Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.3, Jun. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.3.487

모의해킹 기반 사전 예방적 클라우드 침해 사고 대응 프레임워크*

노 현,[1†] 옥 지 원,[1] 김 성 민[2‡]
[1,2]성신여자대학교 (대학원생, 교수)

Pentesting-Based Proactive Cloud Infringement Incident Response Framework*

Hyeon No,[1†] Ji-won Ock,[1] Seong-min Kim[2‡]
[1,2]Sungshin Women's University (Graduate student, Professor)

요 약

클라우드 서비스 취약점을 이용한 보안 사고가 발생하고 있으나, 복잡하고 다양한 서비스 모델을 갖는 클라우드 환경에서의 사고 흔적을 수집하고 분석하는 것은 어려운 문제이다. 이에 클라우드 포렌식 연구의 중요성이 대두되며, 퍼블릭 클라우드 서비스 모델에서의 대표적 보안 위협 사례에 기반한 클라우드 서비스 사용자(CSU)와 클라우드 서비스 제공자(CSP) 관점에서 침해 사고 대응 시나리오를 디자인해야 할 필요가 있다. 본 모의해킹 기반 사전 예방적 클라우드 침해 사고 대응 프레임워크가 클라우드를 대상으로 사이버 공격이 발생하기 전, 취약점 탐지 관점에서 클라우드 서비스 중요 자원 공격 프로세스에 대한 대응 방안에 활용할 수 있고, 포렌식 과정에서 침해 사고 포렌식을 위해 데이터 수집(data acquisition)을 위한 목적으로도 기대할 수 있다. 따라서 본 논문에서는 클라우드 침투 테스트 도구인 Cloudfox를 분석 및 활용하여 모의해킹 기반 사전 예방적 클라우드 침해 사고 대응 프레임워크를 제안한다.

ABSTRACT

Security incidents using vulnerabilities in cloud services occur, but it is difficult to collect and analyze traces of incidents in cloud environments with complex and diverse service models. As a result, the importance of cloud forensics research has emerged, and infringement response scenarios must be designed from the perspective of cloud service users (CSUs) and cloud service providers (CSPs) based on representative security threat cases in the public cloud service model. This simulated hacking-based proactive cloud infringement response framework can be used to respond to the cloud service critical resource attack process from the viewpoint of vulnerability detection before cyberattacks occur on the cloud, and can also be expected for data acquisition. Therefore, in this paper, we propose a framework for preventive cloud infringement based on simulated hacking by analyzing and utilizing Cloudfox, a cloud penetration test tool.

Keywords: Public Cloud, Forensic, Pentesting, Incident Response, Proactive

Received(03. 27. 2023), Modified(04. 26. 2023), Accepted(05. 03. 2023)

* 본 연구는 2023년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(NRF-2021R1G1A100632611), 산업통상자원부의 재원으로 한국산업기술진흥원의 지원(P000870 3, 2022년 산업혁신인재성장지원사업), 과학기술정보통신부 및 정보통신기획평가원의 ICT혁신인재4.0 사업(IITP-2022-RS-2022-00156310)의 연구결과로 수행되었음.

† 주저자, 220224007@sungshin.ac.kr
‡ 교신저자, sm.kim@sungshin.ac.kr(Corresponding author)

I. 서 론

클라우드 컴퓨팅 기술이 발전함에 따라, 국내외 기업들의 기존 서버에 대한 클라우드 전환율이 20%에 육박할 정도로 클라우드 시장은 가파르게 성장하고 있다[1]. 클라우드 컴퓨팅은 다양한 형태의 서비스 모델을 제공하는데, 그중에서도 컴퓨팅 및 스토리지 자원과 같은 IT 인프라를 클라우드 형태로 제공하는 IaaS(Infrastructure-as-a-Service) 모델이 높은 점유를 보이며, 대표적인 상용 솔루션으로는 AWS(Amazon Web Service)와 Microsoft Azure가 있다. 하지만 솔루션 활용 과정에서의 사용자의 잘못된 구성(misconfiguration)이나 솔루션 내 보안 취약성을 활용한 공격 등으로 인해 서비스 사용자의 활동 및 데이터가 유출되는 사건이 발생하고 있다. 시장조사기관 가트너(Gartner) 조사에 따르면 사이버 공격 중 클라우드 서비스를 타깃한 공격의 비율은 49%로 클라우드 서비스 보안 위협이 상당한 비중을 차지한다[2]. 따라서, 클라우드 상에서 데이터 유출의 원인을 파악하고 악성 행위를 분석하기 위한 클라우드 포렌식의 중요성이 대두되고 있다.

디지털 포렌식 관점에서 클라우드 서비스 모델 중 IaaS는 게스트(guest) OS를 포함하여 사용자가 운영 및 관리하는 소프트웨어 계층이 넓으므로 SaaS(Software-as-a-Service) 모델이나 PaaS(Platform-as-a-Service) 모델보다 증거로 활용될 수 있는 데이터를 더욱 확보할 수 있다. 하지만, 멀티테넌시(multi-tenancy)를 보장하는 클라우드 가상화 기술 등으로 인해 포렌식을 위한 데이터 수집 과정이 복잡하며, 기존 포렌식 방법론 및 도구를 적용하는 데 한계점이 존재한다.

현재의 IaaS 서비스 모델 구조상 퍼블릭 클라우드 내 취약성 진단의 목적으로 클라우드 서비스 사용자(Cloud Service User, CSU)의 작업 및 이벤트에 대한 데이터를 수집하기 위해서는 클라우드 서비스 제공자(Cloud Service Provider, CSP)의 협력에 의존할 수밖에 없다. 하지만, 클라우드 포렌식의 표준은 존재하지 않을뿐더러, 포렌식 수사관이 데이터를 제공받더라도 데이터의 신뢰성을 확인하는 프로세스가 확립되어 있지 않다는 문제가 있다[3]. 또한, CSP 관점에서도 신뢰할 수 없는 일반 사용자들에게 포렌식을 위한 데이터를 공개적으로 제공하는 것은 부담으로 작용하는 것이 현실이다.

악의적인 목적을 가진 클라우드 서비스 사용자는 계정을 생성하고 클라우드 환경에 액세스하여 공격을 수행한뒤, 언제든 계정을 삭제할 수 있기에 클라우드 포렌식 데이터 수집에 있어 어려움이 있다[4]. 또한, 획득한 정보를 바탕으로 클라우드 인스턴스를 추가적인 범죄에 악용하거나 공격 수행의 경유지로 쓰기도 한다. 따라서, 클라우드 사고가 발생하였을 때 사후 조치가 아닌 사전 예방적 활동으로 포렌식 데이터를 수집 및 분석하는 것은 디지털 증거를 수집하는 환경의 능력을 최대화하고 동시에 사고 대응 중 포렌식 비용을 최소화할 수 있다는 점에서 필수적인 작업이다. 사전 예방적 포렌식(proactive forensics)을 제안한 선행 연구가 존재하나 현재까지 사전 예방적 포렌식의 구체적인 프로세스 형태는 명확히 규정되지 않았다[5]. 사전 예방적 디지털 포렌식 조사 프로세스를 제안한 종래 연구들은 증거 수집을 바탕으로 한 체계적인 사전예방적 접근 방식에 대한 필요성을 주장하고 있으나 체계화된 방법론에 대한 정의는 아직 미흡한 실정이다[6].

본 논문에서는 앞서 언급한 한계점을 극복하기 위해 클라우드를 대상으로 한 모의해킹 기반 사전 예방적 클라우드 침해 사고 대응 프레임워크를 제안한다. 클라우드 침투 테스트 도구인 Cloudfox[7]의 플러그인(plugin)을 사용 목적에 따라 자원, 공격 경로, 권한 요소로 분류하고, 최근까지도 퍼블릭 클라우드 내 보안설정이 취약한 자원을 선정하여 AWS 클라우드 자원별 시나리오를 분석한다. 클라우드 포렌식 시나리오의 한 예로써, AWS에서 제공하는 상용 클라우드 침투 테스트 도구 AWSBucketDump[8]에서 획득한 데이터를 바탕으로 제안한 프레임워크를 활용하여 사용자의 스토리지인 AWS S3 버킷(Bucket)에 대한 잘못된 구성을 입증하였다. Azure에서 제공하는 스토리지 계정에 대해 스캔하는 도구인 Blob Hunter[9]를 사용하여 획득한 데이터를 기반으로 프레임워크를 활용하여 사용자의 스토리지인 Azure Blob Storage에도 AWS S3 버킷과 동일한 시나리오를 적용할 수 있음을 확인하였다. 또한, 클라우드를 대상으로 한 사이버 공격이 발생하기 전 사전 예방의 목적으로 활용할 수 있을 것으로 기대한다. 포렌식 데이터 수집 및 분석을 기반으로 공격 도구 및 보안성을 평가하고, 시나리오 공격에 대한 위험 수준을 낮출 수 있는지 검토의 목적으로도 활용 가능하다.

본 논문의 구성은 다음과 같다. 2장에서 클라우드

포렌식 관련 연구 동향을 살펴보고, 3장에서 국내외 클라우드 포렌식을 위한 법률 및 제도의 필요성을 제시한다. 4장에서는 모의해킹 기반 사전 예방적 클라우드 침해 사고 대응 프레임워크를 통해 클라우드 포렌식 정보 수집을 위한 상용 및 오픈 소스 침투 테스트 도구의 활용 가능성을 검토한다. 5장에서 Amazon와 Azure 클라우드 상용 서비스에 대한 사전 예방적 클라우드 침해 사고 시나리오를 CSU 및 CSP 관점에서 분석하고, 6장에서 결론으로 마무리한다.

II. 배경 지식 및 관련 연구

2.1 퍼블릭 클라우드 포렌식

법적 효력을 가지는 포렌식 증거는 공격자가 범죄 목적으로 CSU 계정을 사용 후 종료하면 클라우드 환경에 남지 않는다[10]. 예를 들어, AWS Free Tier 계정을 생성한 후 사이버 공격에 활용한 뒤 이를 삭제할 수 있다. 하이퍼바이저(hypervisor)와 같은 특권 계층에서의 모니터링 등을 통해 이러한 사이버 공격 범죄 활동에 사용된 증거를 수집하는 것이 원천적으로 불가능한 것은 아니나, 성능 저하 문제 등 어려움이 존재한다. 범죄로 인해 데이터가 삭제되는 경우 이 데이터를 재구성하고 소유자를 식별하여 클라우드 포렌식 분석에 사용하는 것이 하나의 과제로써 적용된다.

Bishop Fox에서 개발한 Cloudfox는 퍼블릭 클라우드 공급업체와 관계없이 다양한 기능들을 제공하기 위해 호환성을 갖춘 클라우드 침투 테스트 도구이다[7]. 현시점에는 AWS, Azure에 대한 플러그인을 지원하며, AWS를 중점적으로 클라우드 자원 탐색 및 클라우드 내 악용 가능한 공격 경로를 찾아주는 플러그인을 제공한다. 침투 테스트를 수행할 수 있는 것과 별개로, 실효성을 갖춘 클라우드 환경에서의 사전 예방적 포렌식을 수행하기 위해서는 시나리오에 따라 상황에 맞게 적절한 플러그인을 조합하고 활용해야 한다. 다시 말해, 모의 해킹 침투 테스트 도구를 클라우드 사전 예방적 포렌식에 적절히 활용하기 위한 구체적 방안은 수행하는 주체가 판단해서 구현해야 한다. 본 연구에서는 실제 상용 퍼블릭 클라우드 AWS와 Azure에서 Cloudfox가 제공하는 플러그인을 개별적으로 활용하는 것에서 더 나아가, 클라우드 시나리오별 적절한 플러그인 셋을 제공해 줌으로써 효율적인 사전 예방적 포렌식 데이터 수집에 활용할 수 있는 방안을 제안한다.

2.2 클라우드 포렌식 관련 연구

Jason E James는 SaaS 환경에 대한 침투 테스트의 포렌식 증거 수집을 시도하여 클라우드 구현에서 디지털 포렌식을 수행하였다[11]. FTK Imager Lite가 AWS EC2(Elastic Compute Cloud)에서 데이터를 원격으로 수집할 수 있음을 보여줬으나, 합법적으로 법정에 증거로 제출이 어려울 수 있기에 신뢰할 수 있는 데이터를 생성하고 클라우드 포렌식 수집 문제를 해결하는 것에 대한 한계점을 언급하였다.

Philomin 외 3인은 IoT 기반의 침투 테스트 프레임워크를 제안한 연구를 수행하였다. 잠재적 디지털 증거 수집을 위해 침투 테스트 방식을 사용하면 수사관이 사이버 공격 활동을 조사하는 데 도움이 될 수 있고, 사전 예방적 포렌식 수행이 가능하다[12]. 제안하는 메커니즘을 사용하여 증거를 확인하여 보안 및 사고 대응할 수 있다는 점에서 기여점이 존재하나, 클라우드의 서비스 모델을 고려한 형태의 침투 테스트 프레임워크라고 보기 어렵다. 정리하면, 클라우드 포렌식에 관한 선행된 연구들은 CSP에서 제공하는 데이터만을 신뢰할 수밖에 없도록 의존성을 가지거나, 사용자의 정보가 충분하지 않은 경우에 대해서는 포렌식 정보 수집이 제한적이다.

Sedighi 외 1인은 Microsoft Azure 클라우드 환경에서 사고가 발생하는 것을 방지하기 위한 도구들과 기능을 사용하여 포렌식 분석을 수행할 수 있는 프로세스를 연구하였다[13]. 이는 포렌식을 통해 사고 후에 공격자를 탐지하는 것이 아닌 클라우드 환경에 침투하는 시나리오를 사전에 제거하는 것이 목적이다. 또한, 방어 메커니즘을 무력화하기 위해 공격자가 남긴 흔적은 원래 방어를 목적으로 한 도구이지만, 포렌식 분석에서 활용될 수 있다. 즉, 이러한 흔적은 공격에 대한 정보를 포함하고 있으며, 방어를 위한 도구로써만 사용되지 않을 수 있다는 것을 의미한다.

Amazon 클라우드의 경우, 유료 서비스 계정을 대상으로 사용자 활동 및 API 사용 추적이 가능한 CloudTrail[14]과 모니터링 되는 AWS 계정 스토리지의 퍼블릭 권한 설정 결과를 제공하는 Guard Duty[15]를 제공한다. CloudTrail의 경우, 각종

EC2 인스턴스, Lambda 서비스 등에 대한 자체 침투 테스트도 지원한다. 그러나, CSU 관점에서 사용자 편의성이 떨어진다는 한계가 존재하고, 허용 서비스에 나열된 8가지 서비스에 대해 사전 승인 없이 AWS 인프라에 대한 보안 평가 또는 침투 테스트 수행을 제한한다.

정리하면, 기존 퍼블릭 클라우드에 대한 포렌식 연구 및 침해 사고 대응 솔루션의 경우 특정 클라우드 서비스 공급자에서 제공하는 클라우드 인스턴스에 종속적일 뿐만 아니라, 유료 계정에 대해서만 활용이 가능하다는 한계가 존재한다.

III. 클라우드 포렌식 법 및 제도 동향

현재 국내 클라우드 포렌식 관련 법률 및 표준은 존재하지 않으며, 클라우드를 대상으로 한 포렌식의 경우 디지털 포렌식 관련한 형사소송법 제215조로 대응하고 있다. 이에 압수수색에는 영장에 기재된 압수·수색의 장소와 해당 전자정보의 서버 등 저장 장소가 다른 원격 압수·수색과 그 원격지가 국내 사법 관할권 밖인 외국에 있는 역외 압수·수색으로 분류된다. 특히, 대다수의 클라우드 서비스를 제공하는 기업들이 외국계 회사에 해당하여 역외 압수·수색 문제를 가지고 있으며, 클라우드 환경에 저장되는 데이터를 수집하거나 확인하는 방안이 명확하지 않다는 한계로 신속한 압수·수색의 어려움을 겪는다.

해외 사례 중 미국의 경우, 미국 연방 민사소송법 절차규칙(FRCP: Federal Rules of Civil Procedure) 34에 따라 클라우드 데이터를 소유하거나 제어하는 다른 당사자에게 요청할 수 있다[16]. 소송 보류 또는 보존 문서가 준수하고 유효하다고 가정하면 이 규칙을 통해 필요한 것을 정확하게 확인 또는 수집하거나 최소한 제공자에게 정보를 요청할 수 있다. 또한, 미국은 합법적인 해외 데이터 활용의 명확화를 위한 법률인 CLOUD(Clarifying Lawful Overseas Use of Data Act, CLOUD Act)법을 제정함에 따라, 미국 내에 소재하고 있는 전기통신사업자가 관리하는 데이터에 대해서는 해당 데이터가 미국 영토밖에 저장되어 있다 하더라도 저장통신법상 제출대상에 해당함을 법률적 근거로 뒷받침한다[17]. 이를 근거로 저장통신법 제2713조를 신설하여 역외적용의 명시적 근거와 데이터 제공 요구에 대한 서비스 제공자의 이의신청권 근거를 제공한다. 하지만, 수사하는 주체를 역내 전기통신사업자로 명시하고 있듯이, 수사기관이 직접 역외에 저장된 디지털 정보를 원격으로 접속하여 압수하는 방안이 필요하다는 한계점이 존재한다.

정리하면, 미국뿐만이 아니라 해외 사법당국으로부터 국내 기업의 데이터 국외 이전 요청이 증가함에 따라, 국내법도 서로 다른 국가 법률의 보호법익 차이에 따른 충돌 가능성 및 데이터 이전과 같은 상황에 대비하여 국내법이 마련되어야 한다. 또한, 클라우드 서비스에 대한 압수·수색을 위한 법률적 방안에 대한 필요성이 논의됨에 따라, 형사소송법과 대법원 판례에 부합하는 역외 압수·수색 방법에 관한 연구가 이루어져야 한다. 본 논문에서 제안하는 모의해킹 기반 사전 예방적 클라우드 침해 사고 대응 프레임워크의 경우, CSP와 CSU 상호 간 합의하에 준사법기관에 사전 예방 포렌식을 위한 침해 사고 대응이 허용되는 상황을 바탕으로 프레임워크를 설계하였다. 구체적으로, 미국의 CLOUD 법을 근거로 뒷받침하여 클라우드와 같이 데이터가 외부에 저장되어 있더라도 저장통신법상 제출대상에 해당한다는 상황을 가정한다.

IV. 모의해킹 기반 클라우드 취약점 탐지 방안 설계

본 연구에서는 상용 퍼블릭 클라우드를 대상으로 한 오픈 소스 침투 테스트 도구인 Cloudfox가 제공하는 플러그인들을 기반으로, 모의해킹 기반 사전 예방적 클라우드 침해 사고 대응 프레임워크 디자인을 탐구한다. Fig. 1.은 전체적인 모의해킹 기반 사전 예방적 클라우드 침해 사고 대응 프레임워크를 위한 구성도를 도식화한 것으로, Free Tier 계정 및 Cloudfox를 사용 가능한 CSU 영역과 Free Tier 계정을 제공하는 CSP 영역을 포함한다. 해당 예시에 도식화한 흐름도는 스토리지에 대한 사전 예방적 클라우드 침해 사고 시나리오를 나타낸 것이다. 사용자가 설정한 스토리지는 기본적으로 비공개 모드로 설정되어 있으나, 사용자 또는 관리자의 잘못으로 인하여 취약하게 설정된다면 스토리지에 공개적으로 누구나 접근할 수 있다. 또한, 국내뿐만이 아니라 해외에서도 스토리지에 접근할 수 있으며, 내부에 존재하는 텍스트 파일, 사진, 영상, 코드 등과 같은 객체에 쉽게 접속하여 정보를 탈취할 수 있다. 공격자는 잘못된 구성의 클라우드 서비스를 찾아 데이터를 유출하는 공격을 시도한다. 스토리지에 대한 접근 제어

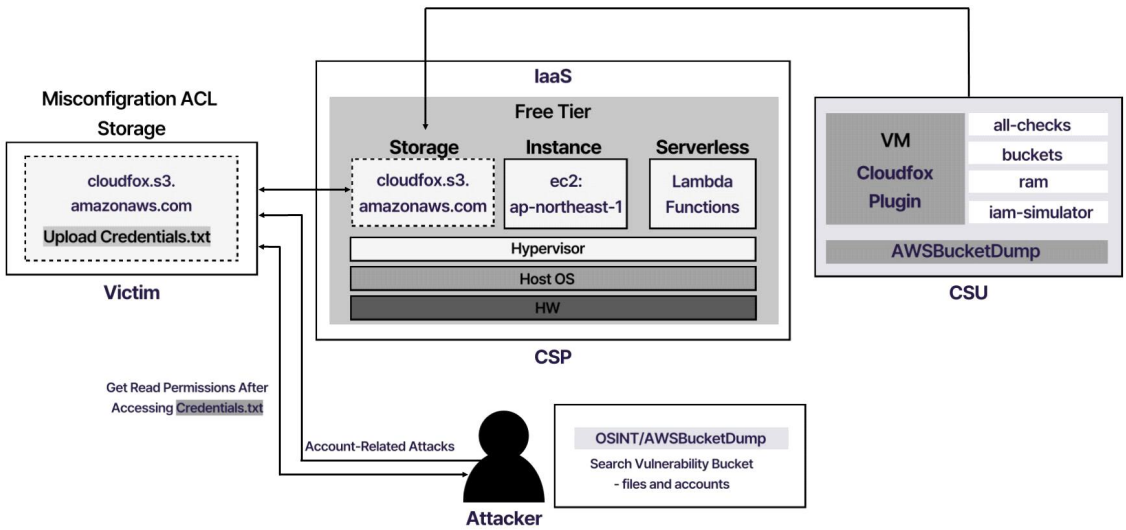

Fig. 1. Pentesting-based Proactive cloud Infringement Incident Response Framework overview

및 차단하는 대응 방안을 조치하지 않을 경우, 유출되는 데이터가 민감하거나 중요할 경우 이를 악용하는 2차 보안 사고가 발생할 수 있다.

4.1 구축 환경

Cloudfox는 기존 침투 테스트 도구를 클라우드 환경에서 실행하는 것과 달리 다양한 형태의 클라우드 서비스 모델을 대상으로 한 잠재적인 공격 경로를 찾을 수 있다. 논문 작성 시점에는 AWS과 Azure를 중점적으로 지원하여 해당 클라우드 서비스를 기준으로 분석한다. 특정 CSP의 서비스에서만 활용 가능한 기존 클라우드 침해 사고 대응 솔루션과 달리 본 모의해킹 기반 사전 예방적 클라우드 침해 사고 대응 프레임워크에서는 CSP에 agnostic하고 다양한 형태의 클라우드 서비스 모델의 Free Tier들에 대한 모의해킹을 수행함으로써 다채로운 공격 경로 파악을 통해 모니터링 기능을 개선하고자 한다.

4.2 취약점 탐지 대상

AWS의 경우 사용자 계정 생성 시 다양한 오퍼 유형을 생성할 수 있는데, 유료 서비스 계정의 경우 AWS CloudTrail을 제공한다. 이는 CSP인 Amazon에 대한 신뢰를 바탕으로 한 의존성을 갖는다. 또 하나의 오퍼 유형으로는 Free Tier 계정이 있다. 본 연구에서는 오퍼 유형 중 Free Tier 계정을 클라우드 취약점 탐지 대상인 CSU로 설정한다. AWS 사용 시 첫 단계로 사용자 계정을 생성한 후 AWS CLI에서 프로필(profile)을 구성한다. 이때, 아이디와 비밀번호와 같은 역할인 AWS Access ID와 Access Key를 입력하고, 사용할 리전(region) 등을 설정하여 Free Tier 계정을 생성할 수 있다.

AWS, Azure, GCP와 같은 퍼블릭 클라우드 서비스에서 가상머신 및 서버, 스토리지, 함수 기능을 서비스하는 자원을 대상으로 클라우드 포렌식 정보를 수집한다. 먼저, 가상머신 및 서버의 역할을 수행하는 인스턴스는 AWS EC2, Azure Virtual Machine, GCP Compute Engine이 해당된다. 이 중 AWS의 대표 서비스인 EC2 인스턴스는 사용자가 가상 컴퓨팅 환경에서 가상화된 하드웨어 자원을 원하는 만큼 확장이 가능하다. 사용자는 원격으로 다양한 가상 서버를 구축하고 스토리지를 관리하는 등 컴퓨팅 자원에 접근 및 사용할 수 있다. 클라우드 포렌식 증거로써 모든 EC2 인스턴스 메타데이터가 해당된다. 영구적인 블록 스토리지 볼륨인 EBS (Elastic Block Store)는 EC2 인스턴스와 조합하여 사용되는데, EBS 디스크 스냅샷도 해당된다.

스토리지는 AWS S3, Azure Blob Storage, GCP Cloud Storage가 해당된다. 객체 스토리지는 데이터를 객체 단위로 관리하는 형식으로 S3는 객체 스토리지 서비스이며, 데이터 가용성과 높은 확장성의 특징을 가진다. S3 서비스에 저장된 데이터

를 웹 브라우저를 통해 다운로드 시 웹 브라우저 다운로더에 종속적으로 동작하기 때문에 웹 브라우저별 다운로더의 로그 기록 확인을 통해 용의자가 어떤 데이터를 다운로드했는지 확인 가능하다[18].

서버리스(serverless) 컴퓨팅 서비스는 AWS Lambda, Azure Functions, GCP Cloud functions에 해당된다. Lambda는 데이터나 요청에 대한 실시간 처리나 백엔드 처리를 자동으로 실행하는 구조이다. 이와 같은 처리를 위해 전용 서버를 구축하거나 따로 관리하지 않아도 필요한 이벤트가 자동으로 실행되어 대표적인 서버리스 컴퓨팅 플랫폼으로 활용된다. Lambda 함수라는 형식의 함수를 통해 API 호출이 가능하며, 자바, C#, 파이썬, 루비, Node.js, Go 프로그래밍 언어에 대한 런타임을 제공한다.

4.3 클라우드 취약점 동향 및 현황 분석

IaaS 기반 클라우드 서비스 모델에서의 대표적 보안 위협 사례로는 사용자 계정 Access Key, AWS 버킷과 Azure Blob와 같은 스토리지, 클라우드 가상머신 서비스인 EC2에 대한 데이터 유출 문제가 있다. 2018 McAfee Cloud 위협 보고서에 따르면, 클라우드에 중요 데이터를 공유하는 파일의 양이 53% 증가하였고, AWS S3 버킷의 5.5%가 World 읽기 권한임이 공개되었다[19]. 실제 발생한 정보 유출 사례를 살펴보면 AWS의 경우 S3와 Lambda, Azure는 Blob Storage와 AD 등에서의 잘못된 구성이 원인으로 밝혀졌으며, Trend Micro에 의하면 Azure Storage 환경에서 Azure Storage 계정 서비스의 잘못된 구성 비율은 60.75%이다[20]. 이는 AWS S3 버킷과 Azure Blob Storage에 대한 데이터 유출에 대한 적절한 보안 조치가 필요함을 나타낸다. 이를 근거로, AWS 클라우드 서비스 중 보안 위협에 대하여 3가지 구체적 사례를 바탕으로 하여 모의해킹 기반 사전 예방적 클라우드 침해 사고 대응 프레임워크가 필요한 시나리오 및 대상을 구체화한다.

첫 번째 사례는 계정, 액세스 목록 및 스토리지의 잘못된 구성이다. 클라우드 이전의 최소 권한의 원칙(Cloud Least Privilege)은 중요하나 실제로 적용되지 않는 경우가 빈번하다. 구체적으로, 필요한 사용량의 데이터 이상으로 액세스할 수 있도록 계정 또는 액세스 목록이 구성되거나 액세스 가능한 계정의 수보다 더 많은 계정에서 사용될 수 있도록 스토리지가 구성되는 경우가 존재한다.

두 번째는 CSU의 Access Key와 같은 자격 증명을 다루는 IAM(Identity and Access Management)에 대한 권한 상승 및 데이터 유출로 이어지는 취약성이다. IAM은 인증 및 사용 권한을 부여받은 사람을 제어하여 클라우드 리소스에 대한 액세스를 안전하게 관리한다. 공격자는 클라우드 서비스를 스캔하고 자격 증명이 취약한 서비스를 식별한다. 또한, 공격자가 취약한 암호가 있는 계정을 탈취하면 계정에서 액세스할 수 있는 항목을 찾기 위해 조사할 가능성이 높다. 이로 인해 계정이 액세스할 수 있는 정보가 손상될 수 있어 최소 권한의 원칙을 지키지 않을 경우 더 심각한 손상이 발생할 수 있다.

마지막은 클라우드 계정에 대한 자격 증명이 공개 저장소(repository)에 게시되는 경우이다. 스토리지 서비스로 많이 사용되는 AWS S3, Azure Blob Storage는 기본적으로 비공개 모드이나, 관리자의 부주의로 인해 잘못된 구성으로 인한 취약한 설정이 될 수 있다. 이로 인해, 접근 권한이 없더라도 객체(object)에 쉽게 접근하여 내부 파일 정보를 탈취할 수 있다. 취약하게 설정된 S3 버킷들은 'buckets.grayhatwarfare.com'와 같은 OSINT(Open Source INTelligent)를 통해서 수집이 가능하다. 또한, AWS 환경에서는 AWSBucketDump처럼 S3 버킷에서 잘못된 구성을 스캔하고 데이터를 덤프하는 오픈 소스 도구인 S3Scanner[21]가 있고, Azure 환경에서는 BlobHunter[9]와 같이 스토리지를 스캔하는 등의 다양한 도구를 활용한다면 더 많은 잘못된 구성으로 인한 보안 설정이 취약한 샘플을 수집할 수 있다. 시장조사기관 컴패리테크(Comparitec)에 의하면 허니팟(honey pot) 목적으로 AWS 자격 증명 파일이 짧은 시간에 업로드했음에도 불구하고 수많은 사용 시도 흔적이 발견되었다[22]. 이는 깃허브(github)에 관리자의 실수로 업로드된 코드를 빠르게 삭제 조치하더라도 공격자가 삭제하기 이전에 탈취할 가능성이 존재할 정도로 중요하게 관리되어야 할 대상임을 의미한다. 클라우드 계정에 대한 자격 증명이 저장되는 스토리지 서비스에 해당되는 AWS S3 버킷, Azure Blob 스토리지 모두 비슷한 취약점을 가지고 있어 공통적으로 공격을 탐지하고 대응할 수 있는 방안이 필요하다.

V. 시나리오에 따른 모의해킹 기반 사전 예방적 클라우드 침해 사고 대응 프레임워크 도출

본 장에서는 시나리오별로 활용할 수 있는 Cloudfox 플러그인의 항목화를 수행하고, 모의해킹 기반 사전 예방적 클라우드 침해 사고 대응 프레임워크 시나리오를 위한 사용성이 높은 AWS 클라우드 자원 동향을 살펴본다. 또한, 스토리지와 인스턴스에 대한 사전 예방적 클라우드 침해 사고 시나리오의 분석 결과를 토대로 CSU 및 CSP 관점에서 본 제안하는 프레임워크의 활용 가능성을 고찰한다.

Table 1.은 AWS와 Azure의 클라우드 자원, 공격 경로, 권한을 항목화하여 관련 특징을 나타내는 플러그인과 매핑하여 나타낸 표이다. AWS를 중점적으로 지원하며 그중 Azure를 지원하는 플러그인에 대해서 애스터리스크(*)로 표기하였다. 기본적으로 Cloudfox의 플러그인은 사용자가 실행하는 권한과는 관계없이 생성, 삭제 또는 수정되지 않는다. 수행 결과는 csv, loot, table 디렉터리에 기록되며, csv 파일 형식을 제공하는 csv 디렉터리를 제외한 디렉터리 내 결과는 텍스트 파일 형식에 맞게 나타낸다. 먼저 Cloudfox는 이름, 공인/사설 IP 및 인스턴스 프로필과 같은 모든 리전의 EC2 인스턴스에 대한 유용한 정보를 열거해 주는 instance 명령을 제공한다. 이러한 서비스 열거를 위해 nmap 및 기타 도구에 제공할 수 있는 loot 파일을 생성한다. 또한, 교차 계정 접근(Cross-Accounts Access) 공격의 경우 교차 계정 접근을 통해 역할(Role)을 사용하면 동일 AWS 계정 내에서는 제한적인 권한으로 안전하게 AWS를 운영하거나 사용할 수 있고, 다른 Account ID를 통해 다른 사용자에게 권한을 위임할 수도 있다.

Fig. 2.은 Cloudfox를 활용할 때 Free Tier에 각 AWS 클라우드 서비스 스토리지, 인스턴스, 서버리스가 생성된 환경에서의 CSU와 CSP 관점에서의

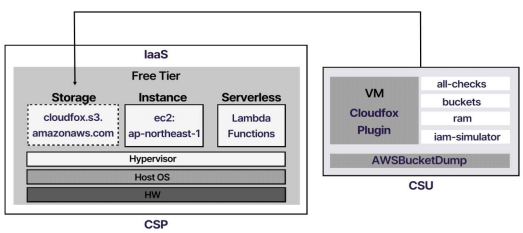

Fig. 2. Components of CSP and CSU

Table 1. AWS/Azure plugin provided by Cloudfox

Category	Plugin	Description
Resource	*inventory	Size of the account and preferred regions
	*instances	Public/private IPs, instance profiles, and other information about EC2 instance
	lambda	Lists the lambda functions in the account, admin roles
	buckets /*storage	Lists the buckets in the account and commands for inspecting them further
	route53	Enumerate all records from all route53 managed zones
Attack Path	ram	Useful for cross-account attack paths
	outbound-assumed-roles	Way to find outbound attack paths that lead into other accounts
authorize	secret	List secrets from SecretsManager and SSM
	accesskey	Lists active access keys for all users
	env-vars	If a sensitive secret is found, use cloudfoxiam-simulator AND pmapper to determine who has access
	iam-simulator	Uses the IAM policy simulator
	permission	Enumerates IAM permissions associated with all users and roles
	principal	IAM user and role
	role-trusts	Enumerates IAM role trust policies

사전 예방적 클라우드 침해 사고 시나리오를 도식화한 것이다. CSP는 IaaS 서비스를 제공하는 AWS에 해당하며, 하드웨어, 호스트 OS(Operating System), 하이퍼바이저의 상위 계층에 Free Tier Cluster 영역을 관리한다. CSU는 가상 머신으로 Free Tier에게 서버리스, 스토리지와 같은 서비스를 제공하는 Free Tier Cluster 영역에 접근하게 된다. 이후, 유틸리티 프로그램 형태로 Free Tier Cluster에서 Cloudfox에서 제공하는 플러그인 셋을 수행한다.

5.1 스토리지 사전 예방적 클라우드 침해 사고 시나리오

클라우드 스토리지에 대한 사전 예방적 클라우드 침해 사고 시나리오 과정을 통해, 잘못된 구성으로 인한 AWS S3 버킷, Azure Blob Storage에서 정보 유출과 같은 사고가 발생하거나 클라우드 기반 포렌식 조사를 계획하는 경우에 효율적인 Cloudfox 플러그인 셋을 제안함으로써 도움이 될 수 있다.

Fig. 3.은 CSU가 잘못된 구성의 스토리지를 생성한 후 사전 예방적 클라우드 침해 사고 시나리오를 나타낸 아키텍처이다. Azure 스토리지인 Blob Storage와 컨테이너에 대한 퍼블릭 권한을 부여하여 잘못된 구성을 수행할 수 있다. 이때, 잘못된 구성이란 Free Tier 영역에서 생성한 스토리지를 생성하고, 이에 적용되는 Bucket ACL(Access Control Lists), 개별 객체에 적용되는 객체 ACL, S3 버킷 IAM 정책에 대하여 모두 Public Access를 허용한 것을 의미한다.

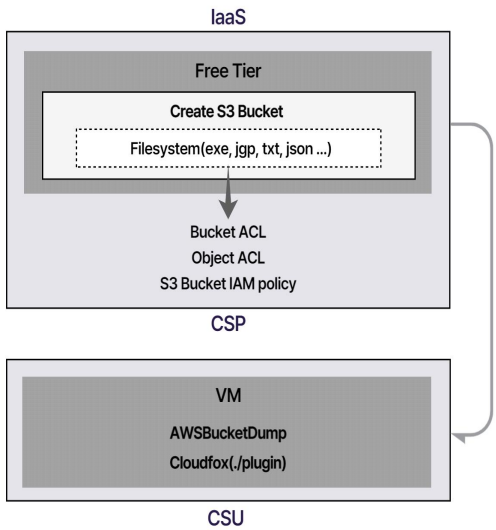

Fig. 3. Misconfiguration Storage Cloud Forensics Scenario Architecture

예를 들어, Victim이 잘못 구성된 스토리지에 계정에 대한 정보가 포함된 credentials.txt 파일을 업로드한 상황에서 모의해킹을 수행한다고 가정한다. 이때, CSU는 잘못된 구성으로 인하여 스토리지에 공개된 경로로 접근 가능한지 확인을 위해 스토리지 중 AWS S3 버킷의 경우 AWSBucketDump을 활용한다. Fig. 4.은 CSU가 AWSBucketDump를 사용하여 앞선 잘못된 구성의 S3 버킷임을 입증하는 과정을 수행한 결과를 나타낸다.

이후, 해당 공격 시나리오에서 공격자는 4.3절에서 언급한 OSINT를 활용하여 공개된 스토리지 중 잘못된 구성의 스토리지를 탐색하고 내부 파일을 확인할 수 있다. AWSBucketDump로 해당 리전의 스토리지에 업로드된 credentials.txt 파일처럼, 리전 내부 파일의 개수 및 내용에 대해서 읽을 수 있는 권한을 가지게 된다. 특히, credentials.txt는 CSU의 계정 정보를 저장하고 있는데, 암호화되지 않은 평문을 그대로 출력한다. 해당 스토리지에 민감한 계정 정보를 저장하고 있는 credentials.txt을 발견하고, 공격자가 Free Tier 계정을 탈취하였다고 가정한다. 공격자는 해당 계정 내 다른 클라우드 서비스 자원에 대해 접근하여 이후 스토리지 내부에 존재하게 되는 객체에 해당하는 jpg, exe, pdf, json 등의 다양한 파일들을 권한이 없더라도 열람하거나 편집할 수 있는 권한으로 접근할 수 있다.

Azure 스토리지에 대한 사전 예방적 클라우드 침해 사고 시나리오는 앞선 S3 버킷 스토리지와 동일한 시나리오로 Victim이 잘못 구성된 스토리지에 Azure 계정 정보가 포함된 credentials.txt 파일을 업로드한 상황에서 모의해킹을 수행한다고 가정한다. CSU가 스토리지 계정에서 스토리지와 컨테이너에 공용 액세스 수준을 설정할 때 퍼블릭 권한으로 부여하여 잘못된 구성을 한다. Fig. 5.은 CSU가 Cloudfox storage 플러그인 수행 후 잘못된 구성

```
hynn@ubuntu:~/cloudfox_pj/env/AWSBucketDump$ cd cloudfox.s3.amazonaws.com/
hynn@ubuntu:~/cloudfox_pj/env/AWSBucketDump/cloudfox.s3.amazonaws.com$ ls
credentials.txt
hynn@ubuntu:~/cloudfox_pj/env/AWSBucketDump/cloudfox.s3.amazonaws.com$ cat credentials.txt
admin: cloudfoxproject1
password: cloudfox123456789hynn@ubuntu:~/cloudfox_pj/env/AWSBucketDump/cloudfox.s3.amazonaw
```

Fig. 4. Internal output of credentials.txt file present on cloudfox.s3.amazons.com

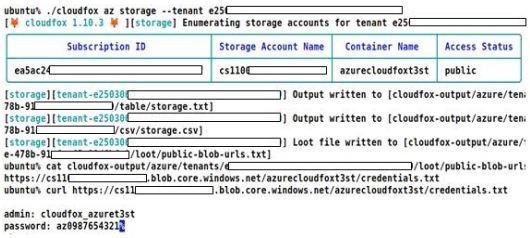

Fig. 5. Internal output of credentials.txt file present on azurecloudfoxt3st Container

의 스토리지임을 입증하는 과정을 수행한 결과이다.

텍스트, 파일, 이미지 등과 같은 바이너리 데이터를 저장할 수 있는 블록 blob에 동일한 방식으로 credentials.txt 파일을 업로드한다. 객체에 권한을 할당하는 절차에서는 Storage Blob 데이터 Contributor, Reader 역할을 할당하여 해당 파일을 열람할 수 있다. 해당 스토리지가 취약함을 입증하기 위해서 공개된 Azure 스토리지를 스캔할 수 있는 Blob Hunter 도구를 사용하여 csv 파일로 저장된 해당 스토리지에 대한 정보를 확인할 수 있다. 마지막 절차로 Cloudfox의 storage 플러그인을 실행한 후 스토리지에 저장된 credentials.txt 파일에 대해 접근할 수 있고, 파일 내부의 내용을 열람할 수 있음을 확인하였다.

이에 대한 모의해킹 기반 사전 예방적 클라우드 침해 사고 대응 프레임워크를 위해, CSU 영역의 VM에서 Table. 1.에 정리된 리스트 중 buckets, ram, iam-simulator를 활용한다. 해당 공격 시나리오에서 buckets을 사용하여 해당 계정의 스토리지들을 나열하고, ram은 교차 계정 공격 경로를 탐지하는 기능을 수행한다. iam-simulator의 경우, 특정 사용자 혹은 권한을 가진 IAM 주체가 어느 자원에 대하여 작업 권한을 수행할 수 있는지를 확인하는 모의해킹을 진행한다. 이를 통해, 스토리지를 공개 액세스로 전환한 IAM 자격 증명을 파악할 수 있고, IAM 사용자에 대한 MFA(Multi-Factor Authentication)를 적용하는 데 사용할 수 있다.

5.2 인스턴스 및 서버리스 사전 예방적 클라우드 침해 사고 시나리오

앞선 해당 시나리오에서 공격 경로 검증 외에도 자원을 확인하고자 인스턴스 및 서버리스 사전 예방적 클라우드 침해 사고 시나리오를 진행하였다. CSU가 AWS EC2 인스턴스, Azure Virtual Machine와 서버리스 컴퓨팅 서비스인 Lambda function을 생성하고 활성화 상태로 설정한다. Free Tier 영역에 접근하여 Cloudfox에서 제공하는 구성(configuration)에 대한 프로파일링 수행 플러그인으로 inventory를 통해, Free Tier가 생성한 인스턴스, Lambda 등에 대하여 실시간적으로 업데이트된 내용을 확인할 수 있다. 자원 타입(Resource Type)과 프로필에서 설정한 리전에 존재하는 리소스(resource)의 개수를 테이블 형태로 저장한다. 인스턴스와 Lambda Function의 생성된 개수를 나타내어 클라우드 서비스 자원의 현황에 대해 파악이 가능하다. 다른 계정으로 연결될 수 있는 아웃바운드(outbound) 공격 경로를 찾을 수 있는 outbound-assumed-roles와 AWS 계정의 모든 사용자에 대한 모든 활성 액세스 키 ID를 매핑하는 accesskey를 수행한다. Free Tier 계정 내 CSU가 사용하는 자원을 파악할 수 있고, Access Key에 접근하고 열람할 수 있다면 해당 자원에 대하여 권한 상승 공격을 시도할 가능성이 존재한다.

5.3 논의 및 고찰

본 절에서는 앞서 논의한 사전 예방적 클라우드 침해 사고 시나리오에 대하여 CSU와 CSP 관점에서 모의해킹 기반 사전 예방적 클라우드 침해 사고 대응 프레임워크를 통해 얻을 수 있는 이점에 대해 논의한다.

5.3.1 CSU 관점

CSU는 CSP에서 수행한 클라우드 로그에서 수행된 분석이 원본 데이터가 맞는지, 분석에 존재해야 하는 기록된 정보가 모두 포함되어 있는지를 침투 테스트를 통해 확인할 수 있다. 또한, 제안한 모의 해킹 기반 프레임워크는 CloudTrail과 같은 서비스와 달리, 하나의 상용 퍼블릭 클라우드에 의존성을 갖지 않아 멀티 클라우드 시나리오에서도 활용 가능하다는 강점을 갖는다. 마지막으로, 실제 유료 계정 구매 전 Free Tier 계정에 대한 모의 해킹을 수행한 뒤 결과를 비교 및 분석하여 이용할 상용 솔루션을 선택하는데 유용한 정보로써 활용될 수 있다.

5.3.2 CSP 관점

악의적인 목적을 가진 CSU가 의도적으로 Free Tier로 공격을 수행했을 때 계정을 삭제한 이후에는 포렌식을 위한 데이터 수집하고 증거를 찾기 쉽지 않다. 또한, 클라우드 환경에서 수많은 인스턴스와 계정에 걸쳐 모든 관련 증거를 수동으로 수집하는 것은 어렵고 시간이 소요되는 작업이다. 하지만, Cloudfox 플러그인을 통하여 클라우드 포렌식 환경의 기초적인 작업을 구현하면 자동화된 모니터링을 사용하여 포렌식 데이터 수집 기능을 반복하고 보안 이벤트가 발생할 때 대응할 수 있다. 특히, 모니터링 시 이상 탐지를 위해 Free Tier 오퍼들에 대해 모두 실시간으로 API Call 등의 행위를 계속 탐지하는 경우에는 오버헤드가 크게 적용될 수 있다. Cloudfox 플러그인의 동작에서 특징적인 행위들만 지정(pinpointing)해서 탐지할 경우 모니터링 오버헤드를 줄이고, 특정한 포렌식 사고에 대한 증거 수집 절차를 정형화하여 제시할 수 있을 것으로 기대한다.

VI. 결 론

본 논문에서는 클라우드 상에서 데이터 유출의 원인을 파악하는 것이 어렵고, Free Tier 계정을 범죄에 악용한 뒤 삭제하거나 데이터를 범죄에 악용하는 등의 악성 행위로 인한 클라우드 포렌식 데이터 수집의 한계점을 확인하였다. Free Tier 계정에서 잠재적으로 악의적인 활동을 발견하기 위해서 클라우드 침투 테스트 도구인 Cloudfox를 활용한 모의해킹 기반 사전 예방적 클라우드 침해 사고 대응 프레임워크를 제안하고, Free Tier 계정 CSU와 CSP 관점에 대한 분석을 수행하였다. Cloudfox가 지원하는 IaaS 유형의 AWS, Azure를 대상으로 분석한 결과, CSU와 CSP 관점에서 클라우드 서비스 내 공격 경로 모니터링 기능의 구현 가능성을 확인하였다. 또한, CSP 관점에서 클라우드 포렌식 데이터를 적절하게 수집할 수 있다면 이를 활용하여 효과적인 프레임워크를 고안할 수 있다. 또한, CSU 관점에서는 제안한 모의해킹 기반 사전 예방적 클라우드 침해 사고 대응 프레임워크를 통해 클라우드에서 발생하는 보안 사고에 대해 사전 예방 및 신속한 사후 대처를 기대할 수 있다. 향후 포렌식 조사관이 범죄에 사용될 수 있는 포렌식 클라우드 기반의 데이터를 획득하고, 추가적으로 신뢰를 입증하는데 취할 수 있는 조치로써 활용될 수 있다.

본 연구에서는 Cloudfox 플러그인을 사용하여 실제 공격 경로를 나타내고, 제안하는 프레임워크 구현에 대해서는 추가적인 탐구가 필요하다. Cloudfox를 활용함에 따라 현재 Cloudfox의 경우 AWS, Azure에 대한 지원만을 제공하기 때문에 추가적인 CSP에 대한 활용이 제한된다. 또한, Cloudfox 수행 결과 파일의 무결성에 대해서 추가적인 분석이 필요할 것으로 보인다. 향후 AWS, Azure 외에도 다양한 클라우드 서비스에서 적용 가능한 일반화된 모의해킹 기반 사전 예방적 클라우드 침해 사고 대응 프레임워크로 확장하고자 한다. CSP 관점에서 Cloudfox를 사용할 때의 모니터링 성능 및 포렌식 사건 대응을 위한 플러그인의 자동화된 프레임워크를 구현하는 연구를 진행할 예정이다.

References

[1] Sarah Park, Beomseok Kim, Sungmin Jo, Korea Cloud Opportunity Forecast by Industry, 2021 - 2025, May. 2022.

[2] eNsecure, “Cloud Transformation and Security Response,” PASCON 2022, 2022.

[3] S. Zawoad, A. K. Dutta and R. Hasan, “Towards building forensics enabled cloud through secure logging-as-a- service,” IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 2, pp. 148-162, Apr. 2016.

[4] Pichan, A. and Lazarescu, M. and Soh, S.T., “Towards a practical cloud forensics logging framework,” Journal of Information Security and Applications, vol. 42, pp. 18-28, 2018.

[5] C. P. Grobler, C. P. Louwrens and S. H. von Solms, “A multi-component view of digital forensics,” 2010 International Conference on Availability, Reliability and Security, pp. 647-652, Mar. 2010.

[6] Soltan Abed Alharbi, Jens H. Weber-Jahnke, Issa Traore, “The

proactive and reactive digital forensics investigation process: A systematic literature review," International Journal of Security and its Applications, vol.5, No.4, pp. 59-72, Aug. 2011.
〔7〕 Github, "Cloudfox" https://github.com/BishopFox/cloudfox, Sep. 2022.
〔8〕 Github, "AWSBucketDump" https://github.com/jordanpotti/AWSBucketDump, Jun. 2017.
〔9〕 Github, "Blob Hunter" https://github.com/cyberark/BlobHunter, Jan. 2021.
〔10〕 A. Sedighi and D. Jacobson, "Forensic analysis of cloud virtual environments," 2019 IEEE International Conference on Computational Science and Engineering and IEEE International Conference on Embedded and Ubiquitous Computing, pp. 323-329, Dec. 2019.
〔11〕 Jason E James, "An exploration in forensic evidence in a cloud computing environment," International Association for Computer Information Systems, vol. 22, pp. 250-259, 2021.
〔12〕 Sebastien Philomin, Avinash Singh, Adeyemi Ikuesan, H.s Venter, "Digital forensic readiness framework for smart homes," International Conference on Cyber Warfare and Security. Academic Conferences International Limited, pp. 627-XVIII, Mar. 2020.
〔13〕 Suleman Khan, Abdullah Gani, Ainuddin Wahid Abdul Wahab, Mustapha Aminu Bagiwa, Muhammad Shiraz, Samee U. Khan, Rajkumar Buyya, Albert Y. Zomaya, "Cloud log forensics: foundations, state of the art, and future directions," ACM Computing Surveys, vol. 49, pp. 1-42, Mar. 2017.
〔14〕 AWS, Amazon CloudTrail, http://awsdocs.s3.amazonaws.com/awscloudtrail/latest/awscloudtrail-ug.pdf, Nov. 2022.
〔15〕 AWS, Amazon GuardDuty, https://docs.aws.amazon.com/pdfs/guardduty/latest/ug/guardduty-ug.pdf, Nov. 2017.
〔16〕 Ivan Orton, J.D., Aaron Alva, Barbara Endicott-Popovsky, "Legal process and requirements for cloud forensic investigations," Cybercrime and Cloud Forensics: Applications for Investigation Processes. IGI Global, pp. 186-229, Jan. 2013.
〔17〕 Kwon Yang-sub, "Major issues and suggestions of investigation procedures for extra-territorial search and seizure of digital information," Journal of Law research, 37(1), pp. 43-64, Mar. 2021.
〔18〕 I.-H. Jeong, J.-H. Oh, J.-H. Park, and S.-J. Lee, "Digital forensic methodology of iaas cloud computing service," Journal of the Korea Institute of Information Security and Cryptology, 21(6), pp. 55 - 65, Dec. 2011.
〔19〕 McAfee, "Cloud Adoption and Risk Report,", 2019.
〔20〕 Trendmicro, "Azure misconfiguration" The Most Common Cloud Misconfigurations That Could Lead to Security Breaches, https://www.trendmicro.com/vinfo/hk-en/security/news/virtualization-and-cloud/the-most-common-cloud-misconfigurations-that-could-lead-to-security-breaches (Accessed on October 25 2022).

[21] Github, “S3Scanner” https://github.com/sa7mon/S3Scanner, Jun. 2017.
[22] Comparitech, “aws bucket credentials” It takes hackers 1 minute to find and abuse credentials exposed on GitHub, https://www.comparitech.com/blog/information-security/github-honeypot/ (Accessed on October 25 2022).

〈저자소개〉

노 현 (Hyeon No) 학생회원
2022년 8월: 성신여자대학교 융합보안공학과 학사
2022년 9월~현재: 성신여자대학교 미래융합기술공학과 석사과정
〈관심분야〉 정보보호, 클라우드 컴퓨팅, 이동통신, 신뢰 실행 환경

옥 지 원 (Ji-won Ock) 학생회원
2022년 8월: 성신여자대학교 융합보안공학과 학사
2022년 9월~현재: 성신여자대학교 미래융합기술공학과 석사과정
〈관심분야〉 정보보호, 인공지능, 통신공학, 클라우드

김 성 민 (Seong-min Kim) 종신회원
2012년 2월: 한국과학기술원 전기 및 전자공학과 졸업
2014년 2월: 한국과학기술원 전기 및 전자공학과 석사
2019년 2월: 한국과학기술원 정보보호대학원 박사
2019년 9월~2020년 8월: 삼성전자 삼성리서치 Staff Engineer
2020년 9월~현재: 성신여자대학교 융합보안공학과 조교수
〈관심분야〉 신뢰 실행 환경, 클라우드 컴퓨팅, 시스템 보안