情 報 保 護 學 會 誌
第22卷 第7號, 2012. 11

클라우드 컴퓨팅 환경에서의 디지털 포렌식 동향 및 전망

정 현 지*, 이 상 진**

요 약

클라우드 컴퓨팅은 네트워크, 스토리지, 서버, 응용프로그램 등과 같은 컴퓨팅 자원에 언제든지 편리하게 접근할 수 있는 새로운 컴퓨팅 모델이다. 클라우드 컴퓨팅은 기존의 컴퓨팅 환경과 다르게 다양한 단말 기기를 통해 접속할 수 있고, 사용자의 데이터를 로컬이 아닌 원격지에 저장하며, 작업 상태를 실시간으로 업데이트한다는 특징이 있다. 클라우드 컴퓨팅 환경에서 사용자의 데이터가 원격지에 존재하고, 서비스 제공자에 의해 관리되기 때문에 데이터 보안의 관점에서 위협 요소가 있을 수 있다. 또한 범죄와 관련된 데이터가 클라우드 시스템에 저장되어 있을 수 있다. 이를 조사하기 위해서 클라우드 컴퓨팅 환경에 적합한 디지털 포렌식 조사 절차와 방법이 필요하다.

본 논문에서는 디지털 포렌식 관점에서의 클라우드 컴퓨팅에 대해 설명한다. 또한 클라우드 포렌식 기술 동향과 클라우드 컴퓨팅 환경에서 발생하는 법적 이슈 동향을 살펴본다. 이를 바탕으로 향후 클라우드 컴퓨팅 포렌식 연구 방향에 대해서 제시한다.

Ⅰ. 서 론

IT 환경이 기존의 컴퓨팅 환경에서 클라우드 컴퓨팅 환경으로 점차 변하고 있다. 기존의 컴퓨팅 환경에서는 개인이 자신의 저장매체와 디지털 데이터를 관리하였다. 클라우드 컴퓨팅 환경에서는 서비스 제공자가 고객들에게 스토리지와 같은 IT 자원을 제공하고, 고객들은 적절한 비용을 지불하고 이를 이용한다. 클라우드 컴퓨팅은 조직의 업무 효율을 개선하고, 낮은 IT 인프라 비용 제공, 소프트웨어의 구매 비용절감, 유지보수 문제 해결, 사용자의 편익 증대 등과 같은 이점을 가진다. 반면에, 개인의 데이터가 제 3자인 서비스 제공자에 의해 관리된다는 점은 보안의 측면에서 위협 요소가 될 가능성이 있다. 이러한 보안 위협으로 인해 보안 사고가 발생한다면, 관련 사고를 조사하기 위해 디지털 포렌식 조사를 수행해야 한다.

디지털 포렌식 조사를 통해 디지털 기기에서 디지털 증거를 수집 및 분석하고, 사실 관계를 규명할 수 있다[1]. 현재까지 기존의 컴퓨팅 환경에서 디지털 포렌식은 디스크 또는 네트워크를 중심으로 한 연구가 이루어졌다. 기존의 컴퓨팅 환경은 클라우드 컴퓨팅 환경과 다르기 때문에 클라우드 컴퓨팅 환경에서 조사를 하기 위해 기존의 디지털 포렌식 조사 절차와 방법을 그대로 적용할 수 없다. 클라우드 컴퓨팅 환경을 구축하는 기업, 기관 등이 늘어남에 따라 클라우드 컴퓨팅 환경에 적합한 디지털 포렌식 조사 절차 및 방법이 필요한 시점이다.

본 논문에서는 클라우드 컴퓨팅 환경에서의 디지털 포렌식 관련 연구 및 이슈 동향을 살펴보고, 향후 연구 방향을 제시한다. 2절에서는 클라우드 컴퓨팅이 무엇인지 설명하고, 디지털 포렌식 관점에서의 클라우드 컴퓨팅을 설명한다. 3절에서는 클라우드 포렌식 관련 기술 연구 동향에 대해 설명하고, 4절에서는 클라우드 포렌식과 관련된 법적 이슈에 대해 언급한다. 5절에서는 기존 연구를 바탕으로 향후 연구 방향을 제시한다. 마지막으로 6절에서는 결론을 내린다.

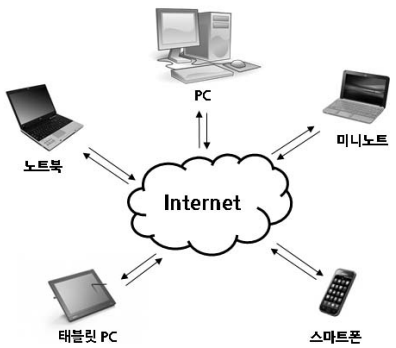
이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단-공공복지안전사업의 지원을 받아 수행된 연구임 (2012M3A2A1051106)

* 고려대학교 정보보호연구원 (foryou7187@korea.ac.kr)
** 고려대학교 정보보호연구원, 교신저자 (sangjin@korea.ac.kr)

Ⅱ. 클라우드 컴퓨팅과 디지털 포렌식

2.1. 클라우드 컴퓨팅

클라우드 컴퓨팅은 인터넷을 이용하여 가상의 IT 자원을 제공한다. 또한 [그림 1]과 같이 다양한 단말 기기를 통해 접근할 수 있는 환경을 제공하기 때문에 사용자는 언제 어디서나 편리하게 클라우드 서비스를 이용할 수 있다[2-5].



〔그림 1〕 클라우드 컴퓨팅

클라우드 컴퓨팅은 서비스의 유형에 따라 IaaS, PaaS, 그리고 SaaS로 나뉜다[6].

IaaS(Infrastructure as a Service)는 서버, 스토리지, 네트워크와 같은 인프라스트럭처를 제공하는 서비스이다[6]. 대표적인 예는 AWS(Amazon Web Service)와 Rackspace가 있다. PaaS(Platform as a Service)는 표준화된 플랫폼을 제공하는 서비스이다[6]. 대표적인 예는 Google AppEngine와 Microsoft Asure가 있다. 그리고 SaaS(Software as a Service)는 웹브라우저를 통해 소프트웨어를 제공하는 서비스이다[7]. 대표적인 예는 Gmail와 Salesforce.com이 있다.

클라우드 컴퓨팅은 배치 모델에 따라 사설 클라우드와 공공 클라우드로 나뉜다. 사설 클라우드는 특정 개인이나 기업 고객만을 위한 클라우드 서비스이다[8]. 기업이 자체적으로 사설 클라우드를 구축하기 때문에 전체 인프라에 대해 완전하게 통제를 할 수 있고, 데이터 보안을 유지할 수 있다. 공공 클라우드는 불특정 다수의 개인이나 기업을 위한 클라우드 서비스이다[8]. 공공 클라우드는 모든 서비스를 외부에서 받을 수 있기 때문에 관리 및 유지 보수비용이 절감된다는 장점이 있다. 하지만 데이터가 외부에 존재하기 때문에 인프라에 대한 통제권을 가질 수 없고, 서비스 중단이 발생하면 개인 또는 기업의 업무가 마비될 수 있다.

2.2. 클라우드 컴퓨팅과 디지털 포렌식

클라우드 컴퓨팅은 범죄의 객체, 주체가 될 수 있고, 범죄의 수단으로 이용될 수 있다[9]. 해커가 CSP(Cloud Service Provider)를 대상으로 DDOS 공격을 행한 경우, 클라우드 컴퓨팅 서비스는 범죄의 객체가 된다. 만약 허가받지 않은 사람이 타인의 클라우드에 존재하는 데이터를 변경 또는 삭제한 다면, 클라우드 컴퓨팅 서비스는 범죄의 주체가 된다. 그리고 범죄와 관련된 증거가 클라우드 상에 존재하는 경우, 클라우드 컴퓨팅 서비스는 범죄의 수단이 된다. 예를 들면, 클라우드 컴퓨팅 서비스는 기술 유출, 저작권 파일 공유, 아동 음란물 공유 등 다양한 범죄에 이용될 수 있다[10]. 이러한 클라우드 범죄가 발생하였을 때, 클라우드 컴퓨팅 서비스를 조사하기 위한 절차를 정립하고, 조사 방법을 연구할 필요가 있다.

클라우드 컴퓨팅은 기존의 컴퓨팅 환경과 다른 특징들을 가지기 때문에 기존 컴퓨팅 환경에서 적용하던 디지털 포렌식 절차와 방법을 그대로 적용할 수 없다. 클라우드 컴퓨팅 환경의 특징에 적합한 새로운 형태의 디지털 포렌식 조사 절차 및 방법이 필요하다.

서비스 유형 또는 배치 모델에 관계없이 클라우드 컴퓨팅 환경은 크게 3가지 특징을 가진다. 첫 번째, 사용자는 클라우드 컴퓨팅 서비스에 PC, 스마트폰, 태블릿 PC 등 다양한 단말기기를 통해 접근할 수 있다. 클라우드 서비스를 사용한 단말기기에 남은 흔적을 통해 어떠한 서비스를, 언제 사용했는지, 그리고 어떤 행위를 했는지 알 수 있다. 특히, 스마트폰에는 클라우드 서비스의 계정 정보가 남아있는 경우가 있기 때문에 사용자가 어떤 계정으로 접근했는지도 알 수 있다. 두 번째, 실제 데이터는 로컬이 아닌 원격지에 존재한다. 기존 컴퓨팅 환경과 달리 사용자가 자신의 가상공간에서 작업한 데이터는 로컬에 존재하지 않고 원격지에 존재한다. 만약 증거 데이터 주체의 국적지와 데이터 저장 위치의 국적지가 다르다면, 사법관할권 문제가 발생한다. 또한 국외의 클라우드 서비스인 경우, 증거 데이터를 획득하기 위해 국제 공조 등의 절차를 거쳐야 한다. 세 번째, 데이

터가 실시간으로 동기화된다. 사용자의 클라우드 상에서 작업한 데이터는 실시간으로 동기화된다. 사용자가 데이터를 생성, 변경, 삭제할 때마다, 데이터의 상태가 실시간으로 업데이트된다. 그렇기 때문에 클라우드 컴퓨팅 서비스를 조사를 할 때, 클라우드 상에 존재하는 증거 데이터의 상태가 변하지 않도록 보호해야 한다.

Ⅲ. 클라우드 포렌식 관련 연구 동향

본 절에서는 현재까지 클라우드 컴퓨팅 포렌식 관련된 기술적인 연구들을 살펴본다. 클라우드 포렌식 기술과 관련된 연구는 [표 1]과 같이 클라우드 포렌식 조사 절차와 관련한 연구, IaaS에 대한 디지털 포렌식 기술 연구, 그리고 SaaS에 대한 디지털 포렌식 기술 연구로 나뉜다.

〔표 1〕 클라우드 포렌식 조사 절차 및 기술 연구 동향

주제	논문제목(저자)
클라우드 컴퓨팅 조사 절차	An integrated conceptual digital forensic framework for cloud computing (Ben Martini 외)
공공클라우드 IaaS	IaaS 유형의 클라우드 컴퓨팅 서비스에 대한 디지털 포렌식 연구 (정일훈 외)
	Acquiring forensic evidence from infrastructure-as-a-service cloud computing:Exploring and evaluating tools, trust, and techniques (Josiah Dykstra 외)
	Digital forensic investigation of cloud storage services (Hyunji Chung 외)
공공클라우드 SaaS	클라이언트 관점의 SaaS 사용 흔적 분석 (강성림 외)

3.1. 클라우드 포렌식 조사 절차 연구 동향

Ben Martini는 클라우드 컴퓨팅 환경을 위한 디지털 포렌식 절차를 제안하였다[11]. Ben Martini가 제안한 절차는 McKemmish가 제안한 절차와 NIST에서 표준화한 절차를 통합한 절차를 제안하였다[12][13]. 이는 기존에 존재하는 절차들을 통합하여 클라우드 컴퓨팅 환경에 적합하도록 개선한 절차이다.

3.2. IaaS에 대한 디지털 포렌식 연구 동향

현재 IaaS에 대한 디지털 포렌식 기술 연구는 크게 두 가지가 존재한다. 첫 번째, AWS나 Rackspace와 같이 가상 머신을 제공해주는 형태의 서비스에 대한 디지털 포렌식 조사 방법에 관한 연구이다[14][15]. 두 번째, Dropbox나 Ndrive와 같은 클라우드 스토리지 서비스에 대한 디지털 포렌식 조사 방법에 관한 연구이다[16].

정일훈은 클라우드 컴퓨팅 서비스를 조사하기 위한 절차와 IaaS 관련 데이터를 수집 및 분석하는 방안을 제시하였다[14]. 이 논문에 따르면, 클라우드 컴퓨팅 서비스를 조사하기 위해서는 기존의 디지털 포렌식 절차에 따라 데이터를 수집한 후, IaaS와 관련한 클라우드 시그니처가 존재한다면 해당 IaaS에 대한 정밀 분석이 필요하다고 설명한다. 또한 정밀 분석을 위해서는 계정 정보를 수집하여 가상의 컴퓨터에 접근한 후, 가상의 컴퓨터 내에 존재하는 데이터를 수집 및 분석해야한다고 설명한다.

Josiah Dykstra는 Amazon EC2와 같이 가상머신을 제공하는 IaaS 내의 데이터를 수집하는 방법을 제시하고, 기존의 도구를 이용하여 데이터를 수집할 수 있다는 것을 확인하였다[15]. Josiah Dykstra는 가상머신에 접근할 수 있는 경우에, 가상머신 내에 존재하는 데이터를 EnCase나 FTK 등 과 같은 도구를 이용하여 수집할 수 있다는 것을 실험을 통해 확인하였다. 또한 데이터를 수집할 때 각 도구들의 성능을 평가하였다.

Hyunji Chung은 IaaS의 한 형태인 클라우드 스토리지 서비스를 대상으로 디지털 포렌식 조사 절차를 제안하였다[16]. 이 논문에 따르면, 클라우드 스토리지 서비스는 다양한 단말기기로 접근할 수 있기 때문에 해당 서비스에 접근하기 위해 사용했던 모든 단말기기로부터 데이터를 수집하고, 이를 함께 분석해야 한다고 주장한다. 특히 스마트폰에는 클라우드 스토리지 서비스의 계정 정보가 남는 경우가 있기 때문에 PC와 더불어 스마트폰을 반드시 조사해야 한다고 설명한다.

3.3. SaaS에 대한 디지털 포렌식 연구 동향

강성림은 SaaS 중 많이 사용되는 서비스를 사용했을 때 PC에 남는 흔적을 정리하고 분석 방안을 제시하였다[17]. 논문에 따르면, SaaS는 웹 브라우저를 통해 접근

할 수 있기 때문에 SaaS를 사용한 흔적을 찾기 위해서는 웹 브라우저 로그파일을 분석해야 한다고 설명한다. 또한 웹 브라우저가 열려있는 상태에서는 로그인한 사용자의 계정 정보와 작업 중인 상태가 물리메모리에 존재하기 때문에 활성시스템에서 데이터를 획득하는 경우 물리메모리를 분석을 통해 SaaS의 사용 흔적을 찾을 수 있다고 설명한다.

Ⅳ. 클라우드 포렌식 관련 법적 이슈

본 절에서는 클라우드 컴퓨팅 환경으로 변함에 따라 발생하는 법적인 이슈들을 살펴본다. 클라우드 포렌식과 관련한 다양한 법적 이슈들 중 사법관할권, 개인 프라이버시와 압수수색, 그리고 증거 보존에 대해 살펴본다.

4.1. 관할권

전통적으로 사람 또는 물건이 존재하거나 행위가 일어난 물리적 위치를 중심으로 관할권(jurisdiction)을 결정하였다. 하지만 클라우드 컴퓨팅 환경에서는 전통적인 방식을 통해 관할권을 결정하기 어렵다. 클라우드 컴퓨팅 환경의 특성상 사용자의 국적지와 사용자의 정보를 저장한 매체가 존재하는 물리적 위치가 동일하지 않은 경우가 발생하기 때문이다. 이러한 경우 정보의 주체인 사용자가 속한 국가와 정보를 저장한 매체가 존재하는 국가 사이에서 관할권의 충돌(jurisdictional conflicts of law)이 발생한다[18]. 관할권의 충돌이 일어난 경우, 정보의 주체가 속한 국가와 정보를 저장한 매체가 존재하는 국가 중 어느 나라가 지배권을 가져야 하는지에 대한 논란이 있다.

4.2. 개인 프라이버시와 압수수색

정보 및 수사기관에게 영장 없이 컴퓨터에 저장된 데이터를 요구할 수 있는 권한이 인정되는 법이 존재하는 국가가 존재한다[19]. 예를 들어, 미국의 애국법(USA PATRIOT Act, 2001), 미국보호법(Protect Americana Act, 2007), 해외정보감시법(Foreign Intelligence Surveillance Act, 2008), 영국의 조사권한 제한법(Regulation of Investigatory Powers Act, 2000, Part2)의 제 28조, 그리고 한국의 통신비밀보호법, 전기통신사업법 등이 있다[19]. 이러한 국가에서는 국가보안 또는 범죄사건 조사를 위해 클라우드 상에 존재하는 데이터를 감시 또는 수색할 가능성이 있다. 이때 해당 범죄와 관련되지 않는 데이터가 압수되는 경우, 데이터 주체자의 프라이버시가 침해당할 수 있다.

또한 클라우드 서비스 사용자는 자신의 데이터를 직접 관리할 수 없기 때문에 자신의 데이터를 누군가가 감시 또는 수색했다고 하더라도 자신의 프라이버시가 침해당했다는 사실을 알지 못할 수 있다.

4.3. 증거 보존

미국에서는 소송과 관련된 모든 데이터를 보존하도록 명령하는 보전명령(litigation hold)이 있다. 종이 서류나 디지털 문서 파일과 같은 데이터가 보존되어야 한다. 보존해야 할 데이터가 클라우드 상에 존재하는 경우, 증거 데이터는 클라우드 서비스 제공자가 관리하기 때문에 보존되기 어려울 가능성이 있다[20]. 미국에서는 이러한 경우에 데이터를 보전해야 하는 주체가 클라우드 상에 존재하는 전자저장정보를 제출하도록 한다[21]. 데이터 보전의 주체는 정보를 물리적으로 소유하지 않더라도, 정보를 실제로 획득할 수 있다면 정보를 보전할 의무를 가지기 때문이다[20].

만약 소송에 참여하는 누군가가 증거를 인멸하였다면, 미국에서는 증거를 인멸한 주체에게 강력한 제재를 가한다. 또한 증거가 존재했던 디지털 기기 또는 저장매체를 조사하도록 한다. 만약 클라우드 상에 존재하는 증거를 인멸하였다면, 문서소환장을 통해 클라우드 서버를 물리적으로 조사할 수 있다[20].

Ⅴ. 클라우드 컴퓨팅 포렌식 관련 연구 방향

본 절에서는 앞 장에서 살펴본 현재 연구 동향을 바탕으로 향후에 필요한 클라우드 컴퓨팅 포렌식 관련 연구 내용을 제시한다.

5.1. PaaS에 대한 디지털 포렌식 연구

공공 클라우드 중 IaaS와 SaaS에 대한 디지털 포렌식 조사 절차 또는 방법에 대한 연구는 진행되었으나,

〔표 2〕 클라우드 컴퓨팅 포렌식 관련 기존 연구

주제	상세 설명	기존 연구
공공클라우드 IaaS	가상머신 서비스에서의 디지털 포렌식 조사 절차 및 방법 연구	O
	클라우드 스토리지 서비스의디지털 포렌식 조사 절차 및 방법 연구	O
공공클라우드 PaaS	PaaS의 디지털 포렌식 조사 절차 및 방법 연구	X
공공클라우드 SaaS	SaaS의 디지털 포렌식 조사 절차 및 방법 연구	O
사설클라우드	사설 클라우드 컴퓨팅 환경에서 디지털 포렌식 조사 절차 및 방법 연구	X
증거인멸차단	법적 측면에서 증거인멸을 차단하기 위한 방안 연구	X
증거보존	기술적 측면에서 증거보존 방법 연구	X

PaaS에 대한 조사 절차 또는 방법은 아직 연구되지 않았다. PaaS는 기업 또는 특정 조직에서 협업하여 플랫폼을 이용한 업무를 진행하는 경우에 필요하다. 이러한 경우, 지적재산권 분쟁과 같은 사건에서 PaaS를 조사해야 할 가능성이 있기 때문에 PaaS에 대한 디지털 포렌식 연구를 할 필요가 있다.

5.2. 사설 클라우드 포렌식

사설 클라우드 컴퓨팅 환경에서 디지털 포렌식 조사를 하기 위한 절차와 방법은 공공 클라우드에서의 조사 절차와 방법과 차이가 있다. 외부 서비스 제공자가 관리하는 공공 클라우드와 달리 사설 클라우드는 기업과 같은 특정 조직의 내부자가 사설 클라우드 환경을 관리하기 때문이다.

사설 클라우드를 사용하는 기업 또는 조직 내부에서 일어난 기술 유출 사건이나 지적재산권 분쟁 등을 조사하기 위해서는 사설 클라우드 환경에 적합한 디지털 포렌식 조사 절차와 방법이 필요하다.

5.3. 증거 인멸 차단 및 증거 보존 방안

클라우드 서비스 사용자는 PC 뿐만 아니라 스마트폰이나 태블릿 PC와 같은 모바일 기기를 이용하여 접근할 수 있다. 이는 PC에서만 접근할 수 있는 서비스보다 클라우드 서비스에 접근하기에 쉽다는 것을 의미한다. 사용자가 단말기기를 잃어버렸다고 하더라도, 새로운 단말기기를 이용하여 클라우드 서비스에 접근하여 데이터를 생성, 수정, 삭제할 수 있다. 이러한 특성 때문에 클라우드 상에 존재하는 데이터를 증거로 보존하기가 어려울 수 있다. 클라우드 상에 존재하는 데이터를 보존하기 위해서는 법적 그리고 기술적인 방안이 필요하다.

현재 우리나라는 미국에 비해 증거보전 의무 불이행에 대하여 제재하는 규정이 없다[19]. 클라우드 컴퓨팅 환경에서는 증거를 인멸하기 쉽고, 증거를 인멸한다하더라도 인멸했다는 증거를 찾기 어렵다. 따라서 증거보전에 대한 제재를 강화하거나 재판 과정에서 증거를 보전하지 않은 사람에게 불이익을 주는 방안이 필요하다[19].

또한 증거 데이터를 보존하기 위한 기술적인 방안에 대한 연구가 필요하다. 클라우드 상에 존재하는 데이터는 인멸되면 다시 복구하는 것이 어렵기 때문이다. PC 또는 모바일 기기를 압수할 때, 전자파를 차단하거나 네트워크에 접속할 수 없도록 조치를 취하는 방법 등과 같은 방법을 이용하여 데이터를 보존할 수 있다.

Ⅵ. 결 론

현재 전세계적으로 IT 환경이 클라우드 컴퓨팅 환경으로 점차 바뀌고 있다. 클라우드 컴퓨팅 환경은 기존 컴퓨팅 환경과 다르기 때문에 기존의 디지털 포렌식 조사 절차와 방법을 그대로 적용할 수 없다. 클라우드 컴퓨팅 환경에 적합한 디지털 포렌식 조사 절차와 방법에 대한 연구가 필요하다.

본 논문에서는 클라우드 컴퓨팅의 개념을 정리하였고, 디지털 포렌식 관점에서의 클라우드 컴퓨팅에 대해 설명하였다. 또한 현재 클라우드 컴퓨팅 환경에서의 디지털 포렌식 조사 절차 또는 방법에 대한 연구가 어느 정도 이루어졌는지 정리하였고, 이를 바탕으로 향후 연구 방향을 제시하였다.

참고문헌

[1] 정익래, 홍도원, 정교일, “디지털 포렌식 기술 및 동향”, 전자통신동향분석, 제 22권, 제 1호, pp.1-8, 2007.

[2] 민옥기, 김학영, 남궁한, “클라우드 컴퓨팅 기술 동향”, 전자통신동향분석, 제 24권, 제 4호, pp. 1-13, 2009.

[3] National Institute of Standards and Technology, “The NIST Definition of Cloud Computing”, 2011.

[4] Rajkumar Buyya, Chee Shin Yeo, and Srikumar Venugopal,“Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities”, 10th IEEE International Conference on High Performance Computing and Communications Keynote, pp. 5-13, 2008.

[5] Chris & Suchitra Narayan, ”클라우드 서비스 도입의 기폭제가 된 경기 침체“, IDC Analyze the Future, 2009.

[6] Ben Kepes, “Understanding The Cloud Computing Stack SaaS, PaaS, IaaS”, Rackspace 2011.

[7] Shayne P. Bates, Ronald Lander, Benjamin M. Butchko, “Cloud Computing and Software as a Service”, ASIS International, pp. 6-9, 2010.

[8] 전용기, 백준기, “클라우드 컴퓨팅:한국의 클라우드 컴퓨팅 및 서비스 시장 주도 기업”, HYUNDAI Research, pp. 6, 2011.

[9] Keyun Ruan, Joe Carthy, Tahar Kechadi, Mark Crosbie, “Cloud forensics: An overview”, 7th IFIP WG 11.9 International Conference on Digital Forensics, Volume 361, pp. 9, 2011.

[10] Josiah Dykstra, Alan T. Sherman, “Understanding issues in cloud forensics: Two hypothetical case studies”, Proceedings of the 2011 ADSFL Conference on Digital Forensics, Security, and Law, 2011.

[11] Ben Martini, Kim-Kwang Raymond Choo, “An integrated conceptual digital forensic framework for cloud computing”, Digital Investigation, Article in press, 2012.

[12] Rodney McKemmish, “What is Forensic Computing? Trends and Issues in Crime and Criminal Justice”, Australian Institute of Criminology, pp. 1-6, 1999.

[13] National Institute of Standards and Technology, “Challenging security requirements for US government cloud computing adoption (Draft)”, Gaithersburg: U.S. Department of Commerce, 2011.

[14] 정일훈, 오정훈, 박정흠, 이상진, “IaaS 유형의 클라우드 컴퓨팅 서비스에 대한 디지털 포렌식 연구”, 정보보호학회 2011.

[15] Josiah Dykstra, Alan T. Sherman, “Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques”, Digital Investigation, Article in press, 2012.

[16] Hyunji Chung, Jungheum Park, Sangjin Lee, Cheulhoon Kang, “Digital forensic investigation of cloud storage services”, Digital Investigation, Article in press, 2012.

[17] 강성림, 박정흠, 이상진, “클라이언트관점의 SaaS 사용 흔적 분석”, 정보처리학회, 2011.

[18] 이창범, 이대희, 이민영, 이병준, 정준현, 김현정, 고영하, “클라우드 컴퓨팅 활성화를 위한 법제도 개선 방안 연구”, 한국인터넷진흥원, pp. 242-247, 2010.

[19] 정연덕, “클라우드 서비스와 개인 정보 보호의 문제점”, 한국정보법학회, 2012.

[20] 이창범, 이대희, 이민영, 이병준, 정준현, 김현정, 고영하, “클라우드 컴퓨팅 활성화를 위한 법제도 개선 방안 연구”, 한국인터넷진흥원, pp. 386-390, 2010.

[21] Tanya Forsheit, “Legal Implications of Cloud Computing, Part 4 and 5(E-Discovery and Digital Evidence)”, 2009.

〈著者紹介〉

정 현 지 (Hyunji Chung)
정회원

2010년 2월: 고려대학교 컴퓨터정보학, 산업시스템공학 공학사
2010년 3월~2012년 2월: 고려대학교 정보보호대학원 공학석사
2012년 3월~현재: 고려대학교 정보보호대학원 박사과정
<관심분야> 디지털 포렌식, 클라우드 포렌식

이 상 진 (Sangjin Lee)
정회원

1987년 2월: 고려대학교 수학과 학사
1989년 2월: 고려대학교 수학과 석사
1994년 8월: 고려대학교 수학과 박사
1989년 10월~1999년 2월: ETRI 선임 연구원
1999년 3월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
<관심분야> 디지털 포렌식, 심층암호, 해쉬 함수