iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 Issue: X Month of publication: October 2016

DOI:

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secure Transaction By Using Wireless Password with Shuffling Keypad

Shweta Jamkavale[1], Ashwini Kute[2], Rupali Pawar[3], Komal Jamkavale[4],Prashant Jawalkar[5]

UG students[1,2,3,4], Guide[5], Department Of Computer Engineering, JSPM's BSIOTR, SPPU University, Pune, India

Abstract— In general, all swiping card authentication system having different possibilities of password guessing by mean of shoulder surfing is an attack and overlooking attack. This problem can be overcome with new advance solution by designing shuffled keypad which displays the shuffled number on user's screen, which is hard to recognize for the person who stand near you to guess the password. The main purpose of this system is to develop a secure ATM PIN in future for transaction purpose and the transaction notification directly goes to the user's application and request PIN to user instead of merchant's hardware machine.

Keywords—ATM card,Swipe card machine,PIN,Android Device.

I. INTRODUCTION

Today, in the banking system has got wide popularization. It provide 24 hours service for customer. In this technology, ATM (Automated Teller Machine) card is the important part of our life. To have transaction ATM pin number is necessary and it must be secure. The existing banking system has got very high popularity with 24 hours service. Use of ATM is helpful for money transaction.The flow of Card Payments are changed in recent months 2014 and made PIN number compulsory to complete the transactions.This is applicable for all types of cards (Debit, Credit, etc).This is done to minimize the fraud/misuse of card payments. When user typing his/her PIN number. There are several problem occured at the time of transaction. He /She has to enter PIN in front of merchant or relatives or any other person. This is a type of Overlooking / Shoulder Attack.His / Her 4 digit secret PIN number gets public. Also we have to type our PIN on merchant's hardware keypad, where he can record our PIN number, this will cause more frauds. So to handle such type of attacks we wanted to developed such a technique which provides more security to a user in typing his password, in a public place, and in case that user is in critical position.As per our propose technique we wanted bank server should accept PIN from users mobile phone and not from merchants keypad. Payment should be made using card and pin number should be entered by user from his mobile.

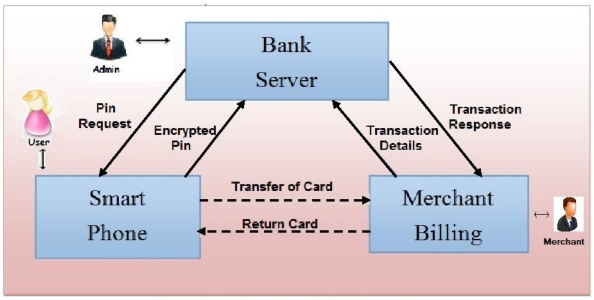
II. LITERATURE SURVEY

[1] An circle based Pin logic has been implemented which is rotate having different symbols. It has drawback that it require a proper LCD screen and here the concept of PIN is not use. [2]In the first paper they develop a novel PIN entry method is called as Switch PIN, which develops a switchable keypad on a smart phone touchscreen devices to effectively prevent shoulder surfing attacks. The basic idea is to render a random mapping in between two switchable keypad, but it is less secure and the password or PIN number can be easily cracked. [3]In this paper the shuffling keypad technique is applied for ATM machine with security, but it has very hard logic and it is too difficult to remember. [4]The main purpose of this system is to develop an android application which perform ATM transaction, this can be install on smartphone with android OS. It contain all option which available in ATM. Virtual memory concept is used, but it is very complicated and need smart user to access.[5]It is purpose fully developed for two face keypad which has one original keypad and another is duplicated keypad which blinks for every ten seconds. It has one drawback that it needs OTP to confirm PIN.

III. PROPOSED SYSTEM

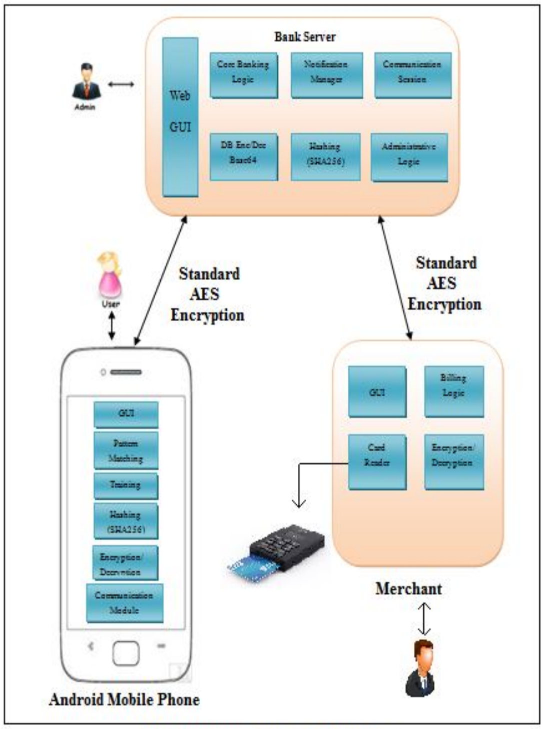
The working of proposed system is, the merchant inserts your card. He enters the transaction amount. Then the bank server will notify user on his android mobile phone to enter PIN number. User can now enter PIN using his/her mobile. After entering pin number bank server will do the authentication, check whether user is valid or not and also he has a sufficient balance to pay. After checking, bank server will transfer the amount in merchant's account. We have entered PIN number in front of merchant as well as friends to do the transaction where those people can record our PIN number. So to manage such type of attacks we are developing to a system which provides more security to a user in typing his password, in a public place, and in case that user is in critical position. As per our propose technique we want bank server should accept PIN from users mobile phone and not from merchants keypad. So whenever merchant swipe user card for payment, bank server will send notification to user on his mobile to enter PIN.

So whenever merchant swipe user card for payment, bank server will send notification to user on his mobile to enter PIN. User can enter PIN number using his/her mobile. Even user is free to provide number as YES/NO or any pattern which he can easily change on daily as well as monthly basis. We will be using Encryption and Decryption security system for communication between bank server, mobile application and Merchant hardware.



Architecture of Card Payment

Merchant swipe the debit or credit card in merchant’s hardware keypad, machine reads the 16 digit ATM number.



Architecture of Card Payment

Transaction details will send to the bank server then bank server will verifies the user account and send the notification to user for requesting to enter PIN. User enter PIN on his android device and this PIN is send to the server side in encrypted format. Money will be deduct from users account and transfer to the merchants account.

IV. SAFETY AND SECURITY REQUIREMENT

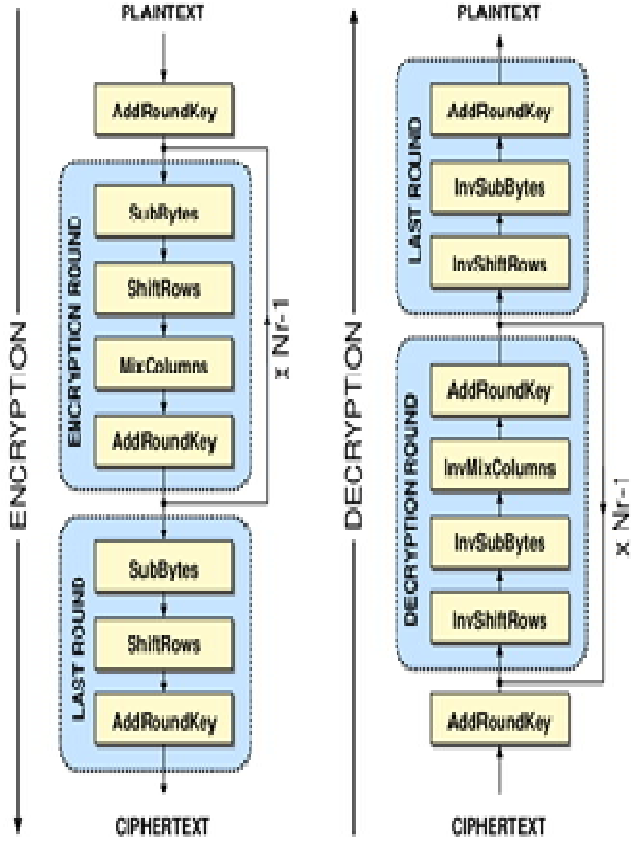
For this architecture different algorithms are used for the security purpose.

A. Use of hash function, SHA256, to create hash of password

The SHA (Secure Hash Algorithm) is one of cryptographic hash functions. A cryptographic hash is same like a signature for a text as well as a data file. SHA-256 algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one way function, it can’t be decrypted again. This makes it suitable for password validation, challenge hash authentication, anti-tamper, digital signatures. SHA-256 is one of the successor hash functions to SHA-1, and is one of the strongest hash functions available.

B. AES algorithm for communication

The Advanced Encryption Standard is a block cipher to secure classified data and can be develop in software and hardware to encode critical data. This new encryption algorithm would be unclassified and had to be "capable of protecting critical government information well into the next 100 years." It was to be easy to develop in hardware and software, as well as in limited environments and offer good defenses against various attack techniques. AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encode and decode data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so the sender and the receiver must know and use the common secret key. All key lengths are deemed enough to secure classified data up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys, a round involve of several processing steps that include substitution, transposition and combining of the input plaintext and transform it into the final output of ciphertext.

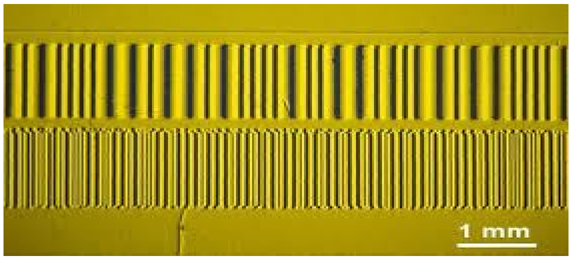


C. BASE64

Base64 is used in bank database to provide decryption.After decryption it gives original 4 digit PIN number as a input to the hashing algorithm .Its quite simple to use-just paste in the base64 text you want to decode and then press the decode button .If the text string you are decoding result in a binary output, it will be send directly back to your client as a stream allow you to save it as its accurate file type. Is a collection of similar binary-to-text encoding schemes that represent binary data in an ASCII string format? By translating it into a radix-64 representation. The general strategy is to choose 64 characters that are members of a subset common to most encodings, and also printable. The particular set of 64 characters choose to represent the 64 place-values for the base varies between implementations .The ratio of output bytes to input bytes is 33% overhead. Specifically, given an input of n bytes, the output will be 4/3 bytes long, including padding characters. We used this algorithm to encrypt users password which is saved present in server database

V. READER INTERFACE

A magnetic strip card is type of card which is used for storing data by modifying magnetism of little iron based magnetic particales on a magnetic material on the card, basically called as swipe card as well as magstrip, is read by swiping past a magneting reading head.Magnetic swipe card are mainly used in credit card, identit card as well as transportation tickets. They also include an RFID tag, a transponder device or a micro chip most of time used for business purpose for access control on electronic payment. Magnetic recording on a steel tape and wire was invented during world war2 for recording the audio.



HTTP protocol used in the Internet. HTTP is an *asymmetric request-response client-server* protocol as stated. An HTTP client sends a request message to an HTTP server, then server returns a response message. HTTP is a *pull protocol*, the client *pulls* data from the server , in place of server *pushes* information down to the client HTTP is a stateless protocol. The current request does not know what has been done in the previous requests. HTTP permits negotiating of information type and representation, so to allowing systems to be built independently of the data being transferred. The HTTP is an application-level protocol for distributed, hypermedia information systems.

VI. CONCLUSION

As per our propose system bank server will accept PIN from users mobile phone and not from merchants keypad.
This will help user to secure his PIN number to become public
Different type of pattern will increase user's PIN security and those patterns can change on daily or monthly basis.
Proposed a new secure hash algorithm based on the previous algorithms, AES and SHA-256 that can be used for secure communication.

REFERENCES

[1] Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks, IEEE 2014 Taekyoung Kwon, Member, IEEE, and Jin Hong- IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY

[2] International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014 Credit Card Fraud Detection System Using Hidden Markov Model and K-Clustering

[3] Lee, Mun-Kyu. "Security notions and advanced method for human shoulder-surfing resistant PIN-entry." Information Forensics and Security, IEEE Transactions on 9.4 (2014): 695-708.

[4] De Luca, Alexander, et al. "Using fake cursors to secure on-screen password entry." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2013.

[5] https://en.wikipedia.org/wiki/EMV

[6] http://www.chipandpin.co.uk/

[7] http://www.axisbank.com/personal/cards/quick-links/do-more-with-your-card/credit-card/chip-pin-cards.aspx