SECURED FRAMEWORKS FOR POCKET SMARTCARDS

Dhawal Hemane
(School of Electrical Engineering)
MITAOE
Pune,India
ddhemane@mitaoe.ac.in

Shubham Kotkar
(School of Computer Science and Technology)
MITAOE
Pune,India
sskotkar@mitaoe.ac.in

Kapil Khairkar
(School of Computer Science and Technology)
MITAOE
Pune,India
kvkhairkar@mitaoe.ac.in

Shubham Kotgire
(School of Computer Science and Technology)
MITAOE
Pune,India
sbkotgire@mitaoe.ac.in

Mrs. Jayshree Kulkarni
(Department of Computer Science and Technology)
MITAOE
Pune,India
japatil@it.maepune.ac.in

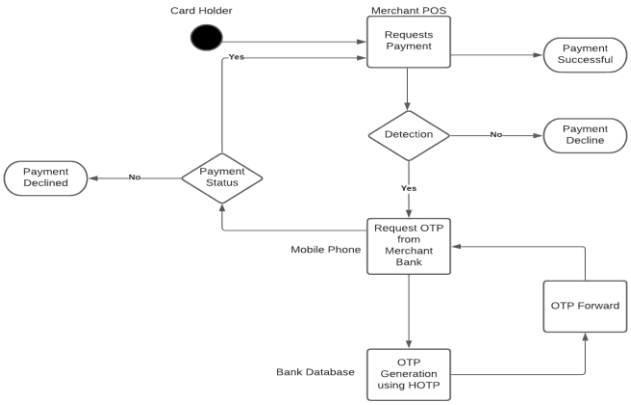
Abstract- 'Digitization' changed the banking system in all aspects to provide customer eased services. Presently most of the bankers are issuing contact less cards, so that customer can do the transactions easily just by tapping a card to the machine using NFC technology. However, due to the nature of airborne communication, contactless cards are vulnerable to a variety of security threats, including card cloning, data removal, and card collision. Hence customers are suffering from fraud payment, resulting in financial loss over time. In order to provide a critical solution to fraudulent contactless card payments, we must concentrate on complicated capital management security, as attackers are undoubtedly devising new ways to get into the system. This paper basically enhances the security level in contactless cards by using two methodologies. First is, one-time password sent to cardholder mobile for authentication. Secondly, by inserting biometric sensors in the card circuit before doing transaction. We propose as we humans have electrons in our body, the circuit will be completed once the card holder holds the card to complete the transaction. These two methodologies can be used to authenticate the end user that is the card holder and if OTP or light weighted chip permits then further transactions are proceeded else transactions can be declined.

Keywords— near-field communication, point of sale, OTP Generation, BiometricAuthentication

1. INTRODUCTION

As in modern era people are suffering through fraud payment which arise to the loss of trust on bankthat allow fraud transaction and also confined under explosion in payment causing financial loss over a period of time. So, to provide a vital solution to fraudulent in credit card payment we need to work upon complex capital management security as the attackers are certainly crafting new mode of attacks for intruding the system. In this a past credit card transactions with knowledge about the ones that turned out to be fraud is part of the Credit Card FraudDetection Problem. This System is then utilized to determine whether a new transaction has occurred is it a fraud or not? Our goal is to find every single one of them. Fraudulent transactions are minimized while erroneous transactions are minimized types of frauds.NFC technology is based on Radio Frequency Identification (RFID) technology. Security and privacy issues of RFID communication, and in particular NFC, have been studied intensively in the literature. Contactless cards are always on and a malicious reader in the proximity of such a device is able to trigger a response from the card, without the user's awareness. More security attacks include different types of relay attacks such as Man-in-The-Middle and Mafia attacks.

2. Block Diagram



2.a. Block Diagram

3. Literature Survey

[1] Explain software-based relay attack in anexisting mobile contactless payment system is examined in this research. The credit card payment mechanism of Google Wallet is examined in detail. They discuss their prototype relay system, which they successfully used to mount a software-based relay attack on Google Wallet. They explore the attack's viability and threat potential, as well as many potential remedies. In a short, this study discusses current developments in contactless smartcard and secure element relay threats. It also demonstrates how these relay attacks may be used on Google Wallet

[8] describes a realistic attack scenario in which a contactless verify PIN is used to make infinite guesses at the cardholder's PIN without the cardholder's knowledge. They have detailedimplementation work and research into attack scenarios in this paper, which collectively offer a convincing case for criminals to profit from attacks combining NFC data skimming, NFC Verify PIN, and NFC transaction relay. They claim that based on the observations; Visa should remove the Verify PIN functionality from its NFC cards because it isn't needed for contactless transactions to function effectively.

[4] works on understanding the common relay attack done using high programmable device called proxy (remote ¬ Majorly focuses on relay attack that use man in the middle approach. ¬ Address basic functionality like ¬ Multiple solutions on single attacks can't get generalized idea which to use. terminal) along with victim contactless card anduser device (smart-mole). This also established about communication protocol and service mechanism which uses half duplex method. Also, in the communication it uses APDU command between proxy and user device electronic channel. It focusses onsystem authentication, digital certification using of cryptographic algorithm that uses mac function and basic functionality like average response time up to certain period so that attacks can be minimized

[6] works on basic functionality of RFID that facilitates usage of NFC used by contactless card and user device. The RFID basicallyfacilities tracking of object using technology namely reader, transceiver, decoder and transponder. This also amplifies the data security issues of RFID tag (unique identification) also called as EPC (Electronic product code). The basic vulnerabilityis that tags can be copied, crack and can be intercepted. In data ¬ Multiple solutions for this technology namely range queries, k nearest neighbors queries and strowman1 and 2 approach. ¬ It allows major secure and cheap base user privacy services ¬ Even though it uses different kind of cryptographic algorithm like aes , des etc. but yet unable to find an exact solution which is vulnerable to all type of attack. ¬ Difficult to find a solution which don't suffer from cure of high dimensions. privacy there are two threats namely data collection and data publishing which uses complex cryptographic algorithm.

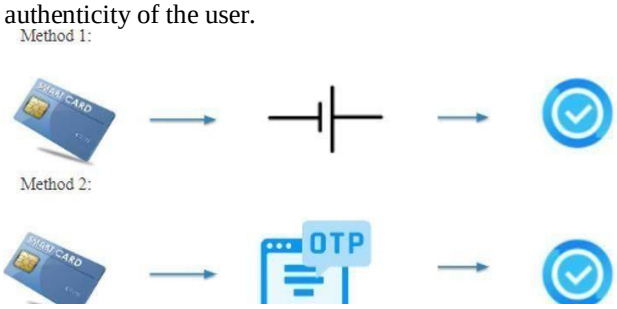
[9] In order to apply security to smart cards and the accompanying algorithms, the article reacts to numerous attacks and the corresponding countermeasures. These fundamental goals take into account the fact that such cards have a limited amount of memory and processing capacity. The solution is based on the card-based assaults, which include intrusive, semi-invasive, and non-invasive attacks, and it interacts with certain smart cards as well as other devices that contain a protected microprocessor. Invasive assaults that targeted the semi-conductor industry's high cost and high investment model have led to some companies installing probes in the bis line that separates blocks of chips. Semi-invasive procedures need that the exposed chips on cards' rough surface remain unaltered.

[10] Setup for android app clone's contactless cards in seconds deals with how to clone any payment cards with an android running apps on a google nexus. In this author focuses on how to recover from down under attacks despite publishing the weakness in NFC problem persist. The cloning can be performed by either stealing the key used in CVV which uses Cryptographic equation which has concatenated ATC and unknown number in a combined encrypted format. The application scans the cards a separate out the ATC data and also retrieve data associated to unknown data corresponding to transaction counter number. This can be performed by cloning the cards which are near into their coverage ideally by using high power antenna for long distance access. This paper specify how cloning can be done using an application via a physical means such as coverage and the in-depth knowledge of processing of CVV data.

4. METHODOLOGY

We can have two approaches for our project:

Hardware Implementation by building a circuit. It will activate the card only when it's in the hands of user. We will use the biometric sensor in the circuit. Software Implementation by creating an OTP Generation System. The user will receive an OTP before making the payment in order the check the authenticity of the user.



4.a. OTP generation method

4.1 Customizing the real time card:

This method is based on customizing the existing contactless credit card by providing additional functionality that is it is aim to authorize user only when the card is in the hands of human being (authorized user). This can only be possible by creating a semi-circuit card. As we humans have electrons in our body, the circuit will be completed once the card holder holds the card to complete the transaction. This will give us the assurance that card is in the hands of cardholder and thus we can initiate the transaction.

4.2 Generating one-time-password:

In order to confirm the user's distinct identity in relation to the smart mole, this second authentication factor is used. Here, we're concentrating on the development of authentication based on one-time pads, which provides an effective and secure solution. The primary one-time password (OTP) generation algorithm we employ is HOTP (HMAC-based one-time password), which supports authenticated service HOTP/OATH (RFC 4226).

Storing message digests as derived passwords in the user database, followed by submitting a specific login request, are the three main components of this technique. Here, the user merely includes her user ID in the login request (not send password not message digest password). We require two distinct login requests, one for user id and the other for some more data. The server then generates a random challenge. The server checks to determine if the user id is a genuine one when it receives the login request. Send an error message if not. If the user answers correctly, the server generates a random challenge (a random number produced using a pseudo random approach) and sends it to them. In order for the server to successfully perform a random challenge, the user must first send the login name associated with the user. If this database entry is successfully retrieved, the server then performs the random challenge, which can be any number generated by a random challenge code. This number is then essentially sent to the client or end user. From this point forward, these random numbers are encrypted with the user password hash value and sent appropriately to the server, which will verify them either by decrypting the data using the login credentials it has previously acquired or by carrying out the same action as the client. If these values match, the related user is verified.

5. Implementation

What is Arduino?

An ATmega328-based microcontroller board is the Arduino Uno (datasheet). It has 6 analogue inputs, a 16 MHz ceramic resonator, 14 digital input/output pins (including 6 PWM outputs), a USB port, a power jack, an ICSP header, and a reset button. Everything you need to get started using the microcontroller is included; all you have to do is plug it into a computer through USB, an AC-to-DC adapter, or a battery. The FTDI USB-to-serial driver chip available on earlier boards is not used by the Uno, making it special. Instead, it makes use of an Atmega16U2-based USB-to-serial converter. (Atmega8U2 up to version R2).

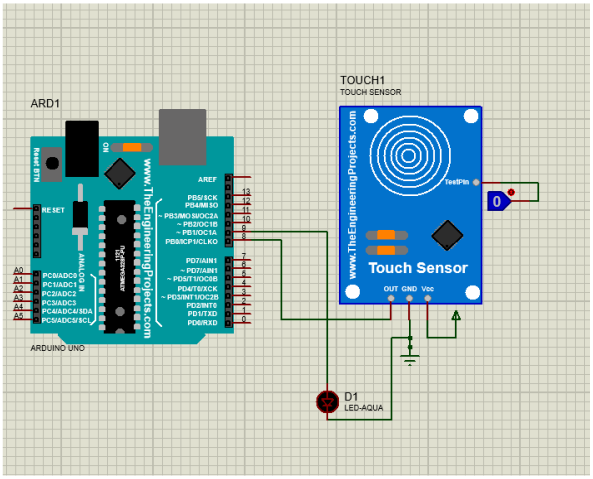
What is Capacitive touch sensing?

Touch interfaces, proximity interfaces, motion, force, and acceleration detectors, and fluid and humidity level sensors all benefit from capacitive sensing. Implementing capacitive sensing can range from simple to sophisticated, depending on your application.

5.1 Proteus Implementation:

We have used the Atmega 328p based Arduino as our board and the capacitive touch sensor. For the purpose of performing the simulation on proteus software we have used the touch sensor library of proteus. In touch sensor library there is a test pin from which we can provide the input to our touch sensor. Suppose someone pressed the touch sensor now the Arduino will see whether the fingerprint is authorized or not andthen only it performs the operation now performingthis similar task in proteus, we are providing the test pin, if the input to the test pin is 1 that means our touchsensor is operating and if its 0 it's not.

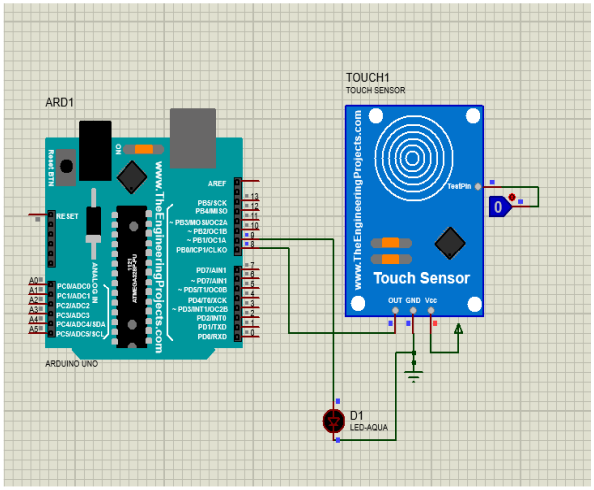
Now that is going to provide the high or low signal to the microcontroller and the we can give one if else condition by which it will check what's the input is coming from the touch sensor and then microcontroller will perform the assigned task.

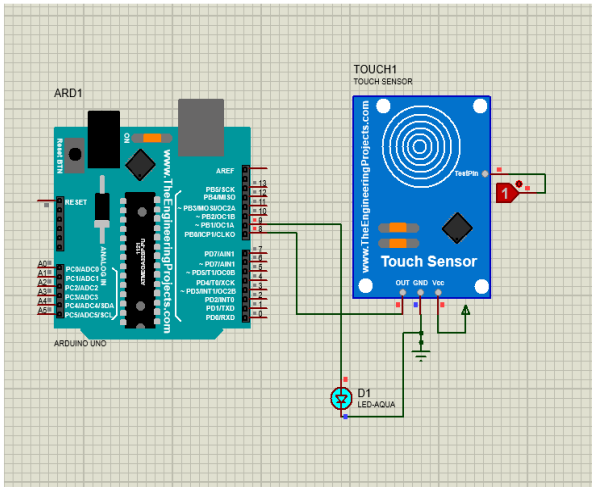


5.1.a. Arduino circuit board

```
void setup()
{
  pinMode(8, INPUT);
  pinMode(9, OUTPUT);

  // Turn builtin LED off
  digitalWrite(9, LOW);
}

void loop()
{

  if(digitalRead(8) == HIGH) {
    digitalWrite(9, HIGH);
  } else {
    digitalWrite(9, LOW);
  }

  delay(100);
}
```

5.1.b. Code for arduino





5.1.c. Result on Arduino

5.2 OTP Generation using Twilio:

• One-Time Passcodes (OTPs) are a simple and effective technique to validate someone's phone number at sign up in order to prevent bots, ensure deliverability to the appropriate person, and more.
• Verifying phone numbers can help to reduce fraud while also improving deliverability and confidence. The Twilio Verify API makes sending and verifying OTPs a breeze. Let's take a look at how to get started using Verify in less than five minutes.

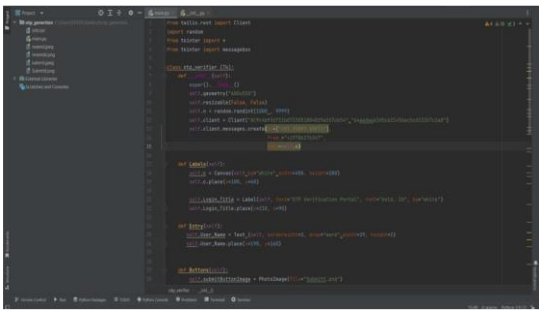
What is Twilio?
Twilio offers a simple API for sending and receiving SMS messages around the world. You may send text messages to users all around the world using just one integration.Twilio Verify is a full solution for confirming end user phone numbers, which we'll utilise to transmit a numeric code to the Android app through text message. Your server application will sit in the intermediate of your Android app and Verify, allowing you to verify a user's phone number when they sign up for your app.

How it works:

• The user provides their phone number or email address.
• The app creates a token for authentication.
• The token is sent to the user via the designated channel after the user enters the right token.

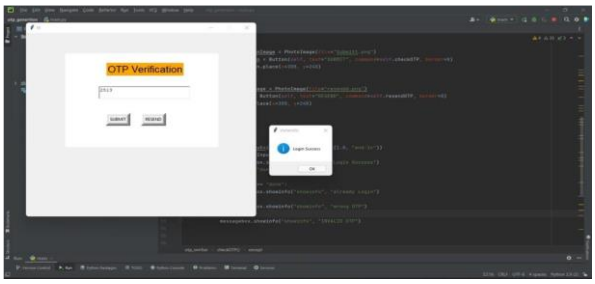
• The app checks the token.

Twilio is ISO/IEC 27001 certified, provides TLS 1.2 encryption, and encrypts data between customer applications. To ensure that data is properly stored, processed, and handled by our people, systems, and technology, we maintain strong governance and protection requirements.

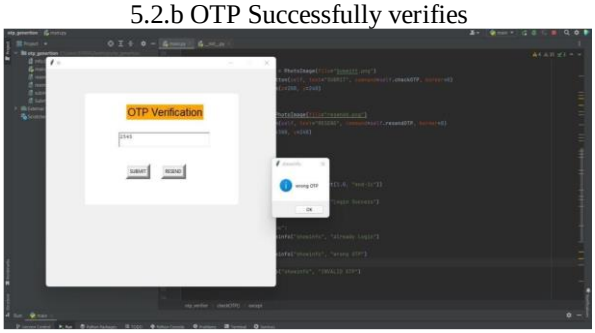


5.2.a. OTP Generation code

Results:



5.2.b OTP Successfully verifies



5.2.c. OTP Failure

6 Conclusion

The purpose of this project was to elaborate effective strategies for dealing with security breaches identified in individuals contactless credit cards. Based on the analysis conveyed, it can be concluded that there is multiple modification are required and important for the improvement of this security to the contactless credit cards. Future exploration is basically divided into two factors by generating one- time-pad along with customizing the contactless cards so that proper authentication can be done using thumb printing. Hence, we conclude that the project will play a crucial role in the industry with respect to the security associated with it in the future timeline.

7. REFERENCES

[1] M. Roland, J. Langer and J. Scharinger, "Applying relay attacks to Google Wallet," 2013 5th International Workshop on Near Field Communication (NFC), 2013, pp. 1-6, doi: 10.1109/NFC.2013.6482441

[2] ISO/IEC 7816-4, "Identification Cards – Integrated Circuit Cards – Part 4: Organization, Security and Commands for Interchange", 2013.

[3] ISO/IEC 21481, "Information technology – Telecommunications and Information Exchange Between Systems – Near Field Communication Interface and Protocol-2 NFCIP-2", 2012.

[4] Luigi Sportiello,"Internet of Smart Cards": A pocket attacks scenario,International Journal of Critical Infrastructure Protection,Volume 26,2019,100302,ISSN 1874-5482,https://doi.org/10.1016/j.ijcip.2019.05.005.

[5] A. Juels, "RFID security and privacy: a research survey" IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 381-394, 2006.

[6] David C. Wyld (Eds) : ICCSEA, SPPR, CSIA, WimoA, UBIC - 2013 pp. 255–261, 2013. © CS & IT-CSCP 2013

[7] Y. Desmedt, C. Goutier, S. Bengio, "Special uses and abuses of the Fiat-Shamir passport protocol", in proceedings of Advances in Cryptology - CRYPTO 87, LNCS 293, pp. 21-39, 1987.

[8] The Dangers of Verify PIN on Contactless Cards [By] M. Emms, B. Arief, T.Defty, J. Hannon, F. Hao, A. van Moorsel Newcastle upon Tyne: Newcastle University: Computing Science, 2012. (Newcastle University, Computing Science, Technical Report Series, No. CS-TR-1332)

[9] Tunstall, Michael & Mayes, Keith & Markantonakis, Konstantinos. (2007).Smart Card Security. 10.1007/978-0-387-72198-9_9.

[10] https://www.blackhat.com/docs/us15/materials/us-15-Fillmore-Crash-Pay-How-To-Own-And-Clone Contactless-Payment-Devices.pdf

[11] G.P. Hancke, K. Mayes, K. Markantonakis, "Confidence in smart token proximity: relay attacks revisited", Computers & Security, Vol. 28, No. 7, pp. 615- 627, 2009.

[12] P. Thevenon, O. Savry, S. Tedjini, "On the weakness of contactless systems under relay attacks", in proceedings of the 19th International Conference on Software, Telecommunications and Computer Networks - SoftCOM2011, pp. 1–5, 2011.

[13] R. Anderson, "Position statement in RFID S&P panel: RFID and the middleman", in proceedings of the 11th International Conference on Financial Cryptography, pp. 46-49, 2007.

[14] W. Issovits, M. Hutter, "Weaknesses of the ISO/IEC 14443 protocol regarding relay attacks", in proceedings of the International Conference on RFID-Technologies and Applications - RFID-TA2011, pp. 335–342, 2011.

[15] R. Silberschneider, T. Korak, M. Hutter, "Access without permission: a practical RFID relay attack", in proceedings of the 21st Austrian Workshop on Microelectronics - Austrochip, Vol. 10, pp. 59-64, 2013.

[16] T. Korak, M. Hutter, "On the power of active relay attacks using custom-made proxies", in proceedings of the 2014 IEEE International Conference on RFID, pp. 126- 133, 2014.

[17] M. WeiB: "Performing relay attacks on ISO 14443 contactless smart cards using NFC mobile equipment", Master Thesis, Der Technischen Universitat Munchen, Germany, pp. 1-89 2010.

[18] L. Francis, G. Hancke, K. Mayes, K. Markantonakis, "Practical relay attack on contactless transactions by using NFC mobile phones", in proceedings of Radio Frequency Identification System Security - RFIDsec2012 Asia, pp. 21–32, 2012.

[19] L. Sportiello, A. Ciardulli, "Long distance relay attack", in proceedings of Radio Frequency Identification-

Security and Privacy Issues - RFIDsec2013, LNCS 8262, pp. 69–85, 2013.

[20] L. Francis, G. Hancke, K. Mayes, K. Markantonakis, "Potential misuse of NFC enabled mobile phones with embedded security elements as contactless attack platforms", in proceedings of International Conference for Internet Technology and Secured Transactions - ICITST 2009, pp. 1–8, 2009.