SECURE PROTOCOL IMPLEMENTATION USING NEAR FIELD COMMUNICATION

Mr. Nikhil M. Shrangare, Prof. S.A.Joshi

Student, Pune University, Sinhgad College of Engineering, Vadgaon (BK), Pune, 411041.Maharashtra, India

Professor, Pune University, Sinhgad College of Engineering, Vadgaon (BK), Pune, 411041.Maharashtra, India

---

Abstract - ***NFC is one of the recent wireless communication technologies. Near field communication is technology for contactless short-range communication based on RFID (Radio Frequency Identification). So there is possibility of eavesdropping, data modification, data corruption, man-in-middle attacks. Solution on these threats is creating a secure channel. The proposed system protocols consider three different factor (Touch, Angle and Time) of user behavior to know the authenticity or authorization of users. In this processing phase, here the touch signals are cleaned for some irregularities via cubic spline smoothing process. Then after the processing, the extracted information represented in vector and stored in database. Here the angle of user touch gets calculated. Also the counter is set for time parameter in NFC devices. All parameter are stored into database. The comparison can be done between stored feature of user and recent feature of user for validation. If user is valid or authenticated then file get transferred to authorized user device. At the end secure communication with NFC device is successful.***

Key Words: Near Field Communication (NFC), Security, RFID, NFC tags, etc.

1. INTRODUCTION:-

Near field communication (NFC) is a technology for contactless short-range communication. Based on the radio frequency identification (RFID), it uses magnetic field induction to enable communication between electronic devices. The number of short- range applications for NFC technology is growing continuously, appearing in all areas of life. Especially the use in conjunction with mobile phones offers great opportunities. One of the main goals of NFC technology has been to make the benefits of short- range contactless Communications available to consumers globally. The existing radio frequency (RF) technology base has so far been driven by various business needs, such as logistics and item tracking. While the technology behind NFC is found in existing applications, there has been a shift in focus most notably, in how the technology is used and what it offers to consumers. With just a point or a touch, NFC enables effortless use of the devices and gadgets we use daily. Here are some examples of what a user can do with an NFC mobile phone in an NFC-enabled environment:

1] Download music or video from a smart poster.
2] Exchange business cards with another phone.
3] Pay bus or train fare.
4] Print an image on a printer.
5] Use a point-of-sale terminal to pay for a purchase, the same way as with a standard contactless credit card.
6] Pair two Bluetooth devices.

2. LITERATURE SURVEY:-

2.1 Principle of NFC technology

The NFC interface can operate in two different modes: active and passive. An active device generates its own radio frequency (RF) field, whereas a device in passive mode has to use inductive coupling to transmit data. For battery-powered devices, like mobile phones, it is better to act in passive mode. In contrast to the active mode, no internal power source is required. In passive mode, a device can be powered by the RF field of an active NFC device and transfers data using load modulation. Hence, the protocol allows for card emulation, e.g., used for ticketing applications, even when the mobile phone is turned off. The communication between two active devices case is called active communication mode, whereas the communication between an active and a passive device is called passive communication mode [2]

Device A	Device B	Description
Active	Active	When a device send data it generates an RF field. When waiting for data a device does not generate an RF field. Thus the RF field is alternately generated by device A and device B
Active	Passive	The RF field generated by Device A only
Passive	Active	The RF field generated by Device B only

Figure 1: Communication Modes

2.1.1 Advantages and Limitation of NFC:-

Advantages of NFC:-
1] Quicker connections.
2] Easy to use, only requires the click of a button.
3] They are compatible with existing RFID structures.
4] Cost efficient for the average customer.

Disadvantages of NFC:-
1] Only works in short ranges
2] Low data transfer rate
3] Can be costly for merchant companies to initially adopt
The technologies [4].

2.4 Security threats in NFC:-

NFC is a wireless communication interface it is obvious that eavesdropping, data corruption, phishing, data modification, man in middle attack is an important issue.

1) Eavesdropping:- NFC is wireless communication interface it is understandable that eavesdropping is an significant topic. When two devices communicate using NFC they use RF waves to commune with each other. An attacker can of course make use of an antenna to also receive the transmitted signals.
2) Data corruption:-
Instead of presently listen an attacker can also try to alter the data which is transmit using the NFC interface. In the simplest crate the attacker just needs to disturb the message such that the receiver is not able to know the data sent by the other device.

3) Phishing:-
Phishing attacks could easily be performed by modifying or replace tags.

4) Data modification:- In data modification the attacker wishes the receiving device to in fact receive some valid, but manipulated data.

5) Data Insertion:- This means that the attacker insert messages into the information exchange between two devices. But this is just possible, in case the answering device wants a very long time to answer.

6) Man-in-the-Middle-Attack:- Two party which wish for to talk to each other , Alice and Bob are trick into a three party conversation by an attacker Eve. Alice and Bob must not be aware of the fact that they are not talking to each other, but that they are both sending and receiving data from Eve. Such a setup is the classical Threat in unauthenticated key agreement protocols like Diffie-Hellmann protocol. Alice and Bob want to agree on a secret key, which they then use for a secure channel. However, as Eve is in the middle, it is possible for Eve to establish a key with Alice and another key with Bob. When Alice and Bob later use their key to secure data, Eve is able to eavesdrop on the communication and also to manipulate data being transferred.

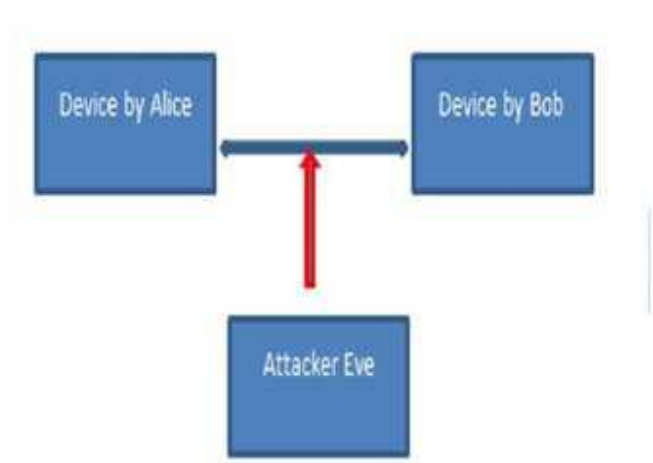

Figure 2: Man-in-the-Middle-Attack

2.5 Comparison with other Technologies:-

1) NFC and RFID Basically, the technologies Radio Frequency Identification and Near Field Communication use the same working standards. However, the essential extension of RFID is the communication mode between two active devices. In addition to contactless smart cards (ISO 14443), which only support communication between powered devices and passive tags, NFC also provides peer to-peer communication. Thus, NFC combines the feature to read out and emulate RFID tags, and furthermore, to share data between electronic devices that both have active power [8].

2) Comparison with Bluetooth and Infrared Compared to other short-range communication technologies, which have been integrated into mobile phones, NFC simplifies the way consumer devices interact with one another and obtains faster connections. The problem with infrared, the oldest wireless technology introduced in 1993, is the fact that a direct line of sight is required, which reacts sensitively to external influences such as light and reflecting objects. The significant advantage over Bluetooth is the shorter set-up time. Instead of performing manual configurations to identify the others phone, the connection between two NFC devices is established at once (<0,1s). Below figure points out these different capabilities of NFC, Bluetooth and infrared. All these protocols are point-to-point protocols. Bluetooth also supports point-to multipoint communications. With less than 10 cm, NFC has the shortest range [8]. This provides a degree of security and makes NFC suitable for crowded areas. The data transfer rate of NFC (424 kbps) is slower than Bluetooth (721 kbps), but faster than infrared (115 kbps). In contrast to Bluetooth and infrared NFC is compatible to RFID.

	NFC	Benefits of NFC	Bluetooth	IrDa
Network Type	Point-to-point	Easy set-up, pairing = bringing close	Point-to-multipoint	Point-to-point
Range	<0.1 m	Safe, suitable for crowded areas	10 m	1 m
Speed	424 kbps (1Mbps coming)		721 kbps	115 kbps
Set-up time	<0.1 s	Fast transactions e.g. for public transport	6 s	0.5 s
Modes	Active-active, active-passive	Reader mode and card-like mode	Active-active	Active-active
Compatible with RF ID	Yes	Can work with existing infrastructure	No	No
Costs	Low	Affordable for most devices	Moderate	Low

Figure 3: Comparison NFC with other Technologies.

3. PROPOSED SYSTEM:-

We propose to use physical parameter such as touch, angle, time as password the touch parameter is basically calculated keeping X,Y coordinates and angle parameter is calculated with axis of rotation and finally time parameter is time taken by performing touch ,angle activity .

3.1 Overview:-

The system is proposed to provide security to NFC devices. It consists of two phases:

(1) Acquisition:- it collect information and stores it in repository
(2) Recognition:- that reads from the interaction files, and classifies the user as imposter or genuine, to identify user valid or invalid .

3.2 Architecture:-

The architecture is shown in Figure 3.1. It consists of three modules:
(1) Information collection:- it collects information such touch, time, and angle from user
(2) Acquisition: - it collects information and stores it in repository
(3) Validation: - it verifies the user validity. If is user valid then we can transfer file Otherwise not.

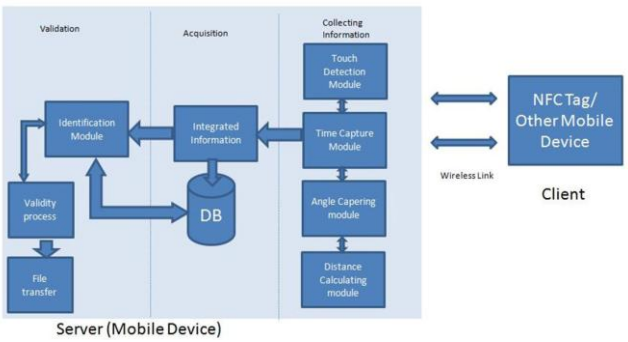

Figure 4: Block diagram

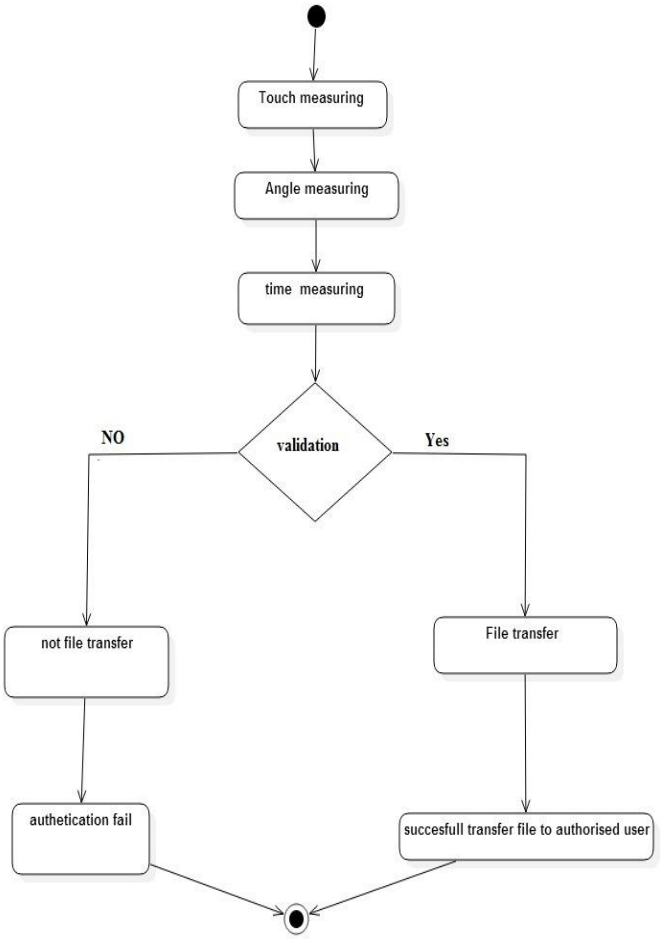

Fig.ure 5: flow diagram

3.3 Modules:-

3.3.1 Information collection:-

it collect information from user such as touch of user, angle of touch , finally time parameter is time taken by performing touch ,angle activity. This collected information will be further used for validation.

3.3.2 Acquisition:-

This phase considers four different factors of user which are touch, time, angle and distance. These factors show the behavior of a particular user which can vary from one to Other during communication. These factors can be used to distinguish between authorized and unauthorized users. Every time when user interacts with system protocol keep the information for further use.
1) Touch can be different for different users.
2) Time taken by user to input.

3) Angle could be different during touching NFC enabled devices.

3.3.3 Validation:-

This module is used for verification of user authentication the recognition phase uses the User interaction data and data stored in the repository. The data in the database and starts a feature extraction procedure, by applying some mathematical operations to decides to accept or reject the user as genuine. In this phase, the global sets of extracted features are used in an algorithm that selects a set of best features for each user, using the equal error rate as performance measure.

3.3.3.1 Cubic Spline:-

Real world numerical data is usually difficult to analyze. Any function which would effectively correlate the data would be difficult to obtain and highly unwieldy. The idea of the cubic spline was developed. Using this process, a series of unique cubic polynomials are fitted between each of the data points, with the stipulation that the curve obtained be continuous and appear smooth. We will only discuss splines which interpolate equally spaced data points, although a more robust form could encompass unequally spaced points. The fundamental idea behind cubic spline interpolation is based on the engineers tool used to draw smooth curves through a number of points. This spline consists of weights attached to a flat surface at the points to be connected. A flexible strip is then bent across each of these weights, resulting in a pleasingly smooth curve. The mathematical spline is similar in principle. The points, in this case, are numerical data. The weights are the coefficients on the cubic polynomials used to interpolate the data. In cubic spine process There are three phases for information extraction such as

1) First phase:- is pre-processing phase in this signals are cleaned from some irregularities with the help of cubic spline smoothing process.

a) On each interval (a,t1), (t1,t2), , (tn,d), g is a cubic polynomial

b) Vectors A, B, C, D are statistically analyzed, and 5 values are computed per vector: the minimum, maximum, average, mean, standard deviation, and range (maximum - minimum). In touch parameter different touch of user (x,y), (x1,y1),(x2,y2),(x3,y3),(x4,y4). Then plotting a curve and taking average of that point

$$X=\frac{x1+x2+x3+x4}{4}$$

$$Y=\frac{y1+y2+y3+y4}{4}$$

For time feature, counter is set. The time counter starts when the touch feature completed.

Then the counter will start measuring the time and stored in database for further

Use in NFC devices.

2) The second phase:- concerns the extraction of spatial and temporal information which

is in the form of intermediate data representation vectors.

3) A third and final step:- generates the features by exploring some statistical information

or data from These vectors, and other general properties of the patterns.

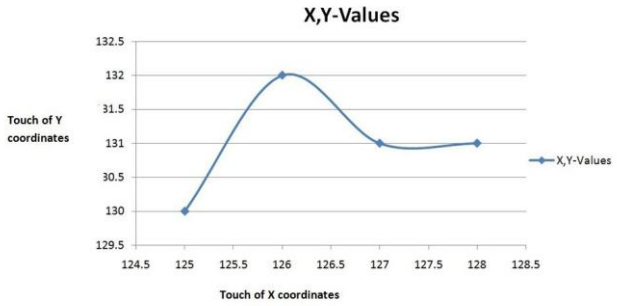

Figure 6:. x, y coordinate of touch

4. RESULTS AND DISCUSSIONS:

The Proposed system we use to NFC enabled devices for secure communication. Here a device collect information about touch detection module, angle detection module and time measuring module. collected information is used for validation. only valid user can transfer file to another device.

4.1 True positive False positive:-

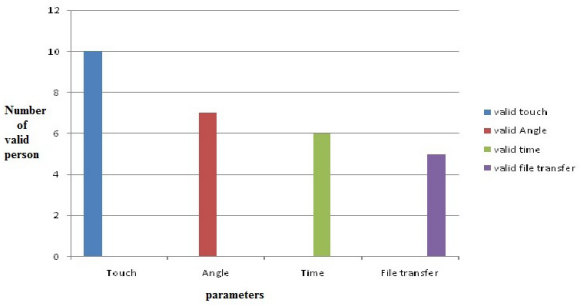

Figure 7: No. of validation person

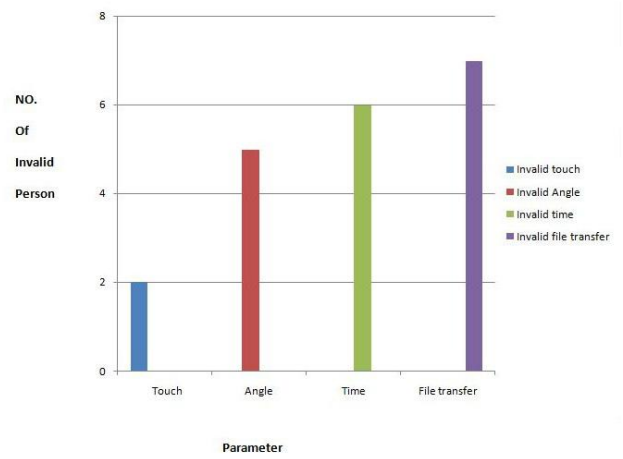

Figure.8: No. of Invalidation person.

4.2 Time for transfer file:-

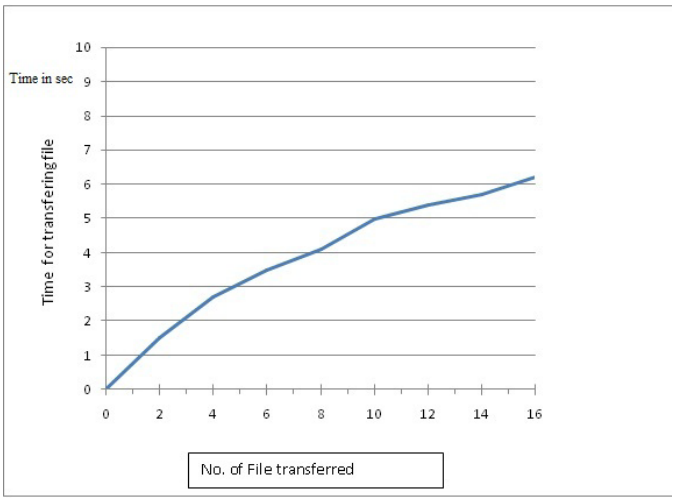

Figure 9: Time for transfer graph.

5. CONCLUSION AND FUTURE WORK

CONCLUSIONS:-

Near Field Communication is an efficient technology for communications with short ranges. It offers an intuitive and simple way to transfer data between electronic devices. This stage concludes that, the proposed system authenticates the user based on touch, time, and angle parameters of the user input. Combination of the above types of input parameter makes the system secure for File transfer from one NFC device to another NFC device.

Future work:-

In future work we will be adding more parameters for making system more secure such as distance parameter. In also we check fuzziness of the user inputs and try to implement a new system.

REFERENCES

[1] Gautam, Vinay, and Vivek Gautam. User Behavior Based Enhanced Protocol (UBEP) for Secure Near Field Communication.

[2] Paus, Annika. Near field communication in cell phones. Chair for Embedded Security
24 (2007).

[3] Eun, Hasoo, Hoonjung Lee, and Heekuck Oh. Conditional privacy preserving security
protocol for NFC applications. Consumer Electronics, IEEE Transactions on 59.1 (2013): 153-160.

[4] Hussien, Hanady, and Hussien Aboelnaga. Design of a Secured E-voting System. Computer Applications Technology (ICCAT), 2013 International Conference on. IEEE, 2013.

[5] Roland, Michael, Josef Langer, and Josef Scharinger.Security vulnerabilities of the NDEF signature record type. Near field communication (NFC), 2011 3rd International Workshop on. IEEE, 2011.

[6] Mantoro, Teddy, and A. Milisic. Smart card authentication for Internet applications using NFC enabled phone. Information and Communication Technology for the Muslim World (ICT4M), 2010 International Conference on. IEEE, 2010.

[7] Plos, Thomas, et al. Security-enabled near-field communication tag with flexible architecture supporting asymmetric cryptography. Very Large Scale Integration
(VLSI) Systems, IEEE Transactions on 21.11 (2013): 1965-1974.

[8] Konidala, Divyan M., et al. Security Framework for RFID-based Applications in Smart Home Environment. JIPS 7.1 (2011): 111-120.

[9] Haselsteiner, Ernst, and Klemens Breitfu. Security in near field communication (NFC). Workshop on RFID security. 2006.