[1]Sandip Shinde

[2]Deepak Mane

[3]Jyoti Kanjalkar

[4]Sangita Jaybhaye

[5]Sheetal Phatangare

[6]Kartik Khilare

Efficient Frontier Rules for Secure NFC Payments and Data Transmission

Abstract: - As a result of advancements in technology areas including mobile communication, semiconductors, and 5G internet, things have changed very quickly.Near field communication [NFC] has gained popularity due simplicity in use and function. Given that the weaknesses in the current technique were discovered, this paper proposed a new protocol for more secure NFC payments and data transfer. And thus conducted a thorough analysis of NFC payments and discovered that the data carried over the air was weak and easily intercepted by using tools like as Pflipper zero, Hackrf-one, and RTL-SRD, and later could be decoded utilising cutting-edge computations and GNU. This suggested protocol entails local-level verification for the creation of a transmission channel between a card and a Point of Sale [POS] at the local-level, allowing a secured point-to-point connection between the two end points. In addition to the first step indicated, the channel will make sure that no data is being eavesdropped by an unauthorised devices or antenna. If so, both the channel and any data that was transmitted over it are immediately destroyed. This protocol would offer more security declarations and aid by making payments secured, safe, and morally correct.

Keywords: Cybersecurity, Network Security, NFC , POS , Secured NFC Payments , Synchronous Trust Number (STN) ,Contactless payments, SDR

I INTRODUCTION

For ages, financial possessions have been viewed as the highest priority by humans. This has resulted in the global establishment of diverse financial organisations from all three sectors, including capitalism, communist, and socialist systems. The increased circulation of monetary funds has spurred several developments all around the world. These inventions include cash, cards, UPI, bank transfers, and other services. The card payment industry has created newer types of card payment systems to improve the payment experience, such as chip-enabled, tap-to-pay NFC, contactless, and mobile-emulated card payment systems. The use of NFC-based methods for streamlined and time-saving work is becoming more popular, not only among individuals but also across sectors. Many digitally evolved countries, such as the United States and Europe, have largely adopted contactless and mobile-emulated NFC payment methods to speed up the billing process. Organisations such as Euro-pay, Mastercard, and Visa [EVM] are working together to set global standards for credit and debit card payment systems. The banking industry engaged in transaction and management functions issues debit and credit cards based on EVM or comparable standards to their clients. The Wi-Fi icon in the corner quickly distinguishes NFC-enabled cards. These cards can imitate mobile payment apps such as Apple Pay and Google Pay, allowing people to make payments without the need for a physical card. These payment options are intended for speedier and smoother transactions and do not normally need the use of a secret PIN.For security reasons, governments in several nations have set maximum transaction limitations. In India, for example, the maximum is Rs 2,000, whereas in the United Kingdom, it is 100 pounds. Despite taking into account both PIN and PIN-less scenarios, the data remains vulnerable to theft. This document presents important protocols targeted at improving the security of contactless and tap card payments. Furthermore, these protocols seek to prevent data tampering and

[1] [1,2,3,4,5,6]*Vishwakarma Institute of Technology, Pune, Pune-411037, Maharashtra, India*

sandeep.shinde@vit.edu

deepak.mane@vit.edu

jyoti.kanjalkar@vit.edu

sangita.jaybhaye@vit.edu

sheetal.phatangare@vit.edu

kartik.khilare20@vit.edu

eavesdropping at the local area level, which is a critical part of the payment process. The paper will explain the essential principles involved, as well as the necessary operating needs and other minor details.

The aim of this paper is

- To identify the unusual vulnerabilities present in the exist NFC models at vicinity level for crucial data transfer.
- To propose a new effective method to tackle such situations.

The outline of this paper is as follows: Overall background along with literature review of various NFC prototypes in section II, Proposed methodology in section III, System architecture in section IV, Working is in the section V,Results along with discussion in section VI, Conclusion in elaborated sections in section VII, References in section VIII.

II. LITERATURE REVIEW

The article examines mobile payment technology and contrasts site charge and remote payment options. Using IRDA, Bluetooth, and RFID for site charge payment delivers ease and security. Due of its benefits, RFID rules the payment industry. The article focuses on RFID technologies for effective site fee payment[1]. This paper discusses the credit card methodology with NFC enabled card payments . it also proposes the researched data that analyses the usage to NFC based credit card and the payment system . it involves the factors like gender , Perceived ease of use, Social influence, Personal innovativeness in information technology, and the adoption of policy by the administrative government. It provides useful information for forming marketing plans for mobile device producers, retailers, banks, software developers, and governments. The study increases TAM's applicability to the developing mobile credit card market[2].The paper discusses methods and procedures for bringing open-loop payment systems to mobile devices are presented. The objective is to create a workable solution that causes the least amount of disturbance to the existing infrastructure while increasing the appeal of joining the NFC ecosystem by lowering integration costs. Technically, there are no obstacles to NFC-based services; the difficulty is in creating an ecosystem that is interoperable and includes all parties[3].This study examines how NFCmobile payment technologies are currently being used in public transport and finds the critical variables influencing consumers' intent to keep using them. 180 users participated in the study, which discovered that users' intentions are influenced by satisfaction, service quality, expected effort, and perceived danger. This presents new economic potential based on user behaviour for organizations providing public services[4].The paper suggests a brand-new payment method for public transport that combines IC card, NFC, and QR code technology. It presents an app that integrates several payment methods, addressing the problems with fragmented payment platforms and providing a thorough and affordable solution. Programming and simulations are used in the creation and testing of the platform. It incorporates a variety of payment options, allowing users to choose their preferred means of transportation. It also makes it possible to get discounts by combining purchases, overcoming the present individual transportation payment systems' restriction on discounts[5].In a new NFC payment structure created for small businesses, this study introduces a methodology that addresses EMV's shortcomings. The suggested design eliminates the requirement for a separate mobile PoS by allowing an NFC smartphone to function as both an NFC reader and a PoS. During transactions, the global EMV standard encrypts communication between a PoS and a payment device. Studies show weaknesses even while authentication, authorization, and integrity are provide[6]. Near Field Communication (NFC) facilitates wireless data transmission over short distances between devices. NFC-based payments are common since mobile devices are used as customer IDs, credit cards, and access cards. Addressing flaws in the present EMV (Europay, Mastercard, and Visa) security system is essential to ensuring widespread adoption. In order to increase the security of NFC payments, this paper suggests adding a security layer to EMV that ensures data confidentiality and mutual authentication between transaction actors[7]. Secure NFC payment model using ECC encryption, ensuring end-to-end security for P2P and P2M transactions. Users input their PIN and transaction amount on NFC devices, with the bank verifying the transaction. Our approach is convenient and rigorously validated for security, offering enhanced features and efficiency compared to existing NFC payment protocols[8].

III PROPOSED METHODOLOGY:

The existing NFC data transmission method consists of loop holes and weakness, that make the data transferred over the air susceptible. The crucial data can be captured by unauthorized access by means of devices compatible of doing so.

The proposedprotocol involves verifying a local-level connection between two end points of the system to ensure secure communication. It also includes security measures to prevent data interception, with immediate data and channel destruction if interception is detected. Overall, this protocol enhances payment security and integrity.

A] Vulnerabilities assessment in existing method

Thus by using the above mentioned tools and technologies and doing the setup. The setups involves particular arrangements as shown in the [Fig.2] and using the desktop version of the SDR application with respect to the operating system being used. Hackrf One should be placed in the vicinity of the POS device. The SDR WAS configured with the Hackrf. This generally involved selecting the input method and the SDR auto detected the refresh code as showed in [Fig.1]. If the device is not able to detect Hackrf One then we had to configure it by changing the USB drivers in Zadig software and restart the process. The bandwidth remained 0 in SDR. Maintained the window frame size of 5-10 Mhz for better visuals. Aim the target region to the desired NFC range of 10 -16 Mhz so that the spike was seen around 13.56 Mhz frequency when any NFC activity is noted by Hackrf's antenna. AUSB cable was used to connect the node device and the laptop. Next step was to activate the Pos device and connect it to the internet via wifi or cellular . Similarly made the NFC enable card or mobile emulation ready. The assessment process involved making the payment with NFC method to the Pos. One can detect the data transfer taking place by placing the Hackrf one antenna as external unauthorized device .Thisdevice had the potential to capture the signals or data transmitted while the payment process takes place between the POS and NFC card. During this process the SDR (Software Defined Radio) connected to the Hackrf via micro USB cable shows the data spike occurring at 13.56 Mhz frequency henceforth making it a noticeable vulnerability in the system. The operation can be seen in the video in below mentioned link.

Figure.1 Default configuration for NFC signals

The fig.1 illustrates the initial configuration of the SDR application in the case of fig.1 SDR ++ was been used. After default configurations we can see the various frequencies detected by Hackrf at 8,9,10 Mhz and other small disturbances leading to spikes in the graph.

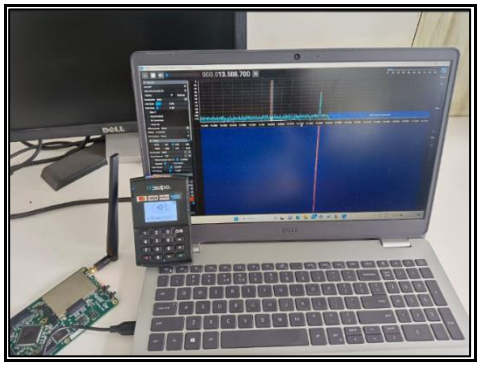

Figure 2 Initial setup review

The Fig.2 explains the setup review for the test. This involves how the connections have to be made and how much should the distance between the external unauthorized antenna of Hackrf One be.

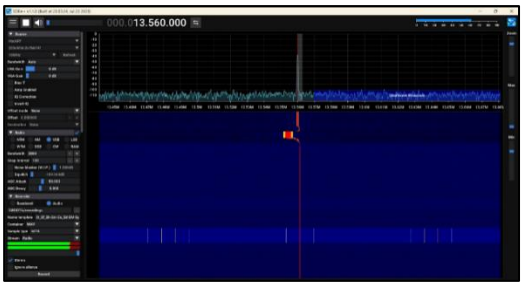

Figure 3 Data or signals being captured and visualized in graph at 13.56 Mhz.

The Fig.3 exhibits the data or signals being captured by the powerful hackrf antenna. The graph clearly spikes up at 13.56 Mhz frequency making it noticeable event for the demonstration of NFC data transfer over the vulnerable channel over the air.

IV. SYSTEM ARCHITECTURE

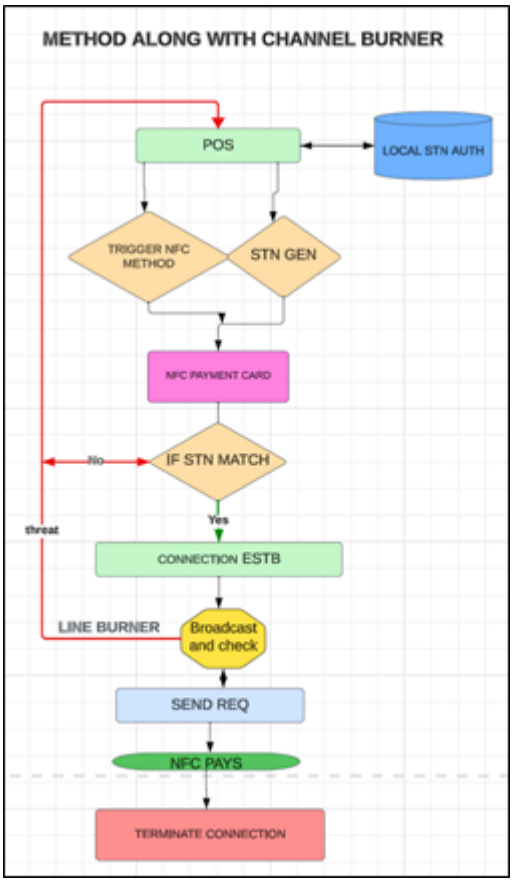

Figure 4 System Architecture for proposed solution

The Fig.4 presents the flowchart of the system architecture. It conveys the work flow mechanism of the proposed solution. The detailed representation of step by step approach is depicted for various conditions been taken into consideration. These mainly include STN match, broadcast check , line burner check, connection establishment etc. the system architecture clarifies various steps involved in new solution for example local STN authentication, connection establishing, sending request ,payment, data deletion in line burner , connection termination and etc. it also makes sure two factor authentication is practiced.

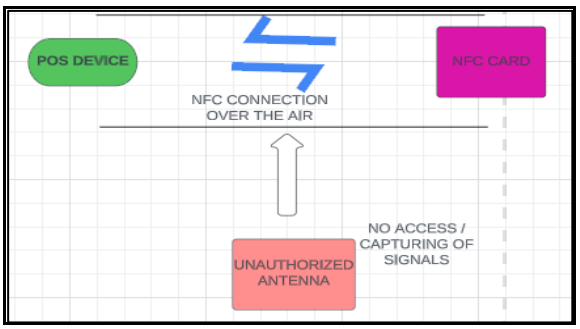

Figure 5 Representation of secured channel establishment

The Fig.5 shows the secure channel creation over the air. The vulnerability to attacks like data stealing , clone , NFC hunting and etc were removed by the technique. The Fig.6 depicts no access to the unauthorized access is gained to anyone or any device in the vicinity while the data is transferred.

A] key concepts:

1. NFC enable card /device: Near Field Communication technology is integrated into NFC-capable cards, enabling efficient transmission of data between nearby devices. Through features like contactless purchases, keyless access, and data exchange with connected devices, these cards maximise convenience. NFC-enabled cards provide a wide range benefits through speeding interactions, making them an important advancement in modern day technology. Due to its simplicity of use and security characteristics, NFC, which runs at a frequency of 13.56 MHz, is frequently employed for many applications.

2.POS Device:A POS (Point of Sale) device streamlines transactions by combining to multiple payment methods. It improves efficiency in the retail and service industries by optimising transactions and payment procedures. They are linked to the bank account and payment gateway.

3. NFC chip : Chips read, write, and simulate the data that has been stored on the chip to carry out contactless data interchange activities. In general, the data transfer rate varies from 106 to 424 Kbps depending on the application context. The storage area could range in size from 96 bytes to 128 kb.

4. Synchronous Trust Number (STN): It will be a random 3-4 digit number generated by the POS and local authentication database inorder to create a secure channel for data transmission . The STN generated by the POS would be different for every payment ,thus allowing only one user to sync into the channel at a time .

5. Software Defined Radio (SDR): A wireless communication technology that replaces hardware components with software control. SDR translates radio waveforms into digital data. A high-frequency front-end for signal capturing and digital processors for data processing are common components of SDR devices. SDR is essential in modern wireless technology, supporting everything from smartphones to military radios and satellite communication.

B] Tools and technology

1. POS device
2. NFC enabled payment card / mobile emulation
3. HackRF One
4. SDR ++ / SDR Sharp

V. WORKING

Line Burner policy:

1)This is the step number 5 in the protocol. After successful completion of STN synchronization from both sides, the next step is the eavesdropping check, which is carried out by the POS device. A random message is broadcast by the POS device to attract and check the existing unauthorized devices in the vicinity.

2) When any acknowledgement is received from any other device except the synced one, the channel will be deleted.

3The existing data over the channel is deleted, and the connection is terminated, forcing the user to carry out the initial tasks from the beginning. This provides a security and trust factor for secure data transfer in the channel.

Algorithm:

P -> LAD

Loop:

NFC?

No: Repeat loop

Yes:

NFC-> STN

STN->S

S->C

Success? Yes:

LBP-> C

Yes ? : D-> PAY -> CD

No: A -> CD

Return NFC

P = Pos Device

STN = Synchronous Transmission Number

S = Channel sync

LAD = Local Authentication Database

C = Channel Establishment

CD = Channel Deletion

LBP = Line Burner Policy

Pseudocode:

```
print("Initializing POS device...")

print("Connecting to the internet...")

# Step 2: Activate the local authentication database.

print("Activating local authentication database...")

LAD = random.int(1000,9999)

while True:

    # Step 3: Check if the NFC is ready.

    nfc_ready = input("Is the NFC  ready? (Yes/No): ")

    if nfc_ready.lower() == "yes":
```

```
        break  # Proceed to the next step
    else:
print("NFC  not ready. Waiting...")
# Step 4: Generate and display the STN.
stn = LAD
print("Generated STN:",stn)
# Step 5: Synchronize STN to a secured channel and establish the connection.
if (stn == true )
print("Synchronizing STN to the secured channel...")
print("Establishing the connection...")
 else goto step 2.
# Step 6: Carry out authentication for unauthorized devices.
LBP()
{
int broadcast_message_reply
if(broadcast_message_reply ==1)
print("No Illegal device found")
else
print("Authenticating unauthorized devices...")
goto step 2
}
# Step 7: Request the user to send data via NFC.
print("Requesting user to send data via NFC...")
# Step 8: After payment is completed, delete the channel and terminate connections.
if payment == "yes":
    print("Deleting the channel and terminating connections.")
else:
    print("Payment not completed. Process aborted.")
   LBP()
```

STEP BY STEP APPROACH:

1) In the initial stages the POS device will be activated by connecting to the internet, making the local authentication database active to use. This will be responsible for sending and verifying the STN everytime.

2) Meanwhile the user must be ready with his NFC based mobile emulated card for contactless payment

3) As soon as the merchant starts the payment process the NFC method will be triggered and the first authentication step will start . The POS will generate and display the STN to sync to the secured channel ,ensuring only one user at a time .

4) After successful STN synchronization the connection will be established , if not then we need to start from step 1.

5) Next the POS will carry next authentication for verifying and resolving unauthorized devices over the air by Line Burner Policy .

6) After all successful validations the POS finally requests the user to send the data via NFC

7) After the payment is done the channel is deleted and connections are terminated.

VI. RESULTS

Below fig.6-fig.14displays the result of various samples taken from different scenarios. Particularly consisted of parameter like number of people present in surrounding, noises from various things. This included collecting data sample from Quiet environments consisting of experiment laboratories, Normal environment consisting of classroom with few students, Noisy environment consisting of auditorium and canteens with each of 3 attempts. It as seen that mostly in all environments the data was seen captured with unauthorized antenna. Resulting in rise of graph in 13.56 or similar range of megahertz frequencies.

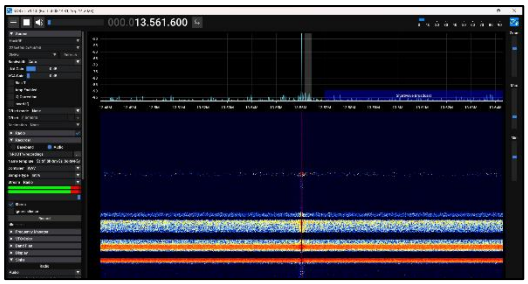

Figure 6 Result: Sample taken from Quiet environment 1

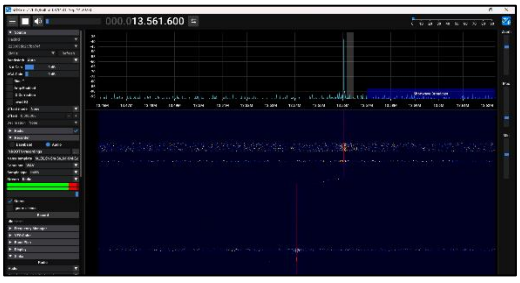

Figure 7 Result: Sample taken from Quiet environment 2

Figure 8 Result: Sample taken from Quiet environment 3

The above mentioned Fig. 6,7,8 represents the processes of signal capturing taking place in the quiet environment where there is no external echos as well as no electronic gadget present in the nearby perimeter. Hence one can notice a smooth graph with single rise around 13.56 Mhz frequnecies.

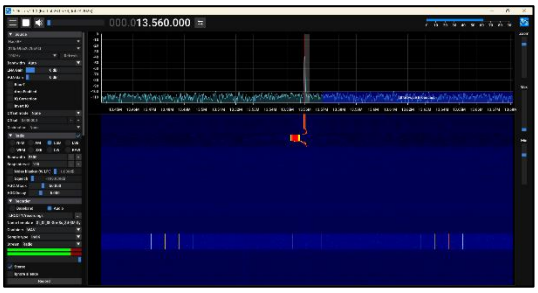

Figure 9 Result: Sample taken from Normal environment1

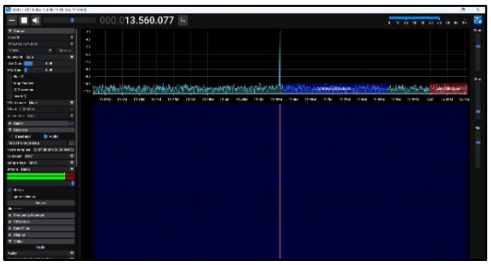

Figure 10 Result: Sample taken from Normal environment2

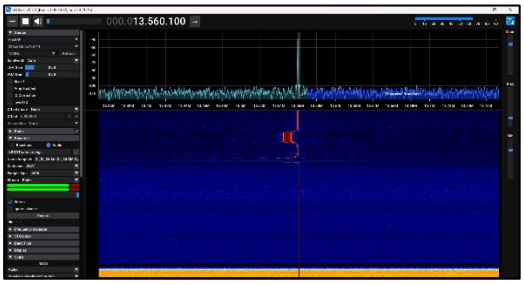

Figure 11 Result: Sample taken from Normal environment 3

The above mentioned Fig.9,10,11 depicts the procedure of capturing the NFC signals transmitted between the nfc device and the Pos machinein the normal envirnment ,wherein theparameters like people, sound, external echos and electronic devices were kept typical. Therefore the graph depicts avgerage rise in surrounding frequency apart from the 13.56 Mhz.

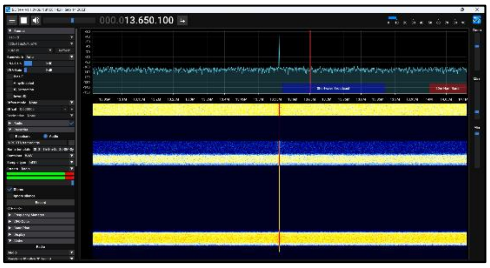

Figure 12 Result: Sample taken from Noisy environment1

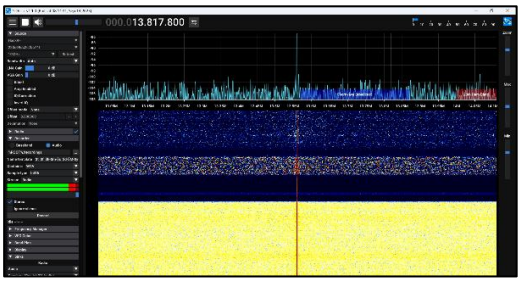

Figure 13 Result: Sample taken from Noisy environment2

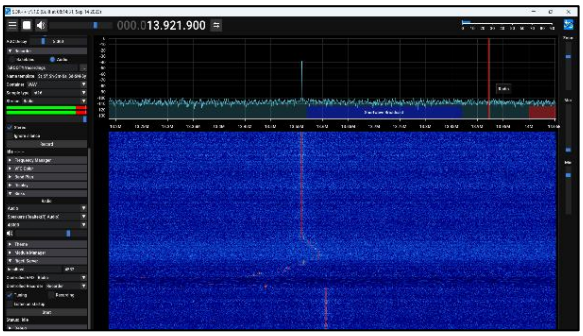

Figure 14 Result: Sample taken from Noisy environment3

The Fig.12,13,14 illustrate the capturing the data been transferred with NFC method in Noisy environment wherein the parameters were in high numbers. This resulted the graph scratchy and full of mixed highs and lows. It also shows the tracing NFC signals around the actual 13.56 Mhz frequency.

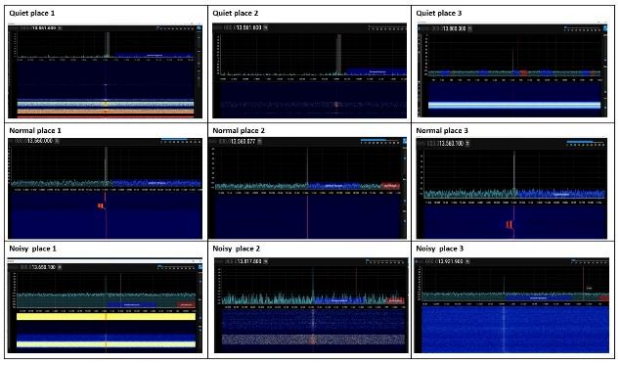

Figure 15 depicts the comparative analysis of the data signal capturing.

The Fig.15 displays the grid result of various samples taken from different scenarios. This particularly consisted of parameter like number of people present in surrounding, noises from various things. This included collecting data sample from noisy , normal and quiet environments with 3 attempts. It as seen that mostly in all environments the data was seen captured with unauthorized antenna. Resulting in rise of graph in 13.56 or similar range of megahertz frequencies.

SR	Sample Category	Jitter severity	Data captured
1	Quiet 1 [fig.6]	Very low	Yes
2	Quiet 2 [fig.7]	Very low	Yes
3	Quiet 3 [fig.8]	Low	Yes
4	Normal 1 [fig.9]	Moderate	Yes
5	Normal 2 [fig.10]	Moderate	Yes
6	Normal 3 [fig.11]	Moderately high	Yes
7	Noisy 1 [fig.12]	High	Yes
8	Noisy 2 [fig.13]	Very high	Yes
9	Noisy 3[fig.14]	High	Yes

Table.1 elaborates the pictorial representation of the data capturing process through various attempts and parameters.

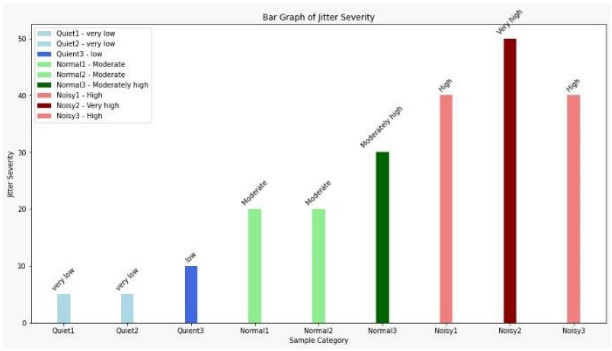

Figure 16 Illustrates the graphical representation of the jitter severity recorded during the signal capturing process.

The Fig.16 displays the graphical visualization of the jitter (echoes and random sound variations) captured while NFC tracking. The shades of Blue, Green and Red colours are used to show the severity of Quiet, Normal, Noisyenvironments respectively. The simple bar graph is used with minimum value set as 0 units and maximum value set to 50 units on Y axis and the X axis represents the different types of sample environments.

VII. CONCLUSION

The paper focuses on the newly proposed method for transferring the data over the secured channel establishment technique in NFC payments. Based on the several samples taken from various environments , parameters , it was observed that, existing NFC approach contains flaws that could result in data loss, cloning, or even emulation.. The new method will surely be helpful for seamless and secured data transfer in the future, not only in the field of payments and funds but also in technology evolution .

Future Scope

The proposed methodology would not only be crucial for NFC ,Contactless payments but also helpful for all the sensitive data transmission techniques that uses High Frequencies (HF) for data exchange over the air. This would result in secured data transmission for various purposes.

For example card based Parking system , IOT Smart grids, Access cards in companies ,public infrastructure like airports , metro stations, as well as in areas of confidentiality.

Acknowledgement

The Authors would like to express their gratitude towards the Computer Engineering department ,Vishwakarma Institute of Technology Pune for providing us the opportunity for conducting this research that ended with a fruitful outcome. His technical knowledge and assistance helped to overcome the obstacles. I would also like to thank “The Trident Lab”,Vishwakarma Institute of Technology Pune from lending their electronic devices.

REFERENCES

[1] Dong Yang and Qingxian Wang, "The study on the application of RFID- based mobile payment to the Internet of Things," 2011 International Conference on Multimedia Technology, Hangzhou, China, 2011, pp. 908-911, doi: 10.1109/ICMT.2011.6001856.

[2] R. Schamberger, G. Madlmayr and T. Grechenig, "Components for an interoperable NFC mobile payment ecosystem," 2013 5th International Workshop on Near Field Communication (NFC), Zurich, Switzerland, 2013, pp. 1-5, doi: 10.1109/NFC.2013.6482440.

[3] Garry Wei-Han Tan, Keng-Boon Ooi, Siong-Choy Chong, Teck-Soon Hew,

[4] NFC mobile credit card: The next frontier of mobile payment?, Telematics and Informatics, Volume 31, Issue 2,2014.

[5] C. Shuran and Y. Xiaoling, "A New Public Transport Payment Method Based on NFC and QR Code," 2020 IEEE 5th International Conference on Intelligent Transportation Engineering (ICITE), Beijing, China, 2020, pp. 240-244, doi: 10.1109/ICITE50838.2020.9231356.

[6] M. Al-Tamimi and A. Al-Haj, "Online security protocol for NFC mobile payment applications," 2017 8th International Conference on Information Technology (ICIT), Amman, Jordan, 2017, pp. 827-832, doi: 10.1109/ICITECH.2017.8079954.

[7] Francisco Liébana-Cabanillas, Sebastian Molinillo, Miguel Ruiz-Montañez, To use or not to use, that is the question: Analysis of the determining factors for using NFC mobile payment systems in public
[8] transportation, Technological Forecasting and Social Change, Volume 139, 2019
[9] N. El Madhoun, E. Bertin and G. Pujolle, "For Small Merchants: A Secure Smartphone-Based Architecture to Process and Accept NFC Payments," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 2018, pp. 403-411, doi: 10.1109/TrustCom/BigDataSE.2018.00067.
[10] R. R. Kanojia and S. Pathak, "Secured Vehicle Toll Payment System Using NFC," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 2018, pp. 1-6, doi: 10.1109/ICCUBEA.2018.8697638.
[11] Sriramulu Bojjagani, V.N. Sastry, A secure end-to-end proximity NFC-based mobile payment protocol,Computer Standards & Interfaces, Volume 66, 2019,ISSN 0920-5489.
[12] Z. Ahmad, A. M. Zeki and A. Olowolayemo, "Security Failures in EMV Smart Card Payment Systems," 2016 6th International Conference on Information and Communication Technology for The Muslim World (ICT4M), Jakarta, Indonesia, 2016, pp. 240-243, doi: 10.1109/ICT4M.2016.056.
[13] M. Pasquet and S. Gerbaix, "Instant payment versus smartphone payment: The big fight?,"2017 Third International Conference on Mobile and Secure Services (MobiSecServ), Miami Beach, FL, USA, 2017, pp. 1-3, doi: 10.1109/MOBISECSERV.2017.7886561.
[14] V. Dudykevych, O. Bakay and Y. Lakh, "Investigation of Payment Cards systems information security control," 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), Berlin, Germany, 2013, pp. 651-654, doi: 10.1109/IDAACS.2013.6663005.
[15] J. Liu, Y. Xiao, H. Chen, S. Ozdemir, S. Dodle and V. Singh, "A Survey of Payment Card Industry Data Security Standard," in IEEE Communications Surveys & Tutorials, vol. 12, no. 3, pp. 287-303, Third Quarter 2010, doi: 10.1109/SURV.2010.031810.00083.
[16] M. Pasquet and S. Gerbaix, "Fraud on host card emulation architecture: Is it possible to fraud a payment transaction realized by a mobile phone using an "Host Card Emulation" system of security ? Invited paper," 2016 Second International Conference on Mobile and Secure Services (MobiSecServ), Gainesville, FL, USA, 2016, pp. 1-3, doi: 10.1109/MOBISECSERV.2016.7440230.
[17] M. Pasquet and S. Gerbaix, "Fraud on host card emulation architecture: Is it possible to fraud a payment transaction realized by a mobile phone using an "Host Card Emulation" system of security ? Invited paper," 2016 Second International Conference on Mobile and Secure Services (MobiSecServ), Gainesville, FL, USA, 2016, pp. 1-3, doi: 10.1109/MOBISECSERV.2016.7440230.
[18] A. P. Abellon, C. J. Ariola, E. Blancaflor, A. K. Danao, D. Medel and M. Z. Santos, "Risk Assessments of Unattended Smart Contactless Cards," 2021 IEEE 8th International Conference on Industrial Engineering and Applications (ICIEA), Chengdu, China, 2021, pp. 338-341, doi: 10.1109/ICIEA52957.2021.9436788.
[19] A. K. Abdulwahab and W. M. El-Medany, "NFC Payments Security in Light of COVID-19 Pandemic: Review of Recent Security Threats and Protection Methods," 2021 International Conference on Data Analytics for Business and Industry (ICDABI), Sakheer, Bahrain, 2021, pp. 615-620, doi: 10.1109/ICDABI53623.2021.9655849.