminal. A lot of people complacent by NFC Technology that makes data transmission a lot easier, but they only see the good side and close their eyes on the bad side. The problem with NFC is that the data becomes a lot more accessible, and this opens wide the windows for the cyber criminals to steal any data as they like. This opens a new window for them to steal any personal data in no time. Our research method is a survey paper that is based on a real-life case, this method can help us identify a lot of case types. These findings may help all of us to understand more about the problem that we don't even realize.

1 Introduction

In this Digital Era, we are facing a lot of threats to protect our data. In this Era, we start to change the method into Data Transmission. This method makes every individual data easily accessible also makes our privacy vulnerable. One of the problems is NFC Stealing, nowadays any of your card barcode/ chips are visible by other people (Alsumait & Al-Musawi, 2013). Without proper NFC protection, this will make all your data (such as identity, account number, balance, etc) more

vulnerable to get stolen. Many people don't aware of this problem and take it only as a simple problem. But if you keep closing your eyes to this problem eventually all your data will get stolen sooner or later (Azuma, *et al*., 2001).

Now that we know what NFC is, how does it work? Just like Bluetooth and WiFi, and all manner of other wireless signals, NFC, or Near Field Communication, is a short-range wireless RFID communication technology (Alcañiz, *et al*., 2010). It implies that two gadgets prepared with NFC innovation are able to communicate with each other and share data as before long as they are near to one another. There is no compelling reason to dispatch an application, bringing the gadgets close to one another consequently triggers the characterized activity - from a single easy "tap"!

Radio Identification or RFID (stands for Radio Frequency Identification) is a technology allowing to identify and characterize an object that will utilize the broadcasting radio waves. RFID is well known as part of Real Time Localization Systems (RTLS) that mainly used for inventory purposes in that mostly focus on varies of sectors where tracking merchandises is a key issue: retailing, health, transport and logistics, military activities, etc. As we can see that technology behind the NFC technology is taken from the technology of RFID (Radio Frequency Identification) that works by creating a "near field" with the distance no more than 10 centimeters using high frequencies that will allow interacting with NFC equipped devices. The innovation started to be utilized in France in 2011, however it is simply beginning to flourish outside the versatile installment use. Hence, cell phones are increasingly more outfitted with NFC, and activities are duplicating to test and improve its utilization (Azuma, 1997).

While many people still think that NFC is the same as RFID actually these opinions are false. The base of these two is kind of similar but there are some points that make them different from one another. One of the most contrasts is the truth that NFC permits restricted information sharing between the tag and the reader. At that point, another one is that NFC incorporates a truly short range compared to RFID (some centimeters versus some meters).

NFC is one of the various communication methods used to allow instant access to any digital information and data from your portable gadget as a contactless innovation. To do this, there are 3 different ways:

1.1 The emulation mode of the host card

This is the "inactive" mode, which works like a savvy contactless chip via a flexible terminal. The telephone sends the information to the Near Field Communication (NFC) gadget, such as a ticket approval booth or a payment terminal. It may meet various requirements: flexible installments, tickets for display or transport, vouchers, access control, etc.

1.2 The reader mode

In this case, as a contactless chip reader, the mobile has a "dynamic" component. This mode allows you to basically "tapping" or "bumping" your phone near an NFC tag to analyze data or cause activities. NFC labels can be set anywhere on all your contact networks on blurbs, notices, landmarks, transport stops or item packages, expanding the usage and opening process. The goal here is to provide a consistent client experience with a specific computerized substance through channels, from offline to versatile. NFC labels are exceptionally comparable to QR code capabilities from this point of view and can be used as the basis for your Offline To Online promotion campaign.

1.3 Styles for the Article Body

In this mode, the data trade operates by means of NFC in both bearings between two portable gadgets communicating with each other. Popular applications include swapping contact information

(vCard) between two smartphones, exchanging records such as images or videos, and executing cash exchanges immediately.

While the NFC exchange is without a doubt more secure than normal credit card installments, this innovation isn't totally free from chance. Fast advancement in innovation continuously comes with an similarly effective negative result.

With this new contactless innovation set to ended up an critical portion of our lives, individuals have a few substantial and justifiable security concerns. When using new technologies, perfect way" the most perfect way to ensure yourself against potential pitfalls is to know the dangers related with them. One of the foremost common concerns with NFC innovation is that of spying. Listening in happens when a third party mediation the flag sent between two gadgets. On the off chance that that third party catching a information transmission between a smartphone and a credit card peruser at that point, in hypothesis, they would have get to to that individual credit card data. They might moreover choose up other individual data passed between two smartphones.

Another security concern is information control or debasement. This happens when a third party mediation the flag being sent, modifies it, and sends it on its way. The data the accepting party gets may be degenerate or adjusted. The aggressor may or may not need to take the data. In a few cases, the aggressor simply wants to avoid the proper data from getting through. This can be frequently known as a dissent of benefit attack.

At last, the final of the security comes within the shape of infections. Whereas smartphone infections are as of now few and far between, they are developing. Security companies have pointed out that when smartphones give small budgetary pick up for programmers, they are focused on less. NFC innovation would permit clients to store profitable bank account and credit card data on their smartphones, in this way making them a target.

· NFC compatible gadgets can as it were communicate when they are within four centimeters of each other.

· NFC tags don't control themselves. Instep, they depend on control from the smartphone or other gadget collaboration with them.

· The first smartphone infection, a Trojan, was recognized in October 2010 and a few more have showed up since.

We trust our investigate from this paper can offer assistance individuals to get it more about NFC. And what anticipation can they did to ensure their claim data.

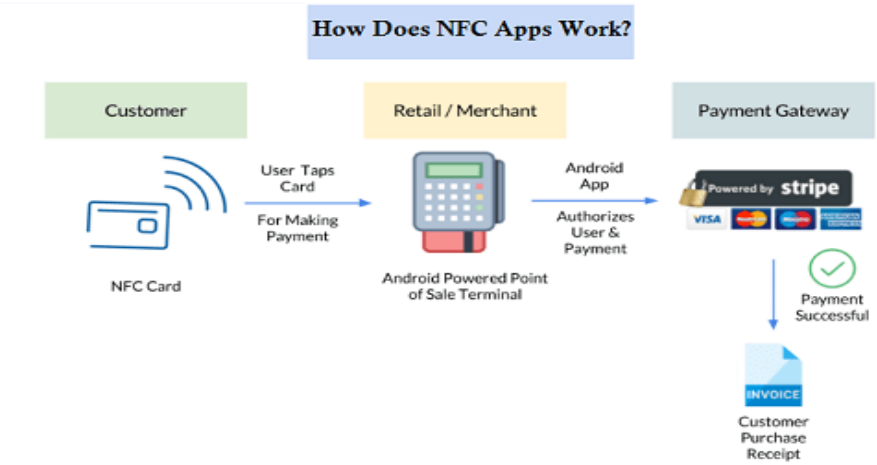

Figure 1: How NFC Operate

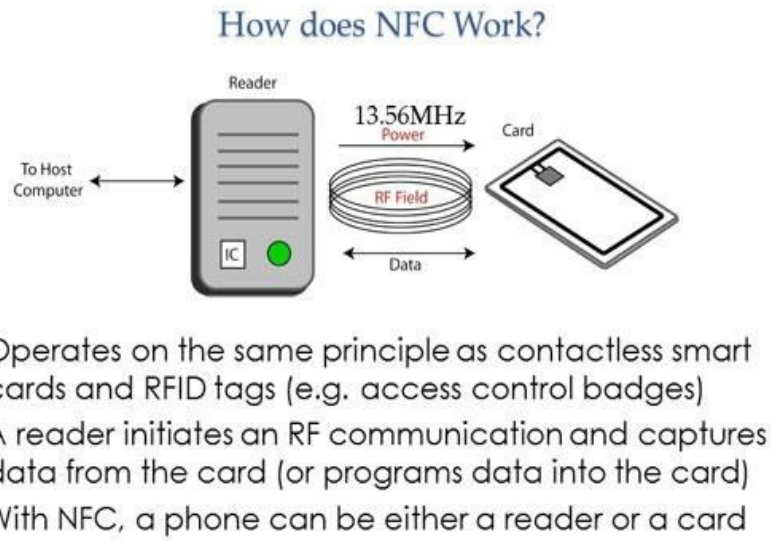

Figure 2: Example of NFC Communication Modes

2 Theory and Concept

Near Field Communication (NFC) A technology change from one computer to the network and the gadgets associated with a single idea from equipment to several gadgets has recently ended. Within the equipment arrangement for the foundation of an arrangement, it is imperative that shoppers do not face complications, driving to approach field communications, the NFC can be a mixture of identity and connectivity via devices that contactless proximity between data. Simple contact between small electronic gadgets will end up being made to facilitate attractive acceptance when they touch the gadgets or end up closer to each other with a number of centimeters to empower communication between them (Moreno, *et al*., 2001). In addition, for knowledge trade, peer-to-peer organizing was created.

If you build a communication network, it is possible to use other remote devices, such as Bluetooth and Wi-Fi, to share an extensive amount of information and extend the range of communication. If you have a tablet and mobile phone prepared with NFC, you can effectively download data from the Web to your cell phone at that stage by simply pressing your cell phone with the portable workstation. Like that, you can only take photos from your mobile phone and if you need to show those photos on a big screen (TV) to your friends at that point, you can just touch your TV phone and show them. Or if you need to print those images at that point by touching the cell phone with the printer prepared by NFC, you will obtain prints of those images (Singhal, *et al*., 2012).

This guideline works for every form of NFC-prepared gadgets to connect with each other. The contact link must not be set up at first. Assume that when using novel technology such as Bluetooth or Wi-Fi, you need to share a record from one laptop to another. You want the contact link between tablets to be manually set up. But in case you're utilizing NFC empowered portable workstations, at that point you will exchange the record by fair touching both portable workstations. In another circumstance, you will build up the connect utilizing NFC and once the communication interface is 94

IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.2, February 2012 set up Bluetooth or Wi-Fi can be utilized to exchange information.

Advantage of utilizing this strategy is to exchange bigger information or continuing the communication session in case gadgets go absent after touching each other. NFC empowers two-way communications between electronic gadgets. And has the capability to compose to the RFID (Radio Recurrence Distinguishing proof) chip.

Bidirectional contact between the NFC-equipped mobile phone and the NFC peruser can be constructed in this way. This provides the plausibility of developing complex applications such as installment, stable information trade, and verification of identity. Touching worldview implements NFC. In human life, touching could be a well-known and intelligent tactic. This makes it easy to memorize and use NFC Creativity. This touching worldview was first used in the invention of RFID (Radio Frequency Distinguishing Proof). Things stamped with labels in RFID innovation include transponders that emit messages within the context of signals. RFID perusers have been used to peruse certain texts. With this RFID breakthrough, NFC is currently organized. The tags that NFC readers can distinguish should have an interesting ID of 4 to 10 bytes. For identifiable evidence of the name, this special ID is used. There are numerous NFC Reader manufacturers within the industry, so the length of the ID can also change (Wojciechowski & Cellary, 2013).

From a technological viewpoint, NFC is paired with the invention of contactless smart cards and mobile phones. NFC gadgets have been developed and operate regularly in three different modes: card emulation mode, peer-to-peer mode, and reader-writer mode. NFC gadgets act like a peruser in the card emulation mode mode, e.g. Label with NFC. This tag has the ability to securely store information . Electronic identification and transactions are the applications of this mode. In peer mode, two NFC- prepared gadgets will directly exchange information by touching each other.

P2P mode applications share information between a tablet and a mobile phone. Printing knowledge by pressing a printer's tablet. The NFC gadget can read or write tags in the same mode as RFID labels in the reader-writer mode. On RFID chips, NFC can read and write information and in anything from paper to apparatus, the RFID (Radio Recurrence Recognizable Proof) chip can be inserted. Basically, RFID is used by radio waves for following and recognizable evidence. The key NFC applications are components of electronic gadget interfacing, computerized material access and contactless exchange.

Payments by NFC Card. An NFC-enabled microchip inserted inside a physical EMV chip credit card can be used to make NFC transactions. These microchips are used to provide the ordinary EMV chip exchange strategy with a prompt, contactless option. The extra security checks and encryption make it much slower than magstripe exchanges, while an EMV chip exchange provides additional levels of security (illustrations of which are examined in Section 2.2). The NFC-enabled microchip instep enables installments to be performed and tested using a point-of-sale system within a fraction of this time. These frameworks are defined to be reliable, since they are different in brief as they are open. They can typically only have the required information to complete the exchange without additional functionality (e.g. customers will not increase their card adjustment via the contactless interface). EMV allows an additional layer of confirmation protection by using a PIN.

In any case, due to pace considerations and the emerging notoriety of cardless installments, this has increasingly been staged within the US. In Europe, the PIN instruction order will be used for exchanges exceeding EUR 20. In addition, RFID cards have a permanent UID to comply with the ISO/IEC 14443 standard, which is free from installation data. This makes it possible for a particular card or client to be followed. Without any authentication, the UID is open, which can lead to security problems.

Smartphone (NFC Cardless) Payments. NFC Cardless (Smartphone) Transactions The NFC chips embedded in smartphones are used by NFC smartphone-based payments and are increasingly becoming well known due to their ease of use. Despite the various security concerns of NFC card-based and EMV installments, by 2020, $190 billion of exchanges will be made by over 60 million

customers. As a consequence, the security guidelines of these frameworks need to be collected. Mobile-based NFC installation applications such as Apple Pay and Google Pay provide the current NFC system with additional layers of protection. The vendor does not need new gadgets due to the use of the current convention. Basically, each clear NFC installment terminal bolsters, then, cardless installments. In addition to an in-depth analysis of the security arrangement and objectives of these frameworks, these additional layers of security use are provided within the following section. The taking after areas and our misuse of NFC installments will be spurred by this exercise (Squire, *et al*., 2008).

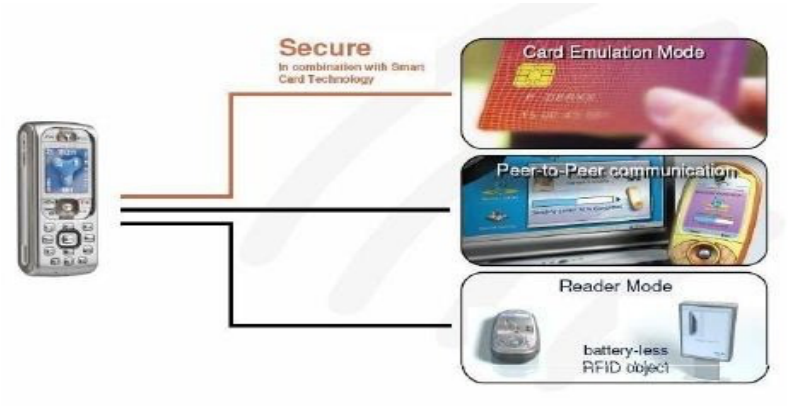

Figure 3: How NFC works on Payment Gateway

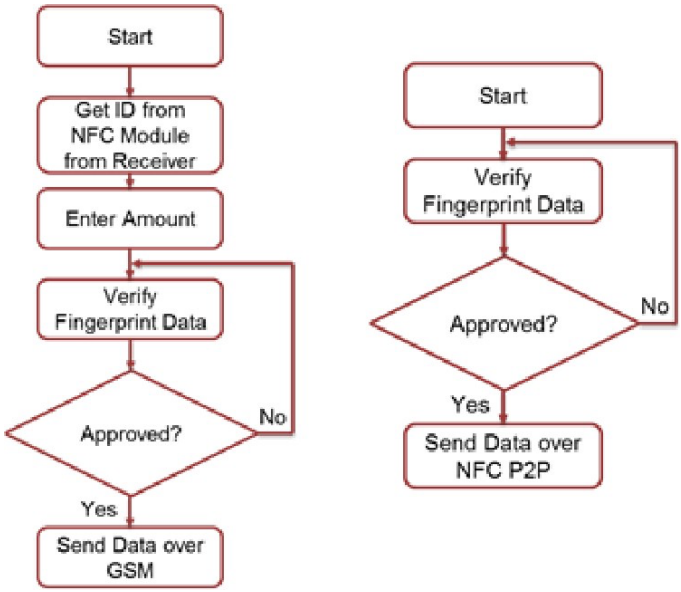

Figure 4: Flowchart of NFC

2.1 The Definition of Data by the Expert

According to Dr. Hanne Albrechtsen, Institute of Knowledge Sharing, Denmark Data. In the areas of computational systems, the coded invariances are knowledge. In human discourse, data is what is conveyed in an empirical analysis, for instance, through sources. Data is connected to the meaning or consciousness of humans. Data is the essence of databases, the net, etc. in computational systems. The sense of articulations as they are aimed by the speaker/writer and understood/misunderstood by the listener/reader is data in human speech systems. In individuals, knowledge is epitomized as the ability to get it, describe and coordinate ideas, events, and eagerly (Wang, *et al*., 2014).

According to Prof. Maria Teresa Biagetti from the University of Rome 1, Italy. She concludes that data is all or any unit that can improve human understanding or broaden our field of understanding, hypothetical or common sense information that can be registered, on whatever help, or orally provided. In our brains, data will stir up information and awareness. Data is the shift selected inside an individual's cognitive legacy. In a cognitive structure, or a knowing subject, knowledge continually creates interior information. Signs that constitute the words created by a record or a book are not information. When signals are correlated with an interpreter, data starts (Morris, 1938). Knowledge is information handled and structured that has built a cognitive context within it or is part of an individual's cognitive legacy (based on C. S. Peirce, 1931, 1958).

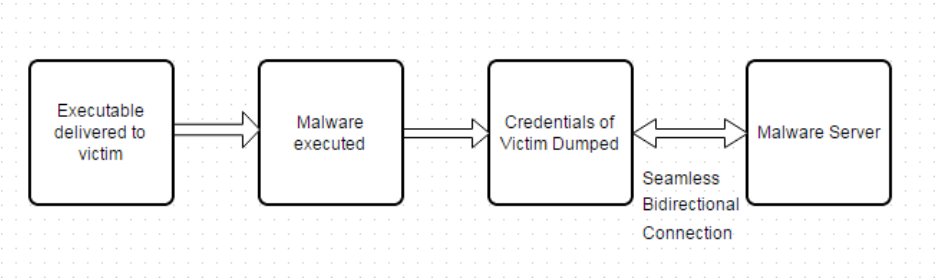

Figure 5: Malwere Schematic

Figure 6: How Cybertheft Get the Data

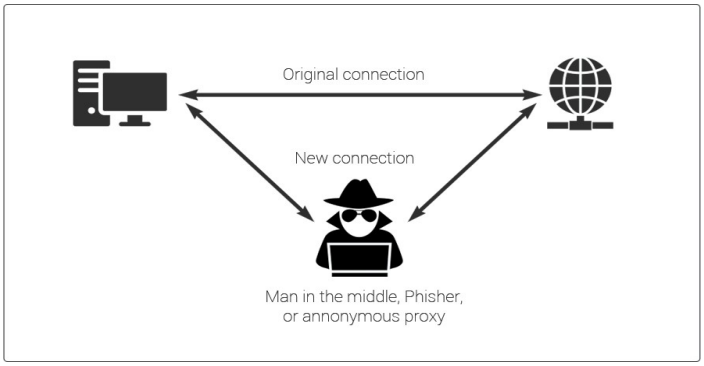

Figure 7: Connection of NFC

2.2 The Definition of Cybertheft and Data Stealing

Cybertheft Law and Legal Definition: Cybertheft means the act of using the network to take away the property of someone or invade the use and delight of the property of someone. Cyber theft, in other words, is the taking of monetary and/or human data by the use of computers to make false or other unauthorized use of it. Cybertheft involves the hacking of the computer records of a bank to wrongfully credit one account and compensate another and interfere with copyright by sending protected fabric over the internet wrongfully. Data Theft Definition: Data Theft is unauthorized taking or interferences of computer-based information Data burglary is the act of taking computer-based data from an accidental casualty with the aim of compromising protection or getting private data. Information robbery is progressively an issue for person computer clients, as well as enormous corporate firms.

3 Methodology

3.1 Case Eavesdropping

A common danger found in all remote communication technologies may be spying. Additionally, NFC is a remote interface for communication between two entities. They use RF signals to interact, so the flag can be obtained by any hardware with a receiving wire inside the sprint. The intruder will extract the data transmitted by experimentation and occasional forms of investigation from the flag. In the case of cash installments, where the consumers use a few hidden keys, this is also particularly vulnerable; the meddler gathers this information and may misuse it. As the intruder who employs a very precise radio wire will potentially get the flag on the off chance that the flag standard is also fragile, it is highly problematic to escape spying. We should make sure that using a safe channel for contact is the only solution to spying.

3.2 Case Data Corruption and Manipulation

In NFC, information is transmitted wirelessly from sender to receiver. For data to be submitted, there are a few unique classes so that it is understood and interpreted by the collector. Data that is not in the adjustment system is refused. Data degradation and control attack occur when an attacker controls the information in between. The assailant may alter the information arrange or alter the

substance in it so that the data gets to be futile or gets rejected because it comes to the collector. For a few coding plans, this assault is conceivable. The strategy for this attack is to use a safe channel between the parties that are communicating.

3.3 Case Man- in- the Middle attack

One move to help data corruption and monitor assault is man within the center assault. We could see that in this attack, the contact between two parties was a third party intrusion. The aggressor serves as a transfer between the receiver and the sender and forwards data (See Figure 5). The aggressor can corrupt, alter, or dispose of the information being sent. In NFC enters, man inside the center assault is very difficult to accomplish and so it's not normal. The scheme for this attack is to use the active-passive mode of communication.

3.4 Case NFC Worm

In NFC-enabled handsets, the NFC virus attack is detected. The Thrust Registry can be managed in this way to collect all URI NDEF messages. Using the standardized NFC Java API, this is achieved. Push Registry allows applications to recruit themselves, such as photos, to deal with any unique details.

4 Solution

4.1 Case 1

The only solution to eavesdropping is to use a secure channel for communication. By using a secure channel for communication, the attacker cannot extract information from the victim because of the encryption of the safe channel. Therefore, the security of the safe channel encryption needs to be powerful so that the information is safely sent between NFC systems that are currently communicating.

4.2 Case 2

Same with the first case, the solution is to use a secure channel between the parties that communicate. If this method can still be broken down, information encryption must be done so that data corruption and manipulation cannot occur. The encryption must make sure the data sent cannot be touched/changed by the attacker.

4.3 Case 3

To overcome the man in the middle attack case, active-passive communication mode can be used. When the sender wants to send data, it enters active mode and the recipient enters passive mode, when the information is about to be sent, the information will be attached with the IDS (Intrusion Detection System) so that it can detect any interference during the delivery. Another way to overcome this is to use a safe channel to communicate where the attacker cannot enter the area of communication.

4.4 Case 4

NFC worm attacks can be overcome by using a shared key where NFC will only approve and start communication if the key matches with the sent code from the sender. If the code does not match, communication is terminated and blocked by an NFC reader.

4.5 Overall Solutions

The finest structure for spying, data corruption, and control assaults is to set up a safe channel between the sender and the collector. Inside the center attack, as NFC has inalienable guarantee against guy, it is a simple errand to set up. Using Diffie-Hellman based on RSA or curved bend, a shared key can be obtained between sender and collector. For deciding a symmetric key like 3DES or AES, this shared key can be used. To empower a safe channel between the communicating substances, the symmetric key can be used. There is also a basic main component of NFC comprehension, which is less computational for setting up a safe channel.

5 Discussion

After doing this research paper our group gets a lot of new knowledge about NFC. Before this, we only know the base of NFC but never know deeper about it. This paper makes us as a team to be more aware of the reality that the new technology has its own risk and not perfect. With knowing this fact, we hope we can also help people to know more about the technology they use. The main difference between our paper with the research that has been done before is we combined all the method and compare it to reality case. With this kind of method, of course, we can find the most used method and also how they did it. Prevention is always better because we can prepare first and not panicking when the real case also happened to us. And in addition, we try to simplify our words as much as possible when writing our paper, so people with basic knowledge doesn’t confuse a lot when reading our paper.

6 Conclusion

In spite of the dangers, NFC Latest Technology is important for easy to use of the shoppers. One individual can get to all their installment data and make buys on a few diverse credit or charge cards all with the wave of a smartphone. To ensure clients against these security dangers, a few measures have been taken. Clients can moreover take their possess safety measures to ensure their individual information. First, the plan of NFC debilitates security issues. Whereas they can still happen, it is ordinarily more challenging to take credit card data through this sort of information exchange. The individual taking the information would have to be be exceptionally near to the smartphone sending it since the flag does not carry exceptionally distant. Secure channels are utilized for sending delicate data, making them difficult to get to. Within the occasion that a programmer did make it past these security measures to take the data, the data itself is encrypted.

Encryptions demonstrate exceptionally difficult to break and the data would likely be useless to the hacker. For clients to decrease their dangers of having their data, or indeed their physical smartphone itself, stolen and utilized to form buys they did not authorize, they ought to secret word ensure their smartphones and introduce anti-virus computer program. The anti-virus program secures against infections and other assaults from noxious programs that the client may inadvertently download onto the smartphone. Having a secret word on the smartphone ensures it within the occasion of a physical burglary. The cheat cannot unlock the phone and so cannot utilize it to form

NFC payments. NFC permits the client to create installments and share data with companions. It can indeed act as a metro or concert ticket. NFC is exceptionally comparative to Bluetooth but offers quicker and simpler associations between smartphones.

The NFC Gathering does not offer assurance against listening in assaults, making it indeed more critical for shoppers and businesses to take preventative security measures. As time goes on, NFC innovation will proceed to advance. Maybe a few of these dangers may be managed absent with totally, or perhaps other vulnerabilities will surface as the innovation accomplishes far reaching utilization. But one thing remains certain: NFC isn't free from risk and perfect technology. The most perfect way to secure yourself is to know what those dangers are. The technology advancing every day. We have must advance as well. We have to become more aware and also wiser in terms of using every new technology. So the choice is yours, will you change for the better future.

References

Alcañiz, M., Contero, M., Pérez-López, D. C., Ortega, M. (2010). Augmented reality technology for education. New achievements in technology education and development. In: Soomro S, editor. InTech. 247-256.

Alsumait, A., Al-Musawi, Z. S. (2013). Creative and innovative e-learning using interactive storytelling. International Journal of Pervasive Computing and Communications, 9(3), 209-226. DOI: 10.1108/IJPCC-07-2013-0016.

Azuma, R. T. (1997). A survey of augmented reality. Presence: Teleoperators and Virtual Environments, 6(4), 355-385.

Azuma, R. T. (2004). Overview of augmented reality. ACM SIGGRAPH 2004 Course Notes, p. 26. DOI: 10.1145/1103900.1103926.

Azuma, R. T., Baillot, Y., Behringer, R., Feiner, S., Julier, S., MacIntyre, B. (2001). Recent advances in augmented reality. IEEE Computer Graphics and Applications, 21, 34-37.

Kirner, T. G., Reis, F. M. V., Kirner, C. (2012). Development of an interactive book with Augmented Reality for teaching and learning geometric shapes. 7th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1-6.

Moreno, E., MacIntyre, B., Bolter, J. D. (2001). Alice's adventure's in new media: An exploration of interactive narratives in augmented reality. Paper presented at CAST'01, Bonn, Germany September 2001.

Morris, C. W. (1938). Foundations of the Theory of Signs. University of Chicago Press Cambridge University Press.

Nischelwitzer, A., Lenz, F.J., Searle, G., Holzinger, A. (2007). Some aspects of the development of low-cost augmented reality learning environments as examples for future interfaces in technology enhanced learning. Universal Access in Human-Computer Interaction Applications and Services Lecture Notes in Computer Science. 4556, 728-737.

O'Brien, H. L., Toms, E. G. (2005). Engagement as Process in Computer Mediated Environments. Paper presented at ASISveT, Charlotte, North Carolina. Nov 2005.

Peirce, C. S. (1931). The Collected Papers of Charles Sanders Peirce. The Principles of Philosophy. Abbreviation, 1.

Peirce, C. S. (1958) Collected Papers of Charles Sanders Peirce. Vols. 1-6, C. Hartshorne, & P. Weiss (Eds.), Vols. 7-8, A.W. Burks (Ed.), Cambridge, MA: Harvard University Press, pp. 1931-1935.

Singhal, S., Bagga, S., Goyal, P., Saxena, V. (2012). Augmented chemistry: Interactive education system.

International Journal of Computer Applications, 49(15), 1-5. DOI: 10.5120/7700-1041

Sumadio, D. D., Rambli, D. R. A. (2010). Preliminary evaluation on user acceptance of the augmented reality use for education. 2010 Second International Conference on Computer Engineering and Applications (ICCEA), 461-465. DOI: 10.1109/ICCEA.2010.239

Squire, K. D., Jan, M., Matthews, J., Wagler, M., Martin, J., Devane, B. and Holden, C. (2008). Wherever You Go, There You Are: Place-Based Augmented Reality Games For Learning.

Wang, D., He, L., Dou, K. (2014). StoryCube: Supporting children's storytelling with a tangible tool. The Journal of Supercomputing, 70.1, 269-283. DOI: 10.1007/s11227-012-0855-x

Wojciechowski, R., Walczak, K., White, M., Cellary, W. (2004). Building virtual and augmented reality museum exhibitions. Proceedings of 9th International Conference on 3D Web Technology (Web3D 2004), 135-144.

Wojciechowski, R., Cellary, W. (2013). Evaluation of learners' attitude toward learning in ARIES augmented reality environments. Computers and Education, 68, 570-585.