AN INNOVATIVE APPROACH FOR SECURING RFID BASED CARD INFORMATION FROM DIGITAL PICK-POCKETING

DIPANKAR SARKAR
Department of Electrical Engineering, Dream Institute of Technology
drds2b@hotmail.com

MANISH ROY
Department of Computer Science & Engineering, Dream Institute of Technology
manishroy4213@gmail.com,

SANTOSH DAS
Department of Computer Science & Engineering, Dream Institute of Technology
das2008.santosh@gmail.com

ABSTRACT

With the influence of both the advancement of technology as well as the Government of India's mission is to achieve Digital India, the use of plastic money have increased drastically in these days. As a result, the probability of cyber theft is also increasing proportionately. With the availability of low-cost RFID scanner in the market, card details are more vulnerable to cyber theft. For this reason, our approach is to make a special device which will block any unauthorized access of card information wirelessly i.e. it actually ensures the security and confidentiality of the card information as well as it provides the portability of the card also. So, anyone and everyone can easily carry the card and doing their necessary transaction anywhere smoothly.

KEYWORDS: RFID, Digital India, plastic money, cyber theft.

I. INTRODUCTION

We live in a digital world we are always connected to the technology around us. We are unable to think about our present lives without technology. But even though we are digitally connected to the world but it is still not safe for us to say that we are protected digitally. Nowadays we are all using smart cards, i.e., cards which are based on RFID technology. These cards have the capability to store and retrieve information of the user. These cards have the capability to be used wirelessly anywhere anytime. Even though these cards are made secure by the companies but newer ways of digital theft are always happening every now and then. One of the most common ways of stealing information from the user is digital pick pocketing. Here, any individual can easily pickpocket or steal the information present on the cards by the use of skimming devices. The skimming devices are cheap and can be found on the market at very cheap rate. The individual then copies all the information present in the skimming devices and use it for ill purposes. Now there are a bunch of devices present on the market which says that they provide security to the cards. These are basically RFID blocking wallets, RFID blocking sleeves, RFID Wallet Blocking Card Protector, etc. But all these products present on the market don't always provide the complete security as promised hence credential stealing is still possible to an extent.

II. PROPOSED SYSTEM

We are devising a solution where we will be able to protect the smart digital cards from getting duplicated by any individual having a skimming device or a RFID reader. Our proposed solution will have a system which will not only have the capability to protect the cards from any incoming signal from a skimming device but it can also alert the user of the cards about the ongoing theft. Thereby, stopping the theft in progress.

Generally, the skimming device sends a signal to the cards during retrieval of the data from the cards. Now in any normal condition what happens is that the signal from the skimming device actually reaches the cards and then the cards sends back information back to the thief that are present in them.

But we will not let that happen by creating a barrier so that the signal never reaches the cards. Thus the cards won’t send back the data to the skimming device. Thus keeping the data within the cards safe from theft. Now, even though we have protected the card we still are left with the fact the cardholder is still unaware of what's going on around him. Hence, we need to let the person know about this. So what we do is that we actually send a signal to the user’s phone via communication module present within the device and send notification message to the user. Thus, letting the user know how the device has protected his card from getting stolen and that there is a thief nearby who is capable of stealing card details.

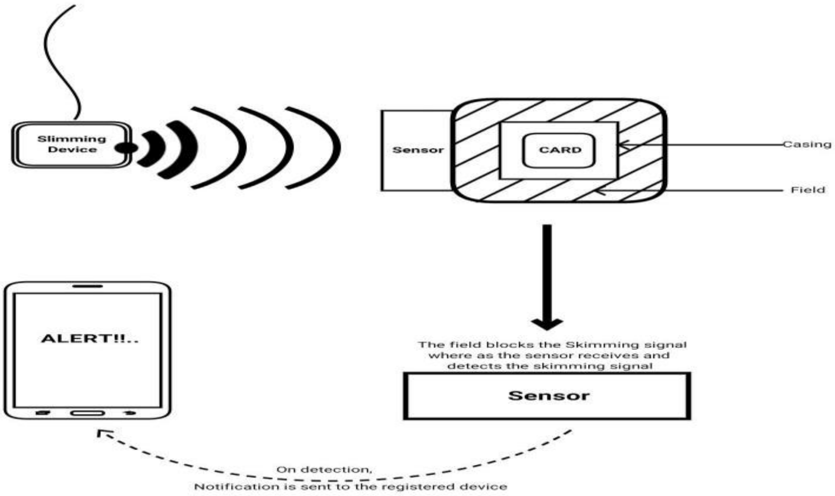
Slimming Device
Sensor
CARD
Casing
Field
ALERT!!..
The field blocks the Skimming signal where as the sensor receives and detects the skimming signal
Sensor
On detection, Notification is sent to the registered device

Fig: Basic Idea of the Approach

III.CONCLUSION

This paper evaluates the advantages of smart card emulation. It is shown that smart card provides a great opportunity to the owners as it smoothens the daily life transactions. Smart card also allows an easy integration of scanning devices for the skimmers. For this card credentials can be easily retrieved and used for illegal purposes. Our proposed idea will protect the card credentials from getting stolen along with, alerting about the ongoing skimming at that moment of time.

REFERENCE

I. Roland M. Software card emulation in NFC-enabled mobile phones: great advantage or security nightmare. In Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use 2012 Jun 18 (pp. 1-6).

II. R. Anderson. Position Statement in RFID S&P Panel: RFID and the Middleman. In Financial Cryptography and Data Security, volume 4886/2007 of LNCS, pp. (46–49). Springer Berlin Heidelberg, 2007.

III. E. Chen. NFC: Short range, long potential. News Article, http://www.assaabloyfuturelab.com/ FutureLab/Templates/Page2Cols____1905.aspx, Aug. 2007.

IV. https://www.androidauthority.com

V. https://www.androidauthority.com

VI. http://ieeexplore.ieee.org/

VII. http://www.emv-connection.com/emv-faq/

VIII. http://www.independent.co.uk/

IX. https://www.tappawallet.com/

X. http://www.securitynewsdesk.com
XI. https://www.thesecurityblogger.com/
XII. http://www.thehindu.com/news/
XIII. https://www.theguardian.com/
XIV. https://www.level2kernel.com/emv-guide.html