ISSN:0975-9646

RFID Detect Credit Card Skimmers using Neural Networks

Dr R.Dhanapal [#1] , Gayathiri.P [#2]
[#1] *Professor and Director*
Research and Development
Procademia

[#2]*Asst.. Professor*
Research Scholar in MSU Univ
Department of Computer Science,
Kanchi Sri Krishna College ,Kanchipuram

***Abstract*— In today's technical world, the safety techniques are being attacked as we usually pay the money by using Credit card, Debit card. Although card skimming techniques are becoming increasingly sophisticated.. In this paper we discuss about skimming The act of using a skimmer to illegally collect data from the magnetic stripe of a credit, debit or ATM card. This information, copied onto another blank card's magnetic stripe, is then used by an identity thief to make purchases or withdraw cash in the name of the actual account holder .skimmers can take card holder information from Gas stations/Restuarants.RFID detect skimmers through RFID electromagnetic waves transmit the Parity bit of data that should be detect the error whether the card holder information such as credit card number ,expiry date and CVV are skimmed or not.it can be implement in Neural Networks , Matlab nftool can detect the error for card holder information encoded in binary format datas are transmit the parity whether if its odd or even parity and detect the error in parity bits.final we will give security for card holders to skimming using Triple-DES(Data Encryption Standard).Triple-DES encryption result analysis in Apache tom cat .**

Keywords :Magnetic Stripe; Neural Networks; Skimming; ATM; RFID; TripleDES

I.INTRODUCTION

In credit card skimming schemes, thieves use a device to steal credit card information in an otherwise legitimate credit or debit card transaction. For example, credit card skimming devices are often placed on ATMs or even held in the hands of waiters and store employees. When a credit card is run through a skimmer, the device stores the credit card information. Thieves use the stolen data to make fraudulent charges either online or with a counterfeit credit card. In the case of ATM and debit cards, thieves withdraw cash from the linked checking account. information can be Skimmed from your credit card using one of these portable scanners.The credit card transaction is then performed normally, and your card is handed back to you. But with your personal information, identity thieves can make counterfeit credit cards which can then be used for illegal shopping .The information contained on hundreds of credit cards' magnetic strips can be read and recorded on these small devices. Skimming can also take place at ATMs, gas stations and restaurants.

A. ATM Skimming

ATM skimming is when thieves attach devices onto the ATM machines that will copy your credit or debit card information on the magnetic strip and even your personal identification number.ATM Machines Theft of card data from ATM machines is known as skimming. This is accomplished with the help of simple card reading equipment and a small camera that records an individual when he punches in his PIN. PIN number is then either observed by a person shoulder surfing or by a hidden pinhole camera installed on the machine and pointed at the keypad.This is why it is a good idea to cover your keypad with your hand even when alone at an ATM machine.Fraudsters don't need to return to the ATM machine to extract the video and card information because many of these skimming devices also have wireless capabilities. Fraudsters can comfortably and anonymously sit in their car, hundreds of feet away, and retrieve the information wirelessly.

B.Gas Station Credit Card Skimming

Gas station Credit Card Skimmers are external devices thieves attach over a real credit card slot at a gas station pump As customers swipe their cards into the skimmer, the device saves and stores card information immediately. If a credit card slot looks different from the other card readers at the station, it may be a setup for gas station credit card skimming fraud. Skimming devices are meant to be placed temporarily for a matter of hours or just a day.For that reason, they are attached using only double-sided tape, so thieves can easily remove them. Before sliding a credit card through the machine, tug on the reader to ensure it is on securely; skimmers will easily pop off with mild effort.

C.Restaurants/Retail store Skimming

Some scammers have devised ways to tamper with the card readers at retail stores. Malicious smart cards that look like legitimate cards are created and then inserted into the machines to make a payment. However, the machine simply says than an error has occurred and the retail store merchant

is unaware of the damage that has been done. When a genuine payment is made with a valid card over the same machine in the future, the details of that card get recorded. Now the scammer revisits the store after a day or two and inserts the fraudulent card into the machine to make another seemingly innocent payment. Details about all the cards that have been inserted in the interim period are now transferred into the malicious card which can be viewed by the scammer via another device. Credit card skimming incidents can be difficult to detect since the credit cards are never lost or stolen. The best way to detect a skimmed credit card is to watch your accounts frequently. Monitor your checking and credit card accounts online daily and immediately report any suspicious activity.Watch where you shop. Restaurants, bars, and gas stations seem to be the places where credit card incidents happen most frequently.

II.RFID CARD DETECT SKIMMERS

RFID(Radio Frequency Identificatiion) credit cards use a radio frequency to transmit personal financial data. They are not swiped through a scanning machine like a traditional credit card. Unfortunately, RFID credit cards can be skimmed when an unauthorized user grabs the unencrypted data from your card using an RFID reader. Credit card companies are aware of the problem and are creating security fixes, but there are a number of steps you can take to protect your financial information.Credit cards that use radio frequency identification, or RFID, technology were developed so cardholders could simply hold or wave their cards in front of a reader instead of swiping it at a machine. The card reader known as a PayPass reader scans the card and processes a transaction without a signature. A traditional credit card uses a magnetic strip to store account information, which is retrieved when swiped through a credit card machine.

A.RFID Card Detecting Error Using Neural Networks

A swipeless or contactless credit card uses RFID to store the same information within a smart chip. The chip is embedded within the credit card itself. When exposed to a contactless credit card reader, the electromagnetic waves emitted by the reader initiate the chip to respond via a small radio antenna, which then transmits the data through a parity bit, or check bit, is a bit added to the end of a card holder data of binary code that indicates whether the number of bits in the card holder data with the value one is even or odd. Parity bits are used as the form of Error Detecting Code.There are two variants of parity bits: even parity bit and odd parity bit. In case of even parity, the parity bit is set to 1, if the number of ones in a given set of bits (not including the parity bit) is odd, making the number of ones in the entire set of bits (including the parity bit) even. If the number of ones in a given set of bits is already even, it is set to a 0. When using odd parity, the parity bit is set to 1 if the number of ones in a given set of bits (not including the parity bit) is even, making the number of ones in the entire set of bits (including the parity bit) odd. When the number of set bits is odd, then the odd parity bit is set to 0 and It can be calculated via an XOR sum of the bits, yielding 0 for even parity and 1 for odd parity. This property of being dependent upon all the bits and changing value if any one bit changes allows for its use in error detection through the card issuer's network Triple Data Encryption Standard (DES) cryptography, and operates at 13.56 MHz. American Express advertising show a fake RFID chip and antenna.for example credit card data information such as card number,expiry date and CVV given in Table 1.

If an odd number of bits (including the parity bit) areTransmitted incorrectly, the parity bit will be incorrect, thus indicating that a parity error occurred in the transmission. The parity bit is only suitable for detecting errors.

Field	Length	Example
Credit Card Number	16 digits	3760666666555551
Expiry date	4 digits	1205
CVV	4 digits	1234
Total	24 digits	

For this example total 24 bits data encoded in to Binary Format.The parity bit sending a 4 bit value such as 3 can be converted in to binary value of 0011 that can compute through XOR gate.Even Parity A wants to transmit the first bit 0011 and its parity is10010 shows in figure 4.

B. Even Parity

A Parity	0	0	1	1	0	
B Paity	0	0	1	1	0	0
Class	B Reports correct even parity Transmission					

C. Odd Parity

A Parity	0	0	1	1	1	
B Paity	0	0	1	1	0	1
Class	B Reports correct Odd parity Transmission					

D. Error Detection in Failed Transmission

A Parity	0	0	1	1	0	
B Paity	1	0	1	1	0	1
Class	Error in first bit incorrect Transmission					

Similar like other 23 bits also detecting error in credit card information.if it is skimming that can shown in Table2.

Table 2 for Detect Errors in Skimming Datas

Card Nos	A	Parity (Even)	Parity (Odd)	Error Detection
3	0 011	00110	00111	10111
7	0111	01110	01111	00111
6	0110	01100	01101	00011
2	0010	00101	00100	00110
5	0101	01010	01011	01110
4	0100	01000	01001	01010
1	0001	00011	00010	01011
0	0000	00000	00001	00010

III. SECURITY FOR RFID

The Triple Data Encryption Standard (DES) is a block cipher encrypting the credit card number as a single block in ECB Mode. Block ciphers are permutations, so this would satisfy the requirements. Block size of Triple DES is 64 bits. If we use ECB mode to encrypt, that's how long the resulting cipher text will be. We'll never be able to encode something that long back to a 16-digit decimal number. Theoretically, a skimmer could build such a device and walk through a crowd, lifting information from nearby credit cards with RFID tags. But here's the good news -- the cards tested in Massachusetts were old, first-generation models with little or no security protection. A TDEA encryption/decryption cipher operation is a compound operation of the DEA encryption/decryption data transformation. A TDEA key consists of three 64 bit keys; these groups of keys (Key1, Key2, and Key3) (In TDEA when key1 = key2 = key3.The plaintext for the example is selected from the ASCII encoding of the phrase Shown in table1 37606666 66555551 12051234 In this example, all keys, plaintext and ciphertext are expressed in ASCII Encoding.of the above phrase is segmented as follows:

Table 1 for encoded data

37606666	7`ff
66555551	fUUQ
12051234	4

P1=37606666 =7`ff

	Input	Output
DES1 – Encrypt – Key1	7`ff	799B3569449FF453
DES2 – Decrypt – Key2	799B3569449FF453	1926087BEFF1D4C8
DES3 – Encrypt – Key3	1926087BEFF1D4C8	9861389E1163B46

The input to DES1 is Plain Text P1, and the output of of DES1 is "799B3569449FF453".The input to DES2 is the output of DES1,and the output of DES2 is 1926087BEFF1D4C8". The input to DES3 is the output of DES2,and the output of DES3 is "9861389E1163B462". The output of DES3 is the cipher text C1.

C1=9861389E1163B462

During the second TDES operation, the input is P2, and the output after the three passes is cipher text C2.

P2 = "66555551" = FUUQ

	Input	Output
DES1 – Encrypt – Key1	fUUQ	87070435EC814413
DES2 – Decrypt – Key2	87070435EC814413	6CD9AEB720EBE653
DES3 – Encrypt – Key3	6CD9AEB720EBE653	DBDCE8A907C3B855

C2= DBDCE8A907C3B855

During the third TDES operation, the input is P3, and the output after the three passes is ciphertext C3.

P3="12051234" = 4

	Input	Output
DES1 – Encrypt – Key1	4	2442BF288152687A
DES2 – Decrypt – Key2	2442BF288152687A	CDF604474BC55F4C
DES3 – Encrypt – Key3	CDF604474BC55F4C	1F690255DB9B9AF7

C3=1F690255DB9B9F7

The resulting ciphertext is the concatenation of C1, C2 and C3 (i.e., 9861389E1163B462DBDCE8A907C3B8551F690255DB9B9AF7

Example using Triple DES

Key

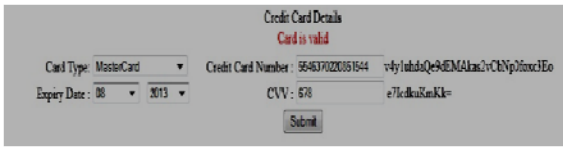
0x0123456789ABCDEFFEDCBA987654321089ABCDEF01234567

3DES INPUT BLOCKS:

55463702208515446780813

3DES OUTPUT:

v4y1uhdaQe9dEMAkas2vCbNp0foxc3EoRZ6MMKOkKwE=e7IcdkuKmKk=

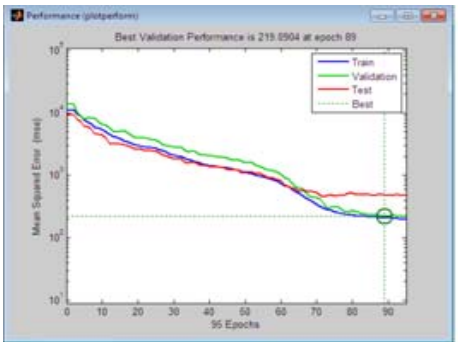


IV. Result Analysis in Neural Networks

We will try a single hidden layer of 20 neurons for this example. In general, more difficult problems require more neurons, and perhaps more layers. Simpler problems require fewer neurons.Now the network is ready to be trained. The samples are automatically divided into training, validation and test sets. The training set is used to teach the network. Training continues as long as the network continues improving on the validation set. The test set provides a completely independent measure of network accuracy.

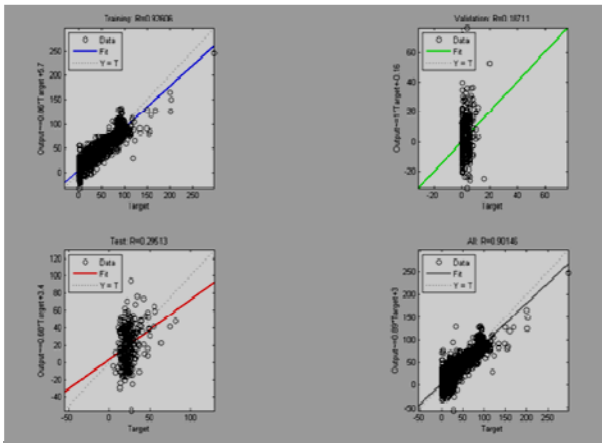
A.Preparing the Data

Data for function fitting problems are set up for a neural network by organizing the data into two matrices, the input matrix X and the target matrix T.We can view the sizes of inputs X =65and targets T=280. These represent 345 attributes (inputs) and associated median class(targets).The network's performance improved during training, Performance is measured in terms of mean squared error, and shown in log scale. It rapidly decreased as the network was trained.Performance is shown for each of the training, validation and test sets.



B.Testing the Neural Network

The mean squared error of the trained neural network can now be measured with respect to the testing samples. This will give us a sense of how well the network will do when applied to data from credit card datas should be skimmed or not.Another measure of how well the neural network has fit the data is the regression plot. Here the regression is plotted across all samples.The regression plot shows the actual network outputs plotted in terms of the associated target values of skimmed card . If the network has learned to fit the data well, the linear fit to this output-target relationship should closely intersect the bottom-left and top-right corners of the plot.



Regression is plotted across all samples.The regression plot shows the actual network outputs plotted in terms of the associated target values of skimmed card . If the network has learned to fit the data well, the linear fit to this output-target relationship should closely intersect the bottom-left and top-right corners of the plot

V Conclusion

RFID electromagnetic waves transmit the Parity bit of data that should be detect the error in the bit through the neural networks Matlab nf tool. encoded binary format data detect the error and find out the performance accuracy is 219.99,valdation accuracy of data is 0.1,training data accuracy is 0.9,test data accuracy is 0.2,overall training ,testing, validating accuracy of data is 0.9.we finally detect the error and protect from skimmers through Triple DES.Triple DES encryption/decryption cipher operation is a compound operation of the DEA encryption/decryption data transformation. The plaintext such as Account Number,Expiry Date and CVV is selected from the ASCII encoding all the information and protect the datas from skimmers.. The results of prediction accuracy are comparable to the trial-and-error method. This research is conducted for the credit card datas should be skimmed or not and protection for skimmers whether the data is skimmed using Triple DES.

ACKNOWLEDGMENT

I Gradually Thanks to Senior Software Programmer K.Ezhil Raja for the encouragement and many helpful suggestions and also thanks to Kanchi Sri Krishna College of Arts and Science and the Department of Computer Science .

REFERENCES

[1] Alomair, Basel, and Radha Poovendran. "Privacy versus Scalability in Radio Frequency Identification Systems." Computer Communication, Elsevier. 2010.

[2] Burmester, Mike and de Medeiros, Breno and Motta, Rossana. "Provably Secure Grouping-Proofs for RFID Tags." Smart Card Research and Advanced Applications (CARDIS), 2008.

[3] Cai, Shaoying, Yingjiu Li, Tieyan Li, Robert H. Deng, and Haixia Yao. "Achieving High Security and Efficiency in RFID-tagged Supply Chains." International Journal of Applied Cryptography. 2010.

[4] Capkun, Srdjan and El Defrawy, Karim and Tsudik, Gene. GDB: Group Distance Bounding Protocols. arXiv.org, 2010.

[5] Chatmon, Christy, Tri van Le, and Mike Burmester. Secure Anonymous RFID Authentication Protocols. Florida State University Technical Report, 2006.

[6] Chothia, Tom, and Vitaliy Smirnov. "A Traceability Attack against e-Passports ." Financial Cryptography, 2010.

[7] Floerkemeier, Christian, Roland Schneider, and Marc Langheinrich. "Scanning with a Purpose -- Supporting the Fair Information Principles in RFID Protocols." International Symposium on Ubiquitous Computing Systems. 2004.

[8] Garcia, Flavio, et al. "Dismantling MIFARE Classic." European Symposium on Research in Computer Security (ESORICS), 2008.

[9] Gershenfeld, Neil, Raffi Krikorian, and Danny Cohen. "The Internet of Things." Scientific American. 2004.

[10] R.Dhanapal ,P.Gayathiri Credit Card Fraud Detection Using Decision Tree For Tracing Email and IP IJCSI International Journal of Computer Science Issues,Vol.9,Issue 5,No 2,ISSN 2012 ISSN(Online):1694-0814

[11]Chip and SPIN!, available at www.chipandspin.co. uk/problems.html.

[12]Associated Press, 2003, “Wave the card for instant credit,” Wired.com, December 14, available at http://tinyurl.com/yc45ll.