정 보 보 호 학 회 지
제26권 제3호, 2016. 6

온라인 게임 결제 데이터 분석 기반의 이상거래 탐지 모델

우 지 영*, 김 하 나**, 곽 병 일***, 김 휘 강****

요 약

소액결제에 대한 규제 완화로 이와 관련한 사기가 급증하고 있으며, 특히 소액결제가 대부분을 차지하는 온라인게임 산업은 관련 사기로 인한 피해가 증가하고 있다. 온라인 게임의 소액결제 사기는 단순히 금액에 대한 피해뿐만이 아니라 회사 브랜드에도 영향을 미치며, 나아가 고객 이탈로 이어질 수 있다. 소액결제 사기를 방지하기 위해 게임 산업에서도 이상거래 탐지 시스템이 요구되고 있다. 본 연구는 게임 사용자의 결제 패턴을 분석하여 이상거래를 탐지할 수 있는 머신러닝 기반의 이상거래 탐지 모델을 제시하며, 제안하는 모델을 글로벌 온라인 게임에 적용한 사례를 소개한다.

Ⅰ. 서 론

2014년 “별보다 그대”에서 나온 천송이 코트를 사기 위해 중국인들이 국내 쇼핑몰에서 구매를 시도하였으나 공인인증서와 Active X의 설치를 요하는 국내 전자상거래 환경으로 인해 구매가 불발되었다. 이러한 천송이 코트 논란으로 각종 규제들이 완화되면서 국내전자결제 제도에 간편결제가 도입되었다. 간편결제란 온라인에서 금융거래 시 지급결제에 필요한 개인정보와 신용정보를 전달하는 과정을 단순화시키는 서비스로 국내에서는 신용카드사, 오픈마켓, 지불결제사업자(Payment Gateway, PG)에서 공인인증서가 적용되지 않은 소액결제에 대해 간편결제 서비스를 제공해왔다. 2014년 5월 금융당국은 공인인증서 사용 의무화 폐지하였고, 그해 7월에는 금융위원회와 미래창조과학부가 전자상거래 결제 간편화 방안을 발표하였다. 2014년도 12월에는 금융감독원에서 FDS 추진 협의체를 출범하였다. 간편결제 도입을 위한 규제 완화 이후 다양한 기업에서 서비스 확대가 추진되었다.

간편결제가 도입되면서 기존의 거래시점 사고 방지를 위한 강력한 보안장치와는 다른 보안 시스템이 필요해졌다. 과거의 시스템은 보안상 발생하는 사용자의 편의를 떨어뜨리고, 사고 발생 시 책임의 대부분을 이용자가 지게 되는 구조였다. 최근의 환경에서는 사용자의 불편함을 야기하지 않으면서, 사고의 위험을 낮추는 보안 시스템이 필요하게 되었는데, 이에 대한 대안이 이상거래 탐지 시스템(Fraud Detection System: FDS)이다.

이상거래 탐지 시스템은 데이터 분석 기반의 보안시스템이다. ICT (Information and Communications Technologies) 기술의 발전으로 다양한 사이버 보안 이슈가 발생하고 있다. 사용자 행동, 환경 등에 대해 다양한 데이터 원천으로부터 체계적으로 자료를 수집하고, 모니터링 하여 이상징후를 찾아내는 것은 모든 보안 이슈에 대한 하나의 해결책이 될 수 있다. 네트워크, 시스템, 응용서비스 등으로부터 발생하는 데이터 및 보안이벤트의 연관성을 분석하여 보안 지능을 향상시키는 차세대 보안정보 분석 기술이 필요하며, 이는 빅데이터 분석 기술을 활용한 시큐리티 인텔리전스로 불리고 있다. 이를 위해서, 데이터 마이닝, 웹 마이닝, 텍스트 마이닝, 소셜 네트워크 분석 기법을 이용하여 빅데이터를 이해하고, 추론 및 학습하는 과정이 필요하다. 이를 통해 위협을 탐지하고, 더 나아가 잠재적인 위협을 예측하고,

* 고려대학교 정보보호대학원 연구교수
** 고려대학교 정보보호학과 석사과정
*** 고려대학교 정보보호학과 석·박사통합과정
**** 고려대학교 정보보호대학원 부교수

능동적인 대응을 수립하는 것이 가능하다. FDS는 이러한 시큐리티 인텔리전스 중 하나이다.

간편결제 또는 금융결제를 수행하는 산업에서는 이상거래 탐지 시스템이 요구되고 있으며, 은행, 신용카드사, 증권사에서 FDS를 도입하고 있다. 연구 부분을 살펴보면, 신용카드, 은행, 보험 등 금융 분야에서의 FDS에 대한 연구는 많이 수행되었지만, 게임분야에서의 FDS에 대한 연구는 거의 없다.

2011년부터 성행하기 시작한 소액결제 사기는 특히 온라인게임 산업에서 자주 발생하고 있으며, 2012~2013년도에 많은 게임 유저들이 소액결제 피해 사기를 입었다.

온라인게임은 인터넷 역사상 WWW (World Wide Web)과 더불어 가장 성공적인 인터넷 응용서비스 중 하나로 자리매김하고 있다. 최근 10년간 국내외 온라인 게임 시장은 꾸준한 성장세를 보여 왔으며, 스마트폰 및 태블릿 기기의 보급 확산으로 인해 모바일 게임 역시 급성장하고 있다. 온라인게임 시장의 비약적인 성장과 함께 온라인게임과 관련된 보안 위협 역시 급증하고 있다. 게임 산업의 경우 국가기반시설이나 금융권, 전자상거래 서비스에 비해 상대적으로 정부의 기술적, 관리적 보안 가이드라인이 약한데 비해 해킹이 발생하였을 경우 해커가 얻을 수 있는 이익이 크며, 해킹에 성공할 경우 대규모 사용자들의 고객개인정보 외에도 온라인게임 아이템을 조작하거나 더 나아가 이를 현금화할 수 있다는 점에서 해커들에게 매력적인 공격대상으로 여겨지고 있다. 더욱이 온라인 게임에서 가상 재화를 현금화할 수 있기 때문에 신용카드 결제사기의 탐지를 우회하는 통로로 사용되기도 한다. 게임 산업은 게임 아이템, 정액권 등 결제가 많이 이루어지지고 있어, 소액결제 사기의 주 타겟이 되며, 꾸준히 사기에 노출되어 있다.

게임 내 소액결제 사기는 단순히 금액에 대한 피해뿐만이 아니라 회사 브랜드에도 영향을 미치고 더 나아가 고객 이탈로 이어질 수 있다. 소액결제 사기를 방지하기 위해 게임 산업에서도 FDS가 요구되고 있다. 본 연구는 게임 내 사용자의 거래 패턴을 분석하여 이상거래를 탐지할 수 있는 모델을 제시한다.

Ⅱ. 관련 연구

다음은 최근의 FDS 관련 연구이다. 특히 알고리즘 측면에서 시사점을 가지는 주요 연구와 게임 산업의 FDS 연구를 [표 1]에 정리하였다. Lim (2014) [4]의 연구에서는 최근 거래에 가중치를 더 주어 학습하는 방법을 제안하였다. Mahmoudi과 Duman (2015) [7]외의 연구에서는 신용 카드 사기검출 문제에 있어 비용에 민감하게 반응 할 수 있도록 Fisher Discriminant Function을 수정하여 정상 거래와 사기 거래에 대한 탐지 및 사기 거래를 통해 얻어질 수 있는 이익을 최대화하는 방법을 제안하였다.

Coppolino외 (2015) [6]은 모바일뱅킹 시스템에서 계정을 탈취하여 남용하는 사례에 대한 FDS를 제안하였다. MMT (Mobile Money Transfer)에서 발생하는 로그들을 기반으로 룰 기반 학습 방법과 확률 이론에 기반한 모델을 적용하였다. 모바일 결제사기를 성공하기 위한 침입자의 행동 패턴을 분석하여 이상거래의 가능성을 산출한다. Vadoodparast와 Hamdan (2015) [8]의 연구에서는 이상거래에 대한 정보가 없는 상황에서 이상거래를 탐지하기 위해 데이터의 유사성을 기반으로 하는 군집화기법을 이용하는 방안을 제시하였다.

Christouet외 (2011) [3] 연구에서는 사행성 게임에 대한 FDS를 다루었다. 거리기반의 군집화기법을 이용하여 자금세탁을 위해 사행성 게임을 악용하는 사용자를 탐지하는 모델을 제안하였다. Schaidnageland와 Laux(2014) [5]의 연구에서는 온라인게임에서 신용카드 거래의 시계열 패턴을 분석하여 이상거래를 탐지하는 모델을 제안하였다.

결제 데이터는 아니지만 게임 내 거래 데이터를 분석하여 불법 행위 및 불법 조직을 탐지하는 연구가 기 수행되었는데, 최화재 외 (2011) [1]에서는 가상재화를 사고 파는 행동을 분석하여 계정 도용을 탐지하는 모델을 제시하였다. Woo 외 (2011) [2]은 사용자간 게임 내 가상재화 거래 내역을 분석하여 불법적 조직을 탐지하는 모델을 제시하였다.

〔표 1〕 최근 FDS 연구

적용영역	최근 주요 연구
신용카드	Lim, Sachan & Thing. (2014)〔4〕 Mahmoudi & Duman (2015)〔7〕
모바일뱅킹	Coppolino외 (2015)〔6〕 Vadoodparast & Hamdan (2015)〔8〕
게임	Christou외 (2011)〔3〕 Schaidnagel & Fritz Laux (2014)〔5〕

Ⅲ. 이상거래 탐지 모델

3.1. 적용 게임

본 연구는 글로벌 온라인 게임 회사인 N사의 MMORPG (Massive Multi-player Online Role Playing Game) 의 실제 데이터를 기반으로 수행되었다.

보통의 MMORPG는 사이버재화를 획득하여 더 강한 캐릭터로 성장시키기 위해 서로 경쟁하는 구조로 되어있다. 게임 플레이를 하거나 좀 더 빨리 높은 레벨의 캐릭터로 성장하기 위해서는 게임 재화가 필요한데 사용자들은 이를 구매하기 위해서 사이버머니를 구매한다. 보통 이 과정을 충전이라고 부르며 사이버머니가 충전되면, 이를 이용해서 게임 재화를 구매할 수 있다. 게임 내 거래는 이렇듯 실제 금전 거래가 이루어지는 충전과정과 사이버재화를 통한 거래가 이루어지는 결제과정으로 나누어진다. 본 연구에서는 게임 내 이상거래 탐지를 위해 충전과 결제의 두 종류의 거래 기록을 이용한다. [표 2]는 본 연구에서 사용한 거래 기록 데이터 필드를 나타낸다.

사용한 데이터는 2015년의 약 6개월의 데이터를 이용하였고, 이 중 10%를 sampling하여 사용하였다.

〔표 2〕 사용로그

충전데이터	구매데이터
Account식별값(GUID)	Account식별값(계정번호)
로그인명(이메일)	로그인명(이메일)
결제일	결제일
결제 상품	서비스코드
수량	결제 상품
결제금액(cash)	수량
결제수단 (ex신용카드, 소액결제)	결제금액 (사이버머니)
결제IP	결제IP

3.2. 게임 내 사기 유형의 예

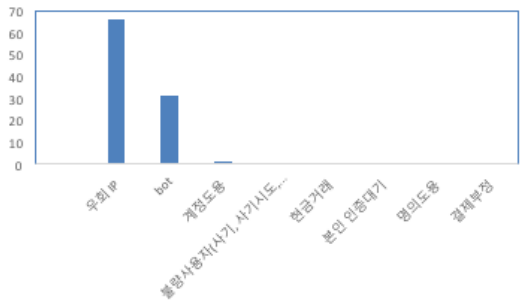
게임 내 이상거래는 결제사기와 관련해서 여러 사기 유형이 관련되어 나타난다. 타인의 결제수단을 도용하여 게임거래에 사용하기 위해서는 명의도용, 계정도용, VPN (Virtual Private Network)의 범죄가 결제사기와 관련되어 행해진다.

명의 도용: 다른 사람의 신용카드를 사용하기 위해 본인의 계정을 이용하기 보다는 제3자의 명의를 도용하여 회원가입을 한 후에 결제를 하는 방식을 취하기 때문에 명의 도용도 결제부정과 관련된 사기 유형임

계정도용: 마찬가지로 부정 결제가 탐지되는 것을 회피하기 위해서 다른 사람의 계정 정보를 이용하여 접속을 시도하기도 한다.

우회 IP: 결제부정을 저지를 때 접속 정보를 숨기기 위한 목적으로 VPN을 이용하기도 한다.

[그림 1]은 제재된 계정의 제재 사유 비율을 나타낸 것이다. 위에서보는 것처럼 부정결제가 직접적으로 발견되기보다는 우회 IP, 계정도용에 의한 탐지 비율이 높은 것을 알 수 있다.



〔그림 1〕 거래 기록 중 제재된 계정의 제재사유

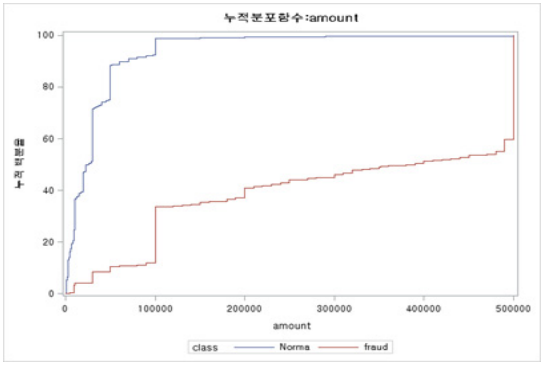
3.3. 거래 변수 도출

유의한 변수를 도출하기 위해 결제과정에서 추출되는 주요 변수의 정상계정과 제재계정에서의 차이를 분석하였다.

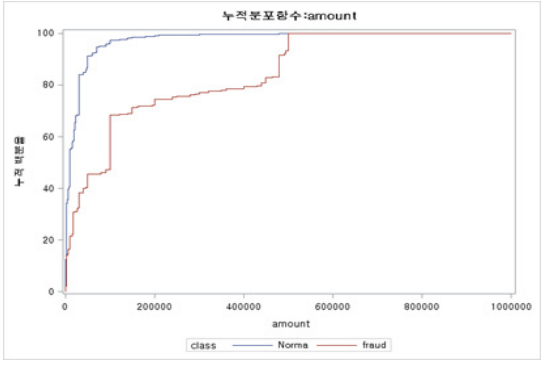
정상계정과 제재계정의 결제비용의 차이는 다음과 같다. 충전금액과 결제금액에서 제재계정의 금액이 훨씬 큰 것을 알 수 있다.

충전 시 결제수단도 유의한 변수가 될 수 있다. 게임 내에서는 사용자 편의를 위해 다양한 결제수단을 제공하고 있다. [표 3]은 정상계정과 제재계정의 결제수단 차이를 나타낸다.

편의점결제 방법은 충전을 편의점에서 결제금액을 납부하게 하는 방법으로, 금액 지불 후 발급 받은 영수



〔그림 2〕 일반유저와 제재유저의 충전 금액을 나타낸 CDF 그래프



〔그림 3〕 일반유저와 제재유저의 거래 금액을 나타낸 CDF 그래프

증의 카드번호로 게임 코인 충전 시 입력하면 결제가 완료된다. 편의점 결제 방법은 24시간 언제나 편의점에서 현금으로 구입이 가능하며, 구입 및 사용 시 개인정보 노출의 염려가 없으므로, PC방이나 공공장소에서 편리하게 이용할 수 있어 게임 결제 시 많이 사용된다. 특히, 게임 사용자 중 많은 수를 차지하는 10대들은 본인 명의의 신용카드나 핸드폰이 없기 때문에 편의점 결제 방법을 많이 이용한다.

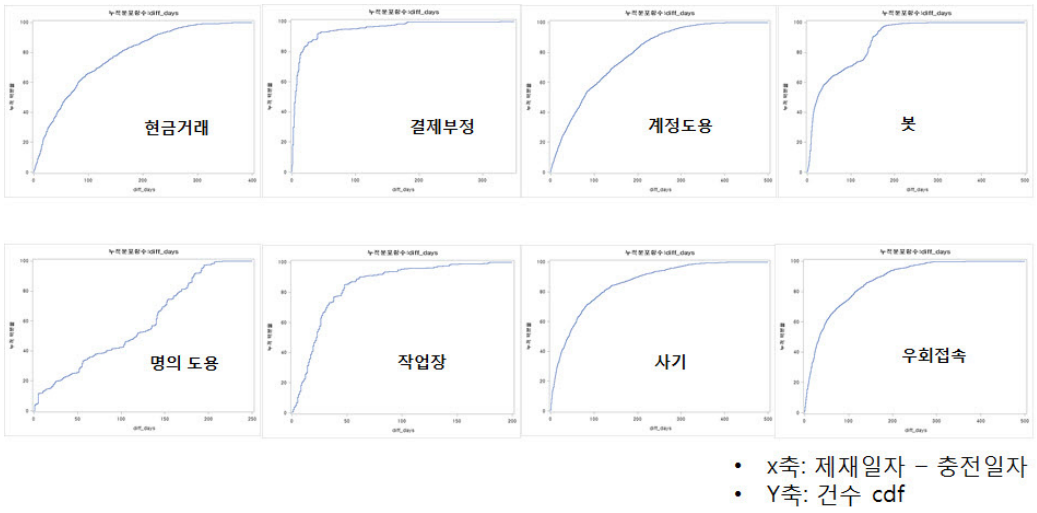
〔표 3〕 결제수단별 비율

결제방법	정상계정 (%)	제재계정 (%)
편의점결제	28.87	78.07
모바일결제	31.3	3.14
신용카드	14.51	2.09
문화상품권	8.02	4.58
무통장입금	9.31	11.22
인터넷뱅킹	4.84	0.7

이러한 차이는 제재계정에서 더욱 두드러지는데, 제재계정의 경우에는 정상계정에 비해 모바일결제나 신용카드의 결제비율이 낮아지고, 편의점결제비율이 높아진다.

3.4. 제안하는 방법론

이상거래를 탐지하기 위해서는 거래합산방법을 이용하는 것을 제안한다. 기존의 연구에서도 최근 거래를 합산하여 사용하는 것이 변별력을 높인다고 밝힌 바 있다 [5]. 사용자별로 봤을 때 매 거래별로는 차이가 있을 수



〔그림 4〕 제재사유별 거래 분포

있지만, 정해진 기간별로 거래를 합산하면 사용자별로 특징화하는 것이 가능하기 때문이다.

[그림 4]는 제재시점을 기준으로 최근 거래의 분포를 CDF (Cumulative Distribution Function)로 표현한 것이다.

[그림4]를 살펴보면 다음과 같은 특징을 찾을 수 있다.

결제부정, 작업장, 봇(BOT), 사기의 경우 제재직전의 거래가 많이 이루어짐

명의 도용의 경우는 제재시점과 충전시점의 차이가 많이 남

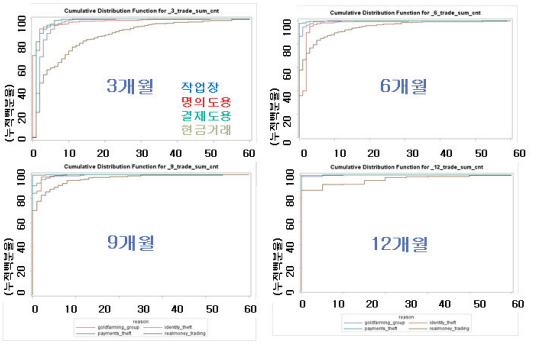
구간별로 나눠서 변수를 생성하는 것이 제재사유를 구분하는데 필요함

최근거래의 유용성을 확인한 후에 제재일자 기준으로 기간별 충전건수를 3개월 단위로 나누어서 살펴보았다. [그림 5]는 제재 직전 3개월, 4~6, 7~9, 10~12개월 기간에 따른 충전건수 분포를 나타낸다. [그림 5]를 살펴보면 최근 데이터가 제재사유를 구분하는데 유용하다는 것을 알 수 있다.

거래합산 변수는 다음과 같이 도출하였다.

제재시점을 기준으로 직전 3개월 4~6개월, 7~9개월, 10~12개월로 나눠서 변수 생성

각 구간별 거래 합산 변수: 거래건수 합, 거래금액 합, 결제방법 수, 아이템별 거래건수 및 거래금액 합, 결제방법별 결제금액, 거래 IP 종류 수



〔그림 5〕 제재시점 기준 구간별 최근거래 건수(제재사유별)

〔그림 6〕 거래합산 변수 도출 과정

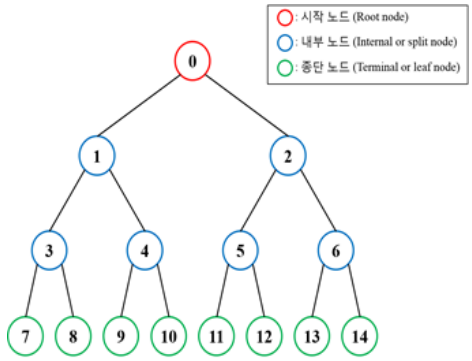
[그림 6]은 거래합산 변수의 도출 과정을 도식화한 것이다.

3.5. 적용 알고리즘

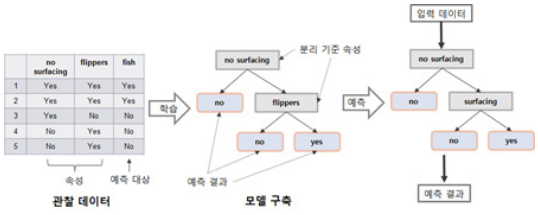
의사결정트리는 데이터 분류(정상 vs. 제재)를 위한 규칙을 추출하는 알고리즘 중 하나이다.

데이터의 변수를 탐색하여 데이터를 분류하는 변수의 조합을 트리 형태로 도출한다. 이때 위에서부터 중요한 변수를 선정하여 트리를 분기시키고, 다시 다른 변수를 이용하여 트리를 세분화해나간다. 이 때 중요한 변수란 정해진 분류기준에 의해 도출되는데, 보통 분기된 가지에 속하는 데이터들이 얼마나 같은 분류에 속하는 지의 정도를 이용한다. 의사결정나무 알고리즘은 학습속도가 빠르고 결과를 시각화하여 이해하기 쉽다는 장점을 가진다.

[그림 7]은 의사결정나무의 예이고, [그림 8]은 의사결정나무를 형성하는 과정을 기술하는 그림이다.



〔그림 7〕 의사결정나무의 예



〔그림 8〕 의사결정나무 형성과정

3.6. 탐지 결과

제안하는 방법을 검증하기 위해 여러 변수의 조합을 생성하여 결과를 비교하였다. 변수의 조합으로 각각 모델을 만들고 실험하여 정확도를 비교한 결과는 다음과 같다.

1) 충전과 거래 변수 비교
   충전 (0.894) >거래 (0.867)
2) 충전과 거래 변수를 모두 사용: 0.896
3) 건별 거래 데이터를 더하는 모델: 0.926

분석결과 거래보다는 충전 데이터가 이상거래를 탐지에 높은 정확도를 보였고, 충전과 거래를 결합하였을 때 약간의 성능이 향상되었다. 거래합산 데이터와 거래 건별 데이터를 종합하여 사용할 경우 가장 좋은 성능을 보였다.

Ⅳ. 결 론

본 연구는 게임 내 사용자의 거래 패턴을 분석하여 이상거래를 탐지할 수 있는 모델을 제시하였다. 기존에 신용카드나 은행에서 도입되었던 이상거래 탐지 시스템을 게임 산업에 적용한 선두 연구라는 점에서 의의를 가진다. 게임 산업은 게임 아이템, 정액권 등 결제가 많이 이루어지지고 있어, 소액결제 사기의 주 타겟이며, 꾸준히 사기에 노출되어 있다. 본 연구는 게임의 특성을 이해하여 변별력이 높은 변수를 도출하기 위해, 결제수단, 결제금액, 결제횟수, 제재시점과 최근 거래시점의 차이를 분석하였다. 분석 결과를 종합해보면 제재계정은 정상계정대비 결제금액과 결제횟수가 높고, 편의성이 높은 결제수단이 많이 사용되는 것을 발견하였다. 또한 제재시점과 최근거래 시점과의 차이에 따라 제재사유도 구분할 수 있는 것을 발견하였다. 이러한 발견들을 토대로 제재시점을 기준으로 시점을 구간화하여 거래합산 방식을 제안하였다. 여러 변수의 조합을 생성하여 실험을 진행한 결과 거래합산변수와 건별 거래 변수를 종합하여 이상거래를 탐지한 결과가 가장 좋은 모델임을 발견하였다.

참 고 문 헌

[1] 최화재, 우지영, 김휘강. “온라인게임 계정도용 탐지모델에 관한 연구”. *한국게임학회 논문지*, 11(6), pp. 81-93, 2011

[2] Woo, K., Kwon, H., Kim, H. C., Kim, C. K., Kim, H. K. “What can free money tell us on the virtual black market?”. *ACM SIGCOMM Computer Communication Review*, 41(4), pp. 392-393, 2011

[3] Christou, I. T., Bakopoulos, M., Dimitriou, T., Amolochitis, E., Tsekeridou, S., Dimitriadis, C. “Detecting fraud in online games of chance and lotteries”. *Expert Systems with Applications*, 38(10), pp. 13158-13169, 2011

[4] Lim, W. Y., Sachan, A., Thing, V. “Conditional Weighted Transaction Aggregation for Credit Card Fraud Detection”. *In Advances in Digital Forensics X* (pp. 3-16). Springer Berlin Heidelberg, 2014.

[5] Schaidnagel, M., Connolly, T., Laux, F. “Automated feature construction for classification of time ordered data sequences”. *International Journal on Advances in Software*, 7(3), pp. 632-64. 2014

[6] Coppolino, L., D’Antonio, S., Formicola, V., Massei, C., Romano, L. “Use of the dempster-shafer theory for fraud detection: the mobile money transfer case study”. *In Intelligent Distributed Computing VIII* (pp. 465-474). Springer International Publishing. 2015

[7] Mahmoudi, N., Duman, E. “Detecting credit card fraud by modified Fisher discriminant analysis.” *Expert Systems with Applications*, 42(5), pp. 2510-2516. 2015

[8] Vadoodparast, M., Hamdan, A. R. ”FRAUDULENT ELECTRONIC TRANSACTION DETECTION USING DYNAMIC KDA MODEL”. *International Journal of Computer Science and Information Security*, 13(3), 90. 2015

〈저 자 소 개〉

우 지 영 (Jiyoung Woo)
정회원

2000년 2월 : KAIST 산업공학과 학사
2002년 2월 : KAIST 산업공학과 석사
2006년 2월 : KAIST 산업공학과 박사
2011년 2월 ~ 현재: 고려대학교 정보보호대학원 연구교수
<관심분야> 데이터 마이닝, 시큐리티 인텔리전스, 온라인게임 보안

김 하 나 (Hana Kim)
학생회원

2013년 2월 : 서울여자대학교 정보보호학과 졸업
2013년 3월~현재 : 고려대학교 정보보호학과 석사과정
<관심분야> 온라인게임 보안, 데이터 마이닝

곽 병 일 (Byung Il Kwak)
일반회원

2013년 2월 : 세종대학교 컴퓨터공학과 졸업
2013년 9월~현재 : 고려대학교 정보보호학과 석·박사통합과정
<관심분야> 온라인게임 보안, 데이터 마이닝, 네트워크 보안, IoT 보안

김 휘 강 (Huy Kang Kim),
종신회원

1998년 2월 : KAIST 산업경영학과 학사
2000년 2월 : KAIST 산업공학과 석사
2009년 2월 : KAIST 산업및시스템공학과 박사
2004년 5월 ~ 2010년 2월 : 엔씨소프트 정보보안실장, Technical Director
2010년 3월 ~ 2015년 2월 : 고려대학교 정보보호대학원 조교수
2015년 3월~현재 : 고려대학교 정보보호대학원 부교수
<관심분야> 온라인게임 보안, 네트워크 보안