# 모바일 클라우드 자원 접근 이상행위 분석 알고리즘 연구

김지연*, 최주영*, 김형종*, 박춘식*, 김정욱**, 정현철**
*서울여자대학교 정보보호학과
**한국인터넷진흥원 연구개발팀
e-mail:jykim07@swu.ac.kr

# A Study on Resource Access Anomaly Detection Algorithm in Mobile Cloud

Ji-Yeon Kim*, Ju-Young Choi*, Hyung-Jong Kim*, Choon-Sik Park*,
Jeong-Wook Kim**, Hyun-Cheol Jeong**
*Dept of Security Information, Seoul Women's University
**Security R&D Team, Korea Internet & Security Agency

요 약

모바일 클라우드 서비스는 사용자가 모바일 단말에 자원을 가지고 있지 않더라도 인터넷을 통해 외부의 다양한 IT 자원을 제공하는 서비스로서 모바일 단말이 가지는 성능적 한계를 극복시킬 수 있다는 장점과 함께 이용자 수가 증가하고 있다. 그러나 클라우드 컴퓨팅 환경에 존재하는 개인 및 기업의 정보 유출과 같은 문제들은 모바일 클라우드 컴퓨팅 환경에도 그대로 상속되기 때문에 이러한 문제에 대응하기 위해서는 모바일 클라우드 컴퓨팅 환경에서 정보유출을 탐지할 수 있는 이상행위 탐지 알고리즘이 마련되어야 한다. 여기서 이상행위란, 모바일 클라우드 자원에 접근하는 방법에 있어 기존에 인지하고 있던 정상적인 행위에서 벗어나는 행위를 의미하며 이상행위로 판단되는 상황이 발생되는 경우, 이를 정보유출이 발생할 수 있는 상황으로 인지함으로써 적절한 대응을 할 수 있게 된다. 따라서 본 논문에서는 모바일 클라우드 자원의 정보유출을 방지하기 위한 목적으로 자원 접근에 대한 이상행위 탐지 알고리즘 개발 모델을 제시한다. 이상행위 탐지 알고리즘을 개발하고 이를 검증하기 위해서는 이상행위를 일으키는 공격 모델 및 대응 모델이 개발되어야 한다. 따라서 본 논문에서는 인증 및 권한관리의 취약점을 이용하여 위협을 일으키는 공격 모델을 개발하는 방법을 제시하고, 사용자의 접속환경 및 클라우드 자원의 정보 흐름을 분석함으로써 이상행위를 탐지하는 알고리즘을 제시한다.

## 1. 서론

모바일 클라우드 서비스란, 모바일 단말을 이용하여 단말 외부에 존재하는 자원을 요청하고 결과를 제공받는 모바일 클라우드 컴퓨팅(Mobile cloud computing)을 이용한 서비스로서 주로 웹상에서 제공되는 애플리케이션에 접속하여 서비스를 이용하는 방식을 의미한다. 클라우드 컴퓨팅은 사용자가 로컬 영역에 자원을 가지고 있지 않더라도 인터넷을 통해 다양한 IT 자원을 제공받을 수 있는 기술이기 때문에 기존의 PC보다 자원의 한계가 많은 모바일 단말의 경우, 클라우드 컴퓨팅으로 인한 효과를 더욱 많이 얻을 수 있게 된다. 특히, 오늘날에는 모바일 단말의 다양한 애플리케이션 지원이 중요시 되고 있기 때문에 모바일 단말이 갖는 저 성능의 처리 능력, 짧은 배터리 수명, 적은 용량의 데이터 저장소와 같은 한계를 극복하기 위하여 모바일 클라우드 서비스가 등장하였다. 현재 모바일 클라우드 서비스는 급격히 증가하고 있으며 ABI 조사기관에서는 전 세계의 모바일 클라우드 컴퓨팅 가입자 수가 2014년에는 전체 모바일 가입자 수의 19%인 약 9998만 명에 이를 것으로 전망하고 있다[1]. 또한, 기업에서의 클라우드 플랫폼 도입과 스마트폰 채택에 따라 2015년에는 전 세계 2억 4000만 명의 기업 사용자가 클라우드 컴퓨팅을 이용할 것이고, 여기에서 52억 달러의 매출이 발생할 것으로 전망하고 있다[2]. 그러나 이러한 전망에도 불구하고, 클라우드 컴퓨팅과 관련된 여러 문제 또한 많이 제기되고 있다. 기술적, 관리적 측면의 많은 문제들 중에서도 사용자들이 클라우드 서비스를 도입할 때 우려하는 가장 큰 문제는 개인 정보 및 자료 유출과 같은 보안 문제이다. 실제로 2010년 IDC 조사 결과에 따르면, IT 관련 임원들이 클라우드 컴퓨팅의 첫 번째 당면과제로서 보안 문제를 선택하고 있다[3].

클라우드 컴퓨팅은 IT 자원의 일부 또는 전부를 아웃소싱하는 형태이기 때문에 개인 사용자의 경우에는 개인 정보의 노출 및 개인 데이터에 대한 감시·사업적 가공과 같은 보안 문제를 우려하여 이에 대한 익명성 보장을 요구하고 있고, 기업 사용자의 경우에는 서비스 중단 및 기업 정보 훼손·유출, 고객 정보 유출 등과 같은 보안 문제를 우려하고 있다[4]. 이러한 보안 문제들은 클라우드 컴퓨팅 환경에 존재하는 보안 취약점을 악용한 공격 결과로서 나타나는 것이기 때문에 공격 시도에 대한 대응책으로서 인증 및 권한 관리가 필요하게 된다. 특히, 모바일 클라우드

서비스는 클라우드 컴퓨팅에서 제기되고 있는 보안 문제를 그대로 상속받고 있기 때문에 모바일 클라우드 서비스의 보안 문제를 다루기 위해서는 기본적으로 클라우드 컴퓨팅 보안 문제를 다루어야 하며 이와 더불어 모바일 환경에서 추가적으로 반영될 수 있는 무선 네트워크 및 모바일 단말의 취약점을 이용한 보안 문제를 고려해야 한다.

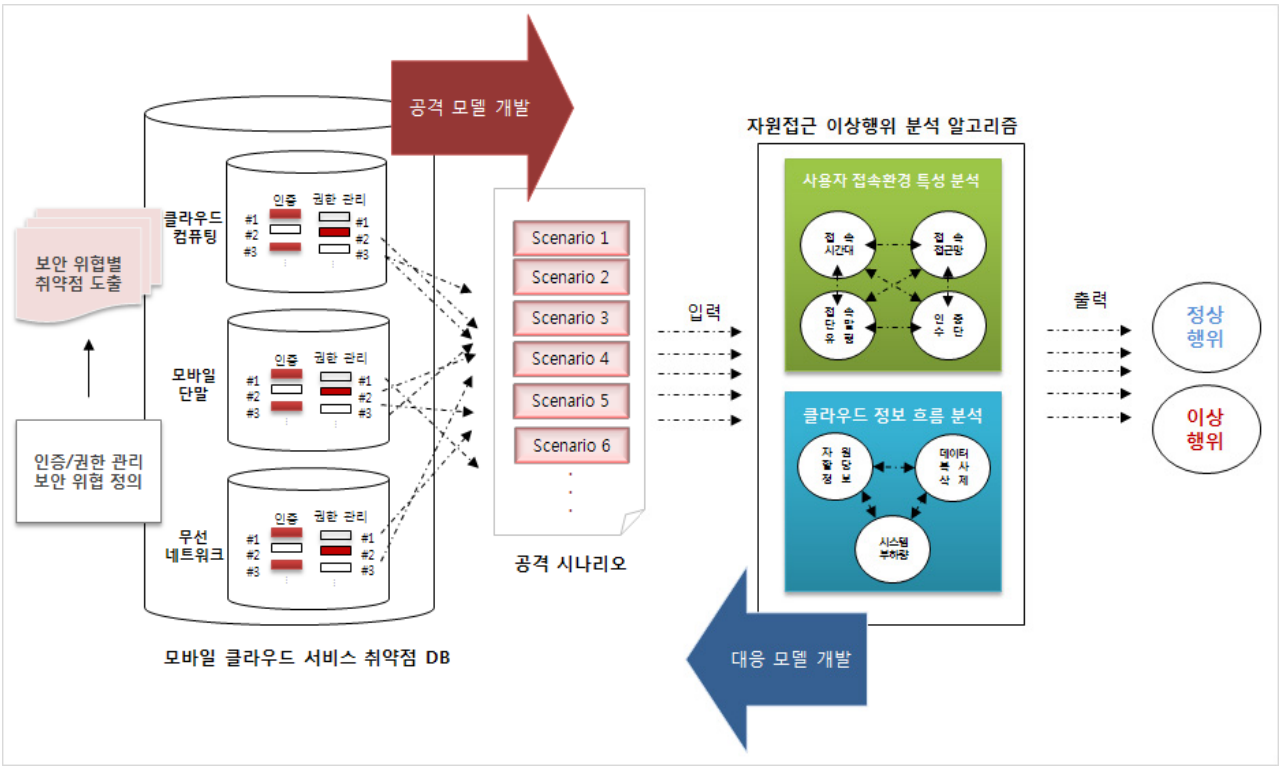
본 논문에서는 모바일 클라우드 컴퓨팅 환경에서 발생할 수 있는 정보유출을 방지하기 위한 목적으로 정보유출을 탐지할 수 있는 이상행위 탐지 알고리즘을 개발한다. 이상행위 탐지 알고리즘을 개발하고, 이를 검증하기 위해서는 (그림 1)과 같이 이상행위를 발생시키는 공격 모델과 이를 탐지해내는 대응모델이 필요하다. 따라서 본 논문에서는 클라우드 컴퓨팅, 무선 네트워크, 모바일 단말 단에서 인증 및 권한관리 취약점을 이용하여 위협을 일으키는 공격 시나리오를 작성하기 위한 방법을 제시하고, 사용자의 접속환경 및 클라우드 자원의 정보 흐름 분석을 통해 모바일 클라우드 자원에 접근하는 이상행위를 탐지하는 알고리즘을 개발하고자 한다.

논문의 구성은 2장에서 공격 모델을 개발하기 위한 방법을 제시하고, 3장에서 사용자의 접속 환경 분석을 통한 이상 행위 탐지 방법을 제시한다. 4장에서는 클라우드 자원의 정보 흐름 분석을 통해 이상행위를 탐지하기 위해 필요한 지표를 정의하고, 5장에서는 3장과 4장에서 제시된 방법을 조합하여 이상행위 탐지 기준을 마련하는 방법을 제시한다.

## 2. 모바일 클라우드 자원 공격 시나리오 개발

공격 시나리오는 다양한 공격기법의 조합을 통해 공격자의 목적을 달성하는 형태로 나타난다. 이는 침해의 주체와 목적으로 구성되는 “공격 시나리오의 목적”이 존재하는데 이 침해의 주체는 통상적으로 위협이라는 이름으로 명명되고, 공격을 실행하는 개인 또는 조직을 의미한다. 또한, 침해의 주체는 항상 침해의 목적을 갖게 되며 공격 시나리오는 침해 주체의 목적을 달성하기 위한 세부 절차로서, 다양한 공격기법들은 공격 대상에 해당하는 시스템들의 취약점을 악용하여 세부적인 목적을 달성하게 된다.

모바일 클라우드 인증 및 권한관리 취약점을 이용한 공격 시나리오를 개발하기 위해서는 (그림 1)의 공격 모델 개발 부분과 같이 먼저 모바일 클라우드 환경인 클라우드 컴퓨팅, 무선 네트워크, 모바일 단말에서의 정보유출 위협이 정의되어야 한다. 이것은 침해를 발생하는 외부 위협 주체 및 위협의 주요 동기에 대한 정의를 수행하는 것으로 정의된 위협을 일으키기 위한 취약점을 파악함으로써 다양한 공격 기법을 도출할 수 있게 한다. 도출된 공격 기법들은 다양한 조합으로 발생할 수 있으며, 이 조합이 공격 시나리오가 되는 것이다. 개발된 공격 시나리오는 대응모델에 해당되는 자원접근 이상행위 탐지 알고리즘에 입력으로 제공되며, 알고리즘에 따라 정상 행위 또는 이상행위로 판단될 수 있다. 이러한 판단 결과는 탐지 알고리즘에 대한 성능을 알려주는 것으로 우리는 이 결과를 통해 알고리즘의 개선 방향을 파악하거나 알고리즘을 검증할 수 있게 된다.




(그림 1) 모바일 클라우드 자원 접근 이상행위 탐지 알고리즘 개발 모델

## 3. 모바일 클라우드 사용자 접속환경 분석 기반 이상행위 탐지 기술

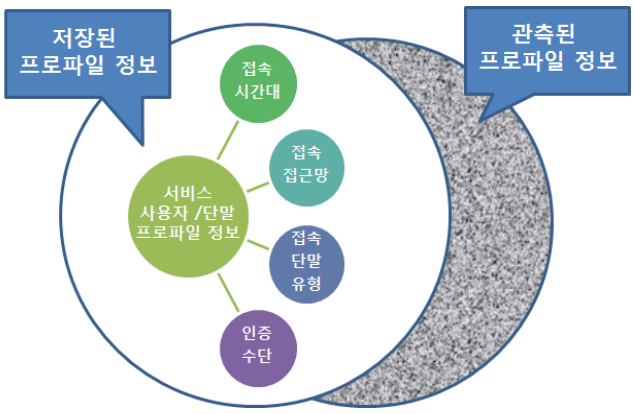
모바일 클라우드 자원에 접근하는 이상행위에 대한 분석 지표로서 사용자의 접속 패턴에 대한 정보가 사용될 수 있다. 모바일 클라우드 서비스 사용자의 접속 환경을 분석하기 위해서는 먼저 사용자와 사용자 단말의 프로파일 정보로서 수집해야 할 지표가 정의되어야 하며 수집된 정보를 어떻게 분석할 것인지 그 방법이 마련되어야 한다.

본 논문에서는 사용자의 접속환경에 대한 분석 지표로서 <표 1>과 같이 접속 시간대, 접근망, 접속 단말 유형, 인증 수단을 도출하였다.

<표 1> 사용자 접속환경 분석 지표 분류 예

| 지표 | 유형 1 | 유형 2 | 유형 3 |
|---|---|---|---|
| 시간대 | 9시-17시 | 17시-22시 | 22시-9시 |
| 접근망 | Wi-Fi | WiBro | 3G |
| 접속 단말 유형 | Android | iOS | Feature phone |
| 인증 수단 | ID / password | 인증서 | 사용자 제공정보 |

<표 1>에서 유형은 각 지표에 대한 분류 기준을 예로 제시한 것으로서 접속 시간대는 일반적인 사람들의 사회 활동 시간을 기준으로 구분할 수 있고, 접근망은 현재 스마트폰에서 접근 가능한 네트워크의 종류로 구분할 수 있다. 또한, 단말 유형은 단말의 운영체제별로 구분할 수 있으며 인증 수단은 사용자별 인증 선호 방식이 다르기 때문에 인증 과정을 수행할 때 사용하는 인증 수단의 종류별로 분류될 수 있다. 이렇게 분류된 지표들은 사용자가 모바일 클라우드 자원에 접속할 때마다 수집 및 저장되어 사용자의 접속 패턴 정보로 가공되고, 이상행위 탐지를 위해서는 (그림 2)와 같이 사용자의 현재 관측된 프로파일 정보가 기존에 저장된 패턴과 어느 정도 유사한지를 판단하는 기준으로 사용된다.




(그림 2) 사용자 프로파일 패턴 정보 비교 방안

(그림 2)에서 음영부분은 저장된 정보와의 상이한 정도를 나타내며, 이 음영 부분의 넓이를 정량화하여 임계값 이상이 나올 경우에 이상 행위로 간주할 수 있다. 단, 사용자의 접속 패턴 저장을 위한 가공 시, 지표별 비중은 서로 다르게 반영될 수 있을 것이다.

## 4. 모바일 클라우드 자원 정보 흐름 분석 기반 이상행위 탐지 기술

사용자가 요청한 서비스를 처리하기 위해 사용되는 자원과 관련된 데이터는 사용자별 자원 이용 패턴을 파악할 수 있는 정보이다. 따라서 모바일 클라우드 자원이 처리되는 클라우드 데이터센터에서의 자원 흐름을 관찰함으로써 <표 2>와 같은 정보를 수집할 수 있다.

<표 2> 사용자 자원이용 패턴 분석 지표 예

| 지표 | 설명 |
|---|---|
| 자원 할당량 | CPU, 메모리, 네트워크 대역폭, 하드디스크 용량 |
| 데이터 운영 | 데이터의 복사 및 삭제 여부 조회 |
| 시스템 부하량 | 서버 및 가상머신의 현재 자원상태 파악 |

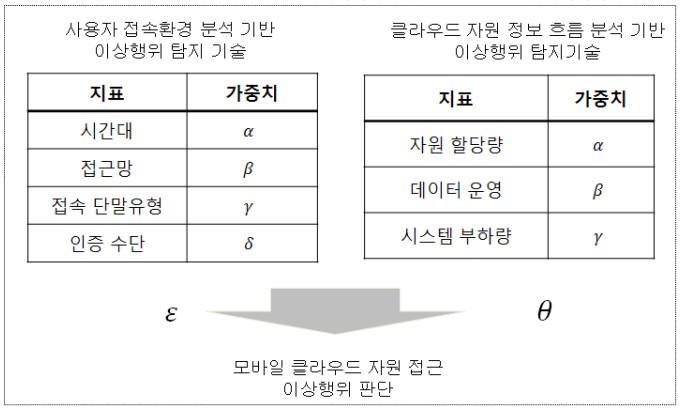
위 지표들은 서비스를 할당한 가상머신에서 얻을 수 있는 정보이며 이 가상머신에 대한 정보는 클라우드 데이터센터에서 자원을 효율적으로 할당하고 가용성을 보장하기 위해 운영하는 중앙의 관리 시스템에서 수집할 수 있다. 또한, 이 지표들은 (그림 2)와 동일한 방법으로 저장된 자원 이용 정보와 관측된 자원 이용 정보를 비교함으로써 이상행위 여부를 판단할 수 있다.

## 5. 모바일 클라우드 자원 접근 이상행위 탐지 알고리즘 개발

본 장에서는 3장과 4장에서 개발된 사용자 접속환경 분석 기반 이상행위 탐지 기술과 클라우드 자원 정보 흐름 분석 기반 이상행위 탐지 기술을 종합하여 최종적으로 이상행위를 탐지하기 위한 알고리즘을 제시한다.

먼저 두 개 기술에서 도출된 각 지표들이 해당 기술에서 차지하는 비중이 모두 다를 수 있다. 이것은 지표들 중 사용자의 특성이 잘 드러나지 않는 지표의 경우, 예를 들면, 사용자가 Wi-Fi, WiBro, 3G망을 통해 접근하는 빈도수가 유사한 경우에는 이 지표에 대한 가중치를 줄일 수 있을 것이다. 또한 두 개 기술 중에 사용자별 특성이 더욱 잘 드러나는 기술의 경우 가중치를 상대적으로 더 높여서 사용할 수 있으며, 두 개 기술이 각각 임계값을 설정하고 있기 때문에 어느 하나의 알고리즘에서 이상행위로 판단된 경우, 다른 한 개의 알고리즘의 탐지여부와 관계없이

이상행위로 판단할 수 있다. 이상행위에 대한 탐지 기준은 탐지 목적 및 적용 분야에 따라 달라질 수 있기 때문에 (그림 3)과 같이 가중치를 고려하여 관리자가 이를 설정할 수 있도록 해야 할 것이다.




(그림 3) 모바일 클라우드 자원접근 이상행위 판단

## 6. 결론 및 향후연구계획

본 논문에서는 모바일 단말을 이용하여 클라우드 서비스를 이용하는 사용자의 정보유출을 방지하기 위하여 모바일 클라우드 자원에 접근하는 이상행위 탐지 알고리즘을 개발하고, 이를 검증할 수 있는 공격 시나리오 개발 방법을 제시하였다. 공격 시나리오는 모바일 클라우드 컴퓨팅 환경인 클라우드 컴퓨팅, 무선 네트워크, 모바일 단말에서 인증 및 권한관리의 취약점을 악용하는 위협을 정의하고, 이 위협을 발생시키는 공격 기법들을 도출함으로써 개발할 수 있으며, 이상행위 탐지 알고리즘은 사용자가 자원에 접속하는 패턴 정보를 기반으로 탐지하는 기술과 사용자의 자원 이용 패턴 정보를 기반으로 탐지하는 기술을 제시하였다. 전자의 경우, 사용자가 단말을 통해 접속하는 프로파일 정보인 접속 시간대, 접근망, 접속 단말 유형, 인증 수단을 지표로 도출하였고, 후자의 경우, 사용자의 서비스 요청에 의한 자원 할당량, 데이터 복사 및 삭제 내역, 시스템 부하량을 지표로 도출하였다. 각 지표들의 중요도는 서로 다를 수 있기 때문에 이상행위 탐지 기준으로서 가중치를 다르게 반영할 수 있으며 두 개 기술의 탐지 정확도에 따라서 다른 비중으로 사용할 수 있다.

본 논문에서 제시한 공격 시나리오 개발 방법은 공격 방법 및 결과를 사전에 예측하고, 취약점을 제거함으로써 안전한 모바일 클라우드 서비스 인프라를 구축하는 데에 기여할 수 있으며, 이상행위 탐지 알고리즘은 모바일 클라우드 환경에서 개인 및 기업 사용자의 자원을 안전하게 관리하기 위한 정보유출 방지 모델에 활용될 수 있다. 또한, 본 논문에서 제시한 지표들은 하나의 예시로서 이 알고리즘의 성능을 향상시키기 위해서는 더 많은 지표가 도출되어야 하며, 이상행위에 대한 오탐율을 줄이기 위한 지표의 비교 및 임계값 설정에 대한 연구가 추가되어야 할 것이다.

## 참고문헌

[1] Christine Gallen, "Mobile Cloud Computing Subscribers to Total Nearly One Billion by 2014", ABI research, 2009. 9.

[2] ABI research, "Enterprise Mobile Cloud Computing", 2009. 12.

[3] IDC, "IDC Executive Telebriefing - Cloud Computing 2010, An IDC Update", 2009. 9.

[4] 은성경 외, "클라우드 컴퓨팅 보안 기술", 전자통신동향분석 제24권 제4호, 2009.

[5] Cloud Security Alliance, "Top Threats to Cloud Computing V1.0", 2010.

[6] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V1.0", 2009.

[7] Cloud Security Alliance, "Security Guidance for Critical Areas of Focust in Cloud Computing V2.1", 2009.

[8] Santosh K. Pandey, "Major Security Threats in Wireless Networks", The Institute of Chartered Accountants of India.

[9] Janson Meyer, "Potential Security Vulnerabilities of a Wireless Network Implementation in a Military Healthcare Environment", 2006.

[10] CenterTolls, LLC, "Threats from Mobile Devices - How to protect your sensitive information", 2007.

## Acknowledgement

본 연구는 방송통신위원회의 정보보호원천기술개발사업의 연구결과로 수행되었음(KCA-2011-11914-06002)