Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 1, 134-148 (2017)

www.astesj.com

Special Issue on Computer Systems, Information Technology, Electrical and Electronics Engineering

ASTESJ

ISSN: 2415-6698

Privacy-by-Design(PbD) IoT Framework : A Case of Location Privacy Mitigation Strategies for Near Field Communication (NFC) Tag Sensor

V.Ragunatha Nadarajah, Manmeet Mahinderjit Singh*

School of Computer Sciences, University of Science Malaysia, 11800, Malaysia

ARTICLE INFO

Article history:
Received: 15 December, 2016
Accepted: 11 January, 2017
Online: 28 January, 2017

Keywords:
NFC- Near Field Communication
RFID - Radio Frequency Identification
MITM - Man-In-The-Middle
PbD – Privacy-by-Design
MIDAS - Multifactor Identifications Attendance System
NDEF - NFC Data Exchange Format

ABSTRACT

Near Field Communication (NFC) technology is a short range (range about 10cm) standard extended from the core standard Radio Frequency Identifier (RFID). These technologies are a portion of wireless communication technology. Even though NFC technologies benefit in various field, but it's still exposed to multiple type of privacy attacks and threat as well since the communication occur in an open environment. The filtering technique been perform on the tag in order to get access to the embedded information. As solution based on tag filtering techniques, existing NFC filtering, Intent filtering has merged together with Bloom filtering from RFID technology. This help in term of elimination the duplicate tag and verify the receiving tag. Meanwhile, as a content protection to NFC Data Exchange Format (NDEF) message been transmitted through the communication channel, Advance Encryption Standard (AES) 128bit has been implemented on the NDEF message. AES provide solution to encrypt the NDEF message which has been communicated. Bloom filtering performed the hashing operation using MD5 technique as a verification of registered user to the NFC system. While the default Intent filtering direct the user to the selected invocation as registered on the tag after the Bloom filtering verification. Besides that, implementation of AES cryptographic in NDEF message, took approximately about 80 trillion years++ to crack the key using brute force attack. Communication of two legitimate entities is secured with AES encryption. Hence, secured user validation or filtering with encrypted message, prevent the possibility for MITM attacker to retrieve sensitive or personal information. The overall framework provide a better security solution compare to the existing framework.

1. Introduction

Near Field Communication (NFC) technology is a short range (range about 10cm) standard extended from the core standard Radio Frequency Identifier (RFID). Extended standard of RFID which is ISO 14443 Type A and Type B were the standards that were incorporated to NFC [1, 3]. These standards are commonly used in NXP Mifare cards [2], followed by Vicinity Cards [5] that are used for item management which was incorporated to ISO 15693 standard and FeliCa [2], the famous NFC technology by Sony that has been standardized to ISO 18092 standard. Since NFC is the extended standard of RFID, most of NFC-embedded devices as well as applications began to be compatible with the RFID devices or infrastructures [2]. These advantages were from the combination of all those standards into NFC standard. Furthermore, NFC-embedded devices such as NFC enabled mobile phones to be switched easily between an active reader modes to passive tag. In other words, it merges the design of a reader and a contactless card on a single device.

Privacy information is about controlling or more generally, filtering access to personal information. The filtering is performed on the tag in order to get access to the particular information. As

*Corresponding Author: Manmeet Mahinderjit Singh, School of Computer Sciences, University of Science Malaysia, 11800, Malaysia
Email: manmeet@usm.my

per statement above, the major focus of this research is on the studying technique in tag filtering and the possible attacks toward NFC, as well as to propose a proper solution or enhancement that can reduce privacy-based attacks. NFC Intent filtering is one of the embedded technologies which is the focus of this research as well.

In reflecting the privacy, content protecting is one of the concern in this research. Encryption of the NDEF message or payload of the communication has been classified by the strength of the key. As per this research, the Advance Encryption Standard (AES) has been selected as the encryption algorithm for the content protection. AES is one of the stronger and faster encryption standard compared with Data Encryption Standard (DES) and Triple-DES.

Privacy by Design (PbD) is a public guideline or approach which concentrates or focuses on privacy spectrum to systems engineering which takes privacy into account throughout the whole engineering process. In this approach, there are seven major principles discussed. Embedded into design, is one of the principle which defines the privacy technique/algorithm which is embedded in the architecture of the system. This particular principle has been used in this research as a guideline in embedding privacy approach in a system.

2. Literature Review

2.1. Near Field Communication (NFC) Technology

Near Field Communication (NFC) technology is an extended from the core standard Radio Frequency Identifier (RFID) which support a short range communication about 10cm. ISO 14443 Type A and Type B were the standards incorporated to NFC [1, 3]. These standards are commonly used in NXP Mifare cards [2], followed by Vicinity Cards [30]that are used for item management which is incorporated to ISO 15693 standard and FeliCa, [2]which is the famous NFC technology by Sony that has been standardized to ISO 18092 standard. Since NFC is the extended standard of RFID, most of the NFC-embedded devices as well as applications have been compatible with the RFID devices or infrastructures [2]. These advantages are from the combination of all those standards into a NFC standard. Furthermore, NFC-embedded devices such as NFC has enabled mobile phones to be switched easily between an active reader modes to passive tag. In other words, it merges the design of a reader and a contactless card on a single device.

NFC operates in three different modes which are the read/write mode, followed by peer-to-peer mode and finally the tag emulation mode. NFC Devices are able to communicate at approximately 10cm and the communication mode indirectly reflects to the standard as it's a short range wireless communication extended from the RFID technology [2]. Furthermore, NFC-embedded devices would be able to perform in the active and passive mode. In reflecting to common RFID type communication where a device acts as the reader (initiator) and as a passive tag (target) explains the passive mode situation [2]. Meanwhile, if both devices are communicating and generating their own induction defines the active mode of NFC technology.

2.2. Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) networks exist in a broad range of environments and their rapid proliferation has been underway for quite some time. Commonly, RFID systems consist of tiny integrated circuits equipped with antennas or well known as RFID tags, that communicate in a few methods with their reading devices also known as RFID readers using electromagnetic fields at one of the several standard radio frequencies [2,4]. Additionally, there is usually a back-end database that collects information related to the physically tagged objects.

RFID systems are vulnerable to a broad range of malicious attacks ranging from passive eavesdropping to active interference. Unlike in wired networks, where computing systems typically have both centralized and host-based defenses such as firewalls, attacks against RFID networks can target decentralized parts of the system infrastructure, since RFID readers and RFID tags operate in an inherently unstable and potentially noisy environment [6]. In addition, the RFID technology is evolving quickly as the tags are multiplying and shrinking and so the threats they are susceptible to, are similarly evolving. Thus, it becomes increasingly difficult to have a global view of the problem as it is vulnerable to a wide range of attacks.

There are four (4) typical frequency ranges that the RFID systems commonly run which is Low Frequency (LF) ranging from 125kHz to 13.2 kHz, High Frequency (HF) operating at 13.56MHz, Ultra-high frequency (UHF) ranging from 860MHz to 960MHz, and microwave frequency starting from 3.1GHz up to about 10GHz [2][3][4].

2.3. NFC Operation Mode

NFC enabled devices can operate in three (3) different operations which are reader/writer mode, peer-to-peer (P2P) mode and card emulation mode as shown in Figure 1. The NFC Forum technical specifications unlock the full capabilities of NFC technology for the different operating modes and are based on the ISO/IEC 18092 NFC IP-1, JIS X 6319-4 and ISO/IEC 14443 contactless smart card standards, also referred to as NFC-A, NFC-B and NFC-F in NFC Forum specifications [4].

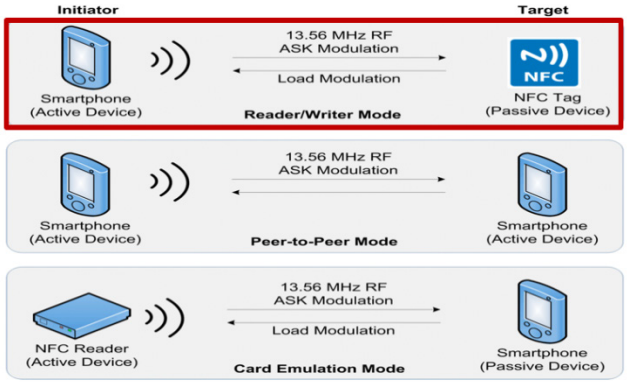

Figure 1: NFC Operation Mode [4]

- Reader/Writer Mode - NFC-enabled device which able to exchange data with NFC Forum-mandated tags, such as a tag embedded in a NFC smart poster [4]. It means that in

the reader/writer mode, when a NFC tag is put in a close range or coverage area to a NFC device, the device can read data from the tag as well as store data into the tag. The reader/writer mode on the RF interface conforms to the ISO 14443 and FeliCa schemes [4].

- Peer-to-Peer (P2P) - can be described as two NFC devices that are able to communicate with each other to exchange data and share files. This means that a NFC device user can exchange information promptly. In our daily life, we can realize that P2P operates as music download, share Bluetooth or WiFi set up parameters or exchange data such as digital photos, videos or phone address book. The Peer-to-Peer mode is standardized on the ISO/IEC 18092 standard [4].
- Card Emulation - threats NFC devices as smart cards, allowing users to perform transactions such as credit cards and smart cards [4]. With just a single touch, the function of purchases, ticketing, and transit access control can be fully achieved. An external reader is required when the NFC device acts like a traditional contactless smart card.

2.4. *Operating Principle of NFC Reader/Writer Mode*

When a NFC application starts to work, the NFC reader/phone generates a Radio Frequency (RF) sine wave to release energy to the tag in its coverage distance and retrieve data from the tag. Usually, the sine wave is transmitted at 13.56MHz frequency and it will form an area of magnetic flux or well known as RF signal transmission tunnel [4]. The tag which is close to the magnetic flux area, will receive energy from the reader and then generate a counter frequency, which can modify the frequency properties of the original sine wave created by the NFC reader/phone. After the NFC reader/phone detects the modification, it confirms that there is a NFC tag nearby. With the target NFC tag lock-in, data are be transferred between the NFC reader/phone and the NFC tag respectively by the radio wave. The reader/writer mode operation supports NFC Data Exchange Format (NDEF) and this mode has been chosen in this research project. NDEF message is the default messaging for NFC communication which support this operation mode are an advantage for us to choose this mode. Meanwhile, this mode is the current commonly used mode in NFC embedded devices as it could provide tag reader and writer operation. Somehow, most of the NFC device manufacturing is tend to use this mode as the default operation mode as it provide the basic operation to read and write on a tag. At the same time, man-in-the-middle attacks is frequently happened in this kind of NFC embedded devices as users able to retrieve data from a tag as well as modify the data. Since our focus is on man-in-the-middle attack, read and write NFC operation mode is the best suite the research project which provided the best platform to perform the research on the attacks and security approach.

2.5. *NFC Data Exchange Format (NDEF)*

NFC Data Exchange Format (NDEF) is a lightweight, binary message format that can be used to encapsulate one or more application-defined payloads of arbitrary type and size into a single message construct [4, 7]. The NDEF specification is well defined as a message encapsulation format to exchange information between a magnetic flux and RF signal transmission tunnel. NDEF message is composed of numerous records. The record amount in an NDEF message depending on the tag type and calling application [4]. Each NDEF record contains a header and a payload. The payload is described by type, length and an optional identifier encoded in an NDEF record header structure. Payload type refers to the data type that is being carried in the payload of a record and this is used to guide the processing of a payload [4, 7]. Usually the payload can be of one of a variety of different types such as text, URL, Multipurpose Internet Mail Extensions (MIME) media, including NFC-specific data type. The optional payload identifier allows user applications to identify the payload carried within an NDEF record. For NFC-specific data types, the payload contents must be defined in a NFC Record Type Definition file, RTD.

2.6. *Privacy by Design (PbD)*

Privacy by Design (PbD) advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks. The objectives of PbD is to ensure privacy and gain personal control over one's information [8]. While for organizations, is to gain a sustainable competitive advantage [8]. There are seven foundational principles of PbD discussed below:

Table 1: PbD Foundational Principles

PbD Foundational Principles	Privacy	Security
1. Proactive not Reactive; Preventative not Remedial	Anticipate and prevent privacy. Prevent from privacy risks to materialize.	Begin with the end in mind. Proactive implementation of security.
2. Default Setting	Build privacy measures directly into any IT system.	Implement "Secure by Default" policies.
3. Embedded into Design	Embed privacy into the design and architecture of It system.	Apply Software Security Assurance practices. Use of Trusted Platform Module.
4. Positive-Sum	Accommodate all legitimate interests and objectives in a positive-sum. "Win-win manner.	Resolve conflicts to seek win-win.
5. End-to-End Security	Secure life-cycle management. Ensure cradle-to-grave.	Ensure confidentiality, integrity and availability.
6. Visibility & Transparency	Component parts of IT systems practices visible and transparent.	Strengthen security through open standard.

7.	**Respect for the User**	Respect and protect interests of the individual. Keep it user-centric.	Respect and protect the interests of all information owners.

2.7. NFC Security Challenges

Security in a communication system is well defined as the prevention of unauthorized access and manipulation of data. Security approach is a basic necessary item that need to be added in every system. Security in a system can be classified into two major parts which are Confidentiality, Integrity, Availability (CIA) and X.800.

- CIA - exposed in three main principles in security which are confidentiality, integrity and availability. Confidentiality defines the authorization principle whereby only those with sufficient privileges and a demonstrated need may be able to get access to certain information. While integrity is the principle of ensuring information is maintained in a complete and uncorrupted state. The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state. Availability is the principle that allows entities either a person or other peripheral devices to access information in a usable format without interference or obstruction. Availability does not imply that the information is accessible to any user; rather, it means availability to authorized users [9]. We could classify those security threats and attacks that are related to CIA in 3 major layers of the NFC system. Most of the attacked happened on the communication as initially NFC architecture has lack of security approach been implemented. At the same time poor communication channel in NFC interactions is also a good reason most of the attack occur at the communication layer. Security approach at hardware and back-end devices can be manage with an authentication process or access control approach. But different at communication layer which will required encryption process to ensure the message communicated is secure.
- X.800 - service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers or communication. X.800 considers on authentication, access control, data confidentiality, data integrity, non-repudiation and availability. Unauthorized tag reading can be considered as one of the X.800 security attacks. Unauthorized tags including hidden tags involves third party attempts to access a secure NFC communication. Key compromise can also be a concern of X.800 treat where multiple type of crypto attacks are tend to open communication of two entities.

2.8. NFC Privacy Challenges

Privacy in NFC threats refers to the sensitive information or data that have been retrieved by an attacker. This can be classified into four major categories including location, user, time and data.

- Location - privacy in terms of location points to the attacks in which the information retrieved is the location of an NFC tag user or the tag location itself. Cloning, reprogramming or spoofing and swapping a tag can be considered as impersonation of a NFC tag which benefic an attacker to retrieve NFC user location details. Relay attack is the intention of Man-in-the-Middle attack [10]. Here, the both legitimate NFC entities are fooled that they are communicating directly with each other but they didn't realize the third party access in between the communication. Tracking and hot listing are the most significant privacy threats. Silent involvement of an unauthorized NFC tags or party without giving any alert or sign of activity describes the tracking [10]. Tracking here refers to collecting of personal information to track a particular user. Meanwhile, hot listing refers to the collection of information or object that could be used in future by an attacker to perform more direct attacks [10, 11].
- Time - privacy in time refers to those attacks or threats which the information gained is the time of an NFC user and the time of the NFC communication that have taken place. Relay attack allows the attacker to retrieve the data or more specifically referring to time [10]. Tag and reader are fooled by the third party access in between the communication where the sender and receiver believe that they are communicating directly with each other. Tracking and hot listing are the most significant privacy threats. Silent involvement of an unauthorized NFC tags or party without giving any alert or sign of activity describes the tracking [10].
- User - privacy in terms of user defines the attacks or threats in which the information retrieved is the user's sensitive or private information via a NFC tag user and the system itself. In impersonation attack, the attacker might imitate the identity of tags or readers and the system to retrieve a particular user identity [12]. Modification and retrieval of the data refers to the sender and receiver details [12] is most commonly referring to relay attack.
- Data - Privacy that points to the data is those attacks of which the information gained is the sensitive information or data of an NFC tag, system and the user's details of the NFC communication that have taken place. Data modification in privacy reflects to impersonation attacks of NFC tags which includes involvement of cloning and reprogramming a tag as well as swapping a tag [12, 13, 14]. This data is modified for their personal purpose as well as for self-satisfaction. While relay attack happened when an attacker played the role as man-in-middle attacker where they usually place their own or personal devices linking the legitimate NFC entities in intention to intercept and modify or retrieve data communicated in between tags and readers. While information injection reflects to buffer overflow attacks. The overflow data will flow over stacks that caused it to be executed as well when the system attempts to process the buffer [1, 16].

2.9. Existing Filtering and Duplication Elimination Technique

Here we have identified a few techniques of duplication elimination which are currently being used in the RFID technology.

- Intersection Algorithm - compares collected/read data between two readers. If the same data exists in both readers on the similar network reader, this data is moved to a specific shelf/database/array [17].

```
Algorithm: Intersection Algorithm
Input: Reader A, Reader B
Output: Shelf S
begin
for (Every member of Reader A) do
for (Every member of Reader B) do
if (Reader A = Reader B) then
Put member of Reader A into Shelf S
else
if (Reader B = Reader A) then
Put member of Reader B into Shelf S
end if
end for
end for
end
```

- Relative Complement Algorithms - also compares collected/read data between two readers. But if there are duplications between both readers and similar network reader, these data is ignored [17].

```
Algorithm: Relative Complement Algorithm
Input: Reader C, Reader D
Output: Shelf S
begin
for (Every member of Reader C) do
for (Every member of Reader D) do
if (Reader C != Reader D) then
Put member of Reader C into Shelf S
else
if (Reader D != Reader C) then
Put member of Reader D into Shelf S
end if
end for
end for
end
```

- Randomization Algorithm - this algorithm will randomly assign values between "0" and "1" to every read tag. If the outcome is equals to "0", the specific collected/read data is allocated to the shelf/database/array one (1). Otherwise, the collected/read data is moved to the shelf/database/array two (2) as the outcome is "1" [17, 18]. However, in the real randomization, there may not be equal number of tags allocated between two shelves/databases/arrays.

```
Algorithm: Randomization Algorithm
Input: Reader E
Output: Shelf SA, Shelf SB
begin
for (Every member of Reader E) do
Randomize number between 0 AND 1
if (Reader E = 0) then
Put member of Reader E into Shelf S1
else
if (Reader E = 1) then
Put member of Reader E into Shelf S2
end if
end if
end for
end
```

- Bloom Filtering - data filtering process that occurs in the RFID middleware can be classified into two types of low level data filtering and semantics data filtering [19]. Raw RFID data stream is cleaned at the low level data filtering while data has been filtered according to the demands from the system at semantic data filtering. Bloom filtering has the capability to identify a data whether the data is in the set or not. This is why Bloom filtering is considered as a space-efficient-probabilistic data structure [19]. Referring to figure 2, k defines the number of hashing function and data which represents in bit array of size m.

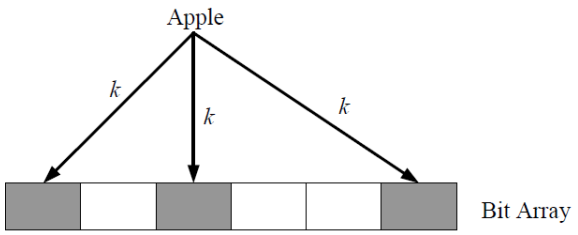

Figure 2: Structure of the Bloom filter [19]

Bloom filtering can perform two basic operations which are test and add. Test operation is used to verify the appearance of an element in the set. Return value of false shows that the element is not in the set while value of true definitely means the element is in the set. Alternatively, add operation provides the functionality to add an element into a set. K different hashing function is feed in order to add an element into bloom filtering. To verify whether the element has been stored in the set, the k value hashing function is feed. Bloom filtering is a best space-efficient probabilistic algorithm for tag filtering technique. While Bloom filtering also, specify the filtering technique according to the tag technologies.

2.10. NFC Intent Filtering Technique

To start a NFC application when an NFC tag is scanned, the NFC application can filter for one, two, or all three of the NFC intents in the Android manifest. However, usually the first filtering option is the ACTION_NDEF_DISCOVERED intent for the most control of when the application starts [33]. The

ACTION_TECH_DISCOVERED intent is a fallback for ACTION_NDEF_DISCOVERED when no applications filter for ACTION_NDEF_DISCOVERED or for when the payload is not NDEF [20,21]. Filtering for ACTION_TAG_DISCOVERED is usually too general of a category to filter on. Most of the time, a NFC applications will filter for ACTION_NDEF_DISCOVERED or ACTION_TECH_DISCOVERED before ACTION_TAG_DISCOVERED, so the application has a low probability of starting. ACTION_TAG_DISCOVERED is only available as a last resort for applications to filter for in the cases where no other applications are installed to handle the ACTION_NDEF_DISCOVERED or ACTION_TECH_DISCOVERED intent [21]. Figure 3 show the processes of intent filtering.

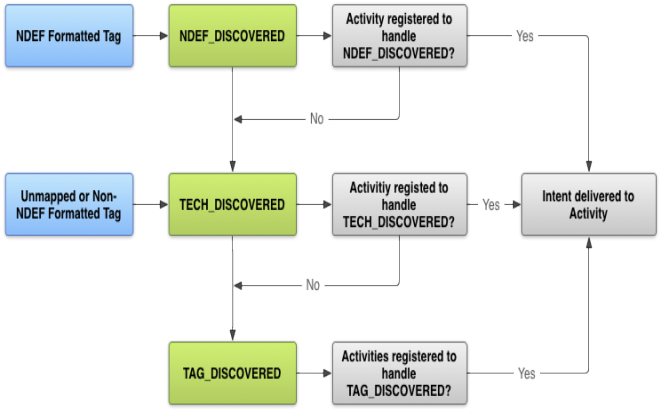

Figure 3: Intent processes [20].

2.11. *Content protection*

Content protection is the security approach on the NDEF message which that began transmitted through the NFC communication channel. Encryption is one of the technique used to protect the NDEF message or content. Below are a few encryption standards that probably could be used as content protection for NDEF message.

Advanced Encryption Standard (AES) has been used as the encryption standard or content protection for the NDEF message transmitted over the NFC communication channel. AES has been selected as it provides better key size compared to DES and 3DES. Table 2 shows the comparison between AES, DES and 3DES.

Table 2: Comparison between AES, DES and 3DES

Algorithms	Strength	Weakness
Data Encryption Standard (DES)	• Brute force search looks hard (56-bit keys)	• Able to encrypt using DES Cracker.
Triple-DES (3DES)	• Able to support up to 128-bit keys.	• Efficiency/security: Bigger block size desirable.
Advance Encryption Standard (AES)	• Stronger & faster than Triple-DES (128-bit block size, 128/192/256-bit keys)	• cost – computational due to implementation characteristics

2.12. *Multifactor Identification Attendance System (MIDAS)*

Multifactor Identification Attendance System (MIDAS), a NFC-based system to handle student attendance [22]. MIDAS is an integrated multi-factor system which means identification knowingly by usage of NFC and biometric via face for a university based attendance system. Figure 4 shows the flow of the MIDAS operation.

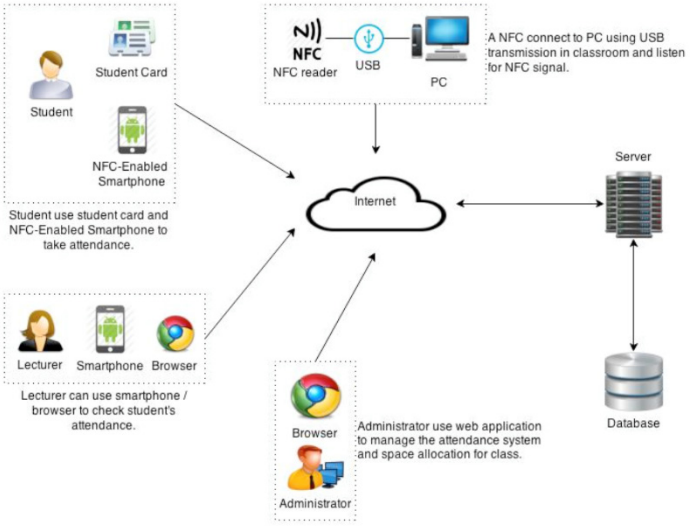

Figure 4: MIDAS operation [22]

The system is implemented with combinations of sensing technologies such as NFC and biometrics including face detection and recognition. NFC reader is used for reading the signal from the NFC-embedded smartphone or card. A dedicated server is deployed to handle requests from the receiving NFC signal and manage the student's attendance information and space allocation for class information. This give a fast and convenient way for administrators, lecturers, and student access system. Students' attendance is presented on the web page as well as android application. This process makes the system look more efficient and faster in terms of data processing. MIDAS has been selected as the real-implementation for the proposed framework as provide a standard operation of NFC system. This application read and write data from a tag as the attendance. Which mean its support read and write mode. Beside that MIDAS is using NDEF message format to transmit the attendance from a tag to reader. These condition suite our research project as in this research project, read/write mode NFC operation tag and also NDEF mapped tag is used. At the same time, since MIDAS using the NDEF format for message transmission, by default intent filtering method is used as the filtering technique.

2.13. *Summary*

In this research project, the NFC reader/writer mode of NFC technology has been chosen. When a NFC tag is put in a close range or coverage area to a NFC device, the device can read data

from the tag as well as store data into the tag. The main reason is, this type of mode has been chosen as MITM attacks is more frequent here. On the other hand, privacy-based has been chosen as it provides personal information of a particular or targeted person as well as the tag information. In most of bank cards or account hack cases, the hacker will look for the last transaction history. Tag and personal information are the main focus of an attacker who perform the MITM attacks.

Intent filtering is the existing filtering technique in NFC technology. In this research, we have merged the NFC intent filtering technique with RFID Bloom filtering technique as this ensure a tight filtering technique. Bloom filtering provides access control process while intent filtering provides tag filtering and process embedded on the NFC tag. In order to provide a preferred privacy protection in NFC communication, the payload should be protected as well. Advance Encryption Standard (AES) has been chosen as the content protection to safeguard the content of payload which will contain the personal and sensitive data. AES could provide big key sizes which makes the encryption more secured when compared to DES and 3DES.

While PbD, discussed the principle which we have chosen to follow in this project. PbD has been chosen as the guideline to this research project as it was the latest or current principle or guideline in ensuring privacy as an aspect of information technology development. Privacy is embedded into the design and architecture of the NFC system based tag filtering technique with content protection. This shows that privacy has become an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

3. Tag filtering

Since NFC technology is new in this information technology era, only few algorithms have been proposed for extending the tag filtering process to perform the filtration on the valid NFC tag as well as the reader. There are a variety of NFC tags that can be read with a handheld device and also desktop applications. The spectrum ranges from simple NFC stickers and NFC key rings to complex NFC cards including bank cards with integrated cryptographic hardware. The tags implemented also differ in their chip technology. The major part is the NDEF, which is supported by most tags and readers. In addition, we could say that NDEF's tags are the most used contactless chip technology worldwide. Some tags can be read and written, while others are read-only or encrypted.

We has proposed an improved algorithm for NFC tag filtering, which combines benefits from the RFID Bloom filtering techniques. The proposed framework is focus on improving the tag filtering techniques which point to privacy-based attacks. The performance or evaluation of the proposed algorithm and previously presented algorithms as the benchmark are compared under a variety of conditions. Here the tag filtering technique has been selected as this process play the major role in NFC communication as tag filtering process react as access control for a tag to communicate with another NFC embedded device. Figure 5 shows how the enhanced tag filtering process.

In order to test the filtering technique, the Multifactor Identifications Attendance System (MIDAS) has been used which was developed by David Ong, Dr. Manmeet. The enhancement has been updated on the filtering techniques where Bloom filtering technique has been merged with the NFC Intent filtering technique.

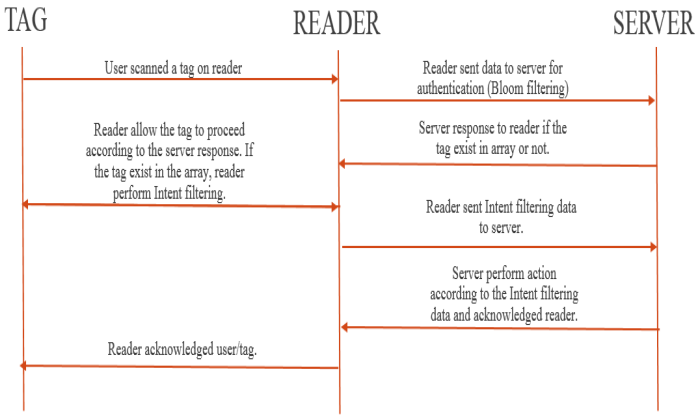

Figure 5: Process of tag filtering enhancement.

3.1. NFC Intent Filtering

In this research we used the MIFARE tag as the NFC tag/card used to store the student details according to the MIDAS system. MIFARE tag uses the standard NFC frequency which is 13.56Mhz and is compatible with most of the latest NFC-embedded devices. At the same time, MIFARE tag is NDEF formatted tag. MIDAS used NDEF technique to discover the tag attached to the reader. Figure 6 shows the NDEF process flow.

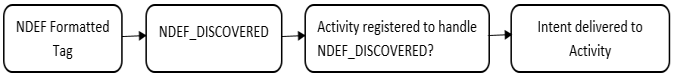

Figure 6: NDEF activity

When the reader detects a tag (MIFARE tag) with NDEF technology and registered with MIDAS, an Intent filtering is triggered which means the tag will direct the user straight to the MIDAS as the tag's activity has been registered to the MIDAS system. This process will not perform any access control verification on the tag. There is a big possibility for the reader to discover a clone tag which has been copied exactly as the registered tag. The table 3 shows the result of what Intent filtering does.

Table 3: Result of Intent filtering

Characters	Responses	
	Yes	No
Authentication Function		x
Responses to un-registered tag		x
Responses to clone / duplicated tag	x	
Access control		x
Perform registered activity	x	

In reflecting to existing NFC intent filtering it only perform those activities registered to the tag. Unfortunately, intent filtering has does not have the capability to authenticate the read tag. Which means a reader will only respond to a tag which has been registered to the specific NFC application. Otherwise it will discard the process. Besides that, intent filtering also not able to identify a clone or duplicate tag. Since intent filtering only direct a user as per the registered tag, it could not validate the read tag. Even though intent filter is the first stage of NFC operation, it does not help much in access control. Intent filtering is not designed for access control instead it only direct user according to the registered activities.

3.2. NFC Intent Filtering Merge with Bloom Filtering

This part discussed the proposed framework that focus on improving the tag filtering techniques which point to privacy-based attacks. Man-In-The-Middle (MITM) attack has been chosen as the major threat to the personal and sensitive information. Connection between two NFC parties or devices can be interrupted by the third party which is called the Man-In-Middle attack. The third party tricks the two legitimate parties to be the other legitimate party thus, routing the communication between the two parties to go through the third party [23]. Particularly, MITM attack has been selected in this project as this kind of attack has high possibility for modification of message contents and replay attacks. In terms of Confidentiality, Integrity and Availability (CIA), MITM attack involved in all three of it. Figure 7 shows the details on the MITM attack.

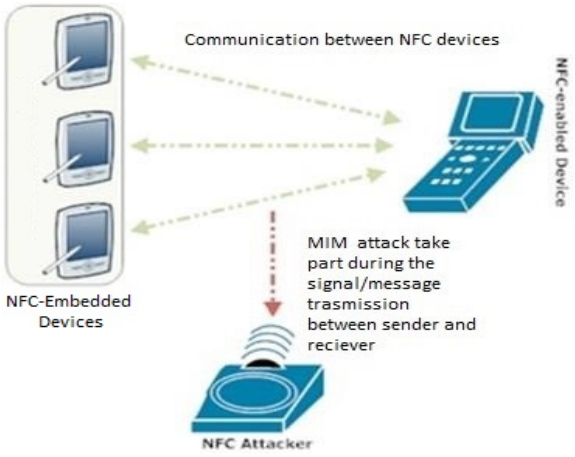

Figure 7: MITM attack performed during NFC communication

The MITM attack is evaluated with the enhanced filtering techniques where the NFC Intent filtering has been merged with Bloom filtering, while the attack is evaluated according to privacy-based. NDEF mapped or embedded tag technology (MIFARE) is used as the tag in order to test the existing Intent filtering and the enhanced filtering technique. Figure 8 shows the proposed filtering techniques.

The enhanced filtering technique performed an additional process of access control and duplication elimination of tag. This process helps to reduce third party or unauthorized access to the system. This means, indirectly the bloom filtering technique will eliminate the clone tag that was discovered and can be considered as the MITM attack. Table 4 is the result of the enhanced tag filtering techniques.

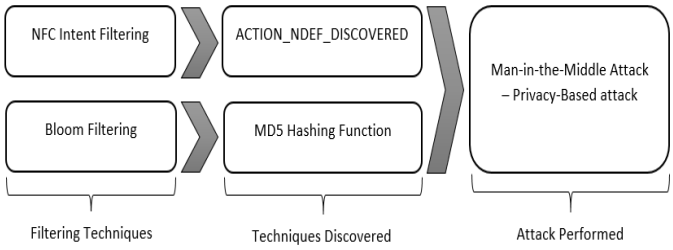

Figure 8: proposed filtering technique against MITM attacks

Table 4: Result of enhanced tag filtering

Characters	Responses	
	Yes	**No**
Authentication Function	x	
Responses to un-registered tag		x
Responses to clone / duplicated tag		x
Access control	x	
Perform registered activity	x	

The proposed framework perform Bloom filtering as an initial process of NFC operation which will indirectly authenticate the tag or user before proceed with intent filtering, perform activities as per registered. Here the intent filtering will only respond the tag or user who registered to the specific NFC application. Since Bloom filter is implemented on the proposed framework, clone or duplicated tag is automatically validated and eliminated. Bloom filter provided a solution as access control to NFC system or application before it perform the activities as per registered. Valid tag or user is carried forward to intent filter that direct the user the registered application.

3.3. Discussion

In reflection to the result of Intent filtering (Table 3), the NFC activities are performed according to what has been registered on the tag. The filtering part tries to discover the registered activities on the tag instead of the duplication or unauthorized tag. The reader detects a tag with NDEF technology and registered with MIDAS, the Intent filtering started to direct the user straight to the MIDAS as the tag's activity has been registered to the MIDAS system and at the same time it reads the information on the tag. First of all, this process does not allow any authentication process on the tag attached to the reader. Indirectly, the tag is not performing any access control verification for unauthorized access. In a case where a clone or duplicate tag has been used, the system still respond to the tag as the registered activities are copied exactly from the original tag. There is a high possibility where MITM attack has been performed on the tag in order to retrieve the personal information on the tag.

While reflecting to the result of the enhanced filtering technique (Table 4), Bloom filtering helps to perform the authentication process in order to verify the authorized access and at the same time, it indirectly eliminate the duplicate or clone tag. As the enhancement has been done on top of Intent filtering technique, the system will discover the registered activities once the bloom filtering process is complete. This means, the tag will direct the user to the registered activities as usual but before that bloom filtering will take place to eliminate the duplicate or unauthorized tag. In this case, signal from MITM attack is eliminated as the duplicate of original tag. At the same time, Intent and Bloom filtering will not response to the un-registered tag, which means, those tags that are not registered to the MIDAS will be automatically eliminated by the system.

4. Content Protection

Content protection is the encryption technique forced on the content of any particular information or message carried on an open network. In this process, we do not use the trusted third party and thus can reduce the communication cost and obtain reliability [24, 25]. Most of the RFID or NFC devices are authenticated to readers and to the backend system using strong cryptography like DES, 3DES, AES and RSA. All modern cards support symmetric cryptography such as 3DES or AES, while some higher-grade cards already support asymmetric cryptography such as RSA [26]. When asymmetric encryption is used, no valuable master keys need to be stored in the door controller, which makes the resulting design and maintenance less complex. Depending on the card capabilities, symmetric AES encryption is used actively by most of the MIFARE card since AES could provide high capability in terms of encryption and decryption. Table 5 shows the strength and weakness of the AES encryption standard.

Table 5: Strengths and Weaknesses of AES

Algorithms	Strength	Weakness
Advance Encryption Standard (AES) [60,61]	• Stronger and faster than Triple-DES. • 128-bit block size. • 128/192/256-bit keys. • Support hardware and Software • Less susceptible to cryptanalysis	• Cost – computational due to implementation characteristics. • Complex encryption and encryption.

4.1. Proposed Algorithm

In this research project, the Advance Encryption Standard (AES) has been chosen as the algorithm for content protection. AES algorithm could provide a stronger and faster encryption when compared to DES and Triple-DES since AES has a maximum of 256-bit keys size as well as 128-bits block size. At the same time, AES is less susceptible to cryptanalysis which can be concluded that AES is more secure than 3DES. Hence, this is the reason why AES begin used in this research project instead of 3DES even though 3DES could support up to 128bit key size. Block size up to 128bit compare to 3DES with 64bit block size, it is less open to security attacks or threats. The number of AES encryption rounds increases with the number of key length. With a big block size and key size, AES provide a better encryption of NDEF message begin communicated between two entities. Which means AES increase the security level against cryptanalysis since it consist a large number of encryption round with a big block and key size. AES could operate in hardware and software which benefit us on this research project as NFC system required NFC devices and NFC applications. Figure 9 shows the flow of AES encryption and decryption as the content protection in the NFC system.

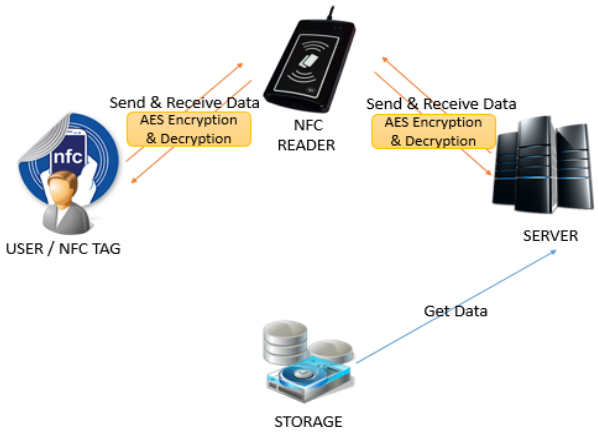

Figure 9: AES implementation in the NFC system

The key length used in the encryption and decryption determines the practical feasibility of performing a brute-force attack. These can be concluded that with big key sizes, it is more difficult to crack or decrypt as compared to small key sizes. Table 6 shows the possible number of key combinations with respect to key size.

Table 6: Key combinations versus key size

Key Size	Possible combinations (2^k)
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^9
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

The exponential increase in possible combinations as the key size increases. "DES" is part of a symmetric cryptographic algorithm with a key size of 56 bits that has been cracked in the past using brute force attack. There is also a physical argument that a 128-bit symmetric key is computationally secure against brute-force attack. Just consider the following:

Faster supercomputer: 33.86 Petaflops = 33.86 x 1015 Flops [28] (Flops = Floating point operations per second)

Number of Flops required per combination check: Assume for now 1000

Number of combination checks per second = (33.86 x 1015) / 1000 = 33.86 x 1012

Number of seconds in one year = 365 x 24 x 60 x 60 = 31536000

Number of years to crack AES with 128-bit Key = (3.4 x 1038) / [(33.86 x 1012) x 31536000]

= (0.103 x 1026)/31536000

= 3.2 x 1016

= 80 trillion years++

Even with a supercomputer, it will take about 80 trillion years++ to crack the 128-bit AES key using brute force attack. Table 13 shows the time taken to crack AES using brute force attack.

Table 7: Time to crack cryptographic

Key Size	Time to Crack
128-bit	3.2×10^{16}
192-bit	5.8×10^{42}
256-bit	1.01×10^{71}

The key size used for encryption should always be large enough so that it could not be cracked by modern computers despite considering advancements in processor speeds.

4.2. Discussion

This research project, AES 128 has been used as the content protection for the payload of NFC message. Referring to table 11 above, even with a supercomputer, it would take 80 trillion years++ to crack 128-bit AES key using brute force attack. This is more than the age of the universe (estimation of 13.75 billion years). By default, NFC message or NDEF record consist of a Type Name Format (TNF), payload, payload type, and payload identifier. Payload is the most important part of an NDEF record where it is the content of the message we are transmitting. Here the TNF is defined on how to interpret the payload type. This means, the default architecture of NFC does not provide protection on the content it carries through an open network. By implementation of AES cryptographic, NDEF message or record that are transmitted through the NFC communication is well protected from unauthorized access and modification. Even though the tag filtering technique has been implemented, as a prevention to privacy attacks, content protection will provide the better solution. Reflecting the PbD approach, as "Embedded into Design" principle is selected, here privacy prevention has been embedded into the NFC system and architecture.

5. Analysis and evaluation

This part discussed further on the analysis and evaluation conducted on the proposed work. Basically, analysis and evaluation defines the research goals into defined functions and operation of the proposed work. Security analysis is a method which helps to calculate the value of various attacks against the proposed work. Below are the few parts where the security analysis has been conducted:

5.1. Man-In-The-Middle (MITM) attack.

The Man-in-the-middle attack (MITM) intercept a communication between two legitimate entities. An adversary placed a hidden device between the legitimate NFC entities in the intention to modify or retrieve data communicated between the tags and readers. This allows the attacker to retrieve the data or more specifically referring to personal information. Tag and reader are fooled by the third party access in between the communication where the sender and receiver believe that they are communicating directly with each other.

Reflecting to default Intent filtering technique in NFC architecture, the filtering technique will discover the registered activities on the tag and allow the user to perform further action accordingly as activities were registered. The reader detects a tag with NDEF technology and registered with particular activities, the Intent filtering will take place and direct the user as the activities registered on it. This process could not detect or eliminate unauthorized access or duplicate tag attempt to access the system. Furthermore, the tag does not perform any access control or verification on the tag read. This situation allows an attacker to use a clone or duplicate tag to access the NFC system and by right the reader will still respond to the tag as the registered activities including tag information are copied exactly as the original tag. There is a high possibility where MITM attack been performed on the communication channel during NFC communication. The attack is performed on the NDEF message intention to retrieve the tag information as well as personal information on the tag. Indirectly, this helped the attacker to prepare a duplicate tag from the information gathered through the attack. In future, the attacker could access the NFC system without any hitch.

While reflecting to the proposed work, Bloom filtering helped to perform the user verification or authentication process in order to verify the authorized access to the NFC system. Bloom filtering has the capability to eliminate the duplicated tag in which Intent filtering do not have. Since the proposed work has been done on top Intent filtering, the system performed Bloom filter first and followed by Intent filter which discovers the registered activities on the tag. Furthermore, the NDEF message which a reader retrieve from a tag is discovered with AES encryption in order to protect the content of NDEF message from MITM attack. In this case, the duplicate tag retrieved from MITM attack is eliminated as the duplicate tag and at the same time, the content of a NDEF message are well protected with AES encryption.

5.2. Brute Force Attack

A brute force attack is an attempt of trial-and-error method used to obtain information or encrypt a key of some cryptographic. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts for testing purpose. An attack of this nature can be time and resource-consuming. Hence the name "brute force attack", it only success in some situation where usually based on computing power and the number of combinations tried rather than an ingenious algorithm. NDEF message with an encryption of AES will require an attacker of MITM attack to encrypt the key in order to get the original message of NDEF.

As content protection of NDEF message, AES 128-bit has been used in the proposed work. Referring to table 6 in the previous chapter, even with a supercomputer with 33.86 Petaflops [28], it would take approximately about 80 trillion years++ to crack 128-bit AES key using brute force attack. This is more than the age of the universe (estimate 13.75 billion years) [28]. A different goes to brute force attack which is performed using a "Brute Force Attack Tool" which is available online nowadays.

By default, NDEF message is implemented with Type Name Format (TNF), payload, payload type, and payload identifier. Payload is the most important part of an NDEF record where it's the content of the message (personal and tag information is located) we are transmitting. Here the TNF define us on how to interpret the payload type. In this case, by default, there is no such content protection technique implemented on the content it is carrying through on the NFC communication. This will give an opportunity to a MITM attacker to simply retrieve NDEF message and interpret the tag and personal information communicated through the network. Implementation of AES cryptographic in NDEF message will cause the attacker in encrypting the key and interpret the original message. Even though the tag filtering technique has been implemented, as a prevention to privacy attack, content protection provided the better solution.

5.3. Privacy Attack

Privacy in NFC threats refers to the sensitive information or data that have been retrieved by an attacker via MITM attack. This can be classified into four major categories which are location, user, time and data. Location based privacy refers to the attacks in which the information retrieved is the geographical location of an NFC tag user. Meanwhile, time based privacy points threats in which the information gained is the time of the NFC communication that have taken place. Usually, location and time come together in a same package or session. Privacy based data, define those attacks where the information gained is the sensitive information including tag information. Finally, privacy based user is the threats in which the information retrieved is the user's sensitive or personal information.

Privacy attack happens when an attacker tries to get the sensitive information on the NDEF message and interpret the message for their personal or some other cybercrime. Usually, those privacy information is located into NDEF message that carried through the network. In reflecting to proposed work, as privacy prevention, the NDEF message has been encrypted with AES 128-bit. Implementation of encryption standard on the message transmitted through an open network, provided better prevention toward privacy attack and leakage of sensitive information on the NFC tag. Besides that, tag validation performed by Bloom filtering also avoided the duplication or clone tag registered to the system.

5.4. Proposed NFC Filtering Framework

The proposed NFC filtering framework offers hashing operations that merges Intent filtering with Bloom filtering to authenticate access, and have AES cryptographic as the prevention to content protection. Figure 10 shows the proposed NFC filtering framework.

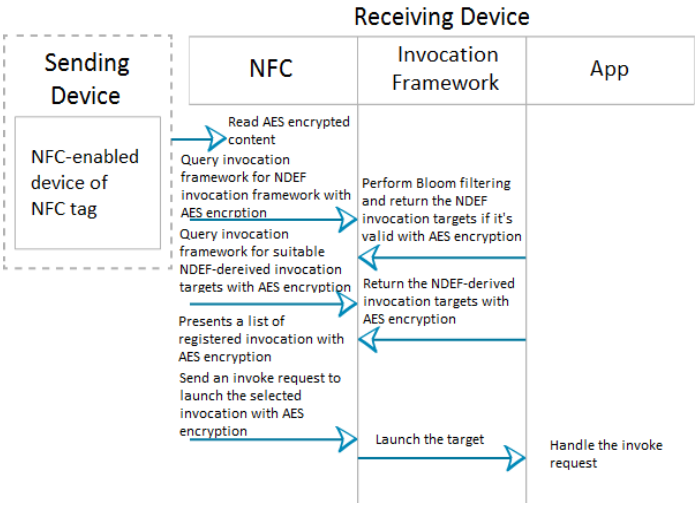

Figure 10: Proposed NFC filtering framework

AES 128bit cryptographic has been implemented into NDEF message and it's indirectly help in encrypting the original NDEF message with a key size of 128bit. The encryption standard performed the encryption on the NDEF message and sent it over the communication channels. MITM attack might be able to retrieve the NDEF message but unfortunately, the message is encrypted with AES encryption. By using brute force attack, it will take about 80 trillion years++ to crack the key and this nature can be timely and resource-consuming. On top of this, Bloom filtering help to perform hashing operation using MD5 technique to verify or authenticate access level to the NFC system. This operation help to prevent from MITM attack by eliminating the duplicate tag which act as the access control to the NFC system. Communication between two legitimate entities are more secure against MITM attack who attempt to retrieve tag or personal information over the network.

5.5. Proposed NFC Filtering with PbD

Privacy by Design (PbD) advances the view that the future of privacy cannot be assured solely by compliance with regulatory guidelines. In this research project, we have referred to PbD's third foundational principle as a guideline which is embedded into the design. In other words, privacy prevention should be implemented into the architecture of IT systems [8]. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

In the proposed NFC filtering, AES encryption standard has been implemented on the NDEF message been transmitted. Bloom filtering has been merged together with the Intent filtering technique. Indirectly, this shows that privacy prevention has been implemented into the system or architecture of the NFC system. We could conclude that the proposed NFC filtering is succeeding the third foundational principle of PbD principles as the privacy approach is embedded on the NFC system itself.

5.6. Possible threats in MIDAS

It is a common issue in most of the IT system, where there are some possible threats that might take place on the system. Below are the possible threats that might occur in MIDAS system.

- Card Cloning - card cloning is the major issue or threat of the MIDAS system. Although each of the card has its own ID and it's only readable. The student ID card can be easily duplicated with the same card information using some online model tools.
- Encryption - the server does not own any security certification or encryption standard to ensure the security of the communication channel. This is very important for the data being transmitted over the communication channel in order to prevent man-in-the-middle attack.

5.7. Proposed Filtering Framework in MIDAS

Students would attempt to tag NFC-enabled smartphone or card to represent their attendance. A NDEF message is sent over through the channel to the reader. Here, the system performed the Bloom filtering to verify the received tag ID. Once the tag has been verified, the system proceed with the Intent filtering by reading the registered activities on the tag. This means the tag directed the user to the selected invocation target that has been registered on the tag. This process carried the operation of ACTION_NDEF_DISCOVERED. According to the MIDAS operation, the activities registered will login the session to the attendance system and followed by submitting of the attendance. The login session is the authentication process to the system while Bloom filtering operates to verify the tag ID and eliminate duplicate tags. In this situation, the system will indirectly prevent towards MITM attack where duplicate tags or ID are automatically eliminated by the Bloom filtering. Meanwhile, the message been transmitted across the communication between the tag and reader has been secured with the AES 128bit encryption standard. The NDEF message communicated is encrypted before it is transmitted through the NFC communication channel. In some cases, if an attacker is able to break the Bloom filtering barriers, he or she is able to retrieve the NDEF message. But unfortunately, this message has been encrypted with AES encryption standard. This cause time and resource-consuming for the attacker to interpret the original NDEF message.

5.8. Comparison of Proposed Framework vs Existing Filtering

NFC tags can range in complexity and standard of the tag selected. Simple tags offer just read and write operations, sometimes with one-time-programmable areas to make the tag read-only. The most common MIFARE tags contain operating environments, allowing NDEF message interactions with code execution on the tag. Figure 11 shows the common NFC operation.

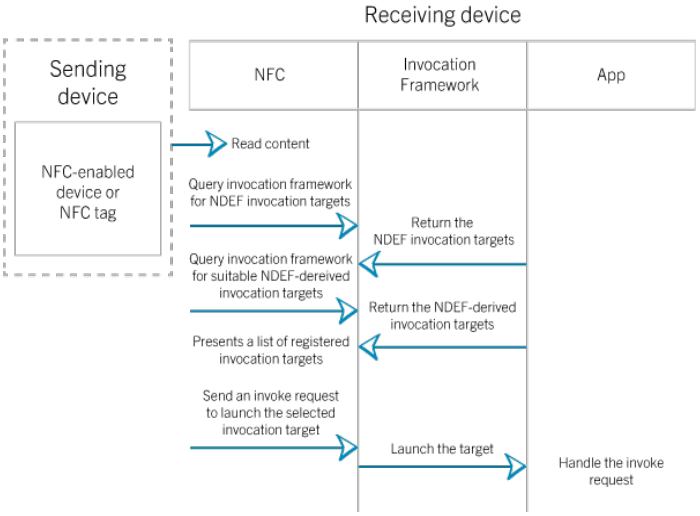

Figure 11: Common NFC Operation

NFC Data Exchange Format (NDEF) is a binary message format that can be used to encapsulate one or more application-defined payloads. NDEF is well defined as a message encapsulation format to exchange information between a RF signal transmission tunnel as well as NFC communication. A reader detects a tag with NDEF technology, then proceed with the Intent filtering in order for the user to gain access to the NFC system. Next, the tag began direct the user to the selected invocation target that has been registered on the tag. This process carried the operation of ACTION_NDEF_DISCOVERED.

Alternatively, proposed NFC filtering framework is more complex which offer hashing operations that merged Intent filtering with Bloom filtering to authenticate access, and have AES cryptographic as the prevention to content protection. Implementation of AES cryptographic in NDEF message, help to encrypt the original NDEF message with a key size of 128bit which will cause approximately about 80 trillion years++ to crack the key using brute force attack.

On top of this, Bloom filtering performed the hashing operation using MD5 technique to verify or authenticate access level to the NFC system. This operation help to eliminate the duplicate tag which Intent filtering does not handle. The Bloom filtering is followed by Intent filtering where the user is directed to the selected invocation as registered on the tag after the Bloom filtering verification. Communication of two legitimate entities is secured with AES encryption. Therefore, the possibility for a MITM attacker to retrieve tag or personal information over the network is very low since the attacker will require a long process to decrypt the NDEF message.

6. Discussion and conclusion

This chapter discussed the overall completed research project including the limitation of the research project. This chapter also discuss the successful achievements and the future enhancement of the research project as the weaknesses of the completed project.

6.1. *Security Enhancement Using Proposed Technique for Filtering*

Bloom filter is a technique used in RFID technology which is space effective and probabilistic data structure. The major benefit of the Bloom filters is its strong space advantage over other data structures for representing sets, such as self-balancing binary search trees, tries, hash tables, or simple arrays or linked lists of the entries. A bloom filter does not store the elements themselves, and this is the crucial point. You do not use a bloom filter to test if an element is present, you use it to test whether it is certainly not present. This lets you to not do extra work for elements that do not exist in a set.

The use of Bloom filtering in NFC technology prevents from MITM attacks in terms of eliminating the duplicate tag by avoiding the third entities who attempt to gain access communication between two legitimate entities. Implementation of Bloom filtering in NFC architecture provided better security solution in which the current Intent filtering does not provide. Besides that, all in significantly less space than something like a hash table which is likely going to be partially on disk for large data sets make Bloom filtering much more capable to be implemented in NFC technologies. You may use a bloom filter in conjunction with a structure like a hash table, once you are certain the element has a chance of being present.

6.2. *Security Enhancement Using Content Protection*

The Advanced Encryption Standard or AES is a symmetric block cipher used to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. In this research project, AES 128-bit has been implemented on the NDEF message as the content protection of the message being communicated. The selection process to find this new encryption algorithm was fully open to ensure a thorough, transparent analysis of the designs. The use of AES 192bit or 256bit could provide a more complex encryption standard. AES is more secure than its predecessors such as DES and 3DES as the algorithm is stronger and uses longer key size. It also enables faster encryption than DES and 3DES, making it ideal for NDEF message as well as NFC technology.

Security enhancement in terms of content protection is highly recommended as encryption standard could provide a better and secure NDEF transmitted message. Indirectly, a MITM attacker would require high time and resource in interpreting the NDEF message in order to get the original message. Since NFC commination occur in an open environment, there is high possibility for an attacker to simply gain access to the channel and retrieve the sensitive and personal information on the tag including the tag information. Encryption of NDEF message avoided this as the NDEF message has been encrypted with complex encryption algorithm and it time and resource-consuming.

6.3. *Framework: PbD with Proposed NFC Filtering*

Privacy by Design (PbD) provides a set of seven major foundational principles that we could follow to prevent privacy threats or attacks. The result is that privacy becomes an essential component of the core functionality being delivered. This approach is rooted in a belief that reliable protection in a complex ecosystem can only be achieved through an integrated design approach. Practice of using privacy guidelines is indirectly guide us to concerns on privacy as an essential component of a core functionality of a system. Since NFC technologies is a new era of wireless communication or sensor networking, there is pretty much possible threats and privacy attacks. This is with the consideration that privacy prevention provide a better protection on securing the sensitive and personal information. In reflecting this research project, privacy prevention would help to prevent leakage of tag and personal information during the commination which might be caused by MITM attack. Table 15 shows the achievement of proposed work on using PbD as the privacy guideline for this research project. We could conclude that the proposed NFC filtering is succeeding the third foundational principle of PbD principles as the privacy approach is embedded on the NFC system itself.

Table 8: PbD with proposed framework

PbD Foundational Principles	**Privacy**	**Achievement**
1. **Proactive not Reactive; Preventative not Remedial**	Anticipate and prevent privacy. Prevent from privacy risks to materialize.	Implementation AES encryption provide prevention of privacy.
2. **Default Setting**	Build privacy measures directly into any IT system.	Filtering technique as the build-in privacy approach.
3. **Embedded into Design**	Embed privacy into the design and architecture of IT system.	Bloom filtering and AES encryption is embedded into NFC architecture.
4. **Positive-Sum**	Accommodate all legitimate interests and objectives in a positive-sum. “Win-win manner.	Privacy approach in proposed framework does not against the security approach in existing NFC architecture.
5. **End-to-End Security**	Secure life-cycle management. Ensure cradle-to-grave.	The proposed framework provide end-to-end security with an encryption technique.
6. **Visibility & Transparency**	Component parts of IT systems practices visible and transparent.	The security and privacy approach implemented is transparent to end-user.
7. **Respect for the User**	Respect and protect interests of the individual. Keep it user-centric.	Interest of end-user is much appreciate and respect without any limitation to utilize the NFC system.

6.4. *Limitation of the Proposed Framework*

Limitations are influences or weaknesses of the proposed framework which can be considered as the future work. They are the shortcomings, conditions or influences that cannot be controlled or can be considered for the future enhancement work. The limitations of the proposed framework are described below.

- Content Protection - AES 128bit has been used as the content protection in this framework. Referring to table 11 above, even with a supercomputer, it would take about 80 trillion years++ to crack 128-bit AES key using brute force attack. But unfortunately, this is not adequate nowadays since there are some tolls available for brute force attacks. This might help an attacker in terms of time and recourse-consumption. For tighter security, we might consider on using AES 192bit or 256bit key size which would require a long time to crack. For public-key cryptosystems, we could go for Rivest-Shamir-Adleman (RSA) cryptographic for secure data transmission.

- Filtering technique - Bloom filtering technique has been merged together with Intent filtering in this research project. Bloom filter is a space with effective and probabilistic data structure. The major benefit of the bloom filter is its size, the constant number of bits and is set upon initialization. Meanwhile, given the fact that the advantages provided by the bloom filter outweigh the small limitation. In this research project, we have used MD5 hashing function instead of MD5. We could consider on using Secure Hash Algorithm 1 (SHA1) which could produce a 160-bit (20-byte) hash value known as a message digest.

6.5. *Research Contribution*

Near Field Communication (NFC) technology play an important role nowadays and depends on contactless equipped devices. NFC technologies or contactless equipment devices minimize human man power or work load on handling varied comprehensive tasks in their daily routine. For example, the use of Smart Card/Tag on highways toll, enables a person to just pass by the sensors and the amount is deducted exactly as how we pay at the toll counter. NFC technology is a part of the RFID technology, core from wireless communication technologies that tent to be exposed to multiple security and privacy threats or issues as the communication occur in an open environment.

The most common threats in NFC communication is Man-in-Middle attacks that attempt to corrupt tag data and the most significant issue is to gain access to personal information and sensitive area. The contribution in this research is towards the issue or problem that most users come across when using NFC devices. This research has focused on the privacy threats caused by Man-in-the-Middle attack. In other words, the sensitive or personal information or data that could be retrieved from a NFC-embedded device which is active in an open environment. For example, an attacker might have the intention to retrieve the last transaction history of an NFC smart card or bank card. Those can be counter measured with access control which could pretend as an unauthorized access or communication as the first level security during when the communication is established.

This research has been conducted on the main purpose to enhance the tag filtering technique in NFC architecture. At the moment, Intent filtering is the build-in technique in NFC architecture which perform filtering according to what has been registered to the read tag. Bloom filter technique has been merged together with Intent filtering, so the bloom filtering could filter the unauthorized access as well as eliminate the duplicate tag readings. Since the existing Intent filtering only be able to filter activities registered to the tag, bloom filter cut off the duplicate tag and pretend from unauthorized access to the NFC system. Additional to this privacy prevention, content protection modules have been implemented on the payload of the NFC message. The AES approach has been used in order to encrypt and decrypt the NFC message before it is sent over to the open network. Indirectly, this encryption technique help in terms of content protection of privacy information.

Both tag filtering and content protecting enhancement on the NFC architecture have followed the PbD foundational principle which consist of 7 major principles. This principles defined that privacy approach should be an essential component of the core functionality being delivered of an IT system.

7. Conclusion

Referring to the research in NFC, near field technology provide a useful impact on the usability of hand held devices in various contexts where it could facilitate a user's experience by making it possible to perform multiple services with a single NFC-enabled device. However, every technology has their own cons where NFC has a potentially dramatic impact on users' privacy since the communication occur in an open environment.

User's privacy refers to personal information or sensitive data and credit card details that are stored in NFC-embedded devices which would become the target for hackers and cyber-criminals such as Man-in-the-Middle attack that could cause multiple threats. Development in the NFC technology, together with some aspects such as usability, and level of security need to account for the reasons explained above.

Poor architecture or system implementation, caused multiple security and privacy attacks. In a case of poor communication channel or lack of implementation of security approach can cause leakage of sensitive and personal information. Implementation of Bloom filtering performed the verification of registered user to the NFC system and eliminate duplicate or third party access. Besides that, implementation of AES cryptographic in NDEF message, ensure communication between two legitimate entities is secured. Hence, secured user validation or filtering with encrypted message, prevent the possibility for MITM attacker to retrieve sensitive or personal information.

Acknowledgment

With grace of God, I managed to complete the research project. Even though I has faced a lot of difficulties upon completing of this research. Here by, I would like to express my gratitude towards several individuals those who directly and indirectly guide, help and support on completing this research. First of all, I would like to express my gratitude to my supervisor, Dr. Manmeet Kaur Mahinderjit Singh for her guidance, encouragement and patience

for conducting this research. Without her supervision, I might not be able to complete this research project.

I would also like to thanks each and every one who support me in term of financial and materials, especially to my mother, Mrs. N.Krishnaveni and also my future wife, Ms. M.Krishnapriyah. I really appreciate their effort in help me toward this research completion. Hopefully, all the experiences that I has gained to complete this research project will eventually come to help in the future. May all praises go to mighty God.

References

[1] Aikaterini Mitrokotsa and Michael Beye and Pedro Peris-Lopez, Classification of RFID Threats based on Security Principles, Delft PhD Thesis, University of Technology, 2012, pg. 1-22.

[2] Bing Dai, The Product Authentication Application Design Based on NFC, Master Degree, Vaasa University of Applied Sciences, 8-17 March 16, 2015.

[3] Aikaterini Mitrokotsa, Melanie R. Rieback and Andrew S. Tanenbaum, Classification of RFID Attacks, PhD, Department of Computer Science, Vrije Universiteit, 5-12, 2012.

[4] Liam Church and Maria Moloney, State of the Art for Near Field Communication: security and privacy within the field, Escher Group Ltd, Ireland, 5-6, May 10th 2012.

[5] Siti Salwani Yaacob, Hairulnizam Mahdin, An Overview on Various RFID Data Filtering Techniques Based on Bloom Filter Approach, Master Degree, Universiti Tun Hussein Onn Malaysia, 8-41, 2013.

[6] David Ong, Dr Manmeet Kaur, MIDAS - Multifactor Identification Attendance System, Bachelor Degree, University of Science, Malaysia, 32-68, 2015.

[7] Ann Cavoukian, Mobile Near Field Communications: Keep It Secure and Private, ISSA Journal, 1-2, August 2012.

[8] Ann Cavoukian, Privacy by design – The 7 Foundational Principles, Information & Privacy Commissioner Ontario, Canada, 1-2, January 2011.

[9] Anurag Kumar Jain and Devendra Shanbhag, Addressing Security and Privacy Risks in Mobile Applications, IEEE Computer Society, 25-29, Sept/Oct 2012.

[10] Prapassara Pupunwiwat, Bela Stantic, Location Filtering and Duplication Elimination for RFID Data Stream, International Journal of Principles and Applications of Information Science and Technology, 13-22, Dec 2007.

[11] EMCA International, NFC-SEC - NFCIP-1 Security Services and Protocol - Cryptography Standard using ECDH and AES, EMCA International, 56-59, Dec 9, 2008.

[12] Andreas Rohr, Karsten Nohl, Henryk Plotz, Establishing Security Best Practices in Access Control, Security Research Labs, Publication version, v.1.0, 78-83, 2007.

[13] BIC, Near Field Communication (NFC) and the use of Radio Frequency Identification (RFID) in Libraries, BIC, 1-2, 2012.

[14] International Organisation for Standardisation. ISO/IEC 15693-1. Identification cards - Contactless integrated circuit(s) cards - Vicinity cards, 2-4, 2000.

[15] [6] NFC Forum, NFC Data Exchange Format (NDEF), NFCForum-TS-NDEF_1.0, 3-8, 2006.

[16] BIC, Near Field Communication (NFC) and the use of Radio Frequency Identification (RFID) in Libraries, BIC, 4-7, 2012.

[17] Uwe Trottmann, NFC – Possibilities and Risks, Seminar Future Internet WS2012, Network Architectures and Services, 13-26, Feb 2013.

[18] Ernst Haselsteiner and Klemens Breitfub, Security in Near Field Communication (NFC) - Strengths and Weaknesses, Philips Semiconductors, 11-13, 2012.

[19] Y. Bai, F.Wang, and P. Liu. Efficiently Filtering RFID Data Streams. In CleanDB, 9-34, 2006.

[20] Min Kyung Jeon, Kee Hyun Choi, Bong Jae Kim, Dong Ryeol Shin, Efficient and Secure Copy Protection System for Digital Content in IoT Environments, Research Notes in Information Science (RNIS), 44-48, June 14th 2013.

[21] Wiem Tounsi, Security and Privacy Controls in RFID Systems Applied to EPCglobal Networks, Telecom Bretagne, 33-48, Jan 16, 2015.

[22] Cheng-Hao Chen, Iuon-Chang Lin, Chou-Chen Yang, NFC Attacks Analysis and Survey, 2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 4-6, 2014.

[23] Reading NFC Tags with Android, 18 Feb 2016, retrieved from: http://code.tutsplus.com/tutorials/reading-nfc-tags-with-android--mobile-17278

[24] Android, NFC Basics, 20 May 2016, retrieved form: https://developer.android.com/guide/topics/connectivity/nfc/nfc.html

[25] Advantages and Disadvantages of NFC, 2 March 2016, retrieved from: http://near-field.blogspot.my/p/pros-cons.html

[26] US to Challenge China for World's Fastest Supercomputer, 16 May 2016, retrieved from: http://thediplomat.com/2015/08/us-to-challenge-china-for-worlds-fastest-supercomputer/