Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 6, Issue 07, July -2019

METHODTO SECURE CRITICAL TRANSCATIONS: COMBINNING THREE WAY & TWO FACTOR AUTHENTICATION

Yoga Lakshmi.P

Assistant professor, SRMIST, Kattankulathur, Chennai.

ABSTRACT: *In the current global scenario, people have migrated from being citizens to netizens where card transactions are most prominent at Automatic Teller Machines (ATM), Online transactions and Point of Sale(POS) terminals. Card breaches are also increasing that leads to many billion dollars of loss by compromising the merchant's server to get card details including account number,Personal Identification Number (PIN) and Card Verification Value (CVV). At present, PIN is the only factor that authenticates any transaction. Apart from that, a very few banks send One Time Password (OTP) for ATM and online transactions which is not completely secure. Present systems do not have enough mechanisms to validate or check who initiates the transaction. This paper proposes to introduce a system in which the user's smart phone is used to secure card transactions by combining 3 way authentication and 2 factor authentication. Firstly, it checks the card holder's biometric viz., Finger print while a transaction is initiated. Secondly, OTP is neither sent nor received but it is auto-generated in the user's smart phone which sends a trigger to the bank server that generates the same random number. This system proposes to use a secure OTP generator algorithm that uses combinedSecure Hash Algorithm 1(SHA1), Hash Based Method Authentication Code (HMAC) HMAC-SHA256 and HMAC-MD5. The user enters the OTP after entering the PIN and it gets validated that the authorized person is the one who has initiated the transaction. Thus, reasonably securing a card transaction as it mandates the presence of the card holder for every transaction to be authenticated.*

KEY WORDS: *OnlineTransaction, Card Transaction Security, 3-Way Authentication, 2-Factor Authentication Method, Hash Algorithms*

INTRODUCTION

The advancement in technology has made everything easy for human beings. One such technology is the usage of credit or debit cards that eases the trouble of handling cash. A swipe of the card is enough to buy anything, anytime and anywhere in the world. A card can be used at any ATM or Merchant's Point Of Sale (POS) Terminal or Internet Payment Gateway. Such increased and diverse usage of cards has developed the Payment Cards Industry as well as the crimes associated with it. In recent years, such credit or debit card frauds are very high that has impacted billions of loss in the business.

Credit card and debit card fraud resulted in losses amounting to $11.27 billion during 2012. Card issuers and merchants incurred 63% and 37% of those losses, respectively, with the following transactional breakdown. Card issuer losses occur mainly at the point of sale from counterfeit cards while merchant losses occur mainly on card-not- present (CNP) transactions on the Web, at a call center or through mail order. (Nilson Report, August 2013)

Fraudsters keep up the pressure online in the burgeoning online channel. Consumer spend is on the rise while criminals continue to steal customer PII and payment information for fraudulent misuse. Forty-two percent of merchants who support online channels are reporting an increase in fraud, matching that of 2013.

EXISTING PROBLEMS IN PAYMENT CARD TRANSACTION SECURITY:

WEAK AUTHENTICATION MECHANISM

When a card is used for transaction, only if PIN is required for authentication, it is vulnerable to many attacks such as Replay attacks, social engineering and shoulder surfing. Replay attack is when the captured user credentials are just used once again by a hacker to make a transaction. Absence of proper mechanisms to authenticate who initiates a transaction leads to increase in frauds.

DETAILS STORED IN MERCHANT'S SERVER ARE COMPROMISED

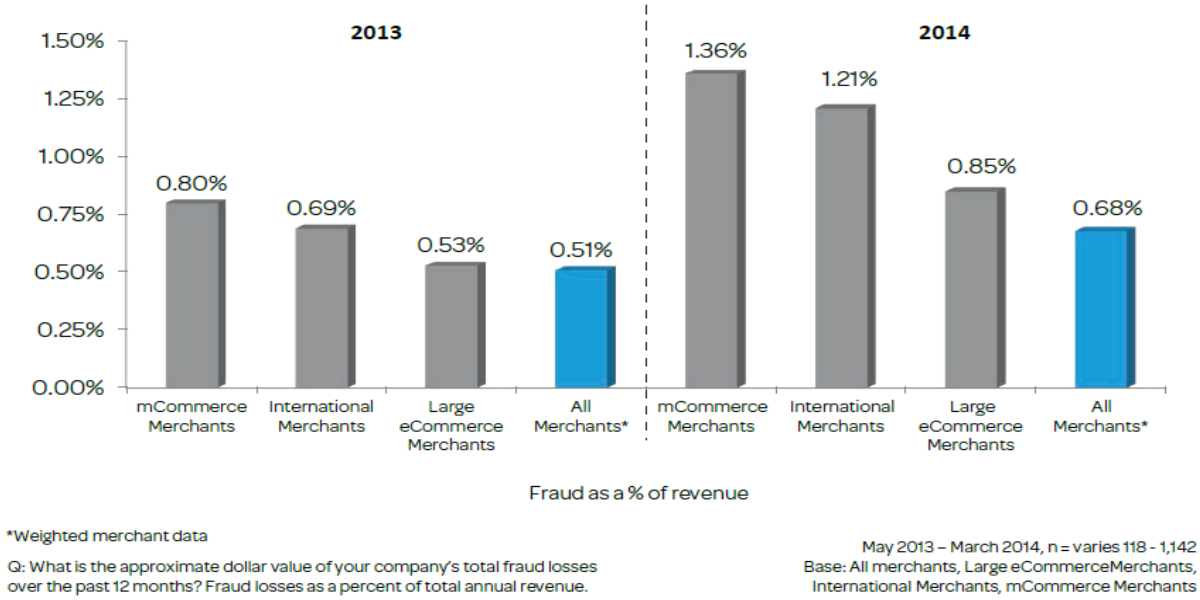
Details stored in merchant's server are compromised with the help of malwares that are installed in the server. Home Depot's store registers had been infected with a new variant of "BlackPOS" (a.k.a. "Kaptoxa"), a malware strain designed to siphon data from cards when they are swiped at infected point-of-sale systems running Microsoft Windows.

The information on the malware adds another indicator that those responsible for the breach at Home Depot also were involved in the December 2013 attack on Target that exposed 40 million customer debit and credit card accounts. BlackPOS also was found on point-of-sale systems at Target. Cards apparently stolen from Home Depot shoppers first turned up for sale

on Rescator[dot]cc, the same underground cybercrime shop that sold millions of cards stolen in the Target attack. (Source: Trend Micro)

Fraud losses have also increased as a percentage of revenue in 2014, reversing the drop from the previous year. Overall, merchants are reporting fraud loss as a percent of revenue at 0.68% this year compared to 0.51% in 2013.

Fig. Fraud As A Percent Of Revenue By Merchant Segment, 2013-2014



A look back at major card data breaches of 2014: (Source: Forbes)

NeimanMarcus

In January, news broke of a card hack at Neiman Marcus where hackers accessed the debit and credit card information of customers who shopped at this chain between July 16, 2013 to October 30, 2013. Only in-store customers were affected, not online transactions. Originally, the company estimated that as many as 1.1 million cardholders could have been affected. But further investigation found that it affected a maximum of 350,000 customers. The breach occurred when malicious software was installed onto the Neiman Marcus system that collected payment card data from customers who made purchases during those dates.

WhiteLodging

In early February, a hotel franchise management company that manages 168 hotels in 21 states suffered a data breach that exposed hundreds of guests' debit and CREDIT CARDS information in 2013. White Lodging Services Corporation maintains hotel franchises for some of the top names in lodging such as Hilton, Marriott, Westin and Sheraton. Sources reported that the data breach centered mainly around the gift shops and restaurants within these hotels managed by White Lodging, not necessarily the front desk computers where guests pay for their rooms.

SallyBeauty

In March, it was reported that over 280,000 debit and credit cards were stolen and sold on an underground crime store. Three different banks bought back their customers' debit and credit card accounts from this store in the hopes of finding a "common point of purchase" among them. That common point turned out to be Sally Beauty stores.

Michaels

Michaels, the nation's largest arts and crafts chain, reported a data breach at the end of January. The company said close to 2.6 million cards used in payments at their stores were potentially exposed between May 8, 2013 and January 27, 2014. Another 400,000 cards may have been affected at Aaron Brothers stores between June 26, 2013 and February 27, 2014.

11Casinos

In May, Affinity Gaming, which operates 11 CASINOS in Nevada, Colorado, Iowa and Missouri, announced they found evidence of a hack on the casino's debit and CREDIT CARD system for non-gaming purchases. While the breach did not impact money spent directly on gambling, it did affect customers who paid for other items and services at casino resort facilities. Hotel rooms, food and drinks are all processed through this system. In December 2013, Affinity Gaming

announced that its card processing system had been infected with malware which may have compromised card data from customers. This data breach apparently took place between December 2013 and April 2014.

PFChangs
In June, P.F. Chang's China Bistro reported a security breach that affected customers at 33 restaurants located in 16 states. The intruder may have stolen some data from certain credit and debit cards that were used during an eight-month period from October 19, 2013 to June 11, 2014. The potentially stolen credit and debit card data included the card number and, in some cases, the cardholder's name and/or the card's expiration date.

Albertsons&SuperValu
In August, some of the country's most popular supermarkets, including Albertson's and SuperValu, reported they experienced data breaches over the summer. Hackers broke into the debit and CREDIT CARD payment networks of the stores under the AB Acquisitions LLC umbrella. This includes Acme, Shaw's Supermarket, Star Market, Cub Foods, Farm Fresh, Hornbacher's, Shop 'N Save and Shoppers Food & Pharmacy. SuperValu said the hack affected 228 of its stores. Albertson's estimated that more than 700 of its locations were impacted in Idaho, Montana, Southern California, Nevada, North Dakota, Oregon, Wyoming, Southern Utah and Washington. SuperValu and Albertson's use the same technology to process their payments.

United Parcel Service
In August, United Parcel Service (UPS) reported a data breach may have occurred in 51 of their UPS Stores, possibly leading to the theft of customer debit and credit card information. Malicious software that was not identified by current anti-virus software led to the breach. Customers who used a debit or credit card at the 51 stores between between January 20, 2014 and August 11, 2014 were warned that their names, postal addresses, email addresses and payment card information may have been exposed. These 51 UPS Stores represented just over 1% of the 4,470 franchised center locations across the United States.

DairyQueen
In August, International Dairy Queen began an investigation into a data breach in its stores. In November, it confirmed the breach took place in 395 locations and may have affected nearly 600,000 debit and credit cards. The company found that Backoff malware, used in so many recent cyber attacks, affected the payment systems in these locations. Customer names, debit card and Credit Card numbers and their expiration dates were compromised.

Goodwill
In early September, Goodwill Industries confirmed that a data breach in 330 of its stores may have compromised an estimated 868,000 debit and credit cards. Payment card information, such as names, payment card numbers and expiration dates, may have been compromised. However, personal information such as addresses and PIN numbers were not affected. According to their investigation, a third-party vendor's systems were attacked by malicious software, enabling criminals to access some payment card data of a number of the vendor's customers. The impacted Goodwill stores used the same affected third-party vendor to process credit card payments.

HomeDepot
In September, Home Depot, the world's largest home improvement chain, confirmed that a whopping 56 million credit and debit cards were affected by a data breach. Then in November, the company disclosed that hackers had also stolen 53 million email addresses. The company said criminals used a third-party vendor's user name and password to enter the perimeter of Home Depot's network. The hackers then acquired elevated rights which allowed them to navigate portions of the company's network and to deploy unique, custom-built malware on its self-checkout systems in the U.S. and Canada.

JimmyJohn's
In late September, sandwich shop chain Jimmy John's confirmed that criminals hacked into their point of sale systems at 216 stores and accessed customer debit and Credit card information. The breach took place between June 16 and September 5. Hackers obtained the account numbers on these cards, and may have access to the cardholder name, verification number and/or expiration date. The company, based in Champaign, Illinois, said the hackers were able to obtain the login credentials from the chain's payment technology vendor and access its point of sale system.

JPMorganChase
JP Morgan Chase, the nation's largest bank in terms of assets, acknowledged a massive data breach that affected 76 million households and 7 million small businesses. The bank disclosed the extent of the breach in a filing in early October with the

Securities and Exchange Commission. The bank reported no unusual customer fraud had resulted from this breach. Hackers obtained personal information such as customer names, addresses, phone numbers and email addresses. However, JP Morgan Chase said that sensitive bank information–account numbers, passwords, social security numbers and birthdates–were not part of the breach. The breach occurred in June and July, and affected customers that used Chase web and mobile services.

Sourcebooks

Most of the major data breaches that occurred in 2014 took place with transactions at store level, not with online purchases. Not so with Sourcebooks, the popular online bookstore. The shopping cart of Sourcebooks was compromised between April and June of 2014. Hackers were able to steal names, addresses, credit card numbers, expiration dates, card security codes and email addresses. Sourcebooks reported that 5,204 customers were affected by the hack.

Staples

Office supply chain Staples acknowledged in December that a credit card breach took place in 119 stores between April and September. The malware intrusion may have resulted in the theft of as many as 1.16 million customer credit and debit cards. (Source: Forbes)

"Fraudsters are now taking the next step as opposed to just getting the card data, going out and trying to use it. They are doing their due diligence based on card holder name or whatever data that they're getting, and are able to [use these] personal identifiers to call into the call center, to make transfers into the DDA's, to check credit lines, to place travel notifications. Anything they can do to make it appear that they are the legitimate customers to increase the take they get on their "cash out" if you will."

Says an Executive, Mid-Sized Card-Issuing Financial Institution (Source: 2014 LexisNexis® True Cost of Fraud Study)

AUTHENTICATION MECHANISMS

1.THREE - WAY AUTHENTICATION

i. What you Have – Card
ii. What you Know – PIN, CVV
iii. What you Are – Bio metrics

Banks use Card, PIN and CVV to validate the first two authentication mechanisms. But they don't authenticate based on the Bio metric features which are unique to every individual such as finger prints or retina scanning.

2.TWO– FACTOR AUTHENTICATION

The use of two-factor authentication to prove one's identity is based on the premise that an unauthorized actor is unlikely to be able to supply both factors required for access. If in an authentication attempt at least one of the components is missing or supplied incorrectly, the user's identity is not established with sufficient certainty and access to the asset (e.g., a building, or data) being protected by two-factor authentication then remains blocked. The authentication factors of a two-factor authentication scheme may include:

- Some physical object in the possession of the user, such as a USB stick with a secret token, a bank card, a key, OTP, etc.,
- Secret known to the user, such as a username, password, PIN, TAN, etc.

(Source: Wikipedia)

3. OTP–One Time Passwords

A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password based authentication. The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. A second major advantage is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further.

Various approaches for the generation of OTPs are listed below:

- Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a short period of time)
- Using a mathematical algorithm to generate a new password based on the previous password (OTPs are effectively a chain and must be used in a predefined order).

- Using a mathematical algorithm where the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and/or a counter.

Systems generate OTPs on the server-side and send them to the user using an out-of-band channel such as Short Message Service (SMS) messaging. (Source: Wikipedia)

4.HMAC-Based One Time Password(HOTP) vs Time-Based One Time Password (TOTP)

The different types of two-factor authentication are primarily distinguished by how the "moving factor" is implemented. HOTP stands for "HMAC-based One Time Password" and the moving factor is a simple counter that increments each time an OTP is generated. TOTP stands for "Time-based One Time Password" and the moving factor in this case is the passage of time (a new OTP is generated by the device every 30 seconds). The TOTP password is short-lived while the HOTP password may be valid for an unknown amount of time. TOTP requires less maintenance but the time between the device and our servers needs to be synchronized while HOTP requires more maintenance but no synchronization. As a result, the TOTP is generally considered the more secure One-Time Password solution.

PROBLEMS IN IMPLEMENTING OTPs

In case of SMS based OTP sending mechanism, today SMS OTP cannot be considered secure. Two reasons contribute to this fact. First, the security of SMS OTP relies on the confidentiality of SMS messages that in turn heavily relies on the security of cellular networks. Lately, several attacks against GSM and even 3G networks have shown that confidentiality for SMS messages cannot necessarily be provided. It is also vulnerable to Man-In-The-Middle-Attack where signals can be hijacked to capture the OTP. Apart from this, one must wait in order to receive the OTP as a message which will be a time consuming task for users.

HOTP and TOTP implementations would have synchronization problems with the client and the server. The user might enter the OTP, then find that the sync was lost and then the sync need to be established before OTP could be entered. This could be tedious process in a shopping outlet where many are waiting for items purchased to get billed on a Point Of Sale Terminal (POS).

Even if Challenge Response method is used to generate Grid OTP, it requires the user to remember the pattern. This would again lead to problems existing with the PIN like being vulnerable to Social engineering attack.

Worldwide, a very few banks use OTP as a 2 factor authentication process to secure their customers. The banks include Ally bank, American Express, Bank Central Asia(BCA), Bank of America, Barclays, Chase, Discover, Everbank.com, Fairwinds, HSBC, Natwest UK, Raiffeisen Bank CZ, SEB, Swedbank, TBC Bank, UW Credit Union, Wells Fargo.

METHODOLOGY OF STRENGTHENING AND SECURING OTP

User's smart phone has an application that acts as software token which is previously synchronized with the bank's server. For every card transaction, either at ATM, POS terminals or Online transactions, the user opens the application and presses 'GENERATE OTP' button. The app checks the user's Bio-metric- finger print which is already stored on it.

Then OTP (6 digits) is neither sent nor received but it is auto-generated by the client using a combination of cryptographic hash algorithms such as SHA1, SHA256 and MD5. The user enters the OTP into the terminal either during an ATM transaction or POS terminal purchase or an online transaction.

Simultaneously, when the OTP gets generated, the client sends a 'TRIGGER REQUEST' to the bank's server for which the server replies with a 'TRIGGER RESPONSE'. This ensures the successful generation of the same OTP at both the client and server end.

OTP once generated is valid only for 60 seconds. Once if an OTP is typed wrong, the user must generate another OTP. If wrong OTP is typed more than thrice, the card transactions would be suspended for the next 24 hour hours. This would prevent any attacks trying to guess the OTP.

USES

The importance that lies very high on the PIN of a card user that acts as the only lock is now added with additional layers of security. Card frauds that are data specific (only account number and PIN is enough to commit a fraud) become victim specific narrowing down the crime rate.

The use of bio-metric verification authorizes that the right person is using the service and is not being misused.

Using OTP avoids Replay attacks and other Identity thefts. Even if user name, password and other credentials are known, there won't be any use in selling them and can't be misused as OTP is an additional factor that authenticates the user.

Even if there is no signal for mobile communication, this system works well as it auto generates the OTP and does not require Time synchronization or any other synchronization that need to be checked by the user.

HOW CAN OTPs BE STRENGTHENED AND SECURED?

METHODOLOGY:

User's smart phone has an application that acts as software token which is previously synchronized with the bank's server. For every card transaction, either at ATM, POS terminals or Online transactions, the user opens the application and presses 'GENERATE OTP' button. The app checks the user's Bio-metric- finger print which is already stored on it.

Then OTP (6 digits) is neither sent nor received but it is auto-generated by the client using a combination of cryptographic hash algorithms such as SHA1, SHA256 and MD5. The user enters the OTP into the terminal either during an ATM transaction or POS terminal purchase or an online transaction.

Simultaneously, when the OTP gets generated, the client sends a 'TRIGGER REQUEST' to the bank's server for which the server replies with a 'TRIGGER RESPONSE'. This ensures the successful generation of the same OTP at both the client and server end.

OTP once generated is valid only for 60 seconds. Once if an OTP is typed wrong, the user must generate another OTP. If wrong OTP is typed more than thrice, the card transactions would be suspended for the next 24 hour hours. This would prevent any attacks trying to guess the OTP.

HOW IT WORKS?

STEP 1: This algorithm uses a Shared Secret Key (K) and a Counter value (CTR). Value K is a secret which is known only to the Bank server and the Client application. CTR's initial value is given by the Server and it increments each time an OTP is generated.

STEP 2: First, CTR is hashed using 2 different algorithms, namely, SHA1 and MD5 to generate the hash values H1 and H2 respectively.

STEP 3: H2 is sent as 'TRIGGER REQUEST' to the server. Once the server receives the 'TRIGGER REQUEST', it calculates the H1 and H2 values and responds with the same hash value H2 that the server generated for CTR as 'TRIGGER RESPONSE'. This way the counter keeps on incrementing without any synchronization problems between the client and the server.

STEP 4: H1 is simultaneously fed into a Function, f(H1) that returns only 2 values, either 0 or 1 randomly. Based on the value, a switch case function is used to switch between the two algorithms that would generate the OTP in random order. It is not necessary that the switching between 0 and 1 is done alternatively. The function of the hash produces the result 0 or 1 which is random. That is, if the function produces 0 as the result after H1 is fed, it may produce even 0 or 1 the next time.

STEP 5.i) If the case is switched to 0, then HMAC-SHA256(K,H1) is used to generate the value 'a'.

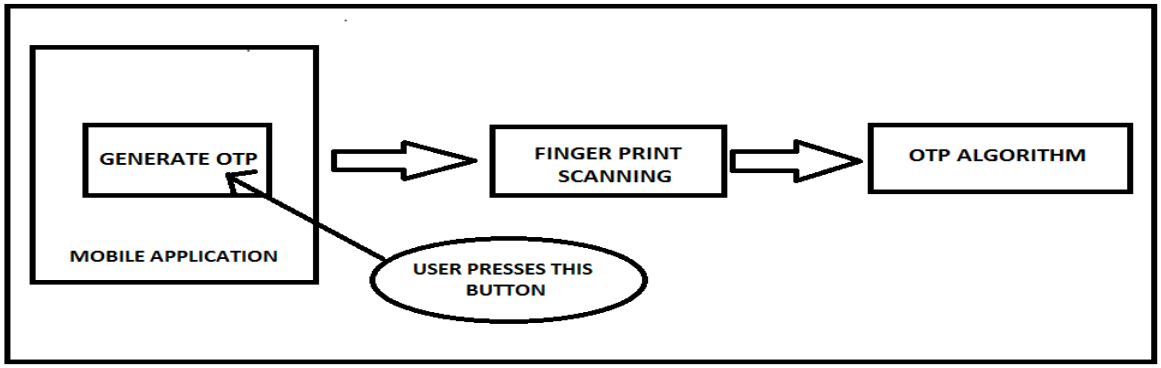
STEP 5.ii) Else if the case is switched to 1, then HMAC-MD5(K,H1) is used to generate the value 'a'.

STEP 6: OTP is generated by Trunc(a).

The client and the server will do the same steps to generate the same OTP at both the ends and it is validated by the Server once the user enters the OTP after the PIN within the next 60 seconds.

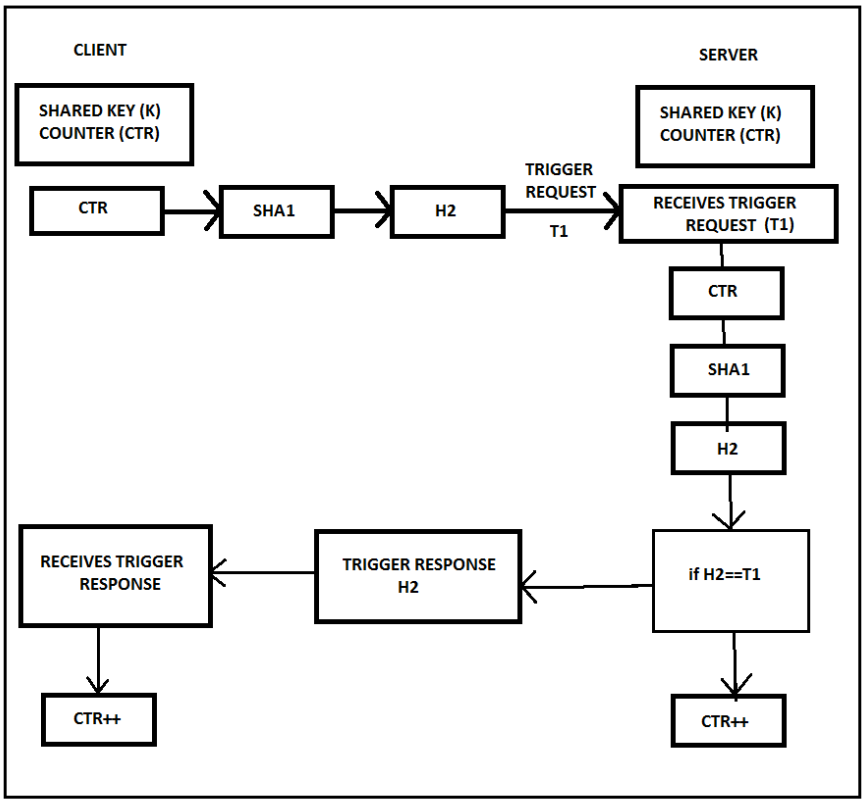
Switching is done so that the way in which the OTP will be generated, i.e., the algorithm that will be used to generate the random number not be known. The OTP once generated, if entered wrongly, even by mistake of the legitimate user, it is required to generate another OTP. This is because, if one of the two possible codes generated by any one of the two algorithms has to be cracked, someone will need two chances to try them within 60 seconds. Since the OTP trial is restricted to only one try per OTP, it will be impossible for a hacker to try both the possible OTPs per OTP generation.

WORKING MECHANISM OF PROPOSED SYSTEM:

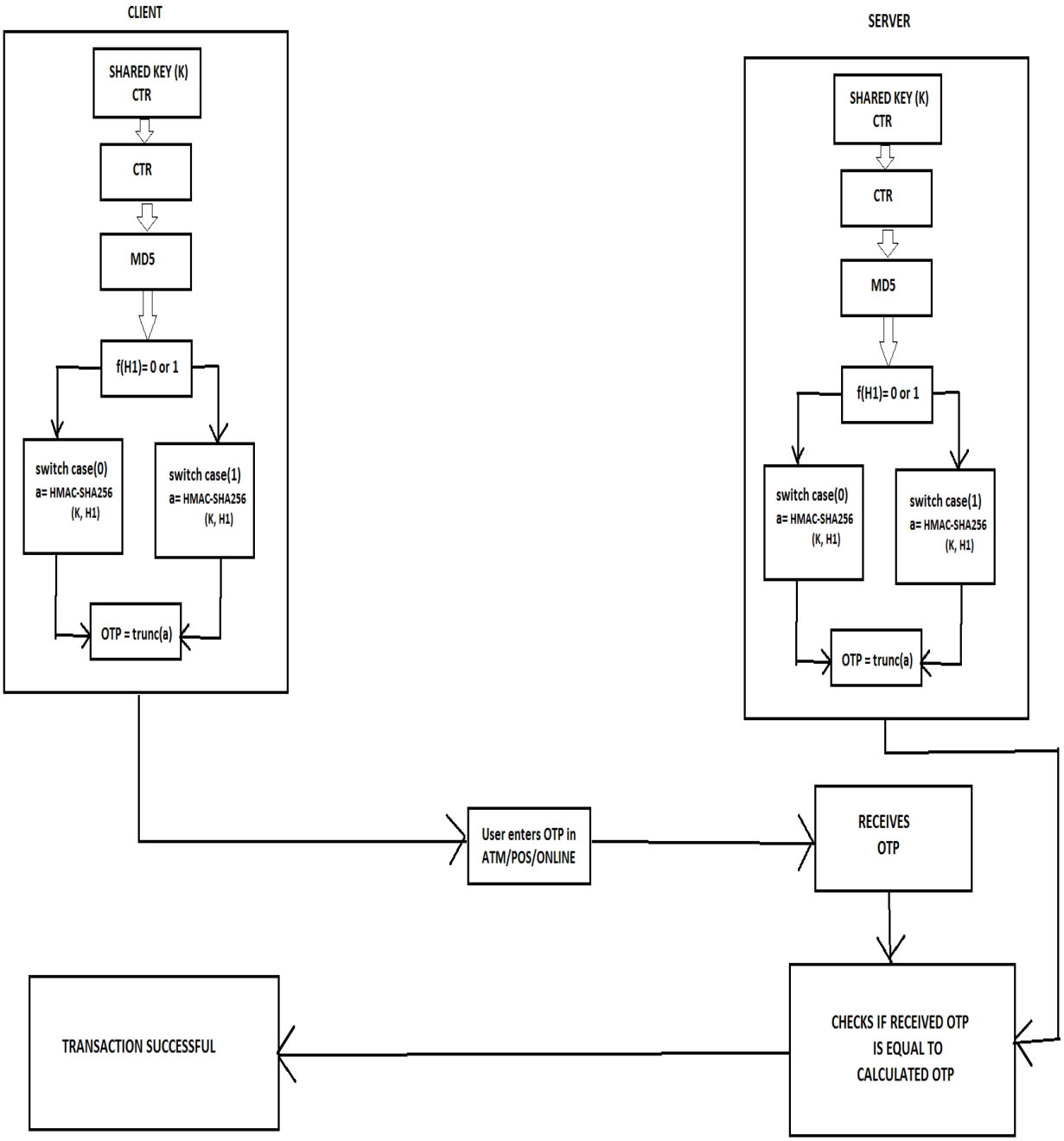


OTP ALGORITHM

COUNTER UPDATION



OTP GENERATION



USES

The importance that lies very high on the PIN of a card user that acts as the only lock is now added with additional layers of security.Card frauds that are data specific (only account number and PIN is enough to commit a fraud) become victim specific narrowing down the crime rate.

The use of bio-metric verification authorizes that the right person is using the service and is not being misused.

Using OTP avoids Replay attacks and other Identity thefts. Even if user name, password and other credentials are known, there won't be any use in selling them and can't be misused as OTP is an additional factor that authenticates the user.

Even if there is no signal for mobile communication, this system works well as it auto generates the OTP and does not require Time synchronization or any other synchronization that need to be checked by the user.

CONCLUSION:

Thus Card transactions can be considerably secured by using the user's smart phones to verify Bio metric and to generate OTP using Secure OTP generation algorithm.

REFERENCES

[1] https://www.pcisecuritystandards.org
[2] https://www.wwpass.com/vulnerability-of-one-time-passwords-over-sms/
[3] http://www.mulliner.org/collin/academic/publications/mulliner_dimva2013.pdf
[4] http://link.springer.com/article/10.1007%2Fs11042-014-1888-3
[5] http://www.ijert.org/view-pdf/9806/sms-based-one-time-password-vulnerabilities-and-safeguarding-otp-over-network
[6] http://searchsecurity.techtarget.com/answer/Are-one-time-password-tokens-susceptible-to-man-in-the-middle-attacks
[7] http://www.openauthentication.org/files/download/oathPdf/FAQ1.pdf
[8] http://en.wikipedia.org/wiki/Hash-based_message_authentication_code
[9] http://krebsonsecurity.com/category/data-breaches/page/2/
[10] http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/
[11] http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf
[12]http://www.economist.com/news/finance-and-economics/21596547-why-america-has-such-high-rate-payment-card-fraud-skimming-top
[13]http://www.forbes.com/sites/clareoconnor/2014/01/16/surprise-target-data-breach-could-include-your-info-from-purchases-made-a-decade-ago/
[14] http://time.com/3086359/target-data-breach-loss/
[15] http://www.aba.com/Tools/Function/Payments/Documents/TargetBreachBankImpact.pdf
[16] http://www.cardhub.com/edu/credit-debit-card-fraud-statistics/
[17] http://blog.kraken.com/post/96737897057/the-importance-of-two-factor-authentication
[18] https://discussions.agilebits.com/discussion/38606/totp-problems-with-google-services

