International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 5, May 2016

Design and Implementation of Safe Multifactor Verification for Customer Payment Method Using NFC

Sasikumar Gurumurthy
Sree Vidhyanikethan Engineering College (Autonomous), Tirupati, Andhra Pradesh, India.
mithrangurugsk@gmail.om

Abstract: **The latest trend of making financial transactions is done by the use of cards or internet banking. A person may have multiple bank accounts across several banks which makes it difficult for him/her to manage the transactions i.e. he/she either has to carry several cards or use a bunch of bank websites for accomplishing his/her transaction purposes. This situation demands the need of a simple, secure and hi-tech system for achieving the purposes of making transactions. We propose such a system that uses the latest technologies like NFC and multifactor authentication which can be used on any NFC enabled Smartphone. The multi factor authentication system uses a 4-digit PIN as the knowledge factor, an NFC enabled Smartphone, instead of cards, as the possession factor and the face of the user as the inherence factor for the purpose of authentication. The proposed system which can be implemented as cross-platform mobile application, not only allows the user to make secure transactions, but also allows him/her to make transactions from his/her multiple accounts.**

Keywords— **Near Field Communication; NFC; Multifactor; Mobile computing; Security; Peer-to-peer; Authentication, Consumer Storage,**

I. INTRODUCTION

Nowadays, online bank transactions have become a routine in day to day life of mankind. Evidently, there is a very high need to provide high security for these online transactions. And at the same time, man also likes the simplicity of the usage. Our system is one which provides security as well as the simplicity, to online bank transactions. This is achieved by the implementation of Multifactor Authentication for the purpose of authentication of transactions and Near Field Communication (NFC) feature in smartphones for providing the ease of use to the users for making bank transactions. Near field communication (NFC) is a new wireless communication technology that is becoming more popular in high end phones[6]. It came up from combined concept features of contactless identification (Radio Frequency Identification - RFID) and mobile phone technology. Even though NFC was officially released in 2004 by Philips, Nokia and Sony. it is gaining more popularity just recently. NFC is used with a wide variety of devices like smartphones, laptops, desktops, printers, Televisions and other consumer electronics. NFC provides users with many kinds of services like payment, advertisements, file sharing, etc. Lately, NFC is making a bang in electronic devices. Across the globe, many organizations/companies are undergoing research on NFC and are forming lots of NFC focused projects. A common ticket or a coupon are issues of past. Nowadays, even mobile phones can be used as transport tickets, virtual vouchers or hypermarket loyalty/reward cards. NFC technology allows three modes of operations: read/write mode, peer-to -peer mode, and card emulation mode[6]. Then, a device with NFC can act as a NFC tag emulator or a tag reader[6].

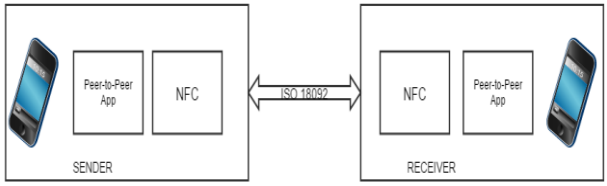

Fig 1: A typical NFC peer-to-peer model

The concept of Multi-factor authentication (MFA) is a specific methodology to authentication process which needs two or more of the three independent authentication factors required for authentication i.e. a knowledge factor, a possession factor and an inherence factor [4]. The knowledge factor is an information entity known only to the user. The possession factor is an entity that is possessed only by the user. And finally, the inherence factor is a

thing that the user only is. After submission of these factors, each factor must be confirmed by a particular party (can be other users) or by the system for the authentication to occur.

Multi-factor authentication is not exactly a new concept. It has been in use for quite a period. For example, when a bank customer visits a local Automated Teller Machine (ATM) for withdrawing money, the possession authentication factor is the physical ATM card which customer inserts into the ATM machine (something the user has). The knowledge factor for authentication is the PIN which the customer enters through the keypad (something the user knows). Without the successful verification of both of these factors, the process results in failure. This example shows the basic concept of most multi-factor authentication systems i.e. the combination of a knowledge factor and a possession factor [4].

Multi-factor authentication is sometimes confused with "strong authentication"[4]. Nonetheless, "strong authentication" and "multi-factor authentication" are basically different processes. Providing multiple answers to challenge/security questions may be considered strong authentication but, unless the process also accepts and checks "an entity user has" or "something that the user is", it cannot be regarded as multi-factor authentication [4].

II. LITERATURE SURVEY

Two-factor authentication provides unmistakable identification of users through the method of blending of two distinct entities. These distinct entities may be any information a user knows, an entity that a user has or something that cannot be separated from the user. A good example of this from everyday life was discussed already, i.e. the withdrawal of money from an ATM. Only the correct combination of a bank ATM card (something that a user has) and a secret PIN (Personal Identification Number, i.e. something that the user knows) permits the transaction to proceed [3]. Today, simply having a strong password on your account won't cut it. Time to time we hear about many gangs of hackers and crackers breaking into our favorite cloud services and stealing a part or sometimes, even entire databases of login credentials and other private data/information (Facebook, Twitter, LinkedIn, Dropbox and Evernote have all had struggles with this in past years). Armed with this kind of information, these people have very light jobs taking over our accounts. As an outcome of this, many companies are adding two-factor authentication, also known as 2FA, to improve the security of user accounts by adding an extra authentication layer[3]

2FA = something you know + something you have

When 2FA is enabled on any of our accounts, we need to enter our login credentials (password as something we know) and then an additional input to prove we really are who we say we are. This might be a single-use password or an OTP (One Time Password) sent to us via a text messages/SMS or an Electronic-mail, or it can be an authentication code generated by an app on our smart phone. The main objective is that even if anyone takes possession of our username and password, he/she will not be able to login without that particular second form of authentication. A very good familiar example of this is the 2 Step Verification used by Gmail. This optional service sends a verification code to the user as SMS and the user is required to type that code so as to sign in to his account[3].

Disadvantages of 2FA:

- It mostly needs an independent device[9].
- Users are required to replace hardware dependent tokens when its battery dies out (probably every 4-7 years)[9].
- We are required to link our cell phone numbers with the organization/company (say, a bank or E-mail service) and update them in case of changes[9].
- Transmission of the passwords/OTP is highly dependent on the cell phone network coverage. There might be some delays if there exist large cell phone network traffic[9].
- We may have to pay extra charges if we use services across seas. The extra charges will be based on your cell phone carrier/plan[9].

The fact that every system will break at some point should be considered here. People lose/forget their keys/passwords and/or smart cards or accidentally ruin them in unintended ways. So we can conclude that the system is not secure enough.

For avoiding this drawback we have started using multifactor authentication. Multiple authentications are commonly found in authentication process of computer/online users, where basic authentication requests entity inputs, presenting multiple evidences of its identity to a second entity. Authentication through two independent/distinct factors paves way to decrease the probability that the client presents false evidence of his/her identity in both of the independent processes.

The number and independence of the factors chosen for authentication is very crucial, as more the independent factors, higher the probability that the identity of requesting client is indeed true. However, we should

consider the reliability of the chosen factors to provide truthful authentication, rather than the number of factors used.

Two-factor authentication involves the use of two out of the three independent authentication factors. The following are the three factors:

- Something only the user knows (e.g., password, PIN, pattern)[4];
- Something only the user has (e.g., ATM card, smart card, mobile phone)[4]; and
- Something only the user is (e.g., biometric characteristic, such as a fingerprint)[4].

Knowledge factor ("something only the user knows") is the normally used form of authentication i.e. the user has to prove his identity with a secret string/data in order to get authenticated. A password is a secret set of characters which is used for the purpose of proof of identity of a user. Many multi-factor authentication techniques rely on password as one factor of authentication [4]. A Personal Identification Number (PIN) is a secret numeric password which is commonly used in ATMs.

Credit and ATM cards don't store the PIN or CVV value in the magnetic stripe of the card. Rather, they are just associated with the PIN. This tells us that a PIN is not a part of "something the user has", i.e. possession factor.

A pattern factor is a regular or stochastic sequence or array of sets of information, used for authenticating the users [4]. For example, pattern factor based authentication may be presented by the bearer to a sensor unit to get authenticated by a processing [4].

Nowadays, we are using Biometric based multifactor authentication to make system more secure[10]. This multi-factor authentication mechanism requires PIN, with biometric authentication such as a fingerprint scan or facial recognition scan [1]. When the user registers with a service they provide a scan of the appropriate biometric (such as a fingerprint or facial scan) as a reference point for the authentication server to compare to[1]. When the user is getting authenticated by the authentication server, user provides a PIN or password along with their biometric scan at the time of registration or enrolment. The authentication server validates both the PIN/password and the biometric scans, and based upon outcome of this, server grants or denies access to the user. A proper implementation of this authentication system is proven as an extremely secure method of multi-factor authentication [10].

Near Field Communication (NFC) allows to exchange the data between two devices which are placed within a few centimeters of each other[8]. For this to happen, both the devices must be armed with an NFC chip [8]. In the real world, there are to ways to implement this work.

- Two-way communication: This involves two devices that can be able to do both read and write. For example, by using NFC, you can operate two Android devices together for transferring data like contacts, photos,links[8].

- One-way communication: Here, a powered device (like a phone, commuter card terminal or credit card reader,) reads and writes to an NFC chip. So, when you tap your credit card on the credit card reader, the NFC-powered terminal subtracts money from your balance written to the card[8].

Apple Pay, the latest technology of Apple implemented in iPhone 6 uses NFC for serving its purpose [8].

Now, the current mobile banking systems use a simple password or PIN for making transactions, which can be risky. Also, to make a transaction to your friend's account, you need his account details or at the least his Mobile Money Identification (MMID) Number.

Using a technology like NFC, we can simplify the whole process of transaction to simply tapping your phone with your friend's phone. Of course, we take the situation when he or she is beside you.

Summing up, we propose a system which uses Biometric based multifactor authentication for authentication purpose and NFC to simplify the process of transaction provided the payer and payee are nearby.

III. PROPOSED SYSTEM

The proposed system uses Biometric based multifactor authentication for the purpose of authentication [1][10]. The knowledge factor, as in most cases, is a 4 digit PIN; the possession factor is a smartphone with an NFC chip; and the possession factor is the face of the account holder which is recorded using camera of the phone at time of registration.

Fig 2: Proposed System

The user who wishes to send the payment opens the app on his phone and enters the payment amount he wishes to transfer. The phone, then, on tapping with receiver's phone, fetches the receiver's details through NFC. On confirmation from the sender, the app now checks for the face of the sender and verifies with the face which was registered. On success, the user is now required to enter his secret 4 digit PIN whose successful authentication completes the transaction. The working is shown as a flowchart in Fig. 3.

To stay protected against attacks from malicious software and crackers, the technology of NFC is uniquely designed to be isolated from the rest of functionalities of the phone and this way, only a single application on the phone would be capable of approving/declining a transaction. This unique design makes near field communications safer.

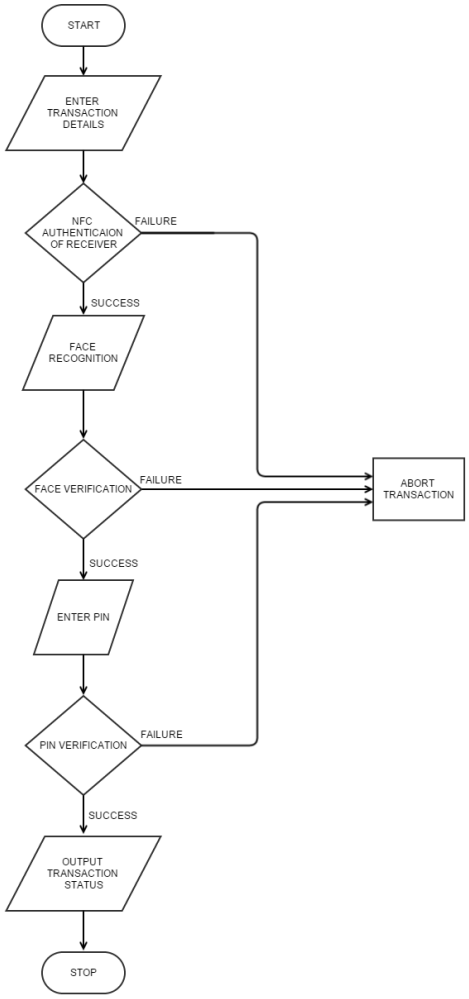

Fig 3: Flowchart of the system

IV. SYSTEM DESIGN

The proposed system consists of a onetime registration phase when the user uses the app for the first time and then he will be directed to a page where he can choose between various options such as send or receive payments and settings page.

In the first phase of registration page, the user is required to enter his name and other basic details along with his bank account number, bank, branch and IFSC. The next phase records the face of the user. This face will be used as the reference for future authentication purposes.

The user's home page consists of menu options to send or receive payments and a settings menu. On choosing the send option, he will be redirected to a page

where he is required to enter payment details such as the amount, remarks, etc. The receive option leads the user to a page where he is just required to enter his PIN for the purpose of receiving payments. The settings page consists of his account details. The user may edit or even add a new bank account which he can choose between before sending payment.

The NFC functionality is invoked when the user submits the details in the send page. On confirming the NFC receiver by the user, the user's face is checked against the one which was registered on whose successful comparison, the PIN is demanded from the user. On successful authentication, the online payment is made from the sender's account to the receiver's account.

As we require the app to be used in multiple platforms, we have used web technologies such as HTML5, CSS3 and JavaScript to develop the system.

V. IMPLEMENTATION

For implementing the functionalities of the system, we are using some modules which are described in this section.

The first module involves the registration phase. The module stores the information given by the user during the time of registration (such as name, account no., bank, branch, email id, face, etc.) and uses the stored information so as to use them for authentication purposes which is done in the other modules. It is also to be noted that the registration is required only at the first run of the app. Otherwise the user is redirected to a home page where he can choose whether to receive or make payment. This is illustrated in Fig 4.

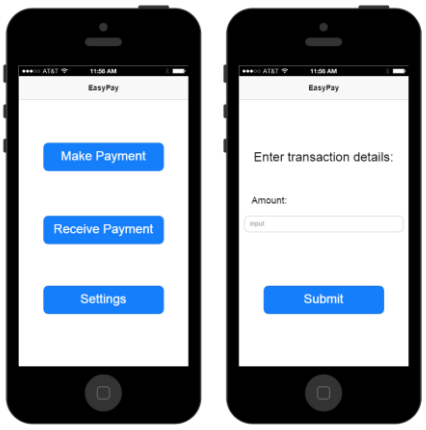

Fig 4: Home Page *Fig5: Entering Details*

This module also includes the process of entering the transaction details by the sender (see Fig 5).

The second module handles the messages shared between the sender and receiver phones through NFC. When the user submits the transaction details, the app indicates that it is waiting for the user to tap his phone with receiver's NFC enabled phone (see Fig 6). As soon as the phones are tapped, the sender is required to confirm the details of the receiver as well as the transaction. This is shown in Fig 7.

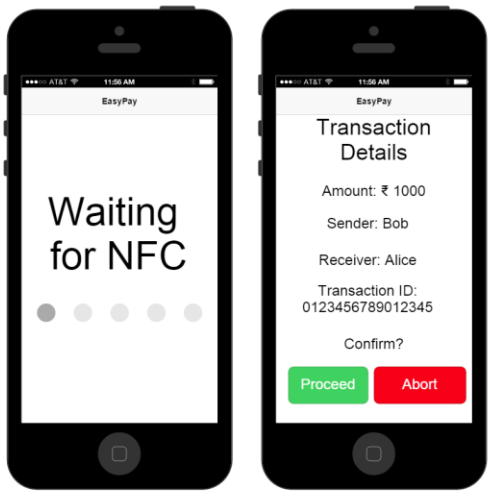

Fig 6: Waiting for NFC *Fig 7: Transaction Confirm*

The transaction will proceed only if it is confirmed by the sender.

When the receiver is confirmed by the sender, the next module comes into action which is Face Recognition.

The front camera is used for recognizing the face of the user and is compared with the registered face for authentication (see Fig 8).

Fig 8: Face Recognition *Fig 9: Entering PIN*

If the face authentication is successful, our final module executes. This module requests the user to enter a 4 digit PIN with which he registered initially. The PIN authentication process is also done in this module. If the PIN entered is correct, then the transaction is committed. This is shown in Fig 9.

The details of the committed transaction are displayed as a result to both sender and receiver. Transaction status in the output states whether the transaction was successful or not. Other details of the transaction such as amount that was transferred, name of the sender, name of the receiver and the transaction ID from bank are also displayed in the final output. This is illustrated in Fig 10.

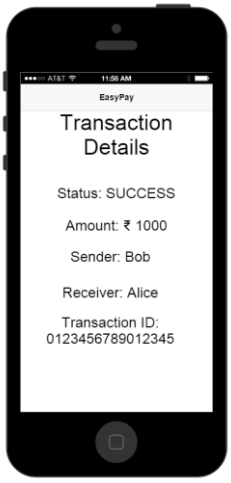

Fig 10: Transaction Result

For the purpose of Face Recognition, an Access Provider Interface (API) provided by Mashape[5]. For the purpose of NFC, a Javascript NFC library is used provided by Mopius and W3[7].

VI. CONCLUSION & FUTURE SCOPE

This system offers good security as well as simplicity for the user to make online transactions to others who are within vicinity. The face recognition along with the PIN and the smartphone (i.e. Three Factor Authentication) ensures the impenetrability of the system. NFC security modules within itself ensure the security of the transaction after tapping the phones with each other.

The future works that can be done include improving security of face recognition. For instance, showing a picture of the user in front of the camera should not be successfully authenticated by the system. Also, facial expressions may be detected and should not allow transactions if the user looks scared or threatened. Efficiency of managing multiple accounts will always have scope for improvement.

Other works include development means. That means the app can be made more efficient by building native apps for each platform so that it is guaranteed to have no errors and to ensure smooth functionality.

REFERENCES

[1]Al-Assam, Sellahewa and Jassim, "On Security of Multi-Factor Biometric Authentication", IEEE 5th

International Conference for Internet Technology and Secured Transactions, London, UK, 2010.

[2]Shinde Swapnil K, Patil Yogesh N and Godase Avinash P, "Secure Web Authentication by Multifactor Password a New Approach", International Journal of Software and Web Sciences, ISSN (Online): 2279-0071, pp. 58-62, 2013.

[3]Wikipedia"Two-factorAuthentication",[online]. Available:http://en.wikipedia.org/wiki/Two_factor_authentication

[4]Wikipedia, "Multi-factor authentication", [Online].Avilable:http://en.wikipedia.org/wiki/Multi-factor_authentication.

[5]Mashape, "Face Recognition API", [Online]. Available: https://www.mashape.com/lambda/face-recognition

[6]Monteiro, Rodrigues, Lloret, "A Secure NFC Application for Credit Transfer Among Mobile Phones", IEEE 978-1-4673-1550-0/12, 2012.

[7]Mopius, "HTML5 Loves NFC", [Online]. Available:http://www.mopius.com/html5-loves-nfc/.

[8]Profis S, "Near Field Communication", [Online].Available:http://www.cnet.com/how-to/how-nfc-works-and-mobile-payments/

[9]"Two factor Authentication". Available: http://www.mas.gov.sg/moneysense/understanding-financial-products/investments/consumer-alerts/understanding-two-factor-authentication-and-transaction-signing.aspx.

[10]"Biometric-based multi-factor authentication". Available:http://www.asd.gov.au/publications/csocprotect/multi_factor_authentication.htm