하이브리드 클라우드의 기존 Reputation-based Trust Management 방식 개선

신동혁*, 정준권**, 정태명***
*성균관대학교 컴퓨터공학과
**성균관대학교 전자전기컴퓨터공학과
***성균관대학교 정보통신대학
e-mail:dh.shin@skku.edu, jkjung@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

Improvement of Reputation-based Trust Management for Hybrid Cloud Computing

Dong-Hyuk Shin*, Jun-Kwon Jung**, Tai-Myoung Chung***
*Dept of Computer Engineering, Sungkyunkwan University
**Department of Electrical and Computer Engineering, Sungkyunkwan University
***College of Information and Communication Engineering, Sungkyunkwan University

요 약

최근에 주목받고 있는 하이브리드 클라우드는 기존 퍼블릭과 프라이빗 클라우드의 이점을 결합한 방식으로, 보안성과 자원 효율성이 뛰어나다는 장점이 있다. 하지만 하이브리드 클라우드 시스템을 구성하는 각각의 클라우드 개체들은 성능이 향상됨에 따라 더 역동적으로 작동하는 반면, 기존에 형성된 개체 간 관계는 차츰 느슨해지고 있기 때문에 개체 간 협력과 지속적인 신뢰 관리가 반드시 필요하다. 신뢰성 관리 시스템(Trust Management System)은 유저들의 피드백을 DB화 해서 신뢰적인 개체를 판별하는데 도움을 준다. 이 시스템은 신뢰성이라는 가치를 판단하는 근거가 매우 주관적이라는 단점을 가지고 있어 부작용이 발생하고 있다. 본 논문에서는 신뢰성 수치(Trust Value)를 계산하기 위한 파라미터에 객관적인 기준을 도입하였다. 따라서 주관적 판단과 객관적 근거가 조화된 수치를 도출하여 개체의 독립적인 의사 결정에 도움을 줌으로써 신뢰성 관리 시스템의 신뢰성을 높였다.

1. 서론

클라우드 서비스는 웹을 통해서 시간과 장소에 구애받지 않고 필요한 만큼 IT리소스를 이용하는 컴퓨팅 방식으로, 어느덧 도입기를 지나 실생활에 자리 잡고 있다. 전 세계의 수많은 기업들은 IT서비스의 효율성을 제고하고 비용을 절감하기 위한 클라우드 서비스에 주목하고 있다. 클라우드 서비스는 플랫폼의 형태에 따라 프라이빗(Private), 퍼블릭(Public), 하이브리드(Hybrid)의 3가지 모델로 나누어지는데, 이 중 프라이빗 모델의 장점인 뛰어난 보안성과 퍼블릭 모델의 자원 효율성이 결합된 방식의 하이브리드 클라우드가 최근 크게 주목을 받고 있다.

하이브리드 클라우드는 자율적으로 동작하는 퍼블릭, 프라이빗 클라우드의 논리적인 결합으로 이루어진다. 프라이빗 클라우드를 중심으로 다수의 퍼블릭 클라우드를 연결함으로써, 하이브리드 클라우드는 사용자의 요구에 따라 외부 자원을 원활히 공급할 수 있다. 이미 알려진 바와 같이 클라우드 서비스는 경제적, 자원적 이점을 비롯한 여러 편의를 제공하지만, 한편으로는 보안성, 신뢰성 이슈가 중요하게 부각되고 있다. 따라서, 하이브리드 클라우드 내에서도 클라우드 개체 간 신뢰관계 형성 문제에 관해 활발한 연구가 진행되고 있다. 각각의 클라우드 개체들은 성능이 향상됨에 따라 더 역동적으로 작동하는 반면, 기존에 형성된 관계는 차츰 느슨해지고 있기 때문에 보안 차원에서 개체 간 협력과 지속적인 신뢰관리가 반드시 필요하다. 그러므로 하이브리드 클라우드에서, 신뢰성이 없는 참여자들로부터 신뢰적인 참여자를 구분하기 위해 신뢰성 관리 시스템(Trust Management System)을 유지하는 것이 중요하다.

지금까지 알려진 대표적인 예로는 사용자가 각각의 클라우드 개체를 사용하고 나서 주관적으로 느낀 개인적인 경험(Personal Experience)과 평판(Reputation)을 데이터베이스로 관리 하는 방법이 있다. 이 데이터베이스를 기반으로, 사용자들이 작성한 피드백의 신뢰성을 계산하고 검증하기 위한 알고리즘을 활용함으로써 정직하지 않은 피드백을 사전에 필터링할 수 있다.

하지만 기존 시스템에서 클라우드 개체의 신뢰성을 검증하는 방법은 개인적인 피드백 데이터베이스를 기반으로 하기 때문에 매우 주관적이고 사용자에게 의존하는 경향이 있어, 피드백 간 유사성을 통해 부적합한 사례를 필터링하기에는 충분하지 않다. 기존의 신뢰성 검증 방법은 피드백을 구성하는 요소들이 근본적으로 충분히 객관적이지 않기 때문에 초기 데이터베이스 빌드 과정에서 악의적 의도에서 비롯된 피드백이 누적된다면 시스템이 무용지물이 될 수 있다. 신뢰성을 계산하는 파라미터에서 주관적 요소

를 최대한 배제하고 객관적 요소를 반영한다면 악의적이고 주관적인 공격을 방지할 수 있을 뿐 아니라 보다 향상된 신뢰성 검증이 가능해질 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 연구의 배경과 관련 기술 현황을 정리하고, 3장에서는 개선된 신뢰성 관리 프레임워크를 제안한다. 마지막으로 4장에서는 앞으로의 과제를 살펴보고 결론을 맺는다.

2. 관련 연구

2.1 배경과 용어 정의

지금부터 살펴보고자 하는 신뢰성 관리 시스템은 특정 클라우드 개체의 신뢰도를 평가함에 있어, 주로 신뢰성과 평판이라는 두 가지 척도를 활용한다.

우선 신뢰성(Trust)이란, 클라우드 개체가 주어진 시간에 특정한 상황에서 기대한 대로 행동한다는 확고한 믿음을 의미한다. 이는 보안 시스템에 대한 Confidence를 측정하는데 사용될 수 있다. 본 논문에서, 신뢰성은 두 피어 개체들 간의 신뢰 관계(Trust Relationship)의 형태로 명시한다. 즉, 이론적으로는 신뢰성을 판단하고 검증하는 주체를 각각의 피어들로 가정한다.

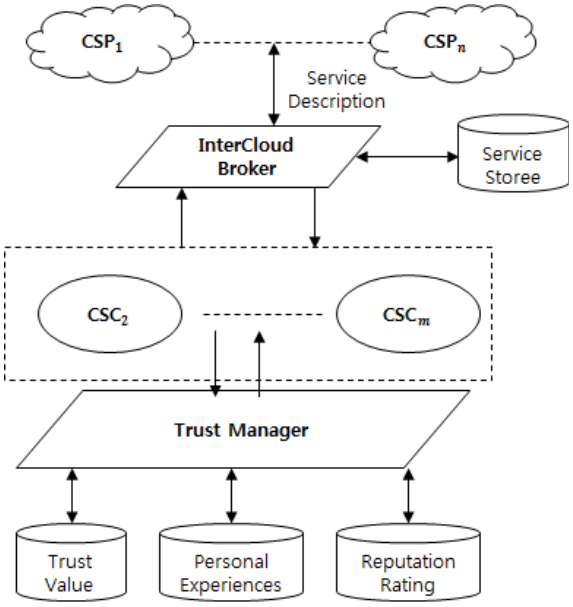
다음으로 평판(Reputation)이란 피어들이 사전에 상호작용하는 과정에서 얻어진 직접적, 간접적 지식으로부터 추리한 측정 단위이다. 이는 신뢰성의 단위로써 사용된다. 피어들이 그들의 과거 개인적 경험과 다른 피어들로부터의 피드백을 기반으로 하여 서로 간의 신뢰를 구축하도록 돕는다. 평판을 관리하는 것은 사용자와 서비스 제공자 간의 관계 구축 차원에서 리스크를 줄여 주는 중요한 역할을 한다.

기존의 클라우드 간 서비스 환경에서는 거래할 클라우드 서비스 제공자를 선택하는데 있어 자원 제공자의 능력, 정직도, 가용성, 서비스의 품질, 평판 등의 정보가 영향을 미쳤다. 하지만 어떤 자원을 사용할 것인가를 결정하는데 있어 충분한 정보가 주어지지 않는 경우가 많았다. 하이브리드 클라우드 서비스 관점에서는 클라우드 개체의 평판을 측정하고 유지하는 것이 필요하다. 이에 따라 클라우드 개체의 행동을 포착하고 능률적으로 저장할 수 있는 평판 관리자(Reputation Manager)를 새로이 만들 필요성이 생겨났다.

2.2 신뢰성 관리 프레임워크

(그림 1)은 기존의 신뢰성 관리 프레임워크를 나타낸다. 이때 자율적인 클라우드들의 전체집합(Universal Set)은 기호 $C_1, C_2, C_3, ..., C_n$으로 가정하고, 하이브리드 클라우드는 전체집합의 한 부분집합 $C = (C_1, C_2, C_3, ..., C_n)$으로 가정한다.

프레임워크 상에서 InterCloud Broker(ICB)는 피어들 간의 자원 교환을 중재하는 역할을 한다. 그리고 사용자(Cloud Service Customer, CSC)가 요구하는 자원을 제공



(그림 1) 기존 신뢰성 관리 프레임워크[1]

할 수 있는 적합한 클라우드 서비스 공급자(Cloud Service Provider, CSP)를 찾아서 선택하는 기능도 제공한다. 이 때 해당 서비스에 대한 정보를 담고 있는 Service Storee와 상호 작용함으로써, 서비스 명세를 업데이트하고 유지하는 역할도 한다.

신뢰성 관리자(Trust Manager)는 사용자가 클라우드 간 서비스를 사용할 때 최선의 자원을 선택할 수 있게 한다. 또한 사용자의 피드백을 얻고, 검증하고, 피드백 보관소에 값을 업데이트하는 역할을 함으로써 모든 다른 클라우드에 대한 평판 등급, 정직도 등급, 개인 경험 등급을 수집하고 유지한다. 등급 부여는 직접적인 관찰과 경험(예. first-hand information)에 근거하거나, 다른 개체들과 관찰과 경험을 공유함으로써 간접적으로 (예. second-hand information) 정해진다. 하지만 이론적으로 간접적인 상황은 고려하지 않기 때문에 클라우드 개체 $C_i \in A$(A는 임의의 하이브리드 클라우드)는 $C_j \in A$에 대해 자신에 겪은 first-hand information을 오직 $C_k \in A$와만 공유한다.

평판 관리자는 개체의 평판을 계산하기 위해 다음의 방식을 사용한다.

1) 개인적 경험(Personal Experiences)

개인적 경험 ($P_{i,j}$)는 $C_j \in A$와 거래 후, $C_i \in A$의 first-hand information을 나타낸다. 이는 $P_{i,j} = < k, S_{i,j} >$의 형태로 표현한다. ($S_{i,j}$: $C_j \in A$와 k^{th}번 거래한 품질을 근거로 한 $C_i \in A$의 개인적 만족도.) 개인적 만족도 측정은 지속적으로 이루어지며, [0, 1]의 값을 가진다. 0은 만족하지 못했음을, 1은 완벽히 만족했음을 의미한다.

2) 평판 등급(Reputation Rating)

평판 등급 ($R_{i,j}$)는 $C_i \in A$가 $C_j \in A$의 행동에 대해 좋은 서비스 제공자라고 판단한 일종의 Confidence를 나타낸다.

이 또한 개인적 경험과 비슷하게 [0, 1]의 값을 가지며, 제공되는 정보에 대해 0은 Confidence가 없음을, 1은 가장 높은 Confidence를 의미한다. 이 요소는 신뢰성 업데이트에 영향을 미치는데, Confidence가 낮고 설득력이 없는 정보(보고)는 그 내용이 긍정적이든 부정적이든 간에 신뢰성 업데이트에 오직 약한 영향만 미친다.

클라우드 개체는 때때로 그들의 개인적 경험 ($P_{i,j}$)를 사전 관계를 맺은 피어들 중 일부에게 등급의 형태로 배포한다. 이는 개인적 만족도 피드백 (f)의 형태로 공유된다. 반면 평판 등급 ($R_{i,j}$)은 개인적으로 보관되고 유지된다.

3. Trust Management 방식 개선

지금까지의 연구에서는 평판과 Confidence, 개인적 경험, 만족도 등의 상당히 주관적인 요소만을 가지고 0과 1 사이의 값을 임의로 매겨서 신뢰성을 판단하는 척도로 활용하였다. 이 방식은 전적으로 피어의 주관적인 판단에 의존하기 때문에, 악의적인 평가, 신뢰성에 대한 의구심을 비롯한 각종 부작용이 발생할 수 있다. 기존 논문에서는 각 클라우드 개체의 피드백을 신뢰적으로 저장하고 관리하기 위한 신뢰성 관리 프레임워크와 피드백 간 유사성 계산 알고리즘 등을 제안하였지만 신뢰성을 평가하는 방식 자체에 대한 근본적인 고찰은 미약한 수준이다. 위의 문제들은 근본적으로 신뢰성을 구성하는 요소들이 충분히 객관적이지 않기 때문에 발생하는 문제이며, 이것을 해결하기 위해 배경에서 언급한 서비스 제공자의 능력, 정직도, 가용성, 서비스의 품질 등과 같은 누구나 인정할 수 있는 객관적인 요소를 평가 기준으로 활용하기로 한다.

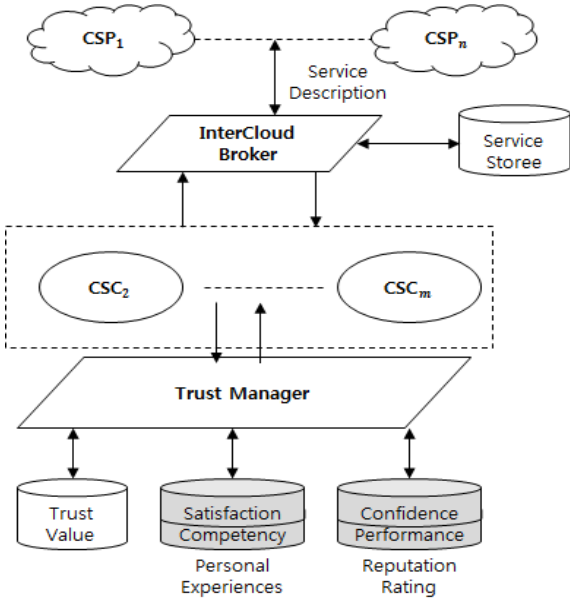
즉, 본 논문에서는 피드백을 구성하는 요소나 정보에서 주관적인 부분을 되도록이면 배제하고 객관적인 평가 요소를 최대한 도입하는 방향으로 개선한다. 전적으로 객관적인 평가에 의존하지 않는 이유는 앞으로 제시하려는 평가 기준이 해당 클라우드 서비스의 모든 성능, 역량, 성과 등의 복합적인 측면을 100% 완벽하게 반영할 수는 없기 때문이며, 나머지 부분에 대해서는 사용자의 주관적 판단을 어느 정도 존중할 필요성이 있기 때문이다.

3.1 신뢰성 관리 프레임워크 개선

본 논문에서는 기존 신뢰성 관리 프레임워크의 신뢰성 평가 방식을 개선한 프레임워크를 제안한다. (그림 2)는 개선된 신뢰성 관리 프레임워크를 나타낸 그림으로써 신뢰성 관리자가 지속적으로 관리하는 3개의 데이터베이스 중 Personal Experiences와 Reputation Rating 두 개의 데이터베이스를 Satisfaction과 Competency, Confidence와 Performance로 각각 세분화 시킨다. 각각의 요소에 대한 세부적인 기능 및 역할은 다음과 같다.

1) 개인적 경험(Personal Experiences)

$C_j \in A$와 거래 후 $C_i \in A$의 first-hand information을 기



(그림 2) 개선된 신뢰성 관리 프레임워크

존과 같이 $P_{i,j} = < k, S_{i,j} >$의 형태로 표현하되, 주관적 만족도는 절반인 [0, 0.5]의 값을 가진다. (0은 만족하지 못했음을, 0.5는 완벽히 만족했음을 의미한다.) 나머지 절반의 값은 해당 클라우드 개체의 객관적인 신뢰성 역량(Competency)을 측정하여 결정한다. 이를 위해 ISO 7498-2 standard에서 규정한 정보 보안 요구사항을 얼마나 철저하게 준수했는가를 세부적으로 검증하고 이를 수치적인 값으로 계산한다[2].

- 사용자 식별 인증(Identification & Authentication): 명시된 유저만 우선적으로 서비스 접속이 가능해야 한다. 유저에 대한 인증은 Username과 Password 보안으로써 검증한다.
- 권한(Authorization): 참조 무결성이 유지되는지 검증한다. 클라우드 내에서 프로세스 흐름의 범위를 넘어서는 제어 혹은 권한이 남용되는지 추적되어야 한다.
- 기밀성(Confidentiality): 사용자 프로필의 기밀성을 확고히 하고 데이터를 보호해야 한다. 이를 위해 클라우드 애플리케이션의 각 레이어에서 정보 보안 프로토콜 적용을 고려한다.
- 무결성(Integrity): 클라우드 데이터의 ACID(원자성, 일관성, 고립성, 영속성)가 확고하게 지켜져야 한다.
- 부인방지(Non-repudiation): 클라우드 애플리케이션 내에서 전통적인 전자상거래 보안 프로토콜과 데이터 전송 토큰을 적용하여 부인을 방지한다. 디지털 서명, 타임스탬프, 확인 영수증 서비스 등의 검증 방법이 있다.
- 가용성(Availability): 클라우드 서비스 이용을 원할 때는 언제든지 항상 사용가능해야 한다. 이것은 클라우드 서비스 제공자를 선택함에 있어 가장 중요한 의사결정 요소이다.

위 6개의 요소에 대해 각각 [0, 1] 사이의 값을 매겨 객관적으로 평가하고 이를 합산 후 [0, 0.5]의 값으로 조정한다. 이 때 <표 1>에서 나타난 서비스 모델 별 필수, 옵션 요구사항을 고려하여 조정한다. 앞에서 계산된 주관적 만족도와 객관적인 역량 점수를 합산하여 최종 피드백 점수 [0, 1]을 도출한다.

<표 1> 하이브리드 클라우드 보안 요구사항[3]

Information Security Requirements	IAAS	SAAS	PAAS
Identification & Authentication	*	X	*
Authorization	*	X	*
Confidentiality	*	X	*
Integrity	X	X	X
Non-repudiation	*	*	*
Availability	*	*	*

(X = 필수 요구사항, * = 옵션 요구사항)

2) 평판 등급(Reputation Rating)

평판 등급 ($R_{i,j}$)는 $C_i \in A$가 $C_j \in A$의 행동에 대해 좋은 서비스 제공자라고 판단한 Confidence를 표현하며, 이 또한 주관적인 요소로서 [0, 0.5] 사이의 값을 가진다. (제공되는 정보에 대해 0은 Confidence가 없음을, 0.5는 가장 높은 Confidence를 의미한다.) 나머지 절반의 값은 해당 클라우드 개체가 현재까지 제공한 서비스의 결과 및 성과(Performance)를 측정하여 결정한다. 비슷한 방식으로 Gartner에서 강조한 클라우드 보안 위협에 대한 메인 이슈[4]를 그동안 올바르게 이행했는지에 대해 검증하고 이를 수치적인 값으로 계산한다.

- 규제 준수(Regulatory compliance): 외부 감사/보안 인증을 적극적으로 받으려 했는가?
- 데이터 위치(Data location): 벤더가 데이터의 위치에 대한 통제권을 허가했는가?
- 데이터 분리(Data segregation): 모든 단계에서 암호화가 가능했는가?
- 복구(Recovery): 재난 등의 상황에서 벤더가 완벽한 복구를 제공했는가? 해당 프로세스가 얼마나 걸렸는가?
- 조사 지원(Investigative Support): 벤더가 부적절하거나 위법적인 행동에 대해 조사할 능력을 가졌는가?
- 데이터 가용성(Data availability): 현재의 환경이 타협되거나 불가능해지면 벤더가 고객의 모든 데이터를 다른 환경에 이전할 수 있는가?

마찬가지로 위 6개의 요소에 대해 각각 [0, 1] 사이의 값을 매겨 객관적으로 평가하고 이를 합산 후 [0, 0.5]의 값으로 조정한다. 앞에서 계산된 주관적 Confidence와 객관적인 성과 점수를 합산하여 최종 평판 등급 [0, 1]을 도출한다.

3.2 성능 평가

기존의 신뢰성 관리 프레임워크가 평가 방식 측면에서 Personal Experiences와 Reputation Rating의 두 가지 주관적 기준을 통해서 이뤄졌다면, 개선된 평가 방식에서는 두 개의 기준이 Satisfaction과 Competency, Confidence와 Performance로 각각 세분화되어 주관적 비율 50%, 객관적 비율 50%의 조화된 평가가 가능해졌다. 객관적인 평가에는 국제 기준(ISO) 및 리서치기관(Gartner)의 검증된 기준이 적용되어 해당 클라우드 개체의 다면적인 역량과 성과를 올바르게 평가할 수 있도록 개선되었다.

4. 결론

본 논문에서, 우리는 하이브리드 클라우드 상에서 기존의 Reputation 기반 Trust Management 방식의 문제점에 주목했다. 신뢰성이라는 가치를 판단하는 근거가 매우 주관적이었기 때문에 단순히 부적합한 피드백을 걸러내는 것만으로는 근본적인 문제를 해결할 수 없었다. 이를 해결하기 위해 신뢰성 수치(Trust Value)를 계산하기 위한 각종 요소(파라미터)에 최대한 객관적인 기준을 적용함으로써 개선점을 이루어냈다. 이렇게 계산된 수치는 특정 클라우드 개체의 신뢰 가치를 판단함에 있어 보다 객관적이고 효율적인 의사 결정을 가능하게 할 것이다. 또한 기존에 문제가 되었던 악의적인 피드백 남용에 대해서도 주관적 평가 비율을 절반으로 낮춤으로써 사전에 방지할 수 있는 장치를 마련하게 되었다.

시간이 지남에 따라 클라우드에 대한 기업들의 보안 요구사항 변화와 각종 보안 이슈, 사고 등의 영향으로 '신뢰성, 평판' 등의 개념과 가치는 얼마든지 변할 수 있다. 향후에는 이러한 변화를 객관적으로, 그리고 효과적으로 인지하고 시스템 상에 계속해서 반영시키는 방향으로 연구를 진행하겠다.

참고문헌

[1] Jemal Abawajy, "Establishing Trust in Hybrid Cloud Computing Environments", *IEEE TrustCom-11*, 2011. 11

[2] ISO. ISO 7498-2:1989. *Information processing systems- Open Systems Interconnection.* ISO 7498-2

[3] Ramgovind S 외 2명, "The Management of Security in Cloud Computing", *ISSA-2010*, 2010. 08

[4] Brodkin J, "Gartner: Seven cloud-computing security risks", *Infoworld*, 2008. 07