The 7th Balkan Conference on Operational Research
"BACOR 05"
Constanta, May 2005, Romania

REDUCING FRAUD IN ELECTRONIC PAYMENT SYSTEMS

DEJAN SIMIĆ

University of Belgrade, Faculty of Organizational Sciences, Belgrade, Serbia and Montenegro

---

Abstract
The number of fraudulent activities is increasing dramatically in telecommunication networks, mobile communications, and E-commerce. Fraud is a major problem in electronic payment systems. For example, card fraud losses are growing every year. Consequently, fraud detection is becoming an important issue for research. Fraud begins to rise as new technologies and new weaknesses are found. Reducing fraud is a complex process which includes the knowledge from many scientific areas and demands a multidisciplinary approach. In this paper the problem of fraud prevention and detection is addressed. Several techniques for fraud prevention and detection are presented. It is important that fraud can be detected as it is happening. Detecting fraud in real-time is not easy so it is not surprising that many fraud systems have serious limitations. New solutions such as fraud management systems can reduce fraud significantly by using and combining many existing techniques, as well as new ones.

Keywords*: Fraud prevention and detection, e-commerce, electronic payment systems, security*

1. INTRODUCTION

Information technology continually changes [9, 12, 13, 15]. E-commerce is evolving rapidly and now it is reality. Efficient and effective electronic payment services are already established and accepted by businesses and consumers. On-line banking and card payments over the Internet are now commonplace. Advances in e-commerce, expansion of modern technologies and global communication provide a large number of business opportunities, as well as new threats for the banking and financial services.

E-commerce provides the capability of buying and selling products, services and information on the Internet by using electronic payment systems. In electronic payment systems the exchange of value is represented by the exchange of data. It is easy, cheap

and fast to transfer data, but the main challenge is security. Contemporary electronic payment systems may be classified into two groups: “account-based” or credit-debit systems and “token-based” or electronic currency systems. Both groups have important characteristics such as trust, security, reliability, easy of use, efficiency, flexibility, convertibility, interoperability, etc. However, in this paper the focus is on the security of the system.

Credit card transactions have become a de facto standard for Internet and Web-based payments. There are millions of credit card transactions processed each day. System architecture of contemporary electronic payment systems is shown in Figure 1. The system is distributed, heterogeneous and hierarchical. The main participants are: Issuer, Acquirer, Payment Gateway, Merchant, Certification Authority, and Cardholder or Buyer. Payment devices such as ATM (Automatic Teller Machine), POS (Point Of Sale) terminal, and kiosk may be located at merchant site. Communication between an acquirer and an issuer is based on ISO 8583 standard for bank card originated messages [7, 8].

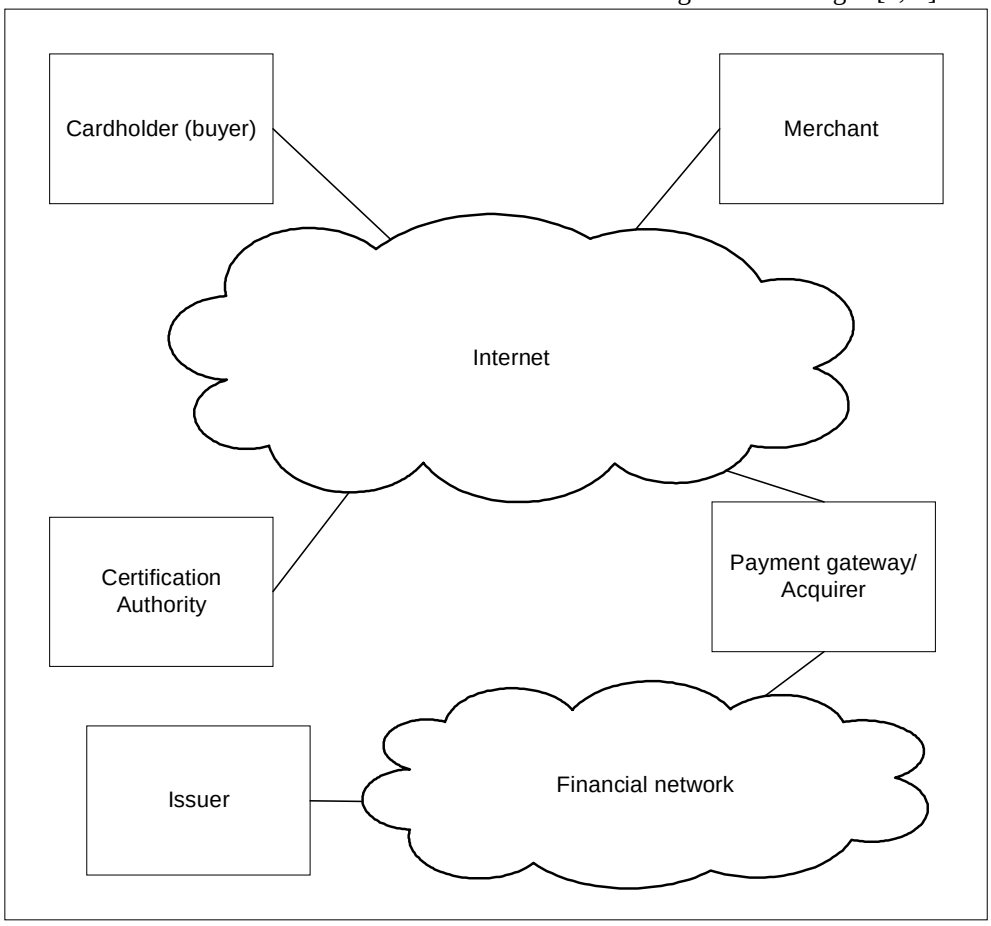

Figure 1 System architecture of electronic payment systems

Fraud is a global problem. Fraudsters operate in all countries and industries. Possible frauds are: credit card fraud, money laundering, mobile communications fraud, insurance fraud and computer intrusion. Credit card fraud may be for "card-not-present" transactions and for "card-present" transactions. The fraud for "card-not-present" transactions is significantly higher than the fraud for "card-present" transactions [14]. Card fraud losses are growing every year. APACS (UK payment authority) forecasts that industry losses will rise to $11 per card issued by 2008. Bearing this in mind in this paper the various techniques that are available and can be used to prevent and detect fraudulent activities are addressed and discussed.

The rest of the paper is organized as follows: Section 2 describes the problem of fraud in electronic payment systems. Section 3 presents the fraud prevention and detection as a solution. Section 4 describes the most important techniques that may be used for fraud prevention and detection. A proactive Fraud Management Systems is also proposed. Section 5 concludes the paper.

2. THE PROBLEM STATEMENT

In this paper credit card fraud is defined as a transaction when an individual uses another individuals' credit card or corresponding data for payment of goods or services while the owner of the card and the card issuer are not aware of that. There are many types of fraud in electronic payment systems. Fraud can occur in a number of ways including:

- Counterfeit fraud,
- Merchant fraud,
- Card-not-present fraud,
- ATM fraud,
- Internet fraud,
- Lost or stolen cards,
- Identity theft,
- Skimming or copying of electronic data contained on magnetic stripe, and
- MOTO (mail order telephone order) fraud.

Credit card fraud is increasing over the Internet. As fraud grows in both number and variety, financial institutions are challenged with the need for cost effective, risk management solutions which can identify and avoid fraudulent activities in real-time.

The fraudulent activity on a card affects the cardholder, the merchant, the acquirer, and the issuer. The most affected participant is the merchant regarding the cost of the fraud. The cost of a fraudulent transaction is greater than the cost of goods sold. There are many hidden cost components such as card association fee, merchant bank fee, administrative cost (each chargeback requires one to two hours to process at the merchant site), and loss of reputation.

Fraudsters are becoming more sophisticated and skillful at discovering any weakness they can exploit. During the time fraud constantly changes as well as behavior of legitimate users. Therefore fraud management tools should "learn" and adapt to the changing behavior of both fraudsters and legitimate users.

There are many methods in the areas of Knowledge Discovery in Databases, Data Mining, Machine Learning and Statistics which are quite applicable in many different

areas. However, the naïve application of these methods can cause difficulties in the area of credit card fraud detection.

3. FRAUD PREVENTION AND DETECTION

Fraud prevention and detection is an important form of risk management in the credit card industry. Fraud prevention describes measures to stop fraud occurring in the first place. When prevention fails then fraud detection comes into play. The objective is to detect fraud quickly when it does occur and stop it as soon as possible. However, detecting fraud in real-time is not easy [1], so it is not surprising that many fraud systems have serious limitations. Credit card fraud detection is confidential and is not much described in public. Fraud prevention and detection involve monitoring the behavior of customers to estimate, plan, detect and avoid risk. The cost of wrongly accusing a customer of fraudulent behavior is high. Therefore false detection of fraud is a big disadvantage and must be avoided. Different techniques may be needed for different kinds of fraud.

The fraudulent data are highly skewed because distribution is not uniform and many more transactions are legitimate than fraudulent. A small percentage of all transactions are fraudulent.

Anti-fraud software modules need to:

- Detect fraud accurately and early,
- Provide relevant information to fraud analysts just in time,
- Automate processes where possible,
- Self adapt to changing patterns of fraud, and
- Self adapt to changing behavior of customers.

Fraud prevention and detection may be implemented on issuer or acquirer side. The major difference is that a suspicious transaction on issuer side may be declined. In this paper the most important techniques which can be applied on both sides are chosen and presented.

Card fraud cycle is shown in Figure 2. There are three stages in the cycle. Stage 1 represents familiarity with weaknesses in cards and technology which drives up the value of fraud. Fraud begins to rise as new technologies and new weaknesses are found. Stage 2 represents new solutions implemented to reduce fraud. The solutions are not implemented immediately, and therefore Stage 3 represents time lag for solutions to take effect.

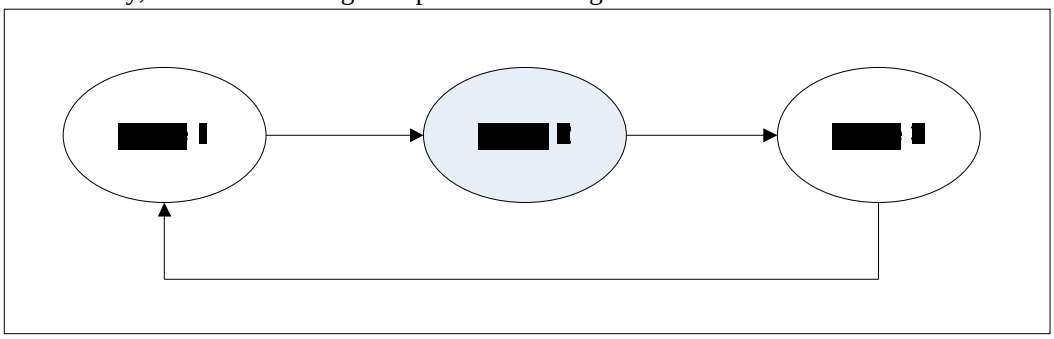

Figure 2 Card fraud cycle

4. TECHNIQUES FOR FRAUD PREVENTION AND DETECTION

The usability of a system depends on its performance, reliability and scalability in the real world. An efficient algorithm of detection has to be found for each method of fraud. Also, every fraud detection technique has its limitation and no tool can identify all types of fraud. The total cost of fraud includes the financial loss due to fraud and the cost of fraud prevention and detection system. Therefore the goal is to use an efficient fraud prevention and detection system that minimizes the total cost of fraud.

There are many techniques that may be used for fraud prevention and detection. The techniques can be grouped into the following groups:

- Applying a set of simple rules,
- Implementing EMV Level 2,
- Using advanced security protocols, and
- Using intelligent tools for fraud prevention and detection.

4.1 APPLYING A SET OF SIMPLE RULES

Rule based systems can be used to identify specific types of high-risk transactions. Online or a real-time authorization for a transaction may include implementation of some simple detection rules such as for example:

- Rule A: That the card has not been reported as lost or stolen,
- Rule B: That the card number is validated with Luhn formula control for check digit,
- Rule C: That CVV2 (for VISA) or CVC2 (for Master Card) or CID code (for American Express) is used as security function,
- Rule D: That orders that come from free email services should be rejected,
- Rule E: That international orders should be specially checked with more controls,
- Rule F: That the number of transactions with the same card number from the same merchant is not greater than a predefined number of transactions for specified time period,
- Rule G: That more than one session from different countries is active at the same time,
- Rule H: That the number of deposits exceeds the normal customer activity,
- Rule I: That the amount of deposit exceeds the normal customer activity,
- Rule J: That the card has valid expiration date,
- Rule K: That the transaction is coming from IP address, which is not on IP black list.

Some rules, such as rule *A*, *G* or *I* are sufficient for transaction decline. Some others, such as rule *F* may require a manual review. A more sophisticated rule based system can combine several simple rules for example, in the following way: *IF D AND E AND H THEN Review*

It is important to say that rule based systems rely on a set of expert rules designed to identify fraudulent transactions. The effectiveness of the system depends directly on the knowledge and expertise of the person designing the rules.

The fraud can be reduced also by using negative and positive lists of customers. An example of a negative list is a file containing all the card numbers that have produced chargebacks in the past. An example of a positive list is a file containing all the card numbers for trusted customers.

4.2 IMPLEMENTING EMV LEVEL 2

Chip or smart cards provide the basis for better security for card transactions. Chip cards have the ability to support future additional services in the fields of electronic commerce and home banking such as loyalty schemes and electronic purse. EMV is the abbreviation for Europay, MasterCard and Visa - the card organizations that have jointly specified the standard [3, 4, 5, 6]. Visa's and MasterCard's implementations of EMV are VSDC (Visa Smart Debit Credit) and M/Chip respectively.

There are many advantages of migration from magnetic to chip cards. First of all, chip cards provide higher security compared with magnetic stripe. For example, fraud can be significantly reduced because chip cards are much more difficult to counterfeit than magnetic stripe cards. EMV provides higher security through use of hardware, software and cryptographic processes. Also, offline capability of the chip enables lower transaction costs.

A comparison of magnetic stripe and CHIP&PIN solutions regarding various types of card fraud is shown in Table 4.1. As can be seen, card-not-present fraud is not solved by using CHIP&PIN payment, as well as Internet fraud, Identity theft, and MOTO fraud. Due to the complexity of the chip, fraudsters will find it uneconomic to copy smart cards. Also, chargebacks and the associated administrative costs will be minimised by using smart cards. CHIP&PIN payment is less time consuming than magnetic stripe payment with signature, because there is no need for the signature.

TYPE OF FRAUD	MAGNETIC STRIPE	CHIP&PIN
Counterfeit fraud	No	Yes
Merchant fraud	No	Yes
Card-not-present fraud	No	No
ATM fraud	No	Yes
Internet fraud	No	No
Lost or stolen cards	No	Yes
Identity theft	No	No
Skimming or copying of electronic data	No	Yes
MOTO	No	No

Table 4.1 Credit card fraud types and possible solutions

EMV does not specify the cryptographic algorithms and key management schemes to be used for authentication of transactions. The cryptogram is handled only by the card itself and Issuers' transaction authorization systems.

4.3 USING ADVANCED SECURITY PROTOCOLS

Secure Sockets Layer (SSL) protocol is used to establish a secure communication channel between two computers. SSL uses authentication based on asymmetric (public key) cryptography. Systems based on SSL are widely used and have enabled the growth of e-commerce. However, SSL was designed as a generic secure communication

protocol, not a payment protocol and therefore a more secure payment protocol is needed.

Easy of use is the most important factor for customers. Some attempts to create and implement a very low risk system as a dominant payment solution have failed. For instance, Secure Electronic Transaction (SET) protocol was designed to provide trusted electronic transactions [10, 11]. SET uses digital certificates to validate the identities of all parties involved in a purchase and encrypts credit card information before sending it across the Internet. However, SET failed to become dominant payment protocol due to the complexities of deployment.

Also, the following advanced security protocols: 3D SET, Visa's 3D Secure and MasterCard's Secure Payment Application (SPA) are very important protocols in electronic payment systems. Their purpose is to replace SET and SSL protocols providing higher level of security in relation to SSL and simpler deployment in relation to SET. 3D Secure is an authentication method designed to allow Merchants, Issuers, Acquirers and cardholders identify themselves in the Internet world for online card not present payments. After agreeing a transaction with an online merchant, cardholder's web browser is redirected to a card issuer server for cardholder authentication. After authentication cardholder's browser is redirected back to the merchant server. Merchants who implement a 3D Secure compliant solution can diminish fraudulent activity. Therefore, acquiring banks are required to support 3D Secure for their online Merchants.

4.4 USING INTELLIGENT TOOLS FOR FRAUD PREVENTION AND DETECTION

Without intelligent tools it is not possible to significantly reduce fraud in electronic payment systems. Important characteristics of credit card transactions data are: large volumes of data, non-uniform distribution of fraudulent data, and changing behaviors of customers and fraudsters. Although performance may be the problem, the best tools are able to work in real-time. Detection procedures can be programmed into separate software modules integrated with electronic payment systems to stop or at least, report problems at the time of transaction.

Intelligent tools for fraud prevention and detection can be subdivided into those that focus on people and those that focus on transactions and reports. Techniques that focus on people are based on fuzzy logic to score personal files or matching individuals against known "bad" lists. Focusing on transactions makes possible to proactively reduce fraud.

An example of intelligent tool is Address Verification Service (AVS). AVS was developed to help MOTO merchants to reduce fraud. AVS checks the numeric part of the street address and the ZIP code information provided by the consumer against the information stored in issuer's database and returns a match/mismatch response. A serious limitation of AVS is that it only works for addresses in some region and it is not much useful in case of international transactions.

Risk scoring systems provide one of the most effective fraud prevention tools available. They are based on statistical models which use the patterns derived from cardholder historical transactions as well as the current transaction attributes. The main difference from rule based systems is a calculation of the final score by weighting several dozens of fraud indicators.

Neural networks approach is a very popular tool for credit card fraud detection. However, due to the lack of available data set it is sometimes difficult to implement. A recently published paper [16] presents a concept involving the use of neural networks to correlate information from a variety of technological and database sources to identify suspicious account activity. Distributed data-mining techniques that combine multiple models produce effective fraud and intrusion detectors [2, 17].

A proposal for proactive rule-based Fraud Management System (FMS) is shown in Figure 3. There are the following three software modules: Web interface for adding and configuring rules (WIAC), Run-time module (RM) and Fraud reporting module (FRM). All modules access to a relational database. WIAC is intended for adding, deleting and modifying rules and for changing configuration parameters for already existing ones. In such way FMS has the ability to generate, manage and implement rules as often as required. RM updates data about current transaction in real-time. FRM is intended for generating various reports, which may be printed on the screen, printer, sent as e-mail or SMS to mobile phones of responsible persons, or delivered in various formats such as PDF, HTML, CSV, XLS, and XML files. FMS may be integrated with any transaction processing system by using Request and Response type of communication. An adequate textual message can be transferred to the merchant through a Response.

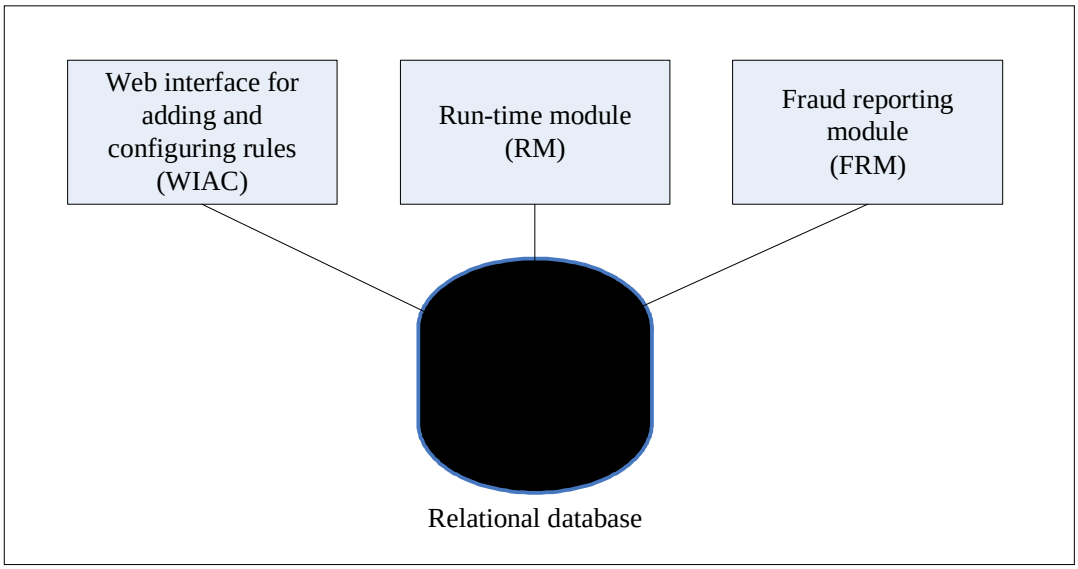

Figure 3 Proactive rule-based Fraud Management System

RM includes various controls such as: hotlist control, velocity control, statistical rules, Luhn formula control, and custom rules as shown in Figure 4. Transactions come from different communication channels and various payment devices. Depending on the result of a control the corresponding decision must be made: to accept, reject or manually review the current transaction.

A combination of tools is always a better solution to any single tool. The best solution is to use layers of fraud protection. Sometimes it is not appropriate to automate everything in transaction processing including fraud detection. It is important to know that there may be a need to manually review a small percentage of orders. The risk of accepting an order is always balanced with the risk of loosing the customer.

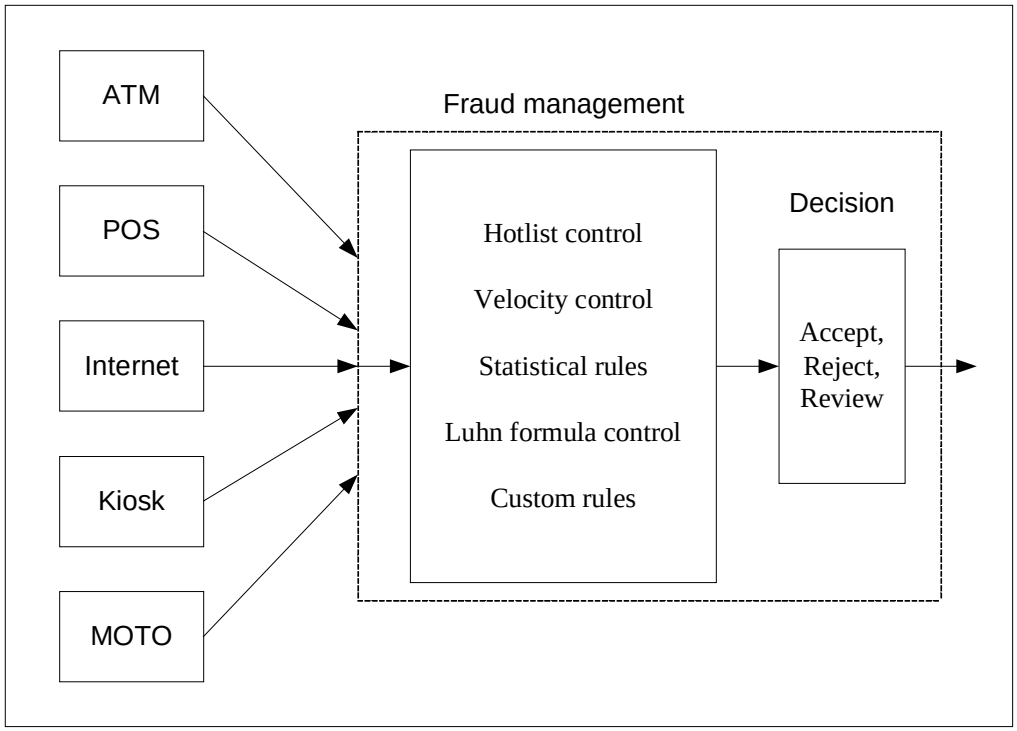

Figure 4 Run-time fraud management module

5. CONCLUSION

In this paper the problem of fraud in electronic payment systems is addressed. Reducing fraud is a very important goal in electronic payment systems, which may be achieved by using prevention and detection techniques. Detecting known and unknown fraud in real-time is not easy but it is feasible. There are many techniques that may be used. In this paper the most important techniques for fraud prevention and detection are chosen and presented. No tool can identify all types of fraud and every tool is best at identifying one particular type of fraud. In addition to industry standard security rules, solutions such as Fraud Management System, described in the paper, are necessary to provide advanced protection from all types of online and offline transaction fraud in electronic payment systems.

Card fraud methods evolve continuously. Therefore fraud prevention and detection techniques have to be proactive and always be ready to minimize fraudulent activities. Combination of different techniques gives best results.

BIBLIOGRAPHY

[1] Cahill M. H., Lambert D., Pinheiro J. C., Sun D. X. (2000), "Detecting fraud in the real world", Handbook of Massive Datasets, Kluwer Academic Publishers, pp. 911-929;
[2] Chan K. Philip, Fan W., Prodromidis A., and Stolfo S. (1999), "Distributed data mining in credit card fraud detection", IEEE Intelligent Systems, Vol. 14, No. 6, 67-74, available at http://www.cs.fit.edu/~pkc/papers/ieee-is99.pdf ;
[3] EMV (2004) "EMV 2000 Integrated Circuit card Specification for Payment Systems Version 4.1 – Book 1: Application Independent IC Card to Terminal Interface Requirements", EMVCo;
[4] EMV (2004) "EMV 2000 Integrated Circuit card Specification for Payment Systems Version 4.1 – Book 2: Security and Key Management", EMVCo;
[5] EMV (2004) "EMV 2000 Integrated Circuit card Specification for Payment Systems Version 4.1 – Book 3: Application Specification", EMVCo;
[6] EMV (2004) "EMV 2000 Integrated Circuit card Specification for Payment Systems Version 4.1 – Book 4: CardHolder, Attendant, and Acquirer Interface Requirements", EMVCo;
[7] ISO 8583 (1987) "ISO 8583: 1987. Bank Card Originated Messages – Interchange Message Specifications – Content for Financial Transactions", available at http://www.iso.ch;
[8] ISO 8583 (1993) "ISO 8583: 1993. Financial Transaction Card Originated Messages – Interchange Message Specifications", available at http://www.iso.ch;
[9] Mrkić Mladen, Simić Dejan (2004), "Porting a Java Web application to z/OS", MVS Update, Published by Xephon 27-35 London Road Newbury Berkshire RG14 1JL, England, April 2004, pp. 9-23;
[10] SET (1997), "SET Secure Electronic Transaction Specification – Book 1: Business Description", available at http://ccc.cs.lakeheadu.ca/set/set_bk1.pdf (accessed May 2005);
[11] SET (1997), "SET Secure Electronic Transaction Specification – Book 2: Programmer's Guide", available at http://ccc.cs.lakeheadu.ca/set/set_bk2.pdf (accessed May 2005);
[12] Simić Branka, Simić Dejan (2001), "Executing applet methods in Lotus Domino forms from Netscape 6", Domino Update, March, published by Xephon 27-35 London Road, Newbury Berkshire RG14 1JL, England, 3-6;
[13] Simić Dejan, Starčević Dušan (1997), "A Distributed Multimedia Bank Office Information System", Multimedia Technology and Applications, Springer-Verlag Singapore Pte. Ltd., 527-536;
[14] Simić Dejan, Starčević Dušan (2002), "E-Commerce Security: Challenges and Solutions for Credit and Debit Cards Payment Systems", 6th Balkan Conference on Operational Research, A Challenge for Scientific and Business Collaboration, Thessaloniki, Greece, (CD Edition);
[15] Starčević Dušan, Simić Dejan, Pantović Vladan (1996), "The evolution of software architecture", International Conference on information products, processes and technologies, Moskva, November, Proceedings of the Conference, 45-47;
[16] Vikram Ashish, Chennuru Sivakumar, Rao H. R., Upadhyaya Shambhu (2004), "A

Solution Architecture for Financial Institutions to Handle Illegal Activities: A Neural Networks Approach", IEEE Proceedings of the 37th Hawaii International Conference on System Sciences, available at http://csdl.computer.org/comp/proceedings/hicss/2004/2056/07/205670181a.pdf (accessed May 2005);
[17] Wang Huaiqing, Mylopoulos John, Liao Stephen (2002), "Intelligent agents and financial risk monitoring systems", Communications of the ACM, March, Volume 45 Issue 3, 83-88.