컨소시움 블록체인을 이용한 내부자 이상행위 탐지의 관한 연구*

최용철, 이덕규**

**서원대학교 정보보안학과

cho6nt@gmail.com, deokgyulee@gmail.com

A Study on Insider Anomaly Detection Using Consortium Blockchain *

Yong cheol Choi, Deok Gyu Lee**

**Dept of information security, Seowon University.

요 약

첨단 기술이 나날히 발전하면서 매년 내부자에 의한 기밀 유출 또한 증가함에 따라 기업에 피해가 발생하고 있다. 기업비밀이 유출될 경우 기업 입장에 막대한 손실을 미칠 수 있으며, 핵심 기술 유출은 해마다 지속적으로 증가하는 추세이다. 본 논문은 기존 기계학습을 이용한 내부자 이상행위 탐지 시스템에 컨소시움 블록체인을 이용하여 꾸준한 기록 관리를 통해 내부자의 이상행위를 탐지하는 솔루션을 제안하여 내부자 유출을 방지하고자 한다.

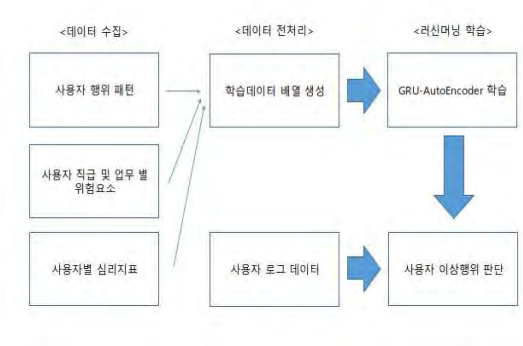
Ⅰ.서론

산업기밀유출범죄는 매년 증가하고 있다. 2013년을 기점으로 해외로 유출하려는 건수가 급격하게 증가하고 있으며 2014년 피해건수는 472건, 피해금액은 50조원으로 중소기업 4,700여 개의 연 매출과 맞먹는 금액이다. 이러한 손실을 최소화하기 위한 범 국가적인 대응체계 마련과 중소 기업의 보안체계 구축을 위한 회사의 관심과 의식향상이 필요하다. 산업기밀보호센터의 기술유출 분야별현황을 보면 우리나라가 높은 경쟁력을 가지고 있는 정밀 기계(34%), 전기 · 전자(26%), 정보통신(14%) 분야에서 많은 산업기밀 유출사건이 일어나고 있다.[1] 산업스파이의 표적 기술은 점점 대기업의 IT 분야 기술에서 중소기업의 정밀기계 분야로 이동 및 확대 되고 있다는 것을 알 수 있다. 이를 방지하기 위해 본 논문에서 기존 내부자 이상행위 탐지를 위한 시스템에 블록체인 사용을 제안하고, 목차로는 2장에서는 본 논문에서 제안하는 시스템을 다루며, 3장에서 결론으로 마무리 짓는다.

Ⅱ. 제안 방식

2.1 시스템 구성

*본 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 2020-0-00326, 블록체인 기반 물류정보의 실시간 트래킹을 통한 스마트 항만 응용 플랫폼 개발)



[Fig. 1] Schematic diagram of existing systems

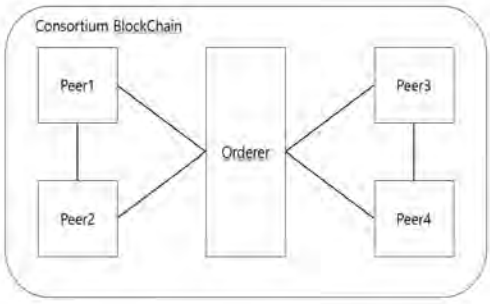
기존 시스템의 시스템 구성은 사용자의 비정상행위를 탐지하기 위해 사용자의 정상행위를 학습한 후 사용자가 정상행위인지 아닌지를 판별하게된다. 이 때 판별하는 기준이 사용자별로 하루 업무는 순서가 있고, 매일 비슷한 흐름으로 업무를 진행하게 될 것이다. 또한 각 개인마다 일정한 패턴을 갖고있는데 이 데이터를 학습해 기준으로 잡아 정상행위로 판단할 것이다. 이 외에 내부자 위협에 이상행위에 대해서 2가지로 나눌수 있는데 첫 번째론 행동적 이상행위로 평소 업무시간 이외에 네트워크 접근과 불필요한 파일에 복사 USB 과다횟수 연결등 평소 업무에 크게 빗나가는 행동을 할 경우와 두 번째론 심리적 요인인데 해당 사용자의 취약한 심리상태와 적대적인 행동이다. 이를 기준삼아 머신러닝에 정상행위를 학습시킨다.

성향	요소
행위적 요인	로그인/로그오프 기록
	웹 활동
	파일 액세스 활동
	전자 메일 사용
	Device 사용
	업무시간 외 컴퓨터 사용
상황적 요인	직위
	부서
	근무기간
	참가 프로젝트
심리적 요인	직무만족도
	심리검사표

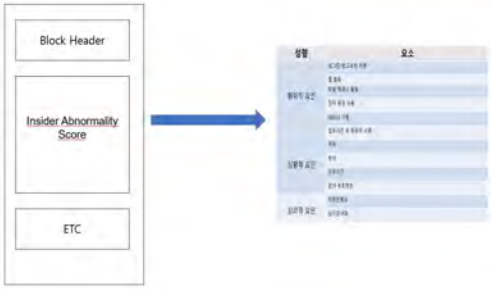
[Fig. 2] Example of data target by user

기계학습을 하기 위해서는 데이터 분석이 필요하다. 데이터 분석을 통해 불필요한 정보를 제거하고 기계학습의 효과를 최대한으로 할 수 있다. 수집 데이터로서는 시간행 순서로 사용자 로그온/로그오프 기록, 웹 활동, 파일 엑세스 활동, 전자 메일 사용, 장치 사용 및 사용자들의 직위, 부서, 근무 기간, 참가 프로젝트, 직무 만족도등을 담은 데이터를 수집할 것이고 그 외에도 각 사원에 대한 심리적 성향 지표도 함께 데이터 배열을 생성할 것이다. 여기서 컨소시움 블록체인을 이용하여 기존의 사용자 데이터를 공유함으로써 기계학습의 데이터량을 더 늘리고 학습 범위도 늘려서 탐지율을 더욱 높일 수 있고, 이상행위 점수 공유에 따른 초기 탐지에도 도움이 될 수 있는 블록체인을 이용한 공유 시스템을 제안한다.

2.2 컨소시움 블록체인 적용



[Fig 3.] Consortium BlockChain Principle



[Fig 4.] Insider abnormality score inside the blockchain

기존의 내부자 이상행위 탐지를 위한 데이터들을 합산하여 내부자 이상행위에 대한 점수를 계산하고, 각 사용자에 대한 점수를 사용자 가상지갑에 저장시키는 방식으로 제안한다. 일종의 가상거래를 통한 평가점수를 저장하며, 사용자 가상지갑을 통해 기존의 내

부자 이상행위에 대한 정보를 파악 할 수 있으며, 마치 신뢰도 평가와 같은 방식으로 작동 할 수 있다. 기업입장에서는 이력서 이외에 기업 비밀 유출에관한 확률또한 계산 할 수 있으며, 신입사원 혹은 경력직을 모집 할 때에 좀 더 유용한 정보로 사용 할 수 있다. 또한 여럿이서 공유함으로써 기존에 있던 내부자 이상행위 평가 점수에 관한 검증도 할 수 있으므로 더욱 유용한 정보로 사용 될 수 있다.

2.3 제시되는 문제점

기존 시스템에 블록체인을 적용하여 평가점수를 이용한 내부자 이상행위 탐지 및 평가에 관한 문제점은 기존 사용자들의 프라이버시가 문제가 될 수 있다. 자신의 평가점수가 기업을 통해 공유됨으로써 과거의 평가점수가 어디에서든지 공유되고 문제가 제시될 수 있고, 또한 개인정보로 분류 될 수 있기 때문에 개인정보에 관한 문제가 있다. 따라서 블록체인 서비스에관한 개인정보 관리에 대한 연구가 더욱 진행되어야하는 과제가 남아 있다.

2.4 제안 방식 평가

	기존 방식 (GRU를 이용한 내부자 이상행위 탐지)	제안 방식 (기존 시스템에 블록체인을 활용한 평가점수 도출)
학습데이터 축적량	↓	↑
지속적인 기록 관리	X	O
내부자 이상행위 검증	X	O

[표 1.] Evaluate proposed method

기존 시스템과의 비교에서 기존 시스템을 유지한다고 할 때, 학습데이터에 관한 축적량은 블록체인을 이용하여 공유하였을 때 더욱 높다. 또한 지속적인 시스템 사용으로 기록관리를 할 때 블록체인을 이용한 방식이 더욱 수월하다는 것을 볼 수 있다. 블록체인을 이용하였을 때 내부자 이상행위의 오탐 및 검증에 관한 문제를 해결 할 수 있으며, 타 기업들과의 컨소시움을 통하여 초기 탐지에 관한 문제도 해결 할 수 있다. 정보가 없을 경우 탐지에 문제가 생길 수 있지만 컨소시움을 맺은 기업들간의 정보가 공유될 시에 더욱 많은 데이터량을 가지고 탐지 할 수 있기 때문이다.

Ⅲ. 결론

첨단 기술이 나날이 발전하면서 매년 산업스파이에 의한 기밀 유출 또한 증가함에 따라 기업들이 막대한 피해가 발생하고 있다. 이에 사내에서는 이상 행위 탐지 도구를 사용해도 사용초기에는 사용자에 대한 데이터가 없을시와 신입사원이 새로 회사에 입사할 시 보안 도구에 변경으로 데이터가 추가될 경우 데이터의 부족으로 어떤 사원이 내부 유출자인지 정확한 판단이 힘들어 질 수 밖에 없다. 이러한 문제점을 개선하기 위해 본 논문에서는 사용자 행위를 탐지하는 기존 시스템에 블록체인을 이용하여 더욱 넓은 탐지 반경을 제공 할 수 있는 환경을 만드는 시스템을 제안하여 기업의 내부자를 통한 비밀 유출을 방지하고자 한다.

[참고문헌]

[1] 한국산업기술보호협회,

http://www.kaits.or.kr/front/bmt/bbs/list.act?bbs_config_nid=2

[2] 박정홍, 'Private 블록체인 특성이 의료분야 수용의도에 미치는 영향' 성균관대학교 일반대학원.

[3] Jerald Lee, "SSDT Hooking", Nevembe r 2006.

[4] 이기영, '기록관리시스템 블록체인 기술 적용 방안 연구' 명지대학교, [2019]

[5] 고필성, '블록체인을 이용한 의료정보시스템 활용방안에 관한 연구' 숭실대학교,

[2019]

[6] 구동균 'Deep Learning을 이용한 택시 승객 승차 예측에 관한 연구' 서울시립대학교 [2018]

[7] 여강국 'H-CNN 알고리즘을 이용한 이미지 데이터 학습과 정확도 측정 및 학습 속도 비교' 동아대학교 [2017]

[8] Keji Zheng, Wei Qi Yan, and Parma Nand, "Video Dynamics Detection Using Deep Neural Networks", Journal of IEEE, pp. 1-11, Dec. 2017.

[9] S. N. Danilin and S. A. Shchanikov, " Neural Network Algorithms for Determining the Values of Signal Parameters in Radio-Electronic Hardware", Journal of IEEE, Vol. 14, Nov. 2017.

[10] 조영복 '딥러닝 기반의 R-CNN을 이용한 악성코드 탐지 기법' 디지털콘텐츠 학회 논문지, 대전대학교 [2018]

[11] 정예나 '블록체인 기반 영상 정보 관리 시스템' 아주대학교 [2019]

[12] 효율적인 이더리움 스마트 콘트랙트에 관한 연구

김대한 (아주대학교 사이버보안학과), 최광훈 (아주대학교 컴퓨터공학과), 김강석 (아주대학교 사이버보안학과), 김재훈 (아주대학교 사이버보안학과)

한국정보처리학회 2018년도 추계학술발표대회 2018 Oct. 31 ,pp. 82 - 84 , 2018

[13] 핀테크를 위한 스마트 컨트랙트 보안

신다혜 (가천대학교), 이종협 (가천대학교)

정보처리학회지 = Korea information processing society review v.22 no.5 ,pp. 54 - 62 , 2015 , 1226-9182 ,

[14] 개인정보보호를 고려한 스마트 컨트랙트 설계 방안 연구

김혜리 , 강희정 , 홍승필

보안공학연구논문지 ,pp. 139 - 154 , 2018 ,