Cyber Retailing – A Concept

Anuradha Bhatia
Sr Lecturer, VES Polytechnic,
Mumbai.
anubhatia1803@gmail.com

Likesh Kolhe
Asst Professor,
TCET, Mumbai.

Gaurav Vaswani
Final Year Student
VESIT, Mumbai.

Abstract: Credit card transactions are becoming life line for financial transaction. But leads to and develops lots of security issues and concerns about the theft of PIN. To prevent fraud transactions by the third part, OTP has come up as a solution. Online transactions are done using PayPal, Paytm. Temporary credit card numbers can be generated and can be used for online transactions along with the OTP generation, which will be send to the customer's registered mobile number. The combination of online capabilities with a physical enterprise is known as Cyber-enhanced retailing. To create a scenario and provide the solution to safe transaction and easy access as an important need.

Keywords: Identity theft, cyber retailing, OTP, PIN, Pseudorandom number generators.

I. INTRODUCTION

Using credit cards in various dealings or transactions is becoming a life service. Easy way of conducting business comes with great risk always. Handing over the credit card to unauthenticated persons like waiters, cashiers brings the risk of identity theft, card number being copied, photographed, even scanned ending with fraud charges or cloning. In the background of credit card protection, fraud transaction prevention, there seem to be no solid solution to ensure the card protection when its securely when it's in used by a third party (cashier, or waiter). Some solutions like OTP (One time Pass word), PIN (Personal Identification Number) came up with security measures whereas OTP failed due to network delays of mobile networks and PIN failed due to compromising the PIN to third party's machine. Some solutions way out to voice authentication if the transaction exceeded a certain limit. Figure 1 shows the credit card usage.

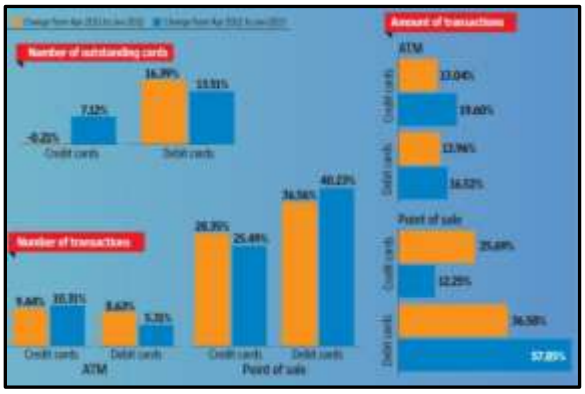


Figure 1: Credit card Usage

II. BACKGROUND

To secure credit card numbers and transactions made by credit cards a vast research has been held. Online systems, such as PayPal, allow more unidentified ways to purchase items without revealing a credit card number to a merchant. Temporary credit card numbers can also be generated that can be used online that also do not render a user's credit card number. Unfortunately, these capabilities do not exist when a user is in an enterprise, such as a restaurant, shopping mall, where they have to use a physical credit card with the above boundaries, there is a terrible need to ensure a secure way of using credit card where the owner of the card is certain that his/her info will not reach the wrong hand. And moreover, the transaction will not be denied due to out of standard flag thrown from the back end. By combining the benefits of online e-commerce security measures with those of traditional physical purchases for the use of credit cards comes to a secure transaction using credit cards. In this paper, we analyze some of the existing methods proposed for secure credit card transaction, also we propose and introduce our approach as a new method that gives the owner to secure his/her card and managing the card by himself/herself to control the payment amount, the time of the transaction, and the merchant whom this transaction is made to.

III. LITERATURE SURVEY

The review and the survey done for the number of frauds happening are compared and shown graphically in Figure 2. The maximum attempts for the frauds are tried on the debit card signatures and customers have suffered the maximum losses.

The debit PINs are saved with key loggers and the customers have suffered the losses.

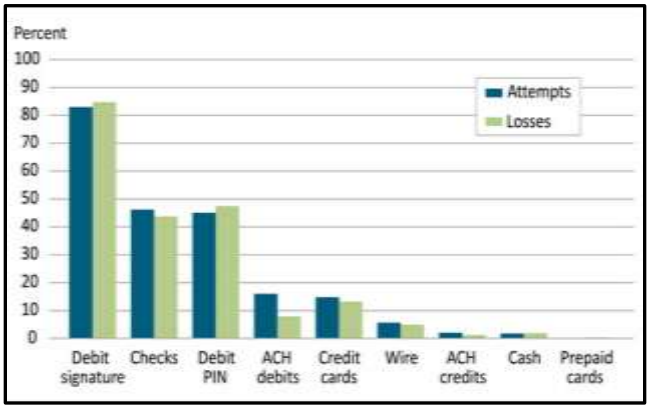


Figure 2: Top three payment types with highest number of fraud attempts

The second survey was carried out to check how often people change their PIN numbers. As shown in the Figure 3, people change only PINs for the first time only when they receive their cards.

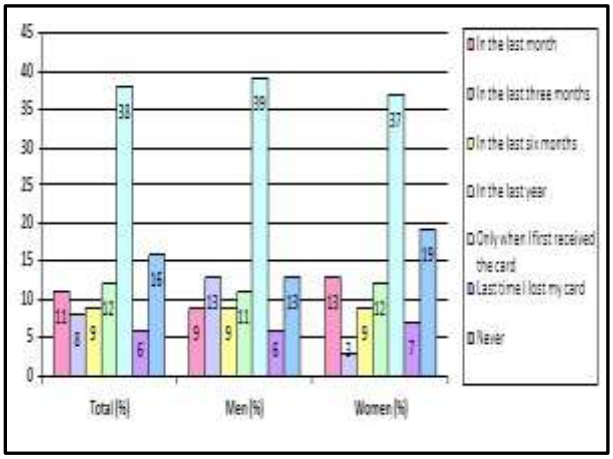


Figure 3: Analysis for the change of PIN

The review and the survey done for the number of frauds happening are compared and shown graphically in Figure 2. The maximum attempts for the frauds are tried on the debit card signatures and customers have suffered the maximum losses.
The debit PINs are saved with key loggers and the customers have suffered the losses.

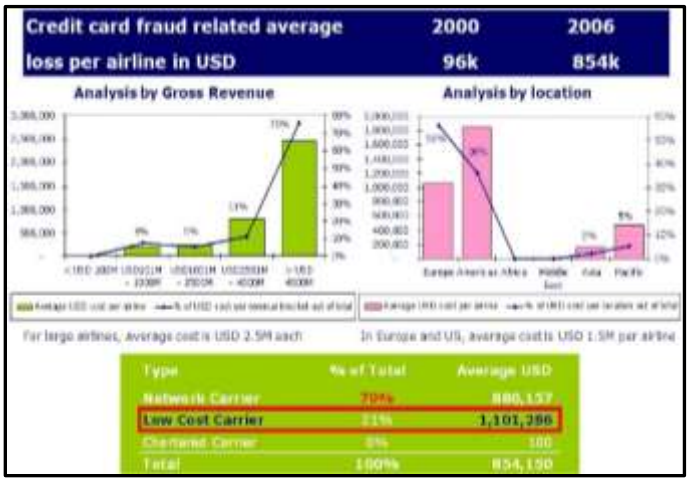


Figure 4: Analysis of Credit Card Fraud

IV. TO GENERATE OTP WILL USE RANDOM NUMBER GENERATION METHOD

Pseudorandom number generators (PRNGs) are algorithms that can automatically create long runs of numbers with good random properties but eventually the sequence repeats (or the memory usage grows without bound. The series of values generated by such algorithms is generally determined by a fixed number called a seed. One of the most common PRNG is the linear congruential generator, which uses the recurrence

$$X_{n+1} = (aX_n + b) \bmod m$$

To generate numbers, where a, b and m are large integers, and X_{n+1} is the next in X as a series of pseudo-random numbers. The maximum number of numbers the formula can produce is the modulus, m. To avoid certain non-random properties of a single linear congruential generator, several such random number generators with slightly different values of the multiplier coefficient a can be used in parallel, with a "master" random number generator that selects from among the several different generators

```
a_b = <choose initializer>;
a_c = <choose initializer>
uint get_random()
{

a_c = 35389 * (a_c & 65535) + (a_c >> 16);

a_b = 16955 * (a_b & 65535) + (a_b >> 16);

return (a_c << 16) + a_b;

}
```

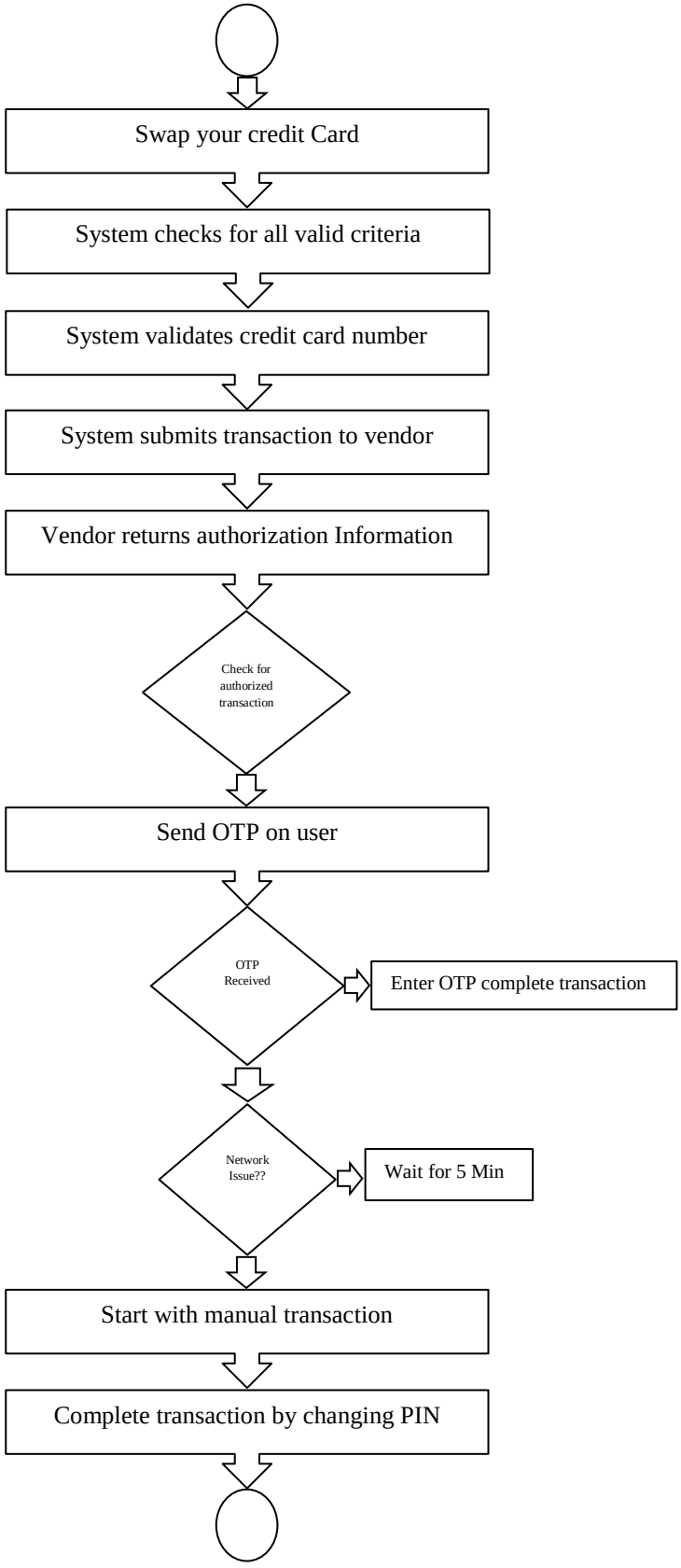
In this method will use recurrence relation to generate random number first will select any two random numbers then with the help of recurrence method will perform some mathematical operations to generate new no and send it to a user as a OTP.

V. TO RESET THE PASSWORD

The best methodology involves authenticating the user, then Message them a one-time reset link. Once the reset link is used, the user is prompted to set a new password. Once that's been done, the link is invalid. Further security can be provided by including expiry times on the links, and enforcing that the link is invalid after the password is set or after the user's session times out.

As we are moving in the era of technology credit card fraud is a very big issue and to avoid it various algorithm and methods are used but it's found that still credit card fraud detection and prevention is biggest issue so to avoid it we can use above method.

Flowchart



Step 1:-Start the process by swapping credit card

Step 2:- System will check for all the requirements (request goes to server for internal verification) server will check for user authentication and if it's found correct it will send response and next step occurs.

Step 3:- Once all above verification procedure is completed then it sends OTP on registered mobile of user to generate OTP its use Random generation method as mention above.

Step 4:- once OTP sends on user mobile user will enter it and complete the transaction process in this way we can improve security and decrease the fraud rate.

Step 5:- Now while performing all above procedure main issue is that there will be a loophole of network issue to solve this issue we address new phenomenon in which if user will not receive an OTP within 5 minutes user will complete transaction by manually. In which user will enter the pin and perform his transaction and whenever user comes in network user will get a message saying that or force to change pin of credit card immediately.

Due to which we can avoid or prevent password catching or grabbing method with the help of fingerprint scanning or camera capturing or any other techniques

And in this way we can't say 100% but will increase security level up to 95%.

VI. RESEARCH METHODOLOGY

Step 1:- Gathering requirement for project like Dataset, Studied Different papers analyzes specification for the project.
Step 2:- Finalize Goals of Project and objectives
Step 3:- Plan and design Research methodology for the project like Business Research Methodology, Problem-solving research, Qualitative Research.
Step 4:- Generate the research result with the help of research methodology and current research data for comparative analysis of project
Step 5: -Interpret result and draw the conclusion that will give more accurate results as compared to existing system.

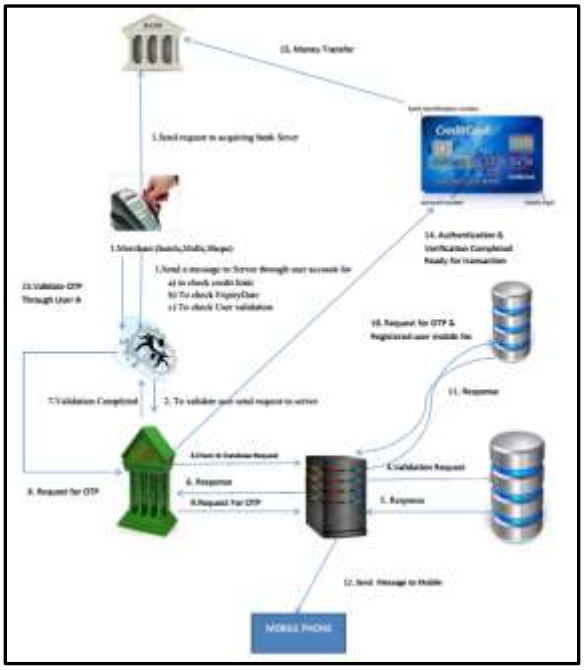


Figure 5: Proposed system

VII. CONCLUSION

Time based number with current solution includes secure credit cards having daily changing security number. The card is divided into two sections. The upper section includes the magnetic strip so it can be read by the commercial credit card readers. The bottom section includes a chip based circuitry that is responsible of generating a new card number every predefined interval. A display window to display the new number and a button to initiate the process and generate a new number as per needed. The security number is the function of the date and their relationship is defined by the predetermined program. Giving a date a corresponding security number can be generated by this predetermined program. Credit Card issuer system would keep track of the card predetermined values and would be able to compute the security number given the date as the number is a function of the timestamp. Both numbers, the one in the credit card issuer and the actual credit card display window are synchronized and identical as both follow the same algorithm. If the card holder decided to use the secure card number, he would enter it to the merchant point of sale and it get communicated to the credit card issuer.

VIII. References

[1] Gemalto's 2014 Breach Level Index
[2] Barclays' Security in Payments: A Look into Fraud, Fraud Prevention, & the Future, May 22, 2015
[3] Financial Fraud Action UK's Fraud The Facts 2015
[4] FICO press release, June 25, 2015
[5] Javelin Strategy & Research 2015 Data Breach Fraud Impact Report
[6] Aite Group's EMV: Lessons Learned and the U.S. Outlook , June 10, 2014
[7] Consumer Sentinel Data Book for January - December 2014
[8] Sallie Mae: How America Pays for College
[9] Forter Study Recap, 2015
[10] Pindrop Security Phone Fraud Report
[11] 2014 LexisNexis True Cost of Fraud mCommerce
[12] Millionaire Corner survey
[13] 2014 Pew Research Center January 2014 survey
[14] Pew Research Center: Americans' Attitudes About Privacy, Security and Surveillance
[15] Telstra's Mobile Identity - The Fusion of Financial Services, Mobile and