A DEFENSE MECHANISM FOR CREDIT CARD FRAUD DETECTION

M.Sasirekha1, Sumaiya Thaseen .I2 and Saira Banu.J3
1,2 & 3School of Computing Science and Engineering, VIT University, Tamil Nadu, India.
sasirekhamahalingam@gmail.com,sumaiyathaseen@gmail.com,
baniu3@gmail.com

ABSTRACT

Computer security is one of the key areas where lot of research is being done. Many intrusion detection techniques are proposed to ensure the network security, protect network resources and network infrastructures. Intrusion detection systems (IDS) attempt to detect attacks by gathering network data and analyze the information from various areas to identify the possible intrusions. This paper proposes a defense mechanism combining three approaches such as anomaly, misuse and decision making model to produce better detection accuracy and a decreased false positive rate. The defense mechanism can be built to detect the attacks in credit card system using Hidden Markov approach in the anomaly detection module. The credit card holder’s behaviours are taken as attributes and the anomalous transactions are found by the spending profile of the user. The transactions that are considered to be anomalous or abnormal are then sent to the misuse detection system. Here, the transactions are compared with predefined attack types such as cross site, SQL injection and denial of service attacks and then sent to the decision making model to classify it as known/unknown type of attack. Finally, the decision-making module is used to integrate the detected results and report the types of attacks in credit card system. As abnormal transactions are analyzed carefully in each of the module, the fraud rate is reduced and system is immune to attacks.

KEYWORDS


1. INTRODUCTION

The amount of online shopping is increasing day by day and millions of people are using the online services to fulfil their needs. As a result a large number of credit card transactions are being carried out in the net. These credit card transactions are vulnerable to malicious intruders attempting to negotiate on the integrity, confidentiality or any resource availability. The spending pattern of the card holder has to be analysed to determine if any inconsistency occurs in comparison with the usual pattern. Hence a defense mechanism is proposed to detect the attackers by analyzing the spending profile of the customer along with the type of purchase. Many fraud detection systems have been proposed using data mining and neural network approaches but a prototype combining anomaly detection, misuse detection and decision making model has not been developed for a credit card fraud system. As the system is of hybrid nature, it attempts to increase the detection attack rate and also reduce the number of false positives which is of major concern in any IDS.

The rest of the paper is organized as follows. In section 2 we summarize the relevant work on intrusion and fraud detection systems. Section 3 discusses the detailed description of the proposed system. The results are discussed in section 4. Section 5 concludes the paper.

DOI:10.5121/ijcis.2012.2308
2. RELATED WORK

Many anomaly defense mechanisms have been proposed in the literature. We briefly discuss some of the proposed solutions. Ghosh and Reilly [10] proposed a neural network for credit card fraud detection. Stolfo et al. [11] [12] developed a credit card fraud detection system (FDS) using meta learning techniques to study models of fraudulent credit card transactions. Performance metrics like True Positive—False Positive (TP-FP) spread and accuracy have been defined by them. The BOAT adaptive method was proposed by sherly et al [15]. Each individual transaction amount depends on the purchase of the corresponding type of item. Standard performance metrics, True Positive (TP) and False Positive (FP) are used to characterize the effectiveness of the system. Then the fraudulent transactions are identified. The difficulty with most of the above specified approaches is that they need labelled data for both real as well as fraudulent transactions to train the classifiers. In contrast, we present a Hidden Markov Model (HMM)-based credit card FDS, which does not need fraud signatures and yet it is able to identify frauds by considering the spending habit of the credit card holder.

Ourston et al. [13] have proposed the application of HMM in identifying multistage network attacks. Hoang et al. [14] present a innovative method to analyze series of system calls for anomaly detection using HMM. Another major advantage of the HMM-based approach is a severe decrease in the number of False Positives (FPs)—transactions detected as malicious by a FDS although they are actually genuine. Hence with the tremendous increase in attacks, there is a need to design an Intrusion Detection System that secures the credit card sector.

3. PROPOSED SYSTEM

The proposed system uses the Hidden Markov Model to identify fraudulent transactions in the anomaly detection module. HMM is advantageous over other statistical approaches because it effectively reduces the false positive rate which is an important metric to measure the performance of Intrusion Detection System. The fraudulent transactions identified in the anomaly detection module are sent to Misuse detection module to identify the type of fraud. The role of anomaly module is to identify the fraud and the role of misuse module is to classify the fraud. Then the results are sent to decision making model.

![Fig 1: Proposed Architecture of Defense model for credit card fraud detection](image-url)
3.1. Anomaly Detection Module

The HMM model is mainly used to identify the false positive attacks. The false positive attack is the number of normal transactions that are identified as anomalous. The types of purchase are the hidden states. The new transaction is classified as anomalous or normal transaction based on the transaction history. Using the HMM [2], the user is grouped based on his spending profile. The false positive rate is the number of normal transactions identified as anomalous. The False Positive Rate (FPR) is identified using the following formula,

\[ \text{FPR} = \left( \frac{\text{Number of anomalous transactions}}{\text{Number of normal transactions}} \right) \times 100\% \]

Figure 2: Block Diagram of Anomaly Detection Model

Figure 3: State Transition Diagram of credit card system
3.2. Misuse Detection Module

Misuse detection is an effective approach to handle attacks that are known by the system. When the particular type of attack is identified, the result is sent to Decision Making Module. The attacks are Cross-site (XSS), SQL, Denial Of Service can be identified using this module. Cross site attack can occur by stealing the cookies, redirecting it into attacker’s site. The XSS attack is identified by encoding the URL and SQL attack can be avoided by using regular expression check mechanism.

![Figure 4: Attack classification and prevention mechanism in Misuse detection model](image)

3.2.1 Cross-site Attack (XSS)

The Cross-site attack (XSS) is the process of injecting malicious code. Cross-site attacks are those against web application in which an attacker gets the control of browser in order to execute a malicious script. The Cross-site attacks are implemented by stealing cookies using `<script>` and by redirecting the user to attacker’s site and then stealing cookies.

The goal of the CSS attack is to steal the client cookies, or any other sensitive information, which can identify the client with the web site and to redirect the user to some other site. The XSS attack is used to steal the cookies and send it to attacker. The script tag `<script>` is used to steal cookies. The simple XSS attack is made by generating alert message box and sending the cookies to attacker.

The XSS attack is of 2 types.

1. Persistent XSS
2. Non-Persistent XSS
3. 

3.2.1.1 Persistent XSS

The attacker performs session hijacking by collecting user cookies using JavaScript and the customer’s web browser will be instructed to redirect to hacker’s site.
3.2.1.2 Non-persistent XSS

The attack is performed by sending links in via email, chat, etc. These attacks require the user to visit a link that attracts the attention and are crafted with malicious code. On visiting such links, the code inserted on the URL will be printed and executes on victim’s browser.

Persistent XSS attack can be identified by checking for script tag and document.cookie. The Non-Persistent XSS attack is identified by clicking on any link and redirecting it into other site.

3.2.2 SQL injection

The SQL injection attack is simple and the attacker passes string input to the application which manipulates SQL statement. There are 2 categories of SQL injection. They are

1. SQL Manipulation
2. Code Injection

SQL Manipulation involves modifying sql statement through set operations such as Union, Where clause, etc. Code injection attack is that inserting multiple sql statements. This works only when multiple sql statements per database request are supported. The SQL injection attacks are prevented by using Prepared Statement, Callable Statement and Stored Procedures. The SQL Injection attack is performed by passing string input through the web page and also manipulates two or more SQL statements. The SQL Injection attack is identified by avoiding special characters such as -, ‘, ;, etc. The size of input character should be fixed.

3.2.3 Denial of Service (DoS)

The Denial of Service (DOS) attack prevents the user from making outgoing connections and floods the network with unwanted messages. This attack can be prevented by setting time interval, by key establishment technique, etc. The key establishment technique is that the secret key is shared among sender and receiver and by providing the key value the data can be accessed.

3.3 Decision Making Module

The decision making module provides the result as attack if both anomaly and misuse detection module identifies it as an attack. The Rule-based method is used for Decision making module. The rules are

- If anomaly detection model detects a fraud and misuse detection model does not detect the same fraud, then the detected fraud is not a fraud and it is an erroneous classification.
- If anomaly detection model detects a fraud and misuse detection model does detects the same fraud, then the detected fraud is a fraud and the fraud mode is classified.
- If anomaly detection model detects a fraud and misuse detection model finds it to be an unknown fraud, then the detected fraud is a new fraud.

4. RESULTS

Initially the users are grouped based on his spending habit. The low range is between 0 and 5000, medium between 5000 and 12500 and high above 12500. The observation symbol for low
cluster is denoted by ‘l’ and medium by ‘m’ and high by ‘h’. The sequence length of 5-10 is used to identify the fraudulent transaction. The fraudulent transaction identification is as follows.

Low=(0-5000), Medium=(5000-12500), High=(above 12500).

The results below specify how fraudulent transactions are identified in each spending profile cluster. Calculations have been shown only for high spending profile. Low and medium profile can be calculated in the similar manner.

### 4.1 Low Spender Profile

α: The user performs new transaction and the amount is 8000. The type of purchase is on grocery(S1) and the observation symbol generated is ‘m’. The first observation symbol ‘l’ is removed and at the end of the sequence ‘m’ is inserted.

\[
\begin{align*}
\alpha_1(l) &= 2/3, \alpha_1(m) = 1/3, \alpha_2(h) = 0 \\
\alpha_2(l) &= 1/2, \alpha_2(m) = 0, \alpha_2(h) = 1/2 \\
\alpha_3(l) &= 2/3, \alpha_3(m) = 1/3, \alpha_3(h) = 0
\end{align*}
\]

\[
\begin{pmatrix}
0.5 & 0 & 0.5 \\
1 & 0 & 0 \\
1/3 & 1/3 & 1/3
\end{pmatrix}
\]

Table 1: Probability of observation sequence based on new transaction amount and amount in normal range for low spending profile.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>α₁</td>
<td>1/9</td>
<td>0</td>
<td>1/9</td>
</tr>
<tr>
<td>α₂</td>
<td>0.061728395</td>
<td>0.018518518</td>
<td>0.061728395</td>
</tr>
<tr>
<td>α₃</td>
<td>0.046639231</td>
<td>0.010288065</td>
<td>0.034293552</td>
</tr>
<tr>
<td>α₄</td>
<td>0.030025909</td>
<td>0.005715592</td>
<td>0.023167199</td>
</tr>
<tr>
<td>α₅</td>
<td>0.018967297</td>
<td>0.001262033</td>
<td>0.015156902</td>
</tr>
<tr>
<td>α₆</td>
<td>0</td>
<td>0.002526150333</td>
<td>0</td>
</tr>
<tr>
<td>α₇</td>
<td>0.0000842050111</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

\[\alpha_5 = P(O|\lambda) = 0.0000842050111\]

\[\delta/\alpha_i = 0.728765767\]
$\alpha_2$:

$b_1(l)=2/3, b_1(m)=1/3, b_2(h)=0$

$b_2(l)=1/2, b_2(m)=0, b_2(h)=1/2$

$b_3(l)=2/4, b_3(m)=1/4, b_3(h)=1/4$

$aij=\begin{bmatrix}
1/3 & 0 & 2/3 \\
1 & 0 & 0 \\
1/3 & 1/3 & 1/3
\end{bmatrix}$

Table 2: Probability of observation sequence based on new transaction amount and amount is in abnormal range in low spending profile.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha_1$</td>
<td>1/9</td>
<td>0</td>
<td>1/12</td>
</tr>
<tr>
<td>$\alpha_2$</td>
<td>0.043209876</td>
<td>0.013888888</td>
<td>0.050925925</td>
</tr>
<tr>
<td>$\alpha_3$</td>
<td>0.030178325</td>
<td>0.008487654167</td>
<td>0.0221890946</td>
</tr>
<tr>
<td>$\alpha_4$</td>
<td>0.017455721</td>
<td>0.00381824333</td>
<td>0.013877685</td>
</tr>
<tr>
<td>$\alpha_5$</td>
<td>0.009508474667</td>
<td>0.0023129475</td>
<td>0.008131521167</td>
</tr>
<tr>
<td>$\alpha_6$</td>
<td>0</td>
<td>0.001355253528</td>
<td>0.002262372542</td>
</tr>
<tr>
<td>$\alpha_7$</td>
<td>0.0007031259029</td>
<td>0</td>
<td>0.0001885310452</td>
</tr>
<tr>
<td>$\alpha_8$</td>
<td>0</td>
<td>0.00003142184087</td>
<td>0.0001328985709</td>
</tr>
</tbody>
</table>

$\alpha_3=P(O|\lambda)=0.000164320418$

$\delta\alpha/\alpha_1=0.981302857$

The value 0.981302857 is greater than threshold (0.7). The values greater than 0.7 are assumed as fraudulent transaction.

Similar calculations are also done for medium spender profile user and high spender profile user to determine whether the transaction is a fraudulent or normal.

### 4.2 Calculating Accuracy Metrics

Testing the proposed system using real data set is a very cumbersome task. As banks do not agree to reveal the customers credit card information to researchers. Hence the efficiency of the system is tested with simulation studies. A mix of normal and fraud transactions generated by the simulator forms the input data in our proposed system. We use standard metric such as false positive [12] to measure the effectiveness of the system. Accuracy is calculated as follows:

Accuracy = \( \frac{\text{No.of normal transactions identified as normal} + \text{No.of transactions identified as fraud}}{\text{Total No.of transactions}} \) [15]
The design parameters of HMM can be chosen by generating transaction sequences using 95 percent low value, 3 percent medium and 2 percent high value transactions. Sequence length of the transaction is varied in steps of 5 from 5 to 15. Threshold values considered are 30 percent, 50 percent and 70 percent.
Fig 9: Persistent Cross site attack
Fig 10: CSS Attack Identification

Table 3: Variation of False Positive with different sequence lengths

<table>
<thead>
<tr>
<th>Threshold ( % )</th>
<th>False positive averaged over all 3 states of different sequence length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
</tr>
<tr>
<td>30</td>
<td>0.06</td>
</tr>
<tr>
<td>50</td>
<td>0.05</td>
</tr>
<tr>
<td>70</td>
<td>0.04</td>
</tr>
</tbody>
</table>

Table 4: Variation of True Positive with different sequence lengths

<table>
<thead>
<tr>
<th>Threshold ( % )</th>
<th>True positive averaged over all 3 states of different sequence length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
</tr>
<tr>
<td>30</td>
<td>0.53</td>
</tr>
<tr>
<td>50</td>
<td>0.55</td>
</tr>
<tr>
<td>70</td>
<td>0.51</td>
</tr>
</tbody>
</table>

From Table 3, it is clear that false positive decreases with higher threshold and smaller sequence length. From Table 4, it is observed that true positive is high for sequence length 15 in most of the cases. Hence we can say that fraud identification increases with the sequence length. The results are obtained for a java implementation on a 2.30 GHz Intel I3 machine. As the proposed mechanism overcomes internet attacks such as cross site, SQL and DOS attacks in comparison with the method proposed by Abhinav et al [2] which uses only the anomaly detection model, the system can identify various credit card attacks.
There is a performance depreciation when the difference between normal and fraud transaction is negligible either because of increase in false positives or decrease in number of true positives.

Fig 11: Variation of True and False positive rates with different sequence lengths for Threshold of 30 percent

Fig 12: Variation of True and False positive rates with different sequence lengths for Threshold of 50 percent
5. CONCLUSION

This paper proposes a defense mechanism for credit card fraud detection by combining three approaches anomaly, misuse and decision making models. Anomaly detection module is implemented using Hidden Markov approach classifies the credit card transaction as normal or abnormal based on the threshold of the spending profile of the credit card user. Comparative studies reveal that the HMM technique results in higher accuracy over a wide variation in the input data and the proposed system can be scalable for handling large transaction data. The false positive rate (FPR) is calculated. Second, the Misuse detection module screens the abnormal transactions for type detection. The main aim of the attacker is to steal the details of the authorised user by using XSS and SQL Injection attack. Finally the results of the two detection modules are integrated by the decision making module to determine the fraud, type of fraud and return the same to the administrator for necessary action. The experimental results discussed are of anomaly detection module. There is an increase in fraud detection accuracy as the anomaly detection model is integrated with the misuse and decision making model and thereby a significant decrease in the false positive rate.

REFERENCES


AUTHORS

[1] Sasirekha received her M.Tech in computer science and Engineering from VIT University in 2012. Her research interest are network security and mobile computing. She is currently a software developer in Cognizant Technology Solutions, Chennai.

[2] Sumaiya Thaseen received her B.E from Madras University and M.Tech from VIT University in 2004 and 2006 respectively. She is currently an Assistant Professor (Senior) in School of Computing Science and Engineering, VIT University with 6 years of experience and also pursuing her PhD degree. A life member of Computer Society of India (CSI). Her areas of interests are ad hoc networks, cryptography and network security. She has published several papers in international peer reviewed journals and conferences.

[3] Saira Banu received her B.E from Madras University and M.Tech from VIT University in 2004 and 2006 respectively. She is currently an Assistant Professor in School of Computing Science and Engineering, VIT University with 6 years of experience and also pursuing her PhD degree. A life member of Computer Society of India (CSI). Her areas of interests are parallel algorithms, computer architecture and multicore programming. She has published several papers in international peer reviewed journals and conferences.