Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.1, Feb. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.1.75

손상 클라우드 식별 가능한 다중 클라우드 일괄 감사 기법에 관한 연구*

신 수 연,† 권 태 경‡
연세대학교 정보대학원

A Study on Batch Auditing with Identification of Corrupted Cloud Storage in Multi-Cloud Environments*

Sooyeon Shin,† Taekyoung Kwon‡
Graduate School of Information, Yonsei University

요 약

최근 클라우드에 원격 저장된 데이터의 무결성 검증을 위해 제 3의 감사자에게 감사 임무를 위탁할 수 있는 다양한 공공 감사 기법이 제안되었으며, 검증 효율성을 높이기 위해 위탁받은 다중 감사 임무를 한 번에 수행할 수 있는 일괄 감사 기법 또한 제안되었다. 하지만 하나의 데이터라도 손상된 경우 일괄 감사의 검증은 실패하게 되고 포함된 모든 감사 임무를 다시 개별적으로 수행해야 한다는 문제점을 가진다. 일괄 감사는 여러 사용자의 데이터 인증자들이 복잡하게 합쳐져 있으므로 일괄 감사가 실패하는 경우 손상된 데이터를 식별하는 것은 매우 어려운 문제이다. 본 논문에서는 프라이버시 보존 가능한 공공 감사 기법인 Wang 등의 기법을 다중 클라우드의 다중 사용자에 대한 일괄 감사가 가능하도록 확장하고, 다중 클라우드 중에서 단일 클라우드의 데이터만 손상된 경우 해당 클라우드를 식별할 수 있는 기법을 제안한다.

ABSTRACT

Recently, many public auditing schemes have been proposed to support public auditability that enables a third party auditor to verify the integrity of data stored in the remote cloud server. To improve the performance of the auditor, several public auditing schemes support batch auditing which allows the auditor to handle simultaneously multiple auditing delegations from different users. However, when even one data is corrupted, the batch auditing will fail and individual and repeated auditing processes will be required. It is difficult to identify the corrupted data from the proof in which distinct data blocks and authenticators of distinct users are intricately aggregated. In this paper, we extend a public auditing scheme of Wang et al. to support batch auditing for multi-cloud and multi-user. We propose an identification scheme of the corrupted cloud when the data of a single cloud is corrupted in the batch auditing of multi-cloud and multi-user.

Keywords: Cloud computing, Public auditing, Batch auditing, Identification of corrupted cloud

접수일(2014년 9월 30일), 수정일(2015년 1월 28일), 게재확정일(2015년 1월 28일)

* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업 [10047212, 1kB 이하 암호문 간의 연산을 지원하는 동형 암호 원천 기술 개발 및 응용기술 연구]과 2012년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업 (No. NRF-2012R1A1B3000965)의 일환으로 수행하였음.

† 주저자, shinsy80@yonsei.ac.kr
‡ 교신저자, taekyoung@yonsei.ac.kr(Corresponding author)

I. 서 론

클라우드 컴퓨팅은 사용자가 소프트웨어, 스토리지, 서버, 네트워크 등 IT 자원을 필요한 만큼 빌려서 사용하고 사용한 만큼 비용을 지불하는 컴퓨팅으로 동적 확장성, 초기 투자 비용과 유지 비용 절감, 인터넷을 활용한 시간과 장소에 구애받지 않은 서비스 사용 가능 등 다양한 장점을 가진다. 클라우드 서비스 중 가장 대표적인 서비스는 클라우드 스토리지 서비스로 사용자는 자신의 데이터를 원격의 클라우드 서버 스토리지에 위탁하게 된다. 클라우드 스토리지 서버는 사용자의 개별 장치에 비해 계산, 저장 등 자원이 풍부하며 신뢰할 수 있는 연산 결과를 제공하지만 내·외부 보안 위협, 서비스 장애가 발생할 수 있으며 이는 사용자 데이터의 기밀성, 무결성, 가용성에 손상을 줄 수 있다. 하지만 클라우드 서비스 제공자는 내·외부 위협과 서비스 장애 등으로 사용자의 데이터가 손상 및 손실 되더라도 평판을 위해 사용자에게 이를 알리지 않을 수 있으며, 저장소의 공간 효율성을 위해 사용자의 데이터 중 접근이 거의 없는 데이터를 임의로 삭제하기도 한다. 이러한 문제를 해결하기 위해 신뢰할 수 없는 클라우드 스토리지에 저장된 사용자 데이터의 무결성 검증을 위한 원격 데이터 감사(remote data auditing) 기법이 많이 제안되어 왔다[1,2, 5].

최근의 감사 기법은 사용자의 계산 효율성을 위해 제3의 감사자(TPA: Third Party Auditor)에게 무결성 검증을 위임하는 공공 감사(public auditing) 방식을 사용하며 제 3의 감사자에 대한 사용자 데이터 프라이버시를 고려한다[8,9]. 또한 사용자에 의해 빈번히 데이터의 업데이트가 발생하는 클라우드 컴퓨팅 환경의 효율적인 감사를 위해 동적 업데이트를 지원하는 동적 감사(dynamic auditing)[10,12,13]와 다중 사용자의 감사를 일괄적으로 처리할 수 있는 일괄 감사(batch auditing)가 가능한 공공 감사 기법[6,12,13]이 제안되었다. 일괄 감사의 경우, 제 3의 감사자의 감사 효율성을 높이기 위해, 위임 받은 다중 감사 임무를 한 번에 처리하지만 하나의 데이터라도 손상되는 경우에는 일괄 감사의 모든 검증이 실패하는 결과를 가져오게 된다. 일부 일괄 감사 기법의 경우, 이러한 문제를 해결하기 위해 분할정복법(divide-and-conquer method)을 사용하거나 인코딩/디코딩 방식을 적용하여 개별 감사를 다시 진행하는 방식을 제안하였지만 많은 계산 비용을 발생시킨다.

본 논문에서는 기존 연구[7]를 바탕으로 Wang 등이 제안한 프라이버시 보존 공공 감사 기법[9]의 다중 사용자 일괄 감사 기능을 다중 클라우드의 다중 사용자에 대한 일괄 감사가 가능하도록 확장하고, 다중 클라우드 중 단일 클라우드가 사용자의 데이터를 손상 및 손실 시켰을 경우, 간단한 방식으로 해당 클라우드를 식별할 수 있는 기법을 제안한다.

본 논문은 다음과 같이 구성된다. 2장에서는 관련 연구를 정리하며, 3장에서는 Wang 등의 프라이버시 공공 감사 기법의 다중 사용자에 대한 일괄 감사를 간략히 소개한다. 4장에서는 손상 클라우드 식별 가능한 다중 클라우드의 다중 사용자 감사를 일괄 처리할 수 있는 감사 기법을 설명하며, 5장에서는 제안 기법의 성능을 분석한다. 6장에서는 결론과 향후 계획을 논의한다.

II. 관련 연구

클라우드 컴퓨팅 환경의 원격 데이터 감사는 신뢰할 수 없는 제공자가 관리하는 클라우드에 저장된 사용자 데이터가 올바르게 저장 및 관리되고 있는지를 저장 데이터를 회수하지 않고도 안전하고 효율적으로 검증할 수 있는 프로토콜의 집합을 의미한다[2]. 2007년 Ateneise 등은 처음으로 원격 데이터 감사를 위한 모델을 처음으로 정의하고 PDP (Provable Data Possesion) 기법[1]을 제안하고 2008년 확장성, 효율성 등을 개선하고 동적 업데이트가 가능한 SPDP (Scalable PDP) 기법을 제안하였다[2]. 하지만 PDP와 SPDP 기법은 공공 감사를 지원하지 않으며 검증의 횟수가 제한적이라는 문제가 있다.

2009년 Wang 등은 짧은 서명[3] 기반으로 블록 태그 인증을 위해 MHT (Merkle Hash Tree)를 사용하는 공공 감사 기법(PPDP: Public PDP)을 제안하였다[10]. 2010년 Wang 등은 TPA로부터의 사용자 데이터 프라이버시가 보존 가능한 공공 감사 기법(PP-PDP I: Privacy-preserving Public PDP)을 제안하였지만[8], Xu 등이 4가지 공격에 취약함을 보이면서[11], Xu 등이 언급한 공격에 취약하지 않으면서 프라이버시 보존 가능한 공공 감사 기법(PP-PDP II)을 제안하였다[9]. PP-PDP II 기법은 동시에 동적 업데트가 가능하고 단일 클라우드의 다중 사용자를 위한 일괄 감사가 가능함을 보였다. PP-PDP II 기법은 일괄 감사가 실패하는 경우, 재귀적인 분할정복법(이진탐색)을 사용하였지만, 검증을 위한 응답 값의 일부를 다시 받아 분할 감사를 진

행해야하므로 통신 및 계산 비용이 발생하게 된다. 이러한 문제를 해결하기 위해 Kai 등은 회복 가능한 코딩 접근 방식[4]을 적용하여 일괄 감사 실패 시, 통합된 응답으로부터 개별 응답을 디코딩하여 개별 감사를 진행 할 수 있는 기법을 제안하였다[6]. 하지만 인코딩/디코딩을 이용하여 PP-PDP II 기법의 통신 비용을 제거하였지만 개별 감사를 다시 진행해야 하므로 계산 비용은 여전히 남아있다.

2012년 Zhu 등은 다중 클라우드의 단일 사용자를 위한 일괄 감사 기법[13]을 제안하였으며, Yang과 Jia는 다중 클라우드의 다중 사용자를 위한 일괄 감사 기법을 제안하였다[12]. 두 가지 기법 모두 데이터 단편화 기법, 인덱스 테이블 등을 활용하여 감사 효율성을 개선하였지만 여전히 손상 데이터 및 손상 클라우드에 대한 식별이 불가능하다.

III. 프라이버시 보존 공공 감사 기법의 다중 사용자 일괄 감사

Wang 등은 클라우드 컴퓨팅 환경의 데이터 무결성 검증을 위해 공개 키 기반의 HLA (Homomorphic Linear Authenticator)과 랜덤 마스킹 기법을 통합하여 PP-PDP II 기법을 제안하였다[9]. PP-PDP II 기법은 데이터의 추가/수정/삭제가 발생하더라도 MHT로부터 일부 데이터의 변화가 생긴 부분만을 감지하여 부분적으로 감사를 진행할 수 있는 동적 감사와 단일 클라우드의 다중 사용자에 대한 감사 임무를 일괄적으로 처리할 수 있는 일괄 감사를 제안하였다.

PP-PDP II 기법의 다중 사용자 일괄 감사에서는 겹선형 사상(bilinear map)과 두 개의 해시 함수 $H(\bullet): \{0,1\}^* \rightarrow G_1$와 $h(\bullet): G_T \rightarrow Z_p^*$를 사용한다. G_1, G_2, G_T가 위수가 소수 p인 곱셈 순환군일 때, $e: G_1 \times G_2 \rightarrow G_T$가 non-degeneracy, bilinearity, computability를 만족하면 겹선형 사상이라고 한다. g는 G_2의 생성원이다. 사용자 $U_k (k \in 1,...,K)$의 파일 F_k는 일정한 크기의 n_k개의 블록으로 나뉘며, $m_{k,1}, m_{k,2}, ..., m_{k,n} \in Z_p^*$로 나타낸다. 80비트의 안전성을 고려한 경우에는 p가 160 비트이므로 각 블록 $m_{k,i}$는 160 비트가 된다. PP-PDP II 기법은 크게 설정 단계(setup phase)와 감사 단계(audit phase)로 나뉜다.

3.1 설정 단계

Fig. 1(a)는 다중 사용자에 대한 설정 단계를 보여주며, K명의 사용자에 대해 설정 단계를 반복한다.

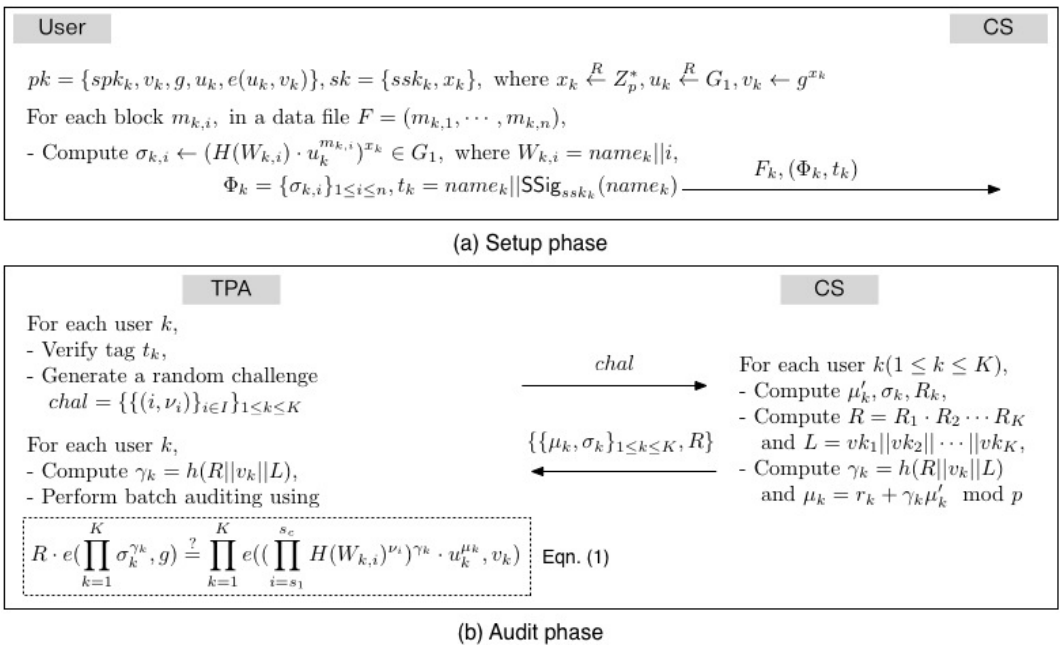

Fig. 1. Batch auditing of PP-PDP II for multiple users: Audit phase.

사용자 k는 파일 태그 생성을 위한 짧은 서명(SSig) 키 쌍 (spk_k, ssk_k)를 포함한 공개 키 값 pk_k와 개인 키 값 sk_k를 생성한다. 생성한 키를 이용하여 파일의 모든 블록 $m_{k,i}$에 대한 인증자 $\sigma_{k,i}$를 계산하고, 인증자 집합 Φ_k를 생성한다. 파일 F_k에 대한 유일한 식별자인 $name_k$를 짧은 서명 방식으로 서명하여 태그 t_k를 생성한다. 클라우드 서버(CS: Cloud Server)에게 파일 F_k와 검증 메타데이터 (Φ_k, t_k)를 전송한다.

3.2 감사 단계

Fig. 1(b)는 다중 사용자에 대한 일괄 감사 단계를 보여준다. TPA는 K명의 사용자로부터 위임받은 감사를 위해 각 사용자 U_k의 파일 태그를 검증하고 랜덤한 $chal$을 생성한다. TPA는 먼저 감사를 요청한 사용자의 파일 태그 t_k를 검증한다. TPA는 파일의 전체 블록을 검사하는 대신 랜덤하게 샘플 블록을 선택하여 감사하기 위해 사용자의 전체 n_k개의 블록 중에서 c개를 랜덤하게 선택($I = \{s_1, \cdots, s_c\}$)한다. 각 블록에 대해 랜덤 값 $\nu_{k,i}$를 선택하여 시도 값 $chal$을 생성하여 CS에게 전송한다. CS는 각 사용자 $k(1 \le k \le K)$에 대한 $\mu_k^{'}, \sigma_k, R_k$를 생성하여 R, L을 계산한다. 각 사용자 k에 대한 γ_k, μ_k를 계산하여 $\left\{\{\sigma_k, \mu_k\}_{1 \le k \le K}, R\right\}$을 응답으로 전송한다. TPA는 받은 응답 값을 이용하여 각 사용자에 대한 γ_k를 계산하고, Eqn. (1)를 이용하여 검증한다. 만약 검증 식을 만족한다면, CS가 감사를 위임한 다중 사용자의 모든 데이터를 제대로 보관하고 있음을 확인할 수 있으며, 만족하지 않는다면 다중 사용자 중 일부 사용자의 데이터가 손상 혹은 손실 됐음을 확인할 수 있다.

IV. 손상 클라우드 식별 가능한 다중 클라우드의 다중 사용자 일괄 감사 기법

Wang 등의 PP-PDP II 기법은 단일 클라우드의 다중 사용자에 대한 일괄 감사만 고려하여 다중 클라우드의 감사를 담당하는 TPA의 경우에는 순차적으로 각 클라우드에 대한 일괄 감사를 처리해야 하므로 효율성이 떨어진다. 이를 해결하기 위한 방안으로 PP-PDP II 기법을 다중 클라우드의 다중 사용자에 대한 일괄 감사가 가능하도록 확장한다. PP-PDP II 기법은 일괄 감사가 실패하는 경우, K 사용자를 반으로 나누어 일괄 감사를 하고 또 다시 실패하는 경우 다시 반으로 나누어 일괄 감사를 진행하는 재귀적인 이진탐색 방식을 사용한다. 다중 클라우드 버전에서도 마찬가지로 손상 클라우드 식별을 위해 L개의 클라우드를 나누어 분할 감사한다고 가정한다. 제안하는 손상 클라우드 식별 가능한 다중 클라우드의 다중 사용자 일괄 감사 기법은 다중 클라우드 중 단일 클라우드 데이터들만 손상되었을 경우에는 부가적인 감사 과정 없이 해당 클라우드를 식별 가능한 프로토콜을 제안한다. Yang과 Jia의 위협모델[12]과 같이 손상 클라우드는 사용자의 데이터 손상을 알리지 않고 TPA를 속이기 위해 손상된 사용자 데이터 블록 및 인증자를 해당 사용자의 다른 블록과 인증자를 사용하거나 아예 다른 사용자의 데이터 블록과 인증자를 사용한다고 가정한다.

4.1 다중 클라우드의 다중 사용자 일괄 감사

총 L개의 클라우드가 존재하고, 각 클라우드 $C_l(1 \le l \le L)$의 최대 K명의 사용자들이 TPA에게 감사를 위임하였으며, TPA가 이를 일괄적으로 감사하는 경우를 고려한다. PP-PDP II 기법의 G_2의 생성자 g 대신 g_2 표기법을 사용하며, G_1의 생성자 g_1를 추가적으로 사용한다. 그림 2는 손상 클라우드 식별 가능한 다중 클라우드의 다중 사용자 일괄 감사 기법을 보여준다. 각 서버 C_l은 TPA의 시도 값과 감사를 요청한 각 사용자 $U_{kl}(1 \le k \le K)$의 파일 F_{kl}, 인증자 집합 Φ_{kl}을 이용하여 응답 값 $proof_l$를 계산하여 TPA에게 전송한다. TPA는 L개의 클라우드로부터 받은 값들을 통합하여 한 번에 검증한다.

4.1.1 설정 단계

PP-PDP II 기법의 다중 사용자 일괄 감사를 위한 설정 단계와 거의 동일하며, 사용자의 공개 키 값 중 하나인 u_{kl}을 생성하는 과정만 차이가 있다.

4.1.2 감사 단계

그림 2(b)는 다중 클라우드의 다중 사용자에 대한 감사 단계를 보여준다. 대부분의 과정은 PP-PDP II 기법의 다중 사용자 감사와 동일하고 시도 값을 클라

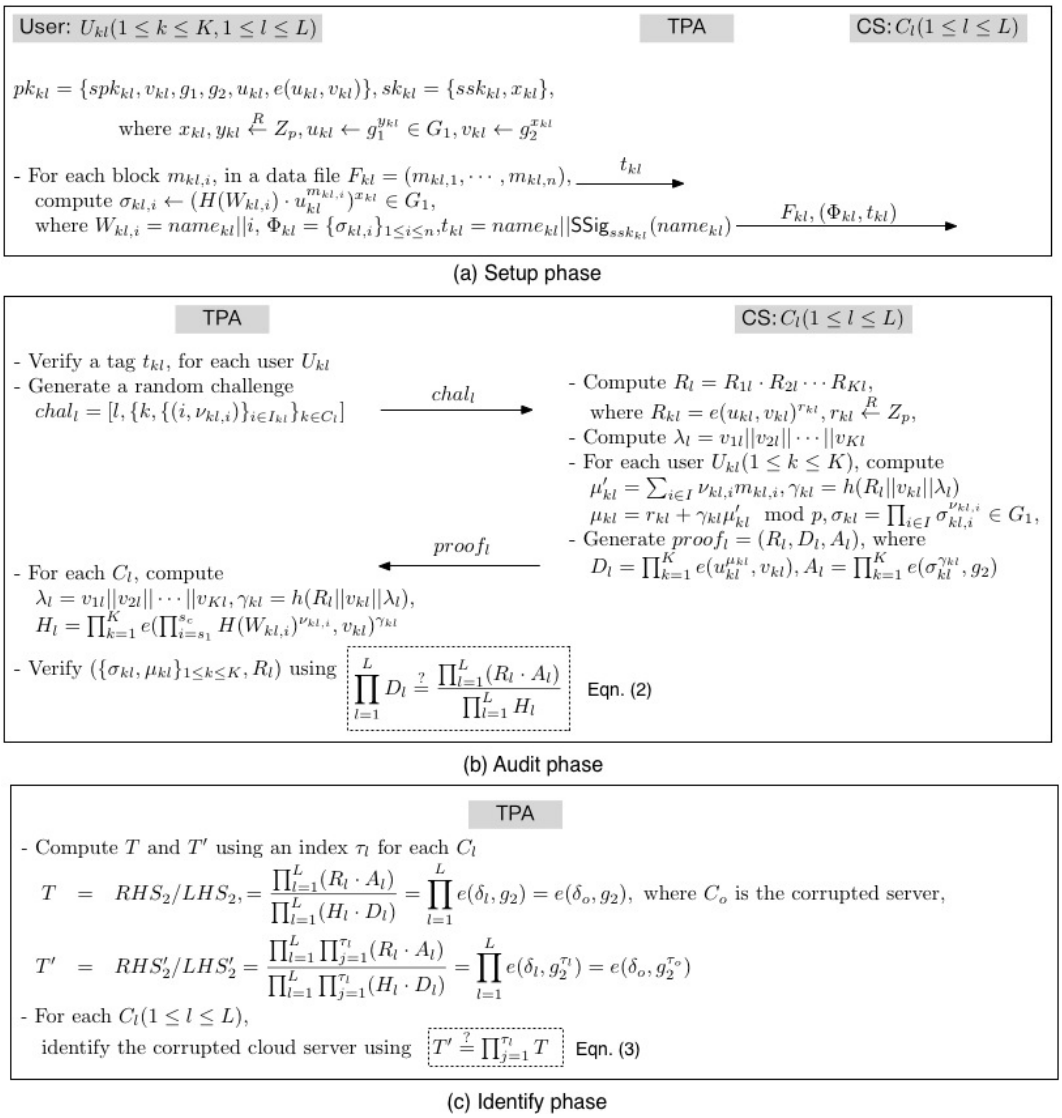

Fig. 2. Batch auditing with the corrupted cloud for multiple users and multiple clouds.

우드의 다중 사용자에 대한 값을 각각 보내는 것이 아니라 한 번에 $chal_l$로 보내며, 마찬가지로 응답 값 또한 다중 사용자의 값을 별개로 나누어 보내는 것이 아니라 R_l과 유사하게 D_l과 A_l을 계산하고 통합된 형태의 $proof_l$을 보낸다. TPA는 각 CS C_l에 대해 다시 계산한 H_l과 C_l로부터 받은 응답 값 $proof_l$을 이용하여 다중 클라우드의 위임된 감사를 Eqn. (2)를 이용하여 일괄적으로 수행한다. 만약 Eqn. (2)가 만족한다면, 감사를 위임한 모든 클라우드의 모든 사용자의 데이터들이 올바르게 저장 및 관리되고 있다고 확인할 수 있다.

4.2 손상 클라우드 식별

만약 감사 단계에서 Eqn. (2)가 만족하지 않아 일괄 감사가 실패하게 되면, 다중 클라우드 중 단일 클라우드의 사용자 데이터들이 손상되었음을 의미하므로 그림 2(c)와 같이 식별 단계(identify phase)를 수행한다. TPA는 먼저 감사 단계의 Eqn. (2)의 좌변(LHS_2)과 우변(RHS_2)을 이용하여 T를 계산하고, 추가적으로 클라우드 별로 1부터 차례로 인덱스 τ_l를 할당한다. 예를 들어, 두 번째 클라우드 서버의 인덱

스 τ_2는 2를 가진다. 각 클라우드의 순차적 인덱스 τ_l을 이용하여 T'을 계산한다. $\delta_l \in G_1$은 각 클라우드의 손상 정도를 나타내는 값으로 단일 클라우드의 데이터만 손상되었다고 가정하였으므로 T와 T'은 결과적으로 손상 클라우드의 손상 정도만을 포함하게 된다. 또한 δ_l의 형태는 사용자의 데이터 블록과 인증자 중 어떤 값이 손상되었으며, 손상된 값을 어떤 값으로 변경했는지에 따라 $g_1^{\sum_{b\in B_o} \triangle_{D-bo}}$, $\prod_{b\in B_o}(\delta_{H-bo})$, $\prod_{b\in B_o}(\delta_{H-bo}\cdot g_1^{\triangle_{D-bo}})$, 세 가지로 표현된다. 손상된 클라우드가 C_o라고 했을 때, B_o는 C_o의 다중 사용자 중에서 데이터가 손상된 사용자들의 집합이며, $\triangle_{D-bo} \in Z_p^*$는 사용자의 데이터 블록과 인증자 손상으로 인해 발생한 손상 정도를 나타낸다. 또한 $\delta_{H-bo} \in G_1$은 사용자의 인증자만 손상되었을 경우의 손상 정도를 나타낸다. 마지막으로 Eqn. (3)을 이용하여 TPA는 T'과 동일한 값이 나올 때까지 T를 계속 반복적으로 곱한다. 이때 누적 곱셈의 수를 M이라고 하자. T를 반복적으로 곱하다가 T'과 일치했을 때, $(M+1)$이 손상 클라우드의 인덱스 τ_o를 의미한다. 예를 들어, 두 번째 클라우드가 손상 클라우드라면, $T' = e(\delta_2, g_2)^2$이며, $T \times T = T'$일 것이므로 $M+1=2$가 되므로 두 번째 클라우드가 손상 클라우드임을 확인하는 것이 가능하다.

V. 성능 분석

제안한 손상 클라우드 식별 가능한 다중 클라우드의 다중 사용자 일괄 감사 기법에서 손상 클라우드 식별 방식에 대한 성능을 Wang 등이 제안한 재귀적인 이진 탐색 방식을 비교분석한다. 모든 실험은 4GB RAM을 이용하는 Intel Core i5 1.7 GHZ 프로세서를 가진 MacOSX 10.9 시스템에서 이루어졌다. 스탠포드 대학의 PBC (Pairing Based Cryptography) 라이브러리[15]와 OpenSSL의 Crypto 라이브러리[14]를 이용하여 C 코드(Xcode)로 겹선형 사상을 구현하였으며, 이 때 기저체(base field) 크기가 159비트이며 임베딩 차수(embedding degree)는 6인 MNT d159 커브를 이용하였다. 80 비트 안전성을 위해 그룹의 위수로 160 비트의 소수 p를 선택하였다.

제안한 손상 클라우드 식별 방식(proposed method)과 재귀적인 이진 탐색 방식(recursive binary search) 모두 파일의 크기, 블록의 개수(n_{kl}), 사용자 수 (K), 시도 블록 수와 독립적이며, 단지 감사를 위임한 사용자들이 포함된 클라우드 수 (L)와 그 중에서 손상 클라우드가 몇 번째 위치하는지에만 영향을 받는다. 따라서 클라우드 수를 3개에서 15개까지 달리하여 실험하였으며, 클라우드 수 별로 손상 클라우드의 위치를 차례로 바꾸어 20번씩 실행하여 평균값을 구하였다. 그림 3은 실험 결과 그래프로 제안한 손상 클라우드 식별 방식이 Wang 등이 제안한 재귀적인 이진 탐색 방식에 비해 효율적임을 확인할 수 있다.

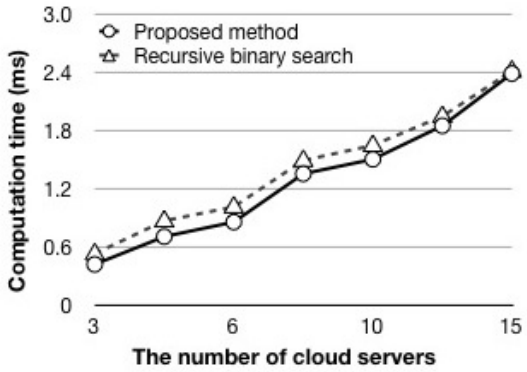

Fig. 3. Comparison of computation cost for identifying the corrupted server.

VI. 결 론

다중 클라우드 환경에서 TPA의 감사 효율성을 높이기 위해서는 다중 클라우드의 다중 사용자의 감사 임무를 한 번에 수행할 수 있는 일괄 감사 기법이 필요하다. 하지만 하나의 데이터 혹은 인증자라도 손상되는 경우에는 일괄 감사가 실패하게 되며 일괄 감사의 장점이 모두 사라지게 된다. 기존 연구들의 경우, 일괄 감사가 실패하는 경우 손상 클라우드를 식별하기 위해 재귀적으로 일괄 감사 혹은 개별 감사를 다시 진행해야하는 문제가 있었다. 비록 단일 클라우드가 손상되었을 경우에만 식별이 가능하지만, 지금까지 일괄 감사 실패 시 반복적인 일괄 감사 혹은 개별 감사의 과정 없이 손상 클라우드를 식별할 수 있는 기법은 존재하지 않았다. 본 논문에서는 단일 클라우드의 데이터 혹은 인증자가 손상되었다고 했을 때, 손상 클라우드를 효율적으로 식별할 수 있는 기법을 제안하였다.

향후 연구로는 다중 클라우드가 손상되었을 경우에도 식별이 가능한 일괄 감사 기법을 연구할 예정이며, Zhu 등의 다중 클라우드의 단일 사용자에 대한 일괄 감사 기법과 Yang과 Jia의 다중 클라우드의 다중 사용자에 대한 일괄 감사 기법에 제안 기법을 적용해 볼 예정이다.

References

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proceedings of ACM CCS'07, pp. 598-609, 2007.

[2] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," Proceedings of the 4th international conference on Security and privacy in communication networks, pp. 1-10, 2008.

[3] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from The Weil Pairing," Journal of Cryptology, vol. 17, no. 4, pp. 297-319, Sept. 2004.

[4] C.M. Chen, Y.H. Lin, Y.C. Lin, H.M. Sun, "RCDA: Recoverable concealed data aggregation for data integrity in wireless sensor networks," IEEE Trans. on Parallel and Distributed Systems, vol. 23, no. 4, pp. 727-734, April 2012.

[5] A. Juels, S. Burton, and J. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proceedings of ACM CCS'07, pp. 584-597, 2007.

[6] H. Kai, H. Chuanhe, W. Jinhai, Z. Hao, C. Xi, L. Yilong, Z. Lianzhen, and W. Bin, "An Efficient Public Batch Auditing Protocol for Data Security in Multi-Cloud Storage," Proceedings of the 8th ChinaGrid Annual Conference, pp. 51-56, 2013.

[7] Sooyeon Shin, Kunhee Lee, and Taekyoung Kwon, "A Study on Privacy-Preserving Batch Auditing for Multiuser and Multicloud," CISC-S'14, 2014.

[8] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security on Cloud Computing," Proceedings of IEEE INFOCOM, pp. 1-9, 2010.

[9] C. Wang, Sherman S.-M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Computing," IEEE Trans. on Computers, vol. 62, issue 2, pp. 362-375, Feb. 2013.

[10] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. of ESORICS'09, LNCS 5789. pp. 355-370, 2009.

[11] C. Xu, X. He, and D. Abraha-Weldemariam, "Cryptoanalysis of Wang's Auditing Protocol for Data Storage Security in Cloud Computing," Proc. of ICICA'12, Part II, CCIS 308, pp. 422-428, 2012.

[12] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Trans. on Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717-1726, Sept. 2013.

[13] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multicloud storage," IEEE Trans. on Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231-2244, Dec. 2012.

[14] The openssl project, 2014. Available: https://www.openssl.org/source/

[15] The pairing-based cryptography library (pbc), 2014. Available: http://crypto.stanford.edu/pbc/

〈저자소개〉

신 수 연 (Sooyeon Shin) 학생회원
2004년 2월: 세종대학교 컴퓨터공학과 학사
2006년 2월: 세종대학교 컴퓨터공학과 석사
2012년 8월: 세종대학교 컴퓨터공학과 박사
2012년 9월~2013년 8월: 세종대학교 컴퓨터공학과 Post Doc.
2013년 9월~현재: 연세대학교 정보대학원 Post Doc.
〈관심분야〉 프라이버시 보호기술, 익명성 기술, RFID, 센서 네트워크 보안, HCI 보안 등

권 태 경 (Taekyoung Kwon) 종신회원
1992년 2월: 연세대학교 컴퓨터과학과 학사
1995년 2월: 연세대학교 컴퓨터과학과 석사
1999년 8월: 연세대학교 컴퓨터과학과 박사
1999년~2000년: U.C. Berkely Post-Doc.
2001년~2013년 8월: 세종대학교 컴퓨터공학과 교수
2007년~2008년: Univ. Maryland at College Park 교환교수
2013년 9월~현재: 연세대학교 정보대학원 부교수
〈관심분야〉 암호프로토콜, 네트워크 프로토콜, 센서네트워크 보안, HCI 보안 등