전자상거래영역에서 전자결제 신용카드 사기방어 시스템에 관한 연구

조문배[0] 석현태
중소기업진흥공단 중소기업연수원 동서대학교
augustc@sbc.or.kr sht@dongseo.ac.kr

A Study of Anti-Fraud System (AFS) for Credit Card Payments in Electronic Commerce

Moon-Bai Jo[0] Hyontai Sug

요약

인터넷 상의 주문 결재로부터 생성되어지는 수백만의 결제로 인해 축적되어진 레코드들을 이용하고, 아울러 고객이 제공하는 데이터 등을 가지고 고객이 실제 카드 소지자인지를 판별하는 전자결제 신용카드 사기방어시스템(Anti-Fraud System(AFS))을 제안하였다. 고객은 거래 콤포넌트에 의한 보안 메세징 프로토콜을 사용해서 인터넷에서의 서비스 요구를 시작한다. 거래의 위험도를 결정하기위해서 데이터마이닝 기법을 이용한 하이브리드 모델링기법을 사용하여 이와 같은 요구에서 생성되는 트랜잭션 정보의 위험도를 계산한 후, 미리 결정된 위험수위와 비교하여 부가적 신용 정보의 필요성을 판단하게 된다.

1. 서론

주소 인증 시스템(Address Verification System : 이하 AVS)[1, 2]은 비자, 마스터카드 그리고 그외의 주요 신용카드들에 대한 사용자의 주소를 확인 할 수 있는 시스템으로 카드 사용자가 온라인 구매 시 기입하는 billing address의 일부분의 데이터를 카드 발급 은행에 있는 사용자의 주소와 관련된 데이터 파일과 비교하게 된다. 이러한 과정은 주소의 앞부분 20자리와 우편번호를 비교함으로써 이루어진다. 그러나 이 방법으로는 카드를 이용하는 고객이 정확한 카드 소지자인지를 판별하는 데는 한계가 있다. 즉, 카드 번호와 가입자 주소를 모두 훔친 신용 카드사기는 인터넷의 완전한 익명성에 의해서 쉽게 AVS 인증 과정을 비켜갈 수 있다. 본 논문에서 주장하는 신용카드 사기방어시스템(Anti- Fraud System :이하AFS)은 AVS시스템 만으로 판단하기 어려운 사기 카드 번호를 카드 번호 인증과 동시에 사기 방어 막을 친다는 의미로서 고안된 시스템이다. 고객에 의해 제공되어진 수백만의 결제로 인해 축적되어진 레코드들을 이용함으로써, 고객이 실제 카드 소지자인지를 효과적으로 판별하는 전자결제 신용카드 사기방어시스템을 제안하였다.

2.본론

2.1 시스템 구성

본 논문에서 제안된 AFS와 AVS를 이용한 사용자 인증을 위한 시스템의 구성은 [그림 1]과 같다. 그림의 주요 요소는 다음과 같다.

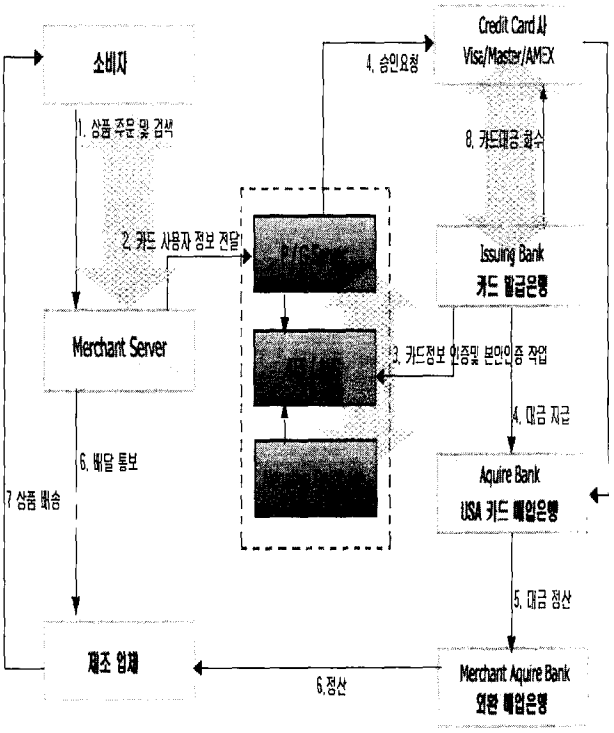
■ **AVS (Address Verification System):** 카드결제시 카드발급정보의 주소지 추적에 의해 전자상거래 카드사용의 본인 여부를 확인 통보하는 시스템.

■ **AFS (Anti Fraud System):** Credit Card를 이용하여 제품을 구매하는 구매자와 운영중인 쇼핑몰의 특성에 맞는 다양한 변수를 사용하는 한편 데이터마이닝 기법을 사용하여 카드결제에 따른 사기행위(Fraud)를 실시간으로 확인 통보처리하는 시스템

■ **P/G Server:** 미국산업규격으로 제공되는 128bit 데이타 암호화 기법을 사용하며 ActiveX 또는 Java 기반의 Payment Application으로 구성되어 있다. UNIX (Linux, Sun Solaris), Windows NT 플랫폼 기반의 웹서버에 쉽게 이식이 가능하도록 설계되었으며, 서버는 또한 각각의 상점으로 부터 데이터를 전달 받기 위해 ActiveX, Java, CGI, ISAPI 등의 국제 표준개발 Tool을 사용한다. [3]

소비자의 상품 주문이 발생하면 Merchant Server에 의해 카드 사용자의 정보가 P/G Server, AFS/AVS, 그리고 Negative Database를 통해서 카드 발급은행으로부터 카드 사용자의 본인 인증을 위한 결과를 받게된다. 그러면 Merchant Server는 제조업체에게 배달 통보를 함으로써 상품의 전송이 이루어지게 된다. Negative database는 카드 거래에 대한 히스토리 데이터베이스 및 데이터마이닝 기법[4]을 적용해 추출한 규칙을 저장하고 있으며 AVS만으로는 탐지가 어려운 사기거래를 탐지하게 된다.

[그림1] 신용카드 사기방어를 위한 사용자 인증 시스템



2.2 AFS 시스템

본 시스템은 데이터마이닝 시스템, IP 주소 추적 시스템 , 전화번호 추적 시스템, 그리고 카드발급은행 추적 시스템으로 구분된다. 고객은 거래 콤포넌트에 의한 보안 메세징 프로토콜을 사용해서 인터넷에서의 서비스 요구를 시작한다. 위험도를 결정하기위해서 데이터마이닝기법을 이용하여 이와 같은 요구에서 생성되는 트랜잭션 정보의 점수를 계산한 후, 미리 결정된 위험수위와 비교한다. 입력된 카드 정보가 사기거래의 가능성이 높은 것으로 판정될 경우, IP 주소라든가 전화번호, 그리고 카드발급은행 등을 추적하여 사기거래를 차단하게 된다. IP 주소추적시스템은 사용자의 IP 주소를 추적하여 본인이 현재 기입한 정보와 Shipping Address가 유용하지 않을 경우 카드 승인을 보류하게 된다. 전화번호 추적 시스템은 모뎀 사용자일 경우 카드 사용자의 전화번호를 추적하여 카드 사기 위험을 사전에 방지해주며, 마지막으로 카드발급 은행 추적 시스템에서는 은행 이름을 기입하도록 하여 발행은행이 틀릴 경우 승인을 취소하게 된다.

2.3 데이터마이닝 시스템

히스토리 데이터베이스의 거래결과를 데이터마이닝하여 도출된 규칙을 이용하여 사기거래의 가능성이 높은지를 판단하게 되는데 다음은 레코드의 한 예이다.

Order#: 20010118094923

Buyer: Christoper T Cox

Mailing Address: 2397 Rio Dosa Dr.,Lexiton, Kentucky, United Stares

Destination Country: United States

Product Receiver: Christopher T Cox

Shipping Address:2937 Rio Dosa Dr.,Lexiton,Kentucky

ZIP/postal code: 40509

Cardholder name: Christoper T Cox

Card#: 5491000914029769

Expiry Date: 1101

Issuing Bank: Fleet

IP Address: 205.188.197.43

Result code: AA

데이터마이닝을 위해서는 각각의 개별 신용정보를 정확하게 유지하는 것이 중요하므로 연관규칙(association rules)발견 알고리듬을 사용한다. 다음은 연관규칙에 대한 간단한 설명 및 본 시스템에서 연관규칙을 발견법을 적용하기 위해 필요한 정의이다.

$I = \{i_1, i_2, \ldots, i_m\}$을 쇼핑몰에서 판매하는 항목(item)에 대한 집합이라고 하자. T는 트랜잭션 레코드를 모아 놓은 것으로 각 트랜잭션은 고객이 한번에 구매한 항목집합(itemset) $X \subseteq I$로 구성된다. 연관 규칙이란 $Y \subset I$, $Z \subset I$, $Y \cap Z = \Phi$일 때 Y => Z와 같은 규칙을 말하며, Y => Z의 신뢰도가 C%란 항목집합 Y를 포함하는 트랜잭션 중 C%는 항목집합 Z도 역시 포함함을 나타낸다. 한 항목집합 $X \subset I$에 대해 X의 지지율(support ratio)이란 전체 트랜잭션 중 X를 포함하는 비율을 말한다. Y => Z와 같은 규칙의 신뢰도는 {(YUZ)의 지지율}/{Y의 지지율}로 계산될 수 있다. 지지율 대신 해당 항목집합이 전체 트랜잭션 중에 몇 번 나타났나를 나타내는 지지수(support number)를 사용하기도 한다. 어떤 지지율 이상 자주 나타나는 항목을 빈번항목집합(frequent itemset)이라 한다. 항목집합을 구성하는 항목의 수가 n이면 n항목집합이라고 말한다. 빈번항목집합은 이미 구한 (n-1)빈번항목집합을 이용해 n후보항목집합을 만들고 이를 데이터베이스에서 확인해 n빈번항목집합을 구하게 된다. 본 시스템에서는 히스토리데이터베이스의 특성상 긴 연관규칙보다는 실용적인 면에서 길이가 2 내지 3인 연관규칙을 효율적으로 찾는 것이 중요하므로 해쉬기법을 이용한 DHP(Dynamic Hashing and pruning)[5]방식을 사용하되, 원 알고리듬이 항목을 구성하는데 있어 레코드 내의 속성(attribute) 구분이 필요없는 일차원적(single-dimensional, intra-attribute) 발견법이라면, 항목은 값 뿐만 아니라 속성을 포함하며 같은 속성끼리는 항목집합을 구성할 수 없는 다차원적 (multi-dimensional, inter-attribute) 연관규칙 발견법을 적

용한다. 즉 항목은 속성-값(attribute-value)의 쌍이된다. 단, 주소의 경우 보다 의미 있는 규칙을 발견하기 위해 주소를 구성하는 각 부항목을 값으로 사용한다. 예를 들어, 앞에서 예로 든 레코드의 경우 '주소-2397 Rio Dosa Dr.,' '주소-Lexiton,' '주소-Kentucky, United States'처럼 항목을 만든다. DHP 알고리듬에서는 후보항목집합을 만들기 위해 역시 연관규칙발견 알고리듬인 Apriori알고리듬[6]의 apriori_gen() 알고리듬을 원용하는데 다차원적 연관규칙을 발견하기 위해서는 약간의 수정이 필요하다. 다음은 그 알고리듬이다. DHP의 알고리듬의 자세한 내용은 논문 [5, 7]을 참조하기 바란다.

```
apriori_gen( F_{k-1} )
  Forall itemset ∈ F_{k-1} do
    Select item i_1,i_2,...,i_{k-1},j_{k-1}
    from F_{I,(k-1)},F_{J,(k-1)} where
    i_1=j_1,...,i_{k-2}=j_{k-2},i_{k-1}≠j_{k-1},attr(i_{k-1})≠attr(j_{k-1})
 // F_{I,(k-1)}은 F_{k-1}에 속하는 I번째 항목집합,
 // i_{k-1}은 그 항목집합의 (k-1)번째 항목
     Insert into Ck'
  Endfor
  Forall itemset c'' ∈ Ck' do
// c''를 사용해 크기 (k-1)의 조합을 생성
    t = generate_(k-1)_itemsets(c'', k-1)
    If all itemsets ∈ t Exist in F_{k-1} Then
      c''.candidate = OK
    Endif
  Endfor
   Ck = { c'' ∈ Ck' | c''.candidate = OK }
End apriori_gen
```

본 시스템은 공유 history DB에 기반을 둔 실시간 검증방식에 기반을 두고있는 사기 차단 시스템으로 사용자의 결제로 계속 축적되어지는 레코드들을 이용함으로써 새로운 결제가 이루어질 때마다 성능이 향상되기 때문에 앞으로 시간을 두고 더 많은 사용자의 결제와 세계각지의 주소들을 효과적으로 DB화 한다면 전세계적으로 통용될 수 있는 강력한 신용 카드 사기차단 시스템 완성을 달성할 수 있을 것이다.

3. 결론

AVS 시스템은 카드 사용자가 결제 요청 시 온라인상에서 기입한 billing address 의 일부분과 카드 발급 은행의 서버의 DBMS 내의 billing address를 비교함으로써 이루어진다. AVS 는 VISA, MasterCard, 그리고 다른 주요 메이저 신용카드사에 대해 billing address를 검증 가능하다. 현재 미국과 캐나다에서만 사용되는 시스템이지만 그 효용성을 고려하면 앞으로 전 세계적으로 확산될 전망이다. 그러나 카드 번호와 가입자 주소를 모두 훔친 신용 카드사기는 인터넷의 완전한 익명성에 의해서 쉽게 AVS 인증 과정을 비켜갈 수 있다. 아울러 전 세계적으로 주소 기입 체계가 똑같지 않기 때문에 여러 나라의 주소 데이터를 공통된 코드로 단일화하는 것에 많은 시간이 소요된다. 따라서 이러한 문제점을 해결하기 위한 여러가지 방법이 강구되었는데 본 논문에서는 AVS 시스템만으로 판단하기 어려운 사기 거래를 카드 번호 인증과 동시에 사기 방어 막을 친다는 의미로서 고안된 시스템이다. 특히 billing address 까지 해킹 된 정보일 경우 AFS는 필수적이라 할 수 있다.

4. 참고문헌

[1] 하토리 미츠토시저 강철희, 이재기, 정제창, 한치문역, "최신 컴퓨터 통신/방송 표준기술", pp.730-750, 교보문고, 1999

[2] CFX_CyberCash White Paper at http://www.cfxoncrcybercash.com/whitepaper.cfm

[3] MasterCard International's web site, the developments of the SET protocol at http://www.mastercard.com/set

[4] Han, J., and Kamber, M., Data Mining: Concepts and Techniques, Morgan Kaufmann Publishers, 2000

[5] Park, J.S., Chen, M., and Yu, P.S., "Using a Hash-Based Method with Transaction Trimming for Mining Association Rules," *IEEE Transactions on Knowledge and Data Engineering*, Vol. 9, No. 5, pp.813-825, Sept. 1997

[6] Agrawal, R., Mannila, H., Srikant, R., Toivonen, H., and Verkamo, A.I., "Fast Discovery of Association Rules," In *Advances in Knowledge Discovery and Data Mining*, Fayyad, U.M., Piatetsky-Shapiro, G., Smith, P., and Uthurusamy, R. ed., AAAI Press/The MIT Press, pp.307-328, 1996

[7] Holt, J.D., and Chung, S.M., "Multipass Algorithms for Mining Association Rules in Text Databases," Knowledge and Information Systems, Vol.3, No.2, Springer-Verlag, 2001, pp.168-183