

Master's Project
Android Application
NFC Dashboard



Northeastern Illinois University
MS in Computer Science

Anju Shrestha
0641000

Motivation

Technology has become an integral part of our life. We have seen the growing technology day by day. NFC has evolved everywhere in the past few years. We can see the use of NFC in a lot of places. We can pay for our groceries just by one touch. We can make the use of NFC in the Universities where we can have the NFC card in the office of the professors which will have information like office hours, website and other information about the professors. Students can use their smartphone to get all the information about the professor they are looking for in one touch.

Saying the pros of technology, security has been a main issue in today's world with the use of technology. If we are writing our personal information in the NFC tag, we do not want it to be shared to unauthorized person. In NFC, communication standard defines very close read range, therefore significantly reducing the probability of a threat.

However this does not mean it is totally safe when deploying NFC tags. Any tag can be breached with time and knowhow. So, it is very important to secure the data written in the tag.

What is NFC?

NFC stands for "Near Field Communication" and, as the name implies, it enables short-range wireless communication between compatible devices. This requires at least one transmitting device, and another to receive the signal. It's a method of wireless data transfer that detects and then enables technology in close proximity to communicate without the need for an internet connection. It's easy, fast and works automatically.

NFC fulfills the need to provide secure, short-distance, and implicit paired communication capability in smartphones. One of the most important aspects of NFC technology is its inherent security since the communication range is extremely short. In NFC communication, bringing two devices very close to each other starts

communication and separating the devices beyond a certain limit terminates the communication immediately. NFC technology offers great and varied promise in services such as payment, ticketing, gaming, crowdsourcing, voting, navigation, and many others.

Types

- Active Device
- Passive Device

Active Device

Active devices are able to both send and receive data and can communicate with each other as well as with passive devices. Smartphones are by far the most common form of active NFC device. Public transport card readers and touch payment terminals are also good examples of the technology.

Passive Device

Passive NFC devices include tags and other small transmitters that can send information to other NFC devices without the need for a power source of their own. However, they don't process any information sent from other sources, and can't connect to other passive components. These often take the form of interactive signs on walls or advertisements.

How Does NFC Works

Just like Bluetooth and Wi-Fi, and all manner of other wireless signals, NFC works on the principle of sending information over radio waves. Near Field Communication is another standard for wireless data transitions. This means that devices must adhere to certain specifications in order to communicate with each other properly. The technology used in NFC is based on older RFID (Radio-frequency identification) ideas, which used electromagnetic induction in order to transmit information.

The tech involved is deceptively simple tech, an NFC chip operates as one part of a wireless link. Once it's activated by another chip, small amounts of data between the two devices can be transferred when held a few centimeters from each other.

No pairing code is necessary to link up and because it uses chips that run on very low amounts of power (or passively, using even less), it's much more power-efficient than other wireless communication types.

NFC Applications in Service Domains

NFC technology covers a wide range of applications including healthcare, location, finance, social networking, entertainment, education, etc.

Education Application

It is seen from the surveyed studies that NFC is potentially related to education and training. After the development of NFC technology, the existing mobile computing and application development courses in universities were devoted to NFC technology in varying proportions, with entire courses on NFC subsequently developing.

Smart school and university environments implemented using NFC technology and NFC- equipped classrooms for course enrollment, attendance and registration control, information gathering and related cases have been developed. In one study, an anonymous assessment of exam papers using NFC technology is presented. According to the model, each student has NFC tags, which consist of user identification data such as name and number. As the student fills in the exam paper, she attaches a tag to the exam sheet and submits it to the exam supervisor. During the grading of exam papers, the evaluating teacher does not see any hint of the identity of the student. In another study, the authors offered a Smart University project that aims to utilize NFC technology in a university environment. The project consists of smartphones, several NFC tags, NFC readers, and servers for enabling different use cases such as class attendance control and registration fee payment.

Payment, E-Money and E-Wallet Applications

NFC technology enables smartphones to be used for contactless payment instead of credit or debit cards.

A payment protocol, named as MobiTag, enriches the EMV(Europay, Mastercard and Visa) protocol to upgrade it from a payment protocol to a complete transaction protocol. Mobitag enables using, redeeming and acquiring other valuables representing vouchers, coupons, or tickets. The authors present a system that collects tolls using NFC technology. Another study emphasizes the importance of the agreement between the actors in the NFC ecosystem for enabling beneficial payment services. Most of the existing payment schemes are either user-centric or institutional-centric; either a person or an institution may purchase goods or services. Some authors propose a model that enables cars to make payments by using prepaid accounts. E-wallets are yet another concept for increasing the efficiency of monetary processes. An e-wallet is analogous to traditional wallets that store credit cards, debit cards, gift cards, loyalty cards, and so on. Currently, two popular electronic wallets (e-wallets) exist in the market: Google Wallet and Apple Pay.

Security Protocols Used

NFC tags are used in the reader/writer mode of NFC. Two use cases are typical: the smartphone may read data from a previously loaded NFC tag, or the smartphone may write/overwrite to a tag. Read and write permissions of tags are important here; unauthorized read or write functions are unwelcome, of course. Physical security of the tags, unwitting actions weakening the system, as well as threats aiming to damage the system are potential risks of NFC tag security.

I have used Hash Function and AES to secure the information in the application.

Hash Function

A hash function is any function that can be used to map data of arbitrary size to fixed-size values. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes. I have used SHA-256 Algorithm.

SHA-256 Algorithm

SHA-256 stands for Secure Hash Algorithm - 256 bit and is a type of hash function. SHA-256 is a one-way function that converts a text of any length into a string of 256 bits. It is a cryptographically secure hashing function, in that knowing the output tells you very little about the input. It's a keyless hash function, which means an MDC (Manipulation Detection Code).



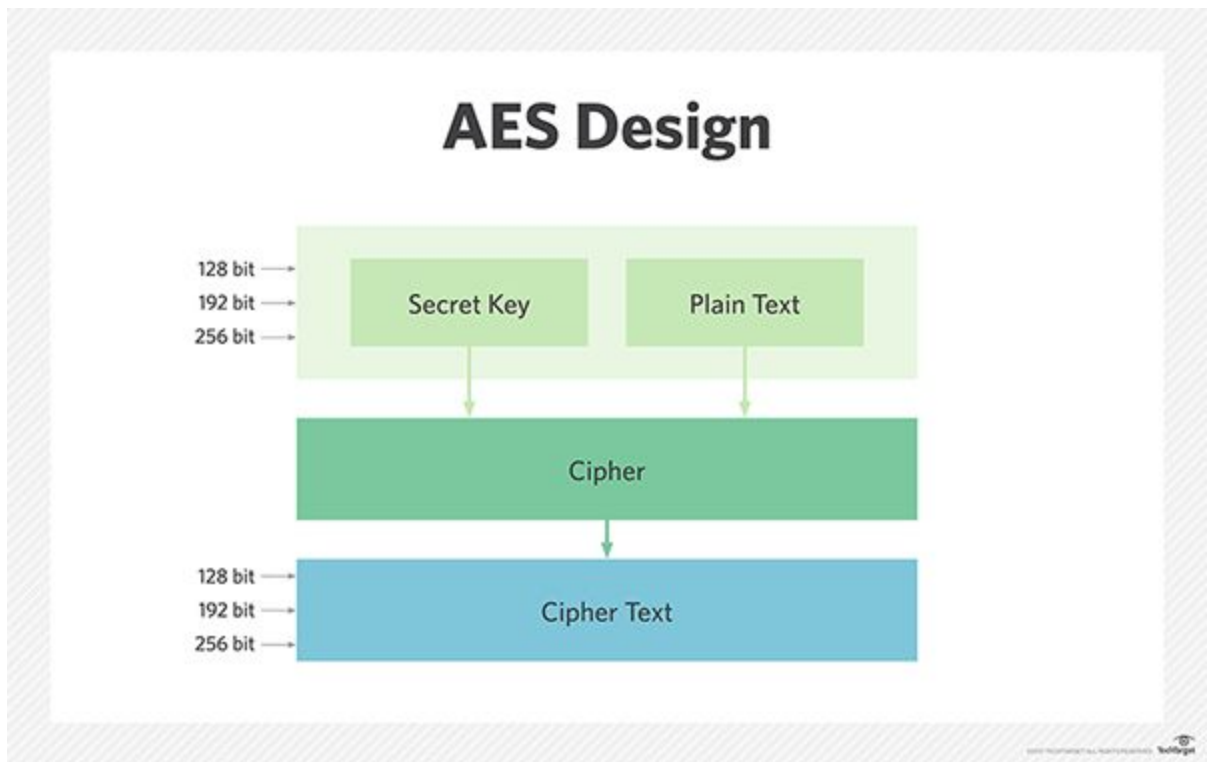
[Image Link](#)

AES

AES or Advanced Encryption Standards is one of the most widely used methods for encrypting and decrypting sensitive information.

This encryption method uses a block cipher algorithm to ensure that data can be stored securely. AES algorithm is symmetric, the same key is used for both encryption and decryption.

AES comprises three block ciphers: AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. For this project, I am using AES-128 to encrypt and decrypt the information. Key used is 16 binary digit characters written and stored in the internal storage of the android device.



[Image Link](#)

Implementation

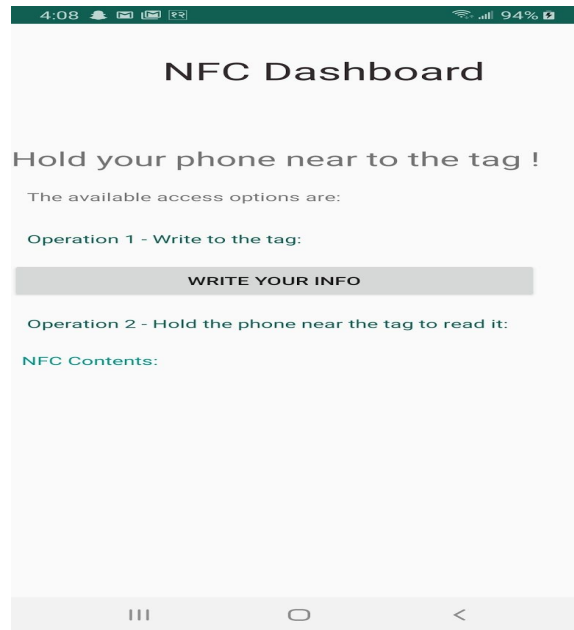
To create this Android application, I used Android studio to develop and test the application.

Functions of the Applications

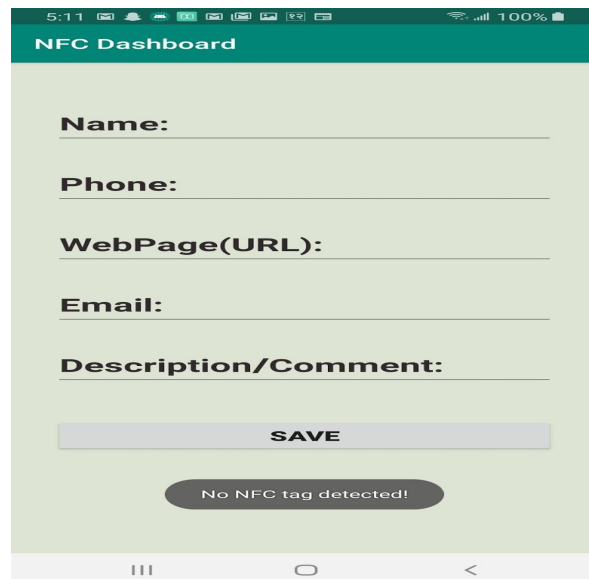
- Detect NFC tags/cards
- Write data to NFC tags/cards
- Read data from the NFC tags/cards

1. Detect NFC tags/cards

This is the main page (Dashboard) of the application. If NFC tag is brought near the device, it displays the information written in the NFC tag/card.



When **WRITE YOUR INFO** button is clicked, this screen is displayed. When we press the SAVE button and there is no NFC tag/card nearby then it displays **No NFC tag detected!** Message.

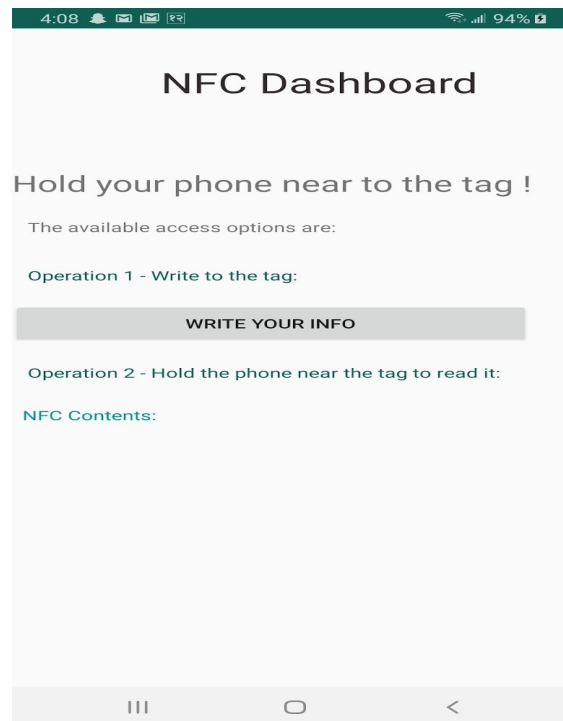


2. Write data to NFC tags/cards

To write to the NFC tag, we first create a NFCAdapter. We then initialize it within our onCreate. We will then need to enable our PendingIntent to run in the foreground of our activity that we created. This is done in the onResume method. We disable this PendingIntent on our onPause method.

Where all the magic happens, is when we override the onNewIntent method. This method is activated when the NFC tag touches our device. This is because of the IntentFilter that we set.

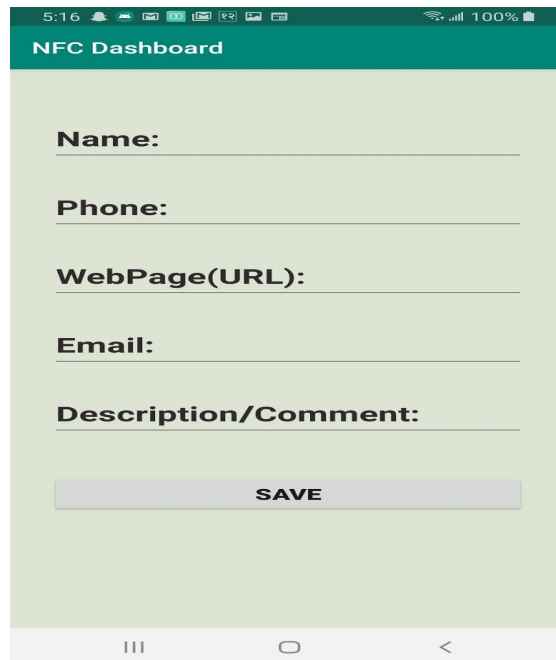
This is the main page(Dashboard) of the application.



This page is opened when **WRITE YOUR INFO** button is clicked. We have a main activity and write activity in the program. So, when the button for the "WRITE YOUR INFO" is clicked, it is taking to WriteEncryptActivity class from the

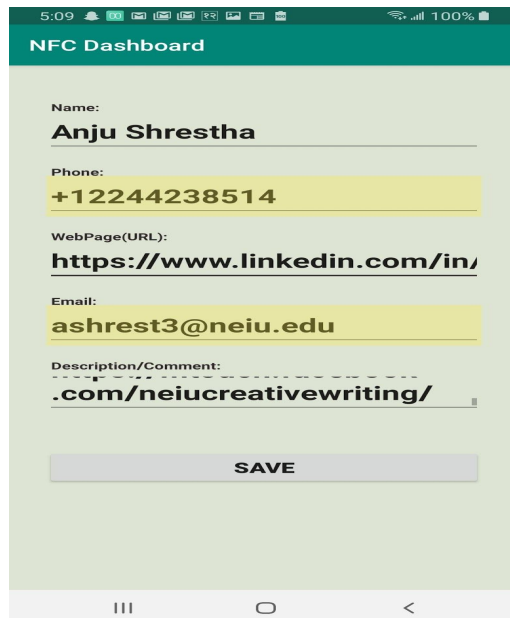
Fall 2019
CS - 490

main activity class which has all the EditText fields and save button as shown in the screen.



A screenshot of a mobile application titled "NFC Dashboard". The app has a teal header bar. Below the header, there are five input fields with labels: "Name:", "Phone:", "WebPage(URL):", "Email:", and "Description/Comment:". Each label is followed by a horizontal line representing the input field. At the bottom of the form is a grey button labeled "SAVE". The status bar at the top shows the time as 5:16 and 100% battery.

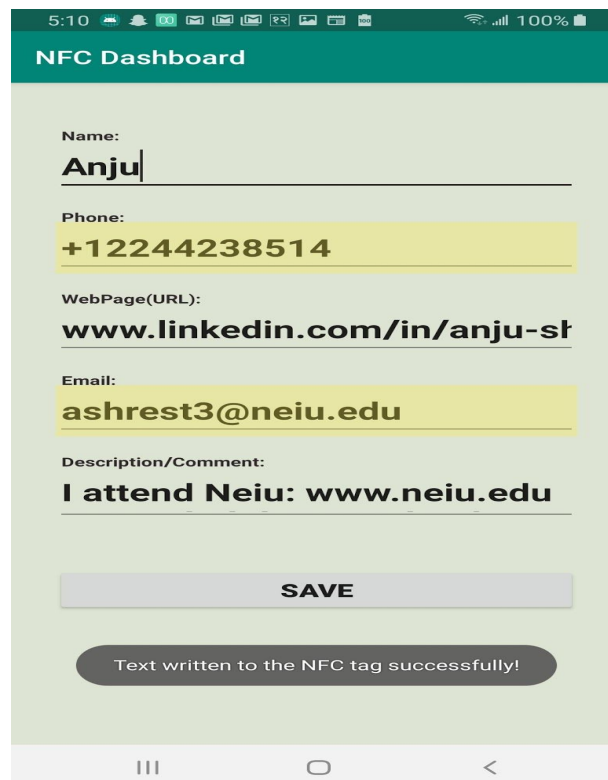
We can fill the information as shown. EditText fields let us edit the fields according to the input type.



A screenshot of the same "NFC Dashboard" app, but now the input fields are filled with text. The "Name:" field contains "Anju Shrestha". The "Phone:" field contains "+12244238514". The "WebPage(URL):" field contains "https://www.linkedin.com/in/". The "Email:" field contains "ashrest3@neiu.edu". The "Description/Comment:" field contains ".com/neiuc creativewriting/". The "SAVE" button is still at the bottom. The status bar at the top shows the time as 5:09 and 100% battery.

After filling the information needed, bring the NFC tag near the android device and click the **SAVE** button. If the NFC tag is detected nearby, it saves the information to the tag and “**Text written to the NFC tag successfully!**” message is displayed.

Once information is filled in the EditText field and Save button is clicked, it looks for the NFC tag, if found new NDEF record is created. Here, all the EditText fields are concatenated first and hashCode of it is generated using SHA-256 algorithm. The combined strings from all the TextEdit field is concatenated with hashCode obtained from the SHA-256 algorithm using “#” sign in between. Then the concatenated string is encrypted using AES algorithm with the master key which is saved in the internal storage of the device. Now, the encrypted message is written in the tag.



The screenshot shows the 'NFC Dashboard' app interface. At the top, there's a teal header with the title 'NFC Dashboard'. Below it, the form contains the following fields and values:

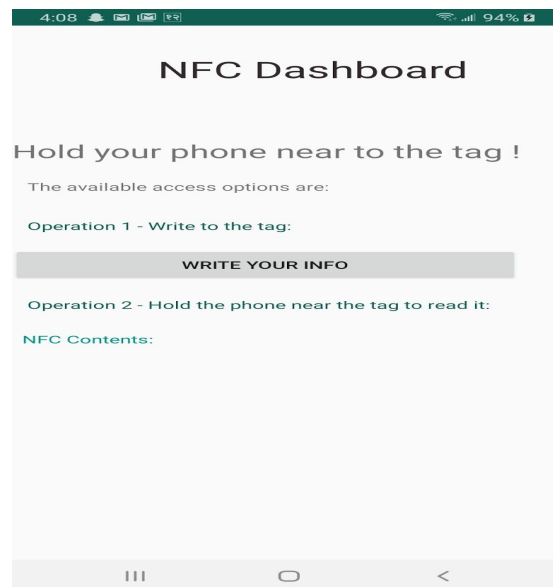
- Name: Anju
- Phone: +12244238514
- WebPage(URL): www.linkedin.com/in/anju-sl
- Email: ashrest3@neiu.edu
- Description/Comment: I attend Neiu: www.neiu.edu

Below the form is a grey 'SAVE' button. At the bottom, a dark grey toast message displays 'Text written to the NFC tag successfully!'. The Android navigation bar is visible at the very bottom.

3. Read data from the NFC tags/cards

Reading NDEF data from an NFC tag is handled with the tag dispatch system, which analyzes discovered NFC tags, appropriately categorizes the data, and starts an application that is interested in the categorized data. An application that wants to handle the scanned NFC tag can declare an intent filter and request to handle the data.

This is the main page(Dashboard) of the application.



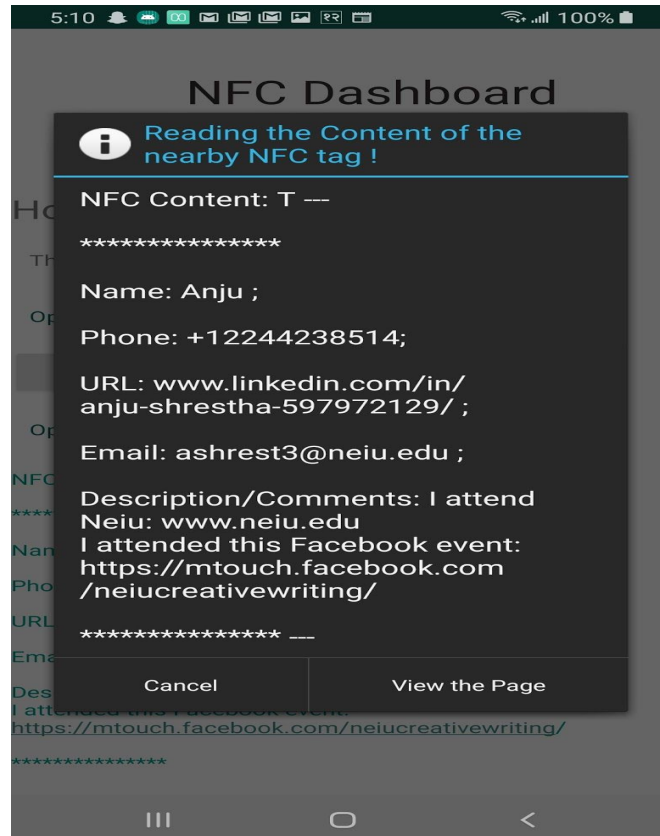
When NFC tag is brought near to the android device, it reads the information written in the NFC tag.

The data written in the NFC tag is encrypted data. When reading the data from the tag, first the data is decrypted using the AES algorithm with the master key which is saved in the internal storage of the device. Now we have the decrypted message with the text fields and hashCode of those text concatenated with “#” sign in between. I am splitting the string with using #. Now we have two string arrays one with text information and other with hashCode. I am taking the first array with text field and generating the hashCode of that String. Finally, I am comparing the hashCode of the text field and the hashCode we got from the second array (from the decrypted message). If both of those

Fall 2019

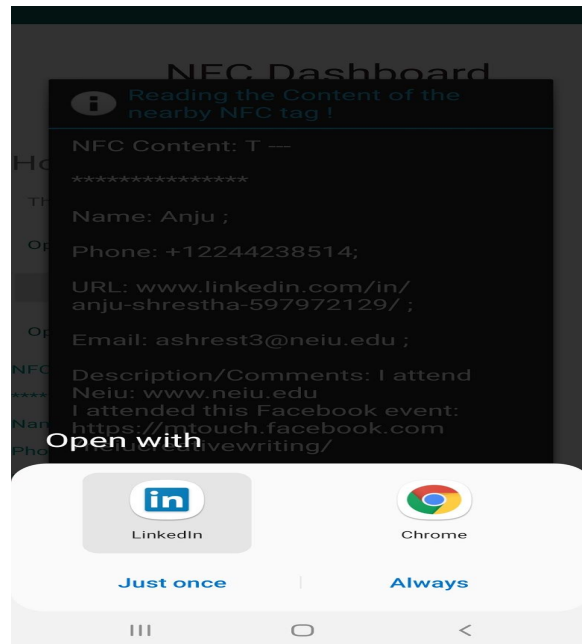
CS - 490

hash values are the same, then the decrypted text information are displayed, else the encrypted message is displayed.

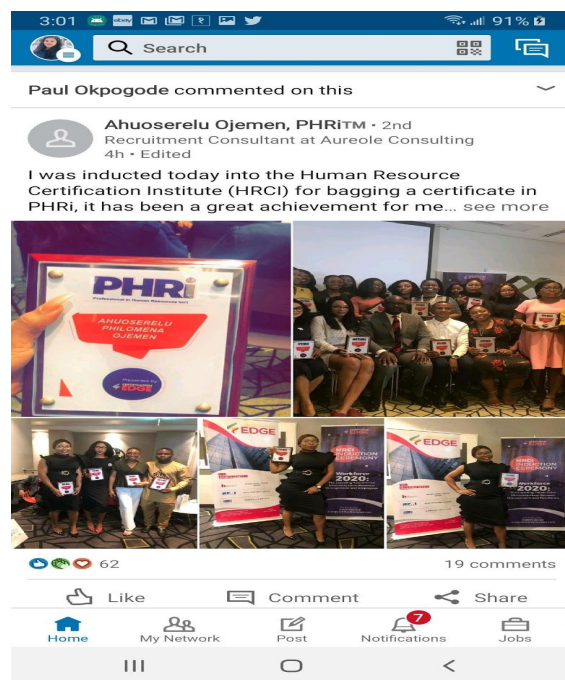


After displaying the dialog box, app looks for the URL link. If it finds the URL, it will automatically redirect to the browser and opens the first link provided.

If Application for the link (like Facebook, LinkedIn, Twitter) is already installed on the cellphone, it asks whether you want to open link through the app or through the browser.



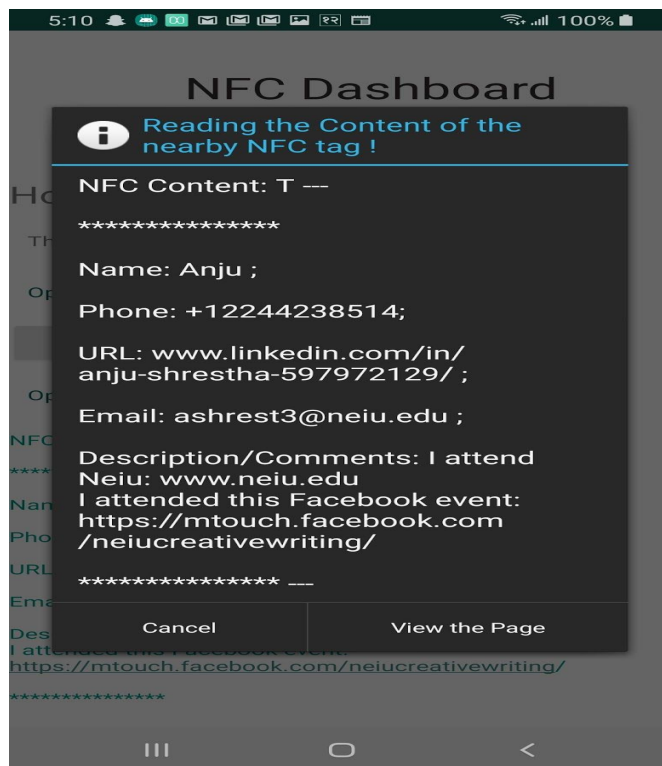
If we choose to open it through application, it opens the application installed to the phone and open the page provided on the URL, else it opens through the browser.



Fall 2019

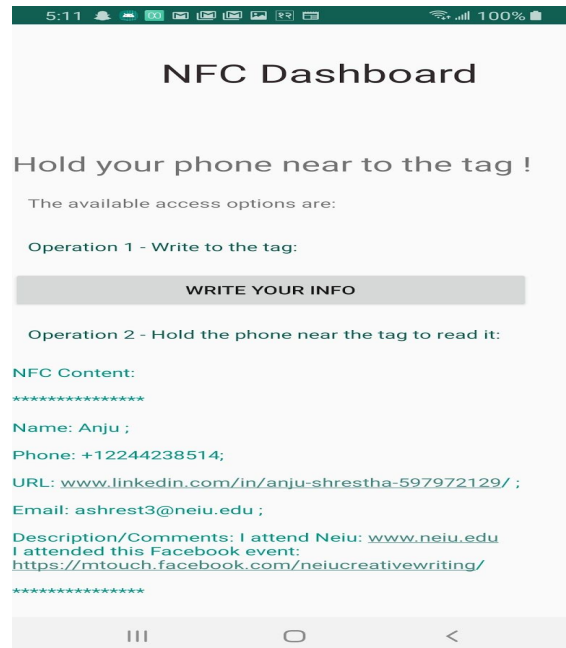
CS - 490

Then when we come back we can see the dialog box with the information.

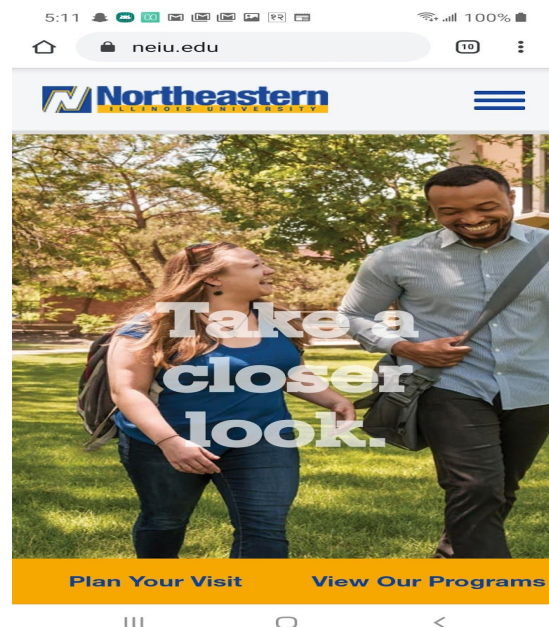


When we press cancel, we can see NFC contents written in the tag.

If there are web Url link with the text, it extracts the Url from the text and those links are underlined and are viewed as clickable URL links. When those links are clicked, it will take to the respective browser or redirect to the application if the application for the Url link is already installed on the android device.



When we click the link, it will redirect to the respective browser or the application if installed in the android device.

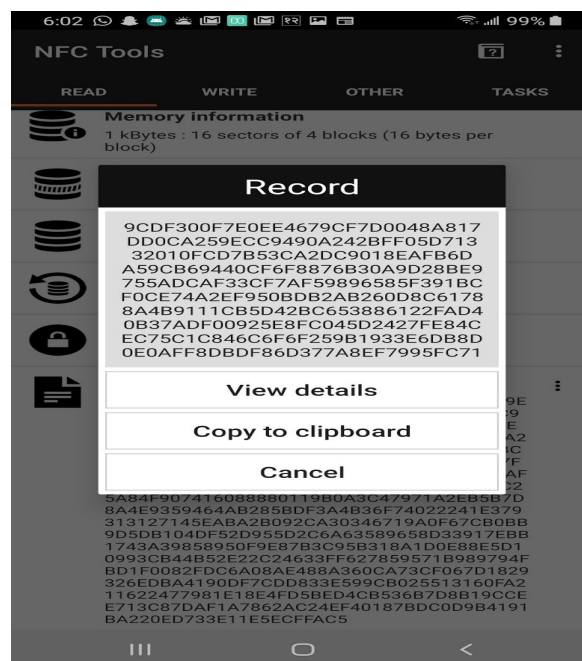


Fall 2019
CS - 490



Security

All these information is secured and no one can view it unless the master key is provided. All the information is encrypted when writing the data to the tag.



Conclusion

Developing an android application was a new experience for me as I did not have a chance to work on the android studio before. Developing this project was a great experience for me. In this project, we are to write the information like name, phone number, email address, web page and description. While reading the tag, we can see all the information written in the tag. It finds the first URL and automatically redirect to the application installed in the phone or the web browser. Also, this app can extract all the URLs from the text and will display the clickable links for all the URLs written in the tag. The most important part of this application is all the information written in the NFC tag is secured. I have used Hash-256 and AES-128 algorithm to secure the information. So, to read the text information written in the tag, we need 16 bit characters key saved on the external storage of the phone otherwise encrypted message will be displayed. For the future work, we can add more functionality to the application. We can work on making the application to read only or lock the tag so no one can change the information written. We can also connect it with database to keep track of all the information written in the tag.

Reference:

1. <https://pdfs.semanticscholar.org/e487/f6e3bcbdfc8efa36678b30e68e736a37b28.pdf>
2. <https://medium.com/@ssaurel/create-a-nfc-reader-application-for-android-74cf24f38a6f>
3. <https://www.sitepoint.com/learn-android-nfc-basics-building-a-simple-messenger/>
4. <https://medium.com/@ssaurel/create-a-nfc-reader-application-for-android-74cf24f38a6f>
5. <https://stackoverflow.com/questions/49542137/how-to-write-values-to-nfc-tag-from-two-activities-without-overwriting-existing>
6. https://developer.nordicsemi.com/nRF_Connect_SDK/doc/latest/nrf/include/nfc/ndef/nfc_ndef.html
7. <https://github.com/android/connectivity>
8. https://github.com/survivingwithandroid/Surviving-with-android/blob/master/Android_NF
9. <C:/app/src/main/java/com/survivingwithandroid/nfc/model/RDTSpRecord.java>
10. <https://www.learn2crack.com/2016/10/android-reading-and-writing-nfc-tags.html>