iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4015

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Towards Detecting Compromised Accounts on Social Networks

S. Santhosinidevi[1], G. R. AnuVarshini[2], S. Annalakshmi[3,] A. M. SenthilKumar[4], M. S. Vijaykumar[5]
[1, 2, 3] *Dept. of CSE, Tejaa Shakthi Inst. of Tech. for Women, Coimbatore, Tamil Nadu, India*
[4]*HOD* , [5]*Assistant professor*
[4, 5]*Dept. of CSE, Tejaa Shakthi Inst. of Tech. for Women, Coimbatore, Tamil Nadu, India*

Abstract: Identity crime is well known, prevalent and costly, where in that credit application fraud is a specific case of identity crime. The existing non data mining detection system of business rules and scorecards and known fraud matching have limitations. To address these limitations and combat identity crime in real time and to deal with the security issue in the early stage of system development, this paper presents a formal method for modeling and verification of online shopping business processes with malicious behavior patterns considered based on User Personal Details. We propose a formal model called E-commerce Business Process Net to model a normal online shopping business process that represent intended functions and malicious behavior patterns representing a potential attack that violates the security goals at the requirement analysis phase. Incidents of this nature put the identity of customers at risk as hackers are able to access their personal data, sometimes including credit card details, email addresses their password, If an incoming credit card transactions is not accepted by the trained value with sufficiently high probability, it is considered to be fraudulent. At the same time, we try to ensure that genuine transaction is not rejected. We focus on the complex malicious behavior patterns that can be used to identify theft and illegitimate behaviors caused by card. It can lead to substantial financial loss to the credit card company. In the second kind of the purchase, only some important information about the card (card number, expiration date, secure code) is required to make the payment. Such purchases are done on the internet or over the telephone. To commit fraud in these types of purchases, a fraudster simply needs to know the card details.

I. INTRODUCTION

Credit-card-based purchases can be categorized into two types, 1.physical card and 2.virtual card. In the first case card holder directly presents his card to the merchant for making the payment, but in this type of purchase the fraudster can easily steal the card holder's card .If the card holder does not realize the loss of card, it can lead to a substantial financial loss to the credit card company. In the second kind of purchase, only some important information about a card (card number, expiration date, secure code) is required to make the payment. Such purchases are normally done on the Internet or over the telephone. To commit fraud in these types of purchases, a fraudster simply needs to know the card details. Most of the time, the genuine cardholder is not aware that someone else has seen or stolen his card information. The only way to detect this kind of fraud is to analyze the spending patterns on every card and to figure out any inconsistency with respect to the "usual" spending patterns. Fraud detection based on the analysis of existing purchase data of cardholder is a promising way to reduce the rate of successful credit card frauds. Since humans tend to exhibit specific behaviorist profiles, every cardholder can be represented by a set of patterns containing information about the typical purchase category, the time since the last purchase, the amount of money spent, etc. Deviation from such patterns is a potential threat to the system.

II. PRELIMINARIES

A. New card

If the customer is new, then he/she have to register his/her contact details. For that they have to create their own username and password for their use.

B. Login

In the login form module, the username and password fields will be there. If the user enters the username and password correctly then only the user will be granted to access the additional resources on websites.

C. Security Information

In the security information module, it will store the information about the user in the database, in the situation when the card is lost or the amount which is given crosses the limit then the security questions will arises and if it correct only the transaction part gets successfully completed. It contain informational privacy and informational self-determination are addressed squarely by the invention affording persons and entities a trusted means to user, secure, search, process, and exchange personal and/or confidential information.

D. Cryptographic Image

This is the new technique which is also arised for the purpose of secure transactions. Here the user have to match the image correctly then only the transaction gets successfully completed.

E. Transaction

The method and apparatus for pre-authorizing transactions includes providing a communications device to a vendor and a credit card owner. The credit card owner initiates a credit card transaction by communicating to a credit card number, and storing therein, a distinguishing piece of information that characterizes a specific transaction to be made by an authorized user of the credit card at a later time. The information is accept as “network data” in the data base only if a correct personal identification code (PIC) is used with the communication. The "network data" will serve to later authorize that specific transaction. Because the transaction is pre-authorized, the vendor does not need to see or transmit a PIC.

F. Verification

Verification information is provided with respect to a transaction between an initiating party and a verification-seeking party, the verification information being given by a third, verifying party, based on confidential information in the possession of the initiating party. In verification the process will seeks card number and if the card number is correct the relevant process will be executed. If the number is wrong, mail will be sent to the user saying the card no has been block and he can’t do the further transaction.

III. RSA ALGORITHM

The asymmetric key algorithm which is also called as public key cryptography is used to encrypt and decrypt the messages called RSA algorithm. Two different keys are used in asymmetric key algorithm. , the encryption key is public and it is different from the decryption key which is kept secret. RSA is one of the first public-key cryptosystems which is widely used for secure data transmission. RSA is a cryptosystem for public-key encryption which is used for securing sensitive data, from the insecure network such as internet.

IV. SMTP ALGORITHM

SMTP uses a process called “store and forward” which act as a part of the application layer of the TCP/IP protocol. Here SMTP works with a Mail Transfer Agent called MTA to send the communication to the right computer and email inbox. To send and receive mail messages the SMTP is used by the e- mail servers and other mail transfer agents. User-level client mail applications typically use SMTP only for sending messages to a mail server for relaying and for retrieving messages, client applications usually use either IMAP or POP3.

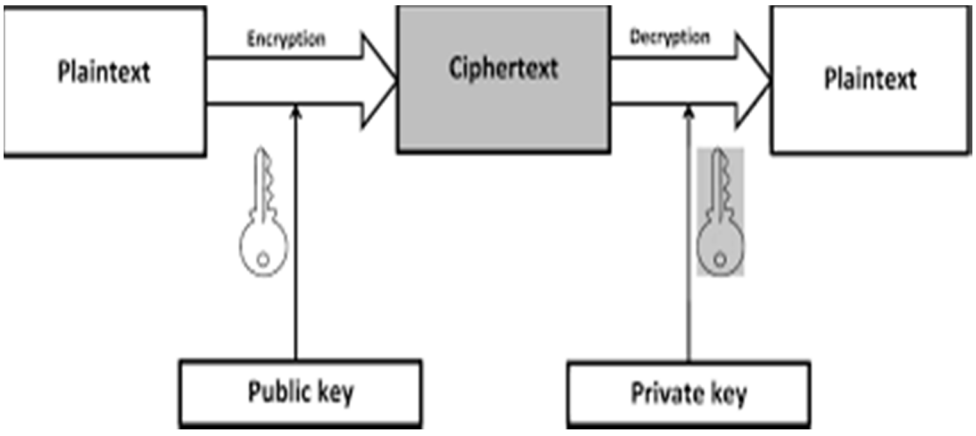


Fig 1: SMTP protocol

V. EXISTING SYSTEM

In case of the existing system the fraud is detected after the fraud is done, the fraud is detected after the complaint of the card holder. The card holder faced a lot of trouble before the investigation finish. And also as all the transaction is maintained in a log, we need to maintain a huge data. And also now a day's lot of online purchase are made so we don't know the person how is using the card online, we just capture the IP address for verification purpose. So there need a help from the cyber-crime to investigate the fraud. To avoid the entire above disadvantage we propose the system to detect the fraud in a best and easy way, and used only symmetric key to Mobile number.

VI. DRAWBACK OF EXISTING SYSTEM

It has a less security level and its key size is fixed. Easily Hacker can access our password using Phishing attack. The larger failure was human, namely, it was in how the risk models were applied.

VII. PROPOSED SYSTEM

In Banking Gateway we demonstrate asymmetric key for protection using RSA algorithm, and we are using SMTP protocol to generate key for e-mail and also we are using SMSC vendor to generate secret key for mobile. The parameters which are passed in an HTTP request and it return value varies between SMS gateways of different SMS service providers and wireless carriers. In transaction of merchant SMTP handles exchange of messages between e-mail servers over TCP/IP network. From the above process we are planned to detect the fraud using credit Limit in Banking Gateway, and using this gateway we protect from phishing attack.

VIII. ADVANTAGES OF PROPOSED SYSTEM

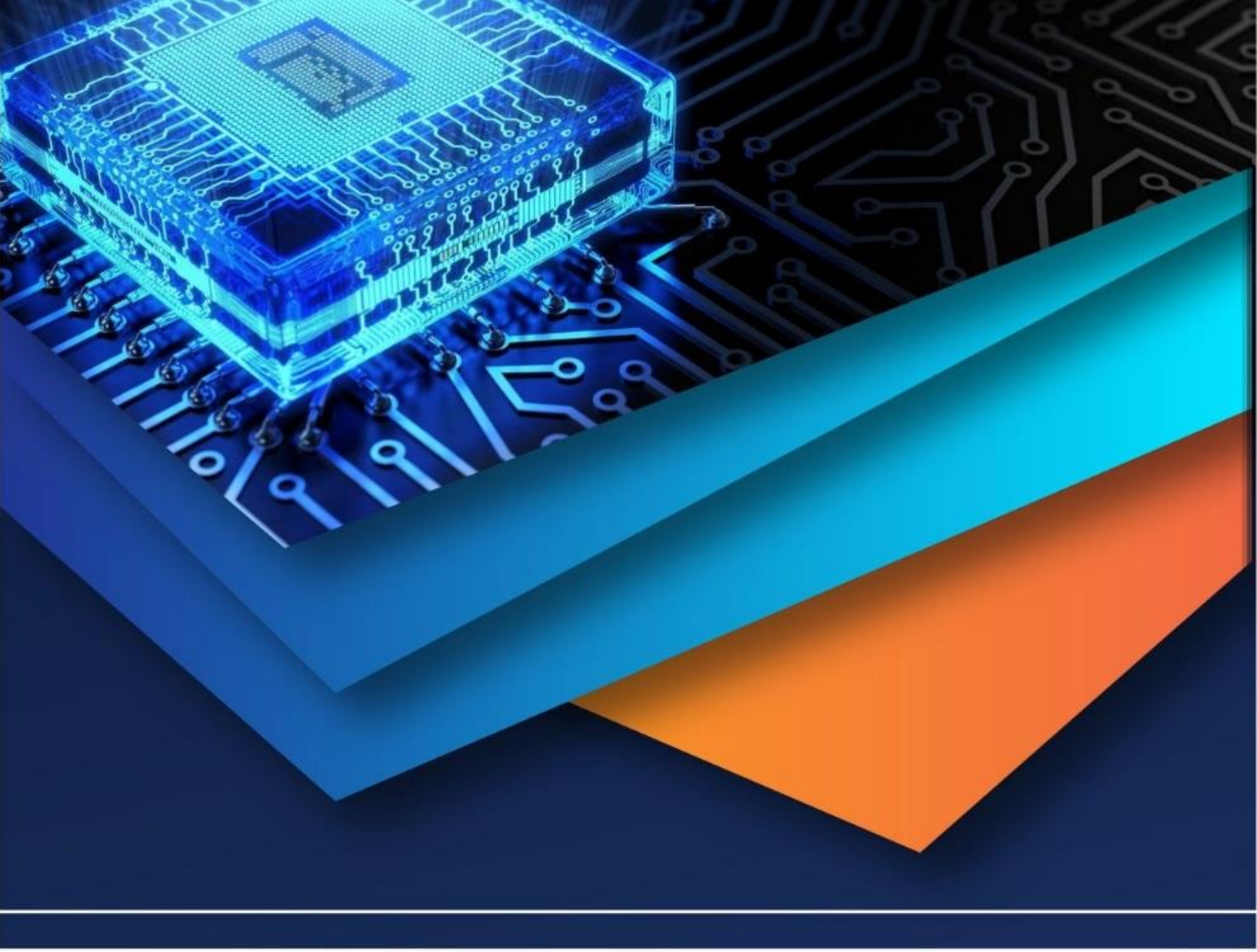
In this length of the Key is not fixed for future prediction .In case, message cannot be delivered, an error report is sent to the sender which makes SMTP a reliable protocol, and using Asymmetric key it increase the security level.

IX. CONCLUSION

In this project, we have proposed an application of HMM in credit card fraud detection. The different steps in credit card transaction processing are represented as the underlying stochastic process of an HMM. We have used the ranges of transaction amount as the observation symbols, whereas the types of item have been considered to be states of the HMM. We have suggested a method for finding the spending profile of cardholders, as well as application of this knowledge in deciding the value of observation symbols, whereas the types of item have been considered to be states of the HMM. We have suggested a method for finding the spending profile of cardholders, as well as application of this knowledge in deciding the value of observation symbols and initial estimate of the model parameters. It has also been explained how the HMM can detect whether an incoming transaction is fraudulent or not

. REFERENCES

[1] Global Consumer Attitude TowardsOlineShopping"http://www2.acnielsen.com/reports/documents/2005_cc_onlineshopping.pdf, Mar. 2007.
[2] D.J.Hand, G. Blunt, M.G. Kelly, and N.M. Adams, "Data Mining for Fun and Profit, "Statistical Science, vol. 15, no. 2, pp. 111-131, 2000.
[3] Statistics for General and On-line Card Fraud"http://epaynews.com/statistics/fraud.html, Mar. 2007.
[4] Ghosh and D.L. Reilly, "Credit Card Fraud Detection with a Neural-Network", Proc. 27th Hawaii Int'l Conf. System Science: Information Systems: Decision Support and Knowledge-Based System, vol. 3, pp. 621-630, 1994
[5] M. Syeda, Y.Q. Zhang, and Y. pan, "Parallel Granular Networks for Fast Credit Card Fraud Detection", Proc. IEEE Int'l Conf. Fuzzy Systems, pp. 572-577, 2002.
[6] C. Li and Y. Cai, "Supervisor control for fuzzy discrete event system with blocking," in Proc. 6th IEEE Int. Conf. Fuzzy Syst. Knowl. Discovery, Tianjin, China, 2009, pp. 432–436. [7] M. Hassan et al., "Passive supervisor for railway fault-tolerant Ethernet networked control systems," in Proc. 16th Conf. Emerging Technol. Factory Autom., Toulense France, 2011, pp. 1–4.
[7] S. G. Wang, C. Y. Wang, and M. C. Zhou, "Design of optimal monitor-based supervisors for a class of Petri nets with uncontrollable transitions," IEEE Trans. Syst., Man, Cybern: Syst., vol. 43, no. 5, pp. 1248–1255, Sep. 2013
[8] R. Cordone and L. Piroddi, "Parsimonious monitor control of Petri net models of flexible manufacturing systems," IEEE Trans. Syst., Man, Cybern., Part A: Syst, vol. 43, no. 1, pp. 215–221, Jan. 2013
[9] H. Hesuanet al.,"Deadlock-free control of automated manufacturing systems with flexible routes and assembly operations using Petri nets," IEEE Trans. Ind. Informat., vol. 9, pp. 109–121, Feb. 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY