An Analysis on Making Secure Payment using Virtual Credit Card Technology for Enhancing Data Security

Abhishek Kumar
Ajeenkya D Y Patil University, Pune

Rahul Kumar
Ajeenkya D Y Patil University, Pune

Nihal Raj
Ajeenkya D Y Patil University, Pune

Altaf Shah
iNurture Education Solutions, Bangalore

ABSTRACT
Today's world moved toward online shopping where everyone has to make online payment. When people make an online shopping, they are confident that our card detail would be safe but the merchant has all my card details. In online shopping people have to share their card details in which sixteen-digit pin number, expiry date, card holder name and cvv required. They need to keep all this information confidential. But in online shopping the requirement is to share all this information that can be hacked and third person can get access to our information about card and they can manipulate and share it with other also and there can be loss of the money and can lose the card too. Security is one of the major concerns in today's era. So, keeping all these problems in mind, technology is trying to create a virtual card. It is randomly generated card depending on issuer. virtual credit card generates a hypothetical card like debit card in which all the details of card like card holder name, sixteen-digit number, expiry date and cvv will mentioned and can make online payment through OTP (one-time password). After the payment the card will automatically blocked and keep the original data safe.

Keywords
Confidential, Authentication, merchants, cvv, pin.

1. INTRODUCTION
The debit or credit card information in online payment doesn't provide proper security. But the implementation of vcc in online payment will make it possible to provide a better security of the sensitive and highly confidential debit/credit card details. So, implementation of vcc in debit or credit card in online payment is a challenging technique. In this paper, there will be a brief introduction to how there can be advancement in online payment, their working and their role and applications. Traditionally, everyone used to purchase our basic need through a merchant like flipkart or Amazon and make the payment online. At the time of making payment one has to fill up all the sensitive card details like card number, card holder name, and most important security pin which is cvv. The virtual credit card will change all of these current trends. One has to upload some balance in it and KYC is important for virtual credit card. These types of card is used for only online transaction ,all the details of card like security pin, expiry date and card number will be generated online only .There is an another option in some cases in which credit card will reach to your doorstep but it is not needed because the talk is about virtual cards only, Those credit card companies which are offering virtual credit card services may utilize a software program that creates a randomly generated virtual card numbers which is a sensitive information that are linked to a customer's physical credit card account or the actual hard copy of the card which user is having. When a customer wants to make an online purchase or payment, they can log in to their credit card account online and utilize their provider's program to generate a temporary account number which is valid for limited minutes.There is a benefit of customer willing to set the spending limits and expiration date for each virtual account number they want; According to convenience, some numerals as well as parameters can be set with an expiry date month in advance, allowing them to create a number to use for purchases expected in the future according to their convenience. In this technology the bank or the credit card company will know that this temporary number is linked to the original cardholder account, but the merchant will not be able to trace this virtual number to the original credit card.

1.2 LOOPHOLES OF TRADITIONALSYSTEMS
a) There was risk of losing the card as people had to carry the physical card wherever they wanted to make payment.
b) In some environments, users used to deliberately share passwords for their own convenience. So, making their sensitive information to risk and increase the chances of fraud.

c) A system that uses only passwords to control access cannot authenticate whether the user identified with a password is really the authorized user.

d) There was high probability of fraudulent activities due to permanent card number allotted and used every time

2. LITERATURE REVIEW
In today's era theft of credit card information is an increasing threat; they use a virtual credit card number that reduces the damage caused by stolen credit card [1]. A user can create multiple virtual credit card numbers that can either be used for single transaction or are attached with particular merchant, but it's all connected to the credit card account [2]. Virtual credit card numbers are more secure than the credit card numbers as it will allocates a random number every time, They generate it but in case of credit cards the number is static [3]. In future there will be widespread acceptance of virtual credit cards as it will provide the implementation of virtual payment automation [4]. virtual credit card provider enhances security and simplicity more suppliers, organizations, travelers credit card holders are seeing opportunities [5].As they know that everything including the creation of vcc is performed online, so there is an enhance in service quality[6].It avoids the unauthorized access in terms of data manipulation as well as currency termination[7].In this technology dynamically allocated credentials can be generated as per users wish[8].If in case of fraudulent activity the card an be blocked remotely which makes it more secure to use[9].This research work lists the advantages and the limitations of electronic digital payment system and tends to be valuable asset towards the technology[10].

2.1 HOW VCC IS DIFFERENT FROM PHYSICAL CREDIT CARD

Although a virtual credit card is called so, it resembles a debit card as the card is already loaded with a certain amount of money, unlike a credit card which has a set credit limit and for which you make payments after your bill cycle is complete and a bill is generated by the issuer.

The uses of virtual card is relatively in small scale because it can only be used for online shopping and only valid for 24-hour after the creation. Due to not issue of physical card, POS (point of sales transaction) is not possible.

The main advantages of a virtual card is in that it can make use of it safely, without any problem, as you do not have to provide details like your credit card number, CVV number and other important details to the merchant. All the details in virtual card are temporary and it is valid for a single purchase only so if it fall somewhere it cannot be reused.

Creation of virtual credit card online for free. It has its own card number, CVV number, Therefore it secures us from online fraud.

When peoples are going to use their credit card for purchasing their needs, but at particular time people are worried about safety for each and every transaction from cyber security.

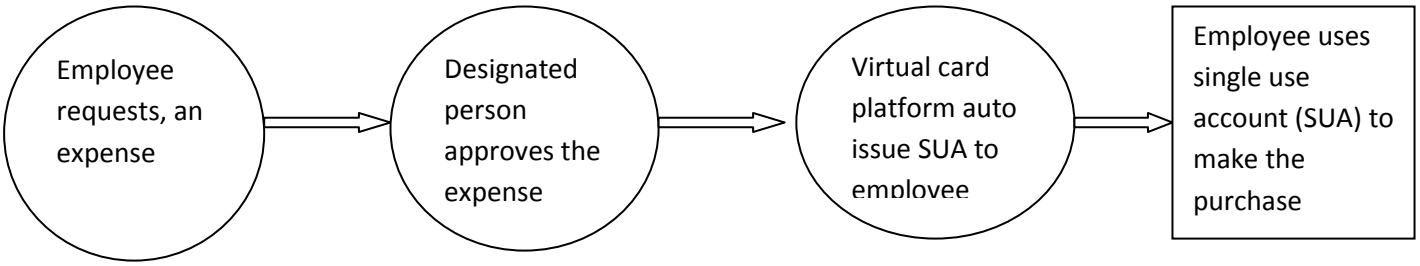

Fig 1: System Architecture

3. STATEMENT OF PROBLEM

The problem with the traditional credit card i.e. physical card Is while applying for credit card they have to do lots of paper work when the customer is applying for the same has to be present there for hours or sometimes for many days and after applying, customer have to pay some minimal amount of money to the bank for proper functioning of the card and its utilization. Once card is issued to customers. Customers have to carry their card with them which is a tedious job which increases the risk of card getting stolen or lost. If it, goes to the wrong hand it can be miss used and may be use for the vulnerable activity that can cause a heavy amount of money loss which will indirectly affect the individual civil score

4. ADVANTAGES

1. This card can be used only once this means chances of misuse is nearly nil
2. This card limit of usage is fixed and cloning of cardinformation is not possible
3. For authentication users will need OTP via SMS same as normal credit card
4. For any amount people can make VCC as per requirement
5. VCC is free card and also banks do not charge anything for card
6. Users can block this card any time you wish to
7. Customer can set their spending limit and the rest of amount on a virtual credit card will be credited back to the original account
8. Virtual card cannot be lost stolen and skimmed
9. If a hacker gets virtual card numbers, they cannot much damage. Because this card number is changed after usesed onces

5. CONCLUSION

It is highly secure because it does not expose customer credit card details. It is valid for 24 hours after the creation and automatically expires after the payment and the remaining amount will be credited back to our saving account. For creation of card, bank will send one-time password (OTP) on registered mobile number and after this verification, transaction considerd as successful.

6. REFERENCES

[1] Molloy, I., Li, J., & Li, N. (2007, February). Dynamic virtual credit card numbers. In International Conference on Financial Cryptography and Data Security (pp. 208-223). Springer, Berlin, Heidelberg.

[2] Chou, Y., Lee, C., & Chung, J. (2004). Understanding m-commerce payment systems through the analytic hierarchy process. Journal of Business Research, 57(12), 1423-1430.

[3] Kfir, Z., & Wool, A. (2005). Picking virtual pockets using relay attacks on contactless smartcard (pp. 47-58). IEEE.

[4] Larsen, J. (2008). De- exoticizing tourist travel: Everyday life and sociality on the move. Leisure Studies, 27(1), 21-34.

[5] Bezos, J. P. (1998). U.S. Patent No. 5,727,163. Washington, DC: U.S. Patent and Trademark Office.

[6] Tushie, D. R., Schaub, S. J., & Younger, T. L. (2001). U.S. Patent No. 6,202,155. Washington, DC: U.S. Patent and Trademark Office.

[7] Ostroff, M. (2006). U.S. Patent No. 7,003,501. Washington, DC: U.S. Patent and Trademark Office.

[8] Kelley, E. E., Motika, F., Motika, P. V., & Motika, E. M. (2003). U.S. Patent No. 6,641,050. Washington, DC: U.S. Patent and Trademark Office.

[9] Tuchler, J., & Crowe, A. (2005). U.S. Patent No. 6,980,969. Washington, DC: U.S. Patent and Trademark Office.

[10] Yu, H. C., Hsi, K. H., & Kuo, P. J. (2002). Electronic payment systems: an analysis and comparison of types. Technology in Society, 24(3), 331-347.