Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.2, Apr. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.2.315

가상머신 마이그레이션을 위한 OTP 기반 동적인증 프레임워크*

이 은 지,[1†] 박 춘 식,[2] 곽 진[3‡]
[1]아주대학교 컴퓨터공학과 정보보호응용및보증연구실
[2]서울여자대학교, [3]아주대학교 사이버보안학과

OTP-Based Dynamic Authentication Framework for Virtual Machine Migration*

Eun-Ji Lee,[1†] Choon-Sik Park,[2] Jin Kwak[3‡]
[1]ISAA Lab., Department of Computer Engineering, Ajou University
[2]Seoul Women's University
[3]Department of Cyber Security, Ajou University

요 약

가상머신 마이그레이션 과정에서 무단 접근, 데이터 변조 등의 보안 위협이 발생할 수 있다. 특히, 가상머신 마이그레이션은 사용자의 주요 데이터 및 중요 인프라 정보를 전송해야하기 때문에 해당 보안 위협이 발생할 경우 다른 클라우드 서비스에 비교적 위험성이 높다. 이러한 이유로 최근 가상머신 마이그레이션을 위한 동적인증의 필요성이 제기되고 있다. 이에 따라, 본 논문은 기존의 가상머신 마이그레이션을 위한 인증 기법의 취약점을 개선하기 위해 OTP 기반의 동적인증 프레임워크를 제안한다. 이는 가상머신 마이그레이션 요청 모듈 및 동작 모듈로 구성된다. 요청 모듈에서는 사용자가 마이그레이션 요청 시 OTP 기반의 사용자의 인증 과정 및 데이터 센터로의 마이그레이션 요청 과정을 포함한다. 동작 모듈에서는 SPEKE을 이용한 데이터 센터 간 안전한 키 교환 과정과 데이터 센터와 물리 서버 간 TOTP 기반의 상호인증 과정을 포함한다.

ABSTRACT

Security threats such as unauthorized access and data tampering can occur during the virtual machine migration process. In particular, since virtual machine migration requires users to transfer important data and infrastructure information, it is relatively risky to other cloud services in case of security threats. For this reason, there is a need for dynamic authentication for virtual machine migration. Therefore, this paper proposes an OTP-based dynamic authentication framework to improve the vulnerabilities of the existing authentication mechanism for virtual machine migration. It consists of a virtual machine migration request module and an operation module. The request module includes an OTP-based user authentication process and a migration request process to a data center when a user requests a migration. The operation module includes a secure key exchange process between the data centers using SPEKE and a TOTP-based mutual authentication process between the data center and the physical server.

Keywords: Virtual Machine Migration, Dynamic Authentication, OTP, Security

Received(02. 27. 2017), Modified(03. 27. 2017), Accepted(03. 27. 2017)

* 이 논문은 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.NRF-2014R1A2A1A11050818).

† 주저자, heo160@ajou.ac.kr
‡ 교신저자, security@ajou.ac.kr(Corresponding author)

I. 서 론

가상머신 마이그레이션은 서버 통합, 위협에 따른 시스템 복구 등을 목적으로 물리 서버의 가상머신을 다른 물리 서버로 복제하는 기술이다. 가상머신 내 운영체제 전체를 다른 위치로 전송하는 과정에서 암호화되지 않은 데이터로부터 사용자 정보, 비밀키 등의 주요정보를 노출 시킬 수 있다[1]. 또한, 권한 없는 마이그레이션은 공격자로부터 공격자의 제어권 내 위치로 마이그레이션 되는 등의 보안 문제가 발생 할 수 있다[2].

이러한 보안 문제는 가상머신 마이그레이션 과정에서의 무단 접근, 데이터 탈취 및 변조, 사용자 권한 탈취 등의 보안 위협에 의해 발생된다. 이에 따라, 해당 보안 위협 방지를 목적으로 안전한 가상머신 마이그레이션을 위한 인증 방안 연구가 활발히 진행되고 있다.

이때, 기존의 인증 기법은 사용자의 계정 패스워드를 통해 언제든 마이그레이션이 가능하기 때문에 로그인 된 상태에서 누구나 접근하기 쉽다. 또한, 공격자가 계정만 탈취하면 여러 세션에 걸쳐 마이그레이션 요청이 가능하다. 하지만, 가상머신 마이그레이션은 사용자의 주요 데이터 및 중요 인프라 정보를 전송해야하기 때문에[2] 해당 보안 위협이 발생할 경우 다른 클라우드 서비스에 비해 비교적 위험성이 높다. 최근, 이러한 이유로 가상머신 마이그레이션을 위한 동적인증 방안의 필요성이 제기 되고 있다.

그 예로, CH. Venkateswara Rao 등[3]은 클라우드 환경에서 사용자 자격증명의 손상을 줄이기 위한 OTP(One Time Password) 기반의 안전한 데이터 공유 방안을 제안하였다. 또한, Wei Peng 등[4]은 클라우드 인프라 보호를 위한 마이그레이션 MTD(Moving Target Defence)기술을 제안하였으며, 마이그레이션 기술 보호를 위한 동적인증 기술의 제안과 함께 그 필요성을 제기한 바 있다.

이에 따라, 본 논문은 안전한 가상머신 마이그레이션을 위한 OTP 기반의 동적인증 프레임워크를 제안한다. 이는 기존 마이그레이션을 위한 인증 기법을 개선하여 마이그레이션 요청 시 사용자의 동적인증 및 데이터 센터와 물리 서버 간 세션 보호를 위한 동적인증을 포함한다. 더불어, 기존 가상머신 마이그레이션의 키 교환 방식에서 발생할 수 있는 취약점을 분석하고 이를 개선하기 위한 방안을 도입한다.

본 논문의 구성은 다음과 같다. 2장에서 기존 가상머신 마이그레이션 기법의 취약점과 OTP 기반의 동적인증 기술을 분석한다. 3장에서는 마이그레이션 과정에서 인증 기법을 도입하기 위해 기존에 연구된 아키텍처들을 바탕으로 가상머신 마이그레이션 아키텍처를 재 정의한다. 4장에서 앞서 분석한 내용들을 통해 도출된 고려사항을 기반으로 OTP 기반의 동적인증 프레임워크를 제안한다. 더불어, 기존 기법들과 안전성을 비교 및 분석하며, 5장에서 결론을 맺는다.

II. 관련연구

2.1 기존 마이그레이션을 위한 인증 기법

CH. Venkateswara Rao 등[3]은 클라우드가 분산 컴퓨팅 기술을 기반으로 하는 특성에 따라 데이터 공유 과정에서 발생 가능한 보안위협을 제기하였다. 이러한 이유로 사용자의 자격 증명 손상을 줄이기 위해 OTP 기반의 PAKE 프로토콜을 포함한 동적인증 시스템을 제안하였다. 이에 따라, 마이그레이션 과정 중 보안적 측면에서 우선적으로 고려해야하는 데이터 공유 과정에서 동적인증이 필요하다.

또한, Wei Peng 등[4]은 마이그레이션에 대한 무단 접근 및 데이터 변조로부터 가상머신의 파일 시스템 이미지를 읽어들일 수 있는 등의 심각한 보안위협이 발생 가능함을 제시하였다. 이러한 보안위협으로부터 마이그레이션 과정에서 동적인증의 필요성을 제기하였다. 이에 따라, 본 절은 기존 마이그레이션을 위한 인증 연구에서 동적인증을 포함하지 않음으로써 발생 가능한 보안위협을 분석한다.

2.1.1 Santosh Kumar Majhi 등[6]의 인증 기법

Santosh Kumar Majhi 등[6]은 기존의 알려진 인증 기법을 통한 가상머신 마이그레이션 프로세스의 인증 프레임워크를 제안하였다. 해당 프레임워크는 인증 모듈, 마이그레이션 관리 모듈, 마이그레이션 분석 및 모니터링 모듈인 3가지 모듈로 구성된다. 이때, 인증 모듈은 마이그레이션이 시작되기 전 Diffie-Hellman과 같은 기존의 방식을 이용해 물리 머신(PM)과 데이터 센터(DC) 간 상호인증 기능을 포함한다.

해당 인증 프로토콜은 PM 및 DC가 각각 계산한 g^x, g^y를 서로의 공개키로 암호화하여 전송하고, 각각의 개인키로 복호화 하여 확인함으로써 상호인증이

가능하다. 하지만, 마이그레이션 요청 시 사용자 인증의 과정을 포함하지 않기 때문에 사용자가 클라우드 서버에 로그인한 상태일 경우 공격자가 사용자 PC에 접근하여 원할 때 마다 마이그레이션을 요청할 수 있다. 이에 따라, 마이그레이션 요청 시 추가적인 사용자 인증단계를 도입할 필요가 있으며 사용자 인증 시 새로운 인증 값이 사용되어야 한다.

2.1.2 Issa Khalil 등[9]의 인증 기법

Issa Khalil 등[9]은 인터 클라우드 환경에서 데이터를 안전하게 복사하고 이동하기 위한 데이터 마이그레이션 메커니즘을 제안하였다. 이는 사용자 데이터의 무결성과 기밀성을 보장하는 데이터 마이그레이션 프로토콜을 포함한다. 이때, 사용자(U)는 근원 클라우드(SC) 및 목적 클라우드(TC)에 대한 계정을 설정했다고 가정한다.

사용자 인증단계에서 사용자가 초기에 SC와 TC 각각에 로그인을 수행하고 대칭키 Kt를 생성한다. Kt는 계정 패스워드로 암호화되어 SC와 TC에 각각 전송된다. Kt는 SC와 TC 간 전송되는 메타 데이터 및 데이터 블록 접근권한의 확인을 위한 토큰을 암호화하는데 사용된다.

해당 프로토콜은 사용자의 동의 및 요청에 의해서만 마이그레이션이 가능하다. 또한, Kt는 메타 데이터 또는 토큰 확인을 통해 데이터 소유자가 마이그레이션을 가능하게 하는 TC 및 SC에 대한 인증 역할을 수행한다.

그러나, 데이터 마이그레이션을 위해 Kt를 알아야 하며, Kt는 초기 생성된 사용자의 계정 패스워드로 암호화 되어 전송된다. 따라서, 공격자가 사용자의 계정 패스워드를 탈취하면 한 번의 로그인을 통해 마이그레이션의 전 과정을 수행할 수 있다. 이에 따라, 공격자가 패스워드를 탈취하더라도 다른 세션에 참여하지 못하도록 세션 보호를 위한 방안을 마련해야한다.

2.1.3 Tayyaba Zeb 등[2]의 인증 기법

Tayyaba Zeb 등[2]은 인터 클라우드 환경에서 근원 클라우드 도메인(SCD)에서 목적 클라우드 도메인(TCD)으로의 가상머신 마이그레이션 과정에서 인증 및 허가된 마이그레이션을 제공하기 위한 아키텍처를 제안하였다.

SCD에서 인증서버와 관리자가 상호인증함으로써 관리자는 인증서버에서 마이그레이션 요청권한을 부여받는다. 더불어, 마이그레이션을 요청 및 응답 과정에서 접근제어를 제공함으로써 권한 없는 마이그레이션을 방지한다.

초기 관리자가 인증서버에 전송하는 인증 요청 메시지는 사용자 ID와 Nonce값의 연접으로, 암호화되지 않은 상태로 전송된다. 또한, 이에 대한 응답 메시지에도 사용자 ID를 이용해 만들어진 인증 티켓을 포함한다. 따라서, 공격자는 사용자 ID를 탈취하여 인증서버에 인증이 가능하며 이후 진행되는 마이그레이션 요청 및 마이그레이션 수행이 가능하다.

더불어, 마이그레이션 과정에서 전송되는 데이터 암호화는 타원곡선 Diffie-Hellman 방식을 통해 생성된 공유키를 이용한다. 하지만, Rakel Haakegaard 등[10]은 타원곡선 Diffie-Hellman 방식이 중간자 공격에 취약함을 밝혔다. 이는 키 교환 중 생성되는 공개키의 정적인 특징에 의해 발생하며, 이를 해결하기 위해 키 설정 과정마다 생성되는 임시키 사용의 필요성을 제기하였다.

2.2 동적인증 기술

동적인증은 공격자가 사용자의 권한을 탈취할 경우 해당 권한에 대한 유효성 상실 및 추가 사용을 금지 하도록 한다[3]. 이에 따라, 본 논문은 가상머신 마이그레이션 과정에서 사용자의 권한 및 세션 보호를 목적으로 OTP를 통한 동적인증 방안을 제안한다. 본 장은 기존의 OTP 기술 분석을 통해 본 논문에서 제안하는 동적인증 프레임워크의 안전성을 높이고, 제안하는 시스템 환경에 적합한 동적인증 기술을 모색한다.

2.2.1 OTP 기반 동적인증 기술

Jing-Chiou Liou[11]는 현재 사용 가능한 OTP 기반의 동적인증 기술을 연구하고 각 기술에 대한 안전성을 평가하였다. 해당 논문에서 설명하는 동적인증 기술은 다음과 같다.

- 보안 토큰

보안 토큰은 시간 동기화 및 이벤트 기반의 알고리즘을 기반으로 한다. 시간 동기화 알고리즘은 사전에 동기화된 시간 간격마다 의사난수 생성기를 통해 의사난수를 생성한다. 반면, 이벤트 기반 알고리즘은

사용자가 토큰 버튼을 누르는 등의 사용자 이벤트를 기반으로 OTP를 생성한다.

- 가상 토큰

가상 토큰은 USB 드라이브를 보안 토큰으로 사용하거나 SMS 기반의 경우 사용자가 입력한 자격증명을 통해 사용자 휴대폰에 OTP를 포함한 메시지가 전송되는 등 휴대용 저장 장치를 인증 토큰으로 활용 한다.

- 소프트웨어 토큰

소프트웨어 토큰은 서버에서 사용자 계정을 설정하면 사용자가 PIN을 입력함으로써 클라이언트 소프트웨어에 토큰 코드가 생성되는 등의 방식이다. 이를 통해 토큰 코드 기반의 OTP, 인증을 위한 암호화키 전송 등이 가능하다.

- GUI 인증 체계

GUI(Graphical User Authentication) 인증은 텍스트 대신 그래프와 같은 그래픽을 암호로 사용된다. 이는 사용자가 등록 단계에서 이전에 생성 또는 선택된 임의의 값을 복제하는 리콜 기반과 등록 단계에서 이전에 선택한 이미지를 식별하기 위해 임의의 이미지가 사용자에게 제공되는 인식 기반이 있다.

- SiFaDA

SiFaDA(Single-Factor Dynamic Authenti-cation)은 사용자가 입력한 자격증명을 통해 사용자 PC에서 선택한 바인딩 코드로부터 OTP를 생성한다. 생성된 OTP는 네트워크를 통해 서버에 전송하고, 서버는 동일한 바인딩 코드로 OTP를 계산하여 사용자로부터 받은 OTP와 일치 시킨다.

2.2.2 TOTP 기반 동적인증 프로토콜

Sheren A. El-Booz 등[12]은 TOTP(Time-bas-ed One-Time-Password)를 이용한 사용자 인증 및 ABP(Automatic Blocker Protocol)를 이용한 허가되지 않은 감사자 차단을 통해 안전한 클라우드 스토리지 시스템을 제안한다. 이때, TOTP는 공유된 비밀키로 부터 현재 시간에서의 OTP를 계산하는 알고리즘으로, 해당 논문에서는 사용자의 데이터 접근 단계에서 사용자와 클라우드 서버 간 하나의 세션에 대한 권한을 얻기 위해 TOTP를 사용한다.

사용자가 생성한 계정으로 클라우드 서버에 로그인을 시도하면 해당 계정이 관리자가 활성화 한 유효한 계정인지 확인한다. 확인이 되면 로그인 되고, 사용자는 TOTP를 입력하여 클라우드 서버의 데이터 파일에 접근 시도한다. 이때, 클라우드 서버에서 사용자가 입력한 TOTP가 확인 되면 사용자는 클라우드 서버의 데이터 파일에 접근권한을 얻는다. 이에 따른 사용자의 데이터 접근 알고리즘은 Fig.1.과 같다.

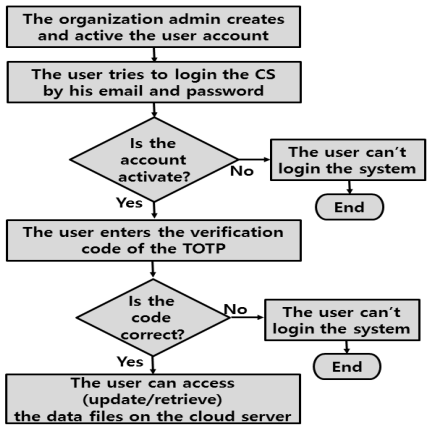

Fig. 1. User's data access algorithm

III. 가상머신 마이그레이션 아키텍처

최근 가상머신 마이그레이션의 효율성 및 안전성을 높이기 위한 가상머신 마이그레이션 아키텍처 연구가 활발히 진행되고 있다. 이때, 가상머신 마이그레이션 과정에서 인증이 필요한 구성을 확인하기 위해 아키텍처를 정의할 필요가 있다. 이에 따라, 기존의 연구된 내용[5,6,7,8]을 바탕으로 재정의한 가상머신 마이그레이션 아키텍처는 Fig.2.와 같고, 각 구성에 대한 설명은 아래와 같다.

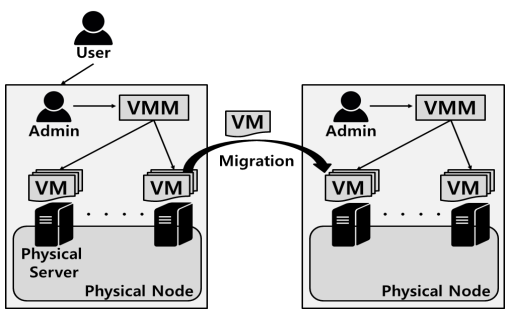

Fig. 2. Virtual Machine migration architecture

● 데이터 센터(Data Center)

데이터 센터는 서버, 스토리지, 네트워크, 물리 노드 등의 자원을 포함한 컨테이너로 데이터 센터 자원은 물리적 자원 과 가상 자원으로 분류된다. 클라우드 서비스 사용자에게 데이터 센터 자원이 할당되고, 사용자는 가상화 기술을 통해 동일한 하드웨어 자원을 공유한다.

● VMM(Virtual Machine Monitor)

VMM은 물리 노드에서 생성된 가상머신을 관리하는 하이퍼바이저 기술이다. 하이퍼바이저는 단일 하드웨어 자원을 통해 여러 OS의 구동 및 호스트 서버의 로컬 자원 모니터링을 담당한다.

● 물리 서버(Physical Server)

물리 노드는 서버가 가상 인스턴스를 실행하는 디스크를 갖는 노드로 스위치, 라우터 등의 네트워크 자원으로부터 물리 서버가 상호 연결되어있다. 각 데이터 센터에는 물리 노드를 통해 여러 물리 서버가 할당된다.

● 가상머신(Virtual Machine)

가상머신은 OS 및 응용프로그램을 실행하는 소프트웨어 컴퓨터로 데이터 센터에 프로비저닝 된다. 가상머신은 하이퍼바이저를 통해 물리 서버에 생성되며 동일한 물리 서버가 여러 가상머신을 실행할 수 있다.

● 관리자(Admin)

관리자는 여러 가상머신과 VMM에서 정보를 가져올 수 있으며, 사용자가 가상머신 마이그레이션을 요청하면 이를 결정한다.

가상머신 마이그레이션 요청을 위해 사용자가 데이터 센터에 접근해야 한다. 이 과정에서 관리자를 통해 데이터 센터는 사용자를 인증해야한다. 또한, 마이그레이션 요청은 사용자가 지정한 데이터 센터 내 VMM을 통해 가상머신 마이그레이션이 필요한 물리 서버에 전달된다. 이때, 본 논문에서 정의한 아키텍처는 데이터 센터 게이트웨이와 물리 서버 게이트웨이를 갖는 VMM을 통해 데이터 센터와 물리 서버 간 수행하며[6], 데이터 센터와 물리 서버 상호 인증이 필요하다.

더불어, 근원 데이터 센터의 물리 서버와 마이그레이션 할 목적 데이터 센터의 물리 서버 간 안전한 데이터 전송이 필요하다. 이는 근원 데이터 센터와 목적 데이터 센터 간 공유되는 세션키를 통해 데이터를 암호화함으로써 가능하다. 따라서 근원 및 목적 데이터 센터 간 안전한 세션키 생성 및 공유가 이뤄져야한다.

IV. 제안 기법

본 논문은 안전한 가상머신 마이그레이션을 위한 OTP 기반 동적인증 프레임워크를 제안한다. 이는 Tayyaba Zeb 등[2]에서 제안한 인증 프로토콜을 기반으로 2.1장에서 기존 인증 기법[2,6,9]을 분석하여 도출된 취약점을 개선한 프로토콜을 포함한다. 이에 앞서 본 논문에서 제안하는 인증 프로토콜의 기능 및 동작을 고려하여, 3장에서 가상머신 마이그레이션 아키텍처를 재구성 및 정의하였다.

4.1 고려 사항

4.1.1 개선 사항

OTP 기반의 동적인증은 짧은 세션동안 고유한 사용자의 자격을 증명한다. 공격자가 이러한 사용자의 자격을 얻는 경우 해당 자격은 더 이상 유효하지 않다. 더불어, OTP 기반의 동적인증을 통해 일회성 지식을 기반으로한 강력한 상호인증이 가능하다[3]. 따라서, 세션 보호, 사용자 자격 증명 및 강력한 상호인증이 필요한 과정에서 OPT 기반 동적인증이 사용될 수 있다.

2.1장에서 기존 마이그레이션을 위한 인증 기법을 분석한 결과와 동적인증의 필요성에 따라, 가상머신 마이그레이션의 인증 과정에서 동적인증을 도입함으로써 추가적으로 개선되어야할 사항은 다음과 같다.

첫째로, 요청 시 별도의 사용자 인증 과정이 추가적으로 필요하다. 둘째로, 마이그레이션 과정에서 사용자 인증이 필요할 때마다 새로운 인증 값을 도입할 필요가 있다. 셋째로, 마이그레이션이 요청되면 근원 물리 서버와 목적 물리 서버가 세션마다 새로운 인증 값을 통해 상호인증이 필요하다. 마지막으로, 마이그레이션 과정에서 전송되는 데이터의 기밀성 보장을 위한 세션키는 안전하게 교환되어야 한다.

4.1.2 제안하는 프레임워크에 적합한 OTP 기술

2.2.1장에서 분석한 OPT 기반 동적인증 기술을 분석한 결과에 따라[3] GUI는 모바일 장치에 적합한 기술로, 제안하는 시스템에는 적합하지 않다. 또한, 본 논문은 마이그레이션 서비스의 매 요청마다 새로운 인증 값을 통해 사용자를 인증하는 방안을 목표로하기 때문에 사용자 계정을 필요로 하는 소프트웨어 토큰은 적합하지 않다.

이에 따라, 본 논문에서 제안하는 사용자 인증단계에는 사용자의 계정 패스워드를 필요로 하지 않고, 기존의 PC 환경에 적합한 보안 토큰, 가상 토큰, SiFaDA 등의 동적인증 기술이 사용될 수 있다.

4.1.3 TOTP 기반 상호인증

2.2.2장에서 분석한 TOTP 프로토콜 및 TOTP 생성 방안에 따라, 본 논문에서는 물리 서버와 데이터 센터 간 세션키를 공유하기 전 상호인증 과정에서 TOTP 기술을 적용한다. 물리적 장치 간 이벤트 기반의 인증 방식은 한계가 있기 때문에, 타임스탬프를 이용해 상호 연산한 값을 OTP로 사용하는 시간 기반의 OTP를 사용한다. 물리 서버와 데이터 센터 간 상호인증에 사용되는 TOTP는 한 세션 동안만 사용 가능하도록 함으로써, 세션 보호를 목적으로 한다.

4.2 제안하는 동적인증 프레임워크

본 논문에서 제안하는 가상머신 마이그레이션을 위한 OTP 기반 동적인증 프레임워크는 가상머신 마이그레이션 요청 모듈 및 가상머신 마이그레이션 동작 모듈로 구성된다.

가상머신 마이그레이션 요청 모듈은 물리 서버 간 가상머신이 마이그레이션되기 전 단계인 마이그레이션을 위한 사용자 인증 단계와 데이터 센터 간 인증 요청 및 응답 단계를 포함한다. 해당 모듈은 세부 모듈인 사용자 동적인증 모듈과 마이그레이션 요청 모듈로 구성된다.

가상머신 마이그레이션 동작 단계는 가상머신 마이그레이션 요청 단계를 통해 근원 및 목적 데이터 센터 간 권한있는 마이그레이션이 가능하게 된 후 실제 마이그레이션의 동작 단계를 포함한다.

제안하는 프레임워크는 Fig.3.과 같고, 각 구성의 기능과 동작은 아래와 같다.

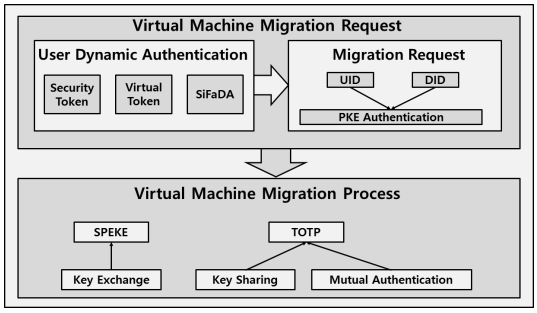

Fig. 3. Proposed OTP-based dynamic authentication framework

4.3 동적인증 프레임워크 기능 및 동작

4.3.1 가상머신 마이그레이션 요청 모듈

가상머신 마이그레이션 요청 모듈 내 세부 모듈인 사용자 동적인증 모듈은 사용자가 마이그레이션 요청 시 OTP 기반의 동적인증을 통해 사용자를 인증한다. 이때 사용되는 OTP 기술은 4.1.2장에서 분석 및 도출한 결과에 따라 보안 토큰, 가상 토큰, SiFaDA 등이 사용될 수 있다.

해당 세부 모듈을 통해 사용자가 인증되면 또 다른 세부 모듈인 마이그레이션 요청 모듈을 통해 데이터 센터 간 마이그레이션이 요청된다. 이 과정에서, 상대방 데이터 센터의 공개키로 암호화된 사용자 ID 및 데이터 센터 ID를 데이터 센터 각각의 개인키로 복호화하여 각 데이터 센터는 자신의 ID 및 사용자 ID를 확인한다. 이에 따라, 근원 및 목적 데이터 센터 간 인증이 가능하며, 마이그레이션을 요청한 사용자 확인이 가능하다.

따라서, 가상머신 마이그레이션 요청 모듈은

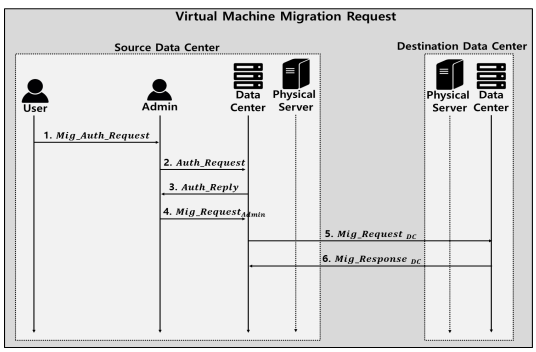

Fig. 4. Virtual machine migration request message exchange protocol

OTP 기반의 사용자 동적인증 단계와 공개키 기반의 데이터 센터 간 인증 및 마이그레이션 단계를 갖는 가상머신 마이그레이션 요청 메시지 교환 프로토콜을 포함한다. 해당 프로토콜은 Fig.4와 같으며, 각 단계별 설명은 아래와 같다.

이때, 각 데이터 센터는 인증기관에서 X.509와 같은 인증서를 발급받은 상태이며, 각 사용자는 마이그레이션 요청 시 데이터 센터의 인증서버에서 해당 OTP를 발급 받는다고 가정한다.

Step 1. 사용자 인증

1. 사용자는 가상머신 마이그레이션을 요청을 위한 사용자 인증을 위해 관리자에게 $Mig\_Auth\_Request$ 메시지를 전송한다. 이때 사용되는 UID는 사용자의 ID이다.

$$Mig\_Auth\_Request = [UID \| E_{OTP}(UID)] \quad (1)$$

2. 관리자는 암호화되지 않은 UID로 사용자를 확인하고 $Auth\_Request$ 메시지를 근원 데이터 센터에 전송한다. $nonce_1$는 관리자가 생성한 난수이고, K_1은 관리자와 근원 데이터 센터 간 사전에 보안 채널을 통해 교환된 대칭키이다.

$$Auth\_Request = [E_{OTP}(UID) \| E_{K_1}(nonce_1)] \quad (2)$$

3. 근원 데이터 센터는 $Auth_Request$에서 자신이 생성한 OTP로 복호화한 UID를 확인함으로써 사용자를 인증할 수 있다. 이후 $nonce_1$을 K_1로 복호화하고 관리자에게 $Auth\_Reply$ 메시지를 전송한다.

$$Auth\_Reply = [E_{K_1}(UID \| nonce_1)] \quad (3)$$

4. 관리자는 $Auth\_Reply$ 메시지를 K_1로 복호화하여 UID와 관리자가 생성했던 $nonce_1$을 얻음으로써 자신이 인증을 요청했던 근원 데이터 센터로부터 온 응답메시지임을 확인할 수 있다. 이로써, 근원 데이터 센터의 사용자 인증이 완료되고 관리자가 근원 데이터 센터로부터 $Auth\_Reply$ 메시지를 받으면 관리자는 근원 데이터 센터에 마이그레이션을 요청하기 위한 $Mig\_Request_{Admin}$ 메시지를 전송한다. 이때, $Dest_DID$는 목적 데이터 센터의 ID이다.

$$Mig\_Request_{Admin} = [E_{K_1}(Mig\_Rqst \| Dest\_DID \| UID)] \quad (4)$$

제안하는 사용자 인증 단계는 마이그레이션 요청 시 매번 OTP를 통해 사용자를 인증하는 단계를 추가함으로써 기존 가상머신 마이그레이션 인증 방식[2,6,9]을 개선하였다. 이는 공격자가 사용자 계정을 탈취하여 사용자의 시스템에 로그인하거나, 사용자 계정을 모르는 공격자가 로그인된 사용자의 시스템에 접근이 가능하더라도 사용자의 계정만으로 마이그레이션 서비스 요청이 불가하다.

Step 2. 데이터 센터 간 마이그레이션 요청

5. 근원 데이터 센터는 관리자로부터 받은 $Mig_Request_{Admin}$를 K_1로 복호화하여 관리자가 마이그레이션 하려는 $Dest_DID$를 확인한다. 이후, 해당 ID를 갖는 목적 데이터 센터에 $Mig\_Request_{DC}$ 메시지를 통해 가상머신 마이그레이션을 요청한다. 이때, Pb_{Dest_DC}는 목적 데이터 센터의 공개키이고, Src_DID는 근원 데이터 센터의 ID이며, $Cert_{Src_DC}$는 앞서 언급한 가정에 따라 인증기관에서 발급받은 근원 데이터 센터의 인증서이다.

$$Mig\_Request_{DC} = [E_{Pb_{Dest\_DC}}(Mig\_Rqst \| Src\_DID \| Dest\_DID \| UID) \| Cert_{Src\_DC}] \quad (5)$$

6. 목적 데이터 센터는 $Mig_Request_{DC}$를 받아 자신의 비밀키로 복호화한다. 복호화 된 값으로부터 자신의 $Dest_DID$를 확인하고, UID를 통해 사용자를 확인한다. 또한, $Cert_{Src_DC}$로 근원 데이터 센터의 자격증명 및 Src_DID로 응답 메시지를 보낼 근원 데이터 센터의 ID를 확인한다.

이후, 목적 데이터 센터는 가상머신 마이그레이션 응답 메시지인 $Mig_Response_{DC}$를 근원 데이터 센터에 전송한다. 해당 메시지에 사용되는 Pb_{Src_DC}는 근원 데이터 센터의 공개키이고, $Cert_{Dest_DC}$는 인증

기관에서 발급받은 목적 데이터 센터의 인증서이다. 더불어, 목적 데이터 센터의 비밀키 $\Pr_{Dest_DC}$로 확인 메시지 Ack와 $Dest_DID$를 서명한 서명 값을 포함함으로써 부인 봉쇄가 가능하다.

$$Mig\_Response_{DC} = [E_{Pb_{Src\_DC}}(Sin_{\Pr_{Dest\_DC}}(Dest\_DID \| Ack)) \| Cert_{Dest\_DC}] \quad (6)$$

$Mig_Response_{DC}$를 받은 근원 데이터 센터는 $Cert_{Src_DC}$를 통해 근원 데이터 센터의 자격증명을 확인한다. 또한, 자신의 비밀키로 복호화하여 얻은 서명 값을 목적 데이터 센터의 공개키를 통해 자신이 보낸 목적 데이터 센터의 ID가 맞는지 확인하고, Ack 메시지를 확인한다. 이로써, 두 데이터 센터 간 권한있는 마이그레이션이 가능하게 된다.

4.3.2 가상머신 마이그레이션 동작 모듈

가상머신 마이그레이션 동작 모듈은 근원 및 목적 데이터 센터 간 세션키 교환, 데이터 센터와 해당 물리 서버 간 세션키 공유, 데이터 센터와 해당 물리 서버 간 상호인증 기능을 포함한다. 세션키 교환은 기존의 마이그레이션 인증 시스템에서 사용되는 Diffie-Hellman 방식의 취약점인 중간자 공격을 개선한 SPEKE(Simple Password Exponential Key Exchange) 방식을 사용한다.

또한, 데이터 센터와 물리 서버 간 상호인증 및 세션키 공유에는 TOTP 기반의 동적인증 기술을 사용하며, 공유 된 세션키를 통해 데이터 전송 과정에서의 기밀성을 보장한다.

이에 따른 가상머신 마이그레이션 동작 메시지 전송 프로토콜은 Fig.5.와 같고, 각 단계별 설명은 아래와 같다.

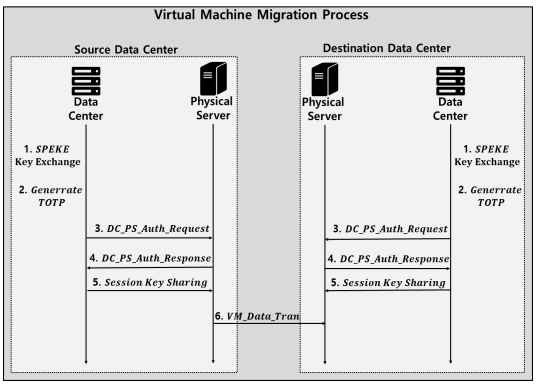

Fig. 5. Virtual machine migration process message exchange protocol

Step 1. 근원 및 목적 데이터 센터 간 세션키 교환

1. 근원 데이터 센터와 목적 데이터 센터 간 세션키 SK의 교환은 SPEKE 키 교환 방식으로 이루어지며, SPEKE에 따른 키 교환 동작은 Fig.6.과 같다[4].

SPEKE는 중간자 공격에 취약한 Diffie-Hellman을 변형한 알고리즘으로 IEEE P1363.2 및 ISO/IEC 11770-4 표준에 포함된 바 있다. Diffie-Hellman 키 교환 방식에서 생성기 g와 소수 p는 공개된 값이지만, SPEKE 방식에서 생성기 g는 비밀 값이며 일부 공유된 키 pw의 해쉬 값을 제곱하여 생성 된다. 근원 및 목적 데이터 센터 각각 생성한 비밀키, g 및 p로 계산된 공개키가 공격자에 의해 탈취되더라도 공격자는 비밀 값 g를 모르기 때문에 중간자 공격을 예방할 수 있다. 이에 따라, 기존의 마이그레이션 인증 시스템[2]에서 사용되는 Diffie-Hellman 방식 대신 SPEKE 방식을 사용하여 알려진 공격에 대해 안전성을 개선시킬 수 있다.

Step 2. 데이터 센터 및 물리 서버 간 상호인증

근원 및 목적 데이터 센터는 SPEKE를 통해 생

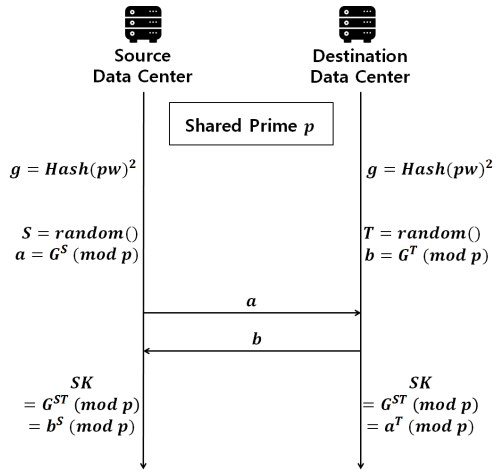

Fig. 6. SPEKE key exchange

성된 SK를 각각의 물리 서버와 공유해야 하며, SK 공유 전 데이터 센터와 물리 서버 간 상호인증과정이 필요하다. 본 논문은 TOTP 기반의 동적인증 기술을 이용하여 데이터 센터와 물리 서버 간 상호인증 및 세션키 공유 방안을 제안한다.

2. 데이터 센터와 물리 서버 간 상호인증은 TOTP 기반으로 이루어지며, 이는 Internet Engineering Task Force 표준 인 RFC 6238[1]로 채택된 바 있다. TOTP는 해쉬 함수를 이용해 비밀키와 타임스탬프를 결합시킴으로써 상호 간 시간 동기화된 OTP를 생성이 가능하다. RFC 6238 표준에 따른 TOTP 생성 과정은 아래와 같다.

TOTP는 타임스탬프가 카운터로 대체된 HOTP를 기반으로 생성되며, HOTP 알고리즘은 Fig.7.과 같다.

타임스탬프와 유닉스 시간인 epoch 시간의 시작 시간인 TO를 통한 TOPT를 계산하는 과정은 Fig.8.과 같다. 이때, d는 OTP의 원하는 자리수를 의미한다.

타임스탬프는 일반적으로 30초 간격으로 증가하므로 동일한 비밀키로 부터 시간에 따라 동일한 암호를 생성 할 수 있다. 사용자와 서버의 시간을 대략적으로 동기화 하기 위해 타임스탬프의 ±1시간 오차를 허용한다[1].

3. 근원 또는 목적 데이터 센터는 가상머신 마이그레이션 시킬 물리 서버에 인증 요청 메시지 $DC_PS_Auth_Request$를 보낸다. 이때, PID는 물리 서버의 ID이며, 근원 데이터 센터의 물리 서버인 경우 Src_PID, 목적 데이터 센터의 물리 서버인 경우 $Dest_PID$가 된다. 또한, $nonce_2$는 데이터 센터가 생성한 난수이다.

$$DC\_PS\_Auth\_Request = [E_{TOTP}(DID \| PID \| nonce_2)] \quad (7)$$

4. 물리 서버는 데이터 센터로 부터 받은 $DC_PS_Auth_Request$를 자신의 $TOTP$로 복호화 하여 자신의 PID를 확인함으로써 데이터 센터를 인증하고, 가상머신 마이그레이션을 지시한 DID 및 $nonce_2$를 확인한다. 이후, 물리 서버는 해당 DID를 갖는 데이터 센터에 응답 메시지 $DC_PS_Auth_Response$를 보낸다.

$$DC\_PS\_Auth\_Response = [E_{TOTP}(DID \| nonce_2)] \quad (8)$$

5. 데이터 센터는 자신의 $TOTP$로 $DC_PS_Auth_Response$를 복호화 하여 자신의 DID와 $nonce_2$를 확인함으로써 물리 서버를 인증한다. 데이터 센터는 상호인증 된 물리 서버에 $TOTP$로 SK를 암호화한 $E_{TOTP}(SK)$ 보내고, 물리 서버는 이를 자신의 $TOTP$로 복호화 하여 SK를 얻음으로써 데이터 센터와 물리 서버 간 세션키 공유가 이루어진다.

기존의 가상머신 마이그레이션 인증 방식[9]에서 상호 전송되는 데이터를 근원 및 목적 클라우드 간의 비밀키를 이용하여 기밀성을 제공하며, 비밀키는 사용자 로그인 계정 패스워드로 암호화 되어 분배한다. 이는 공격자가 사용자의 계정만 알면 마이그레이션의 전 과정에 관여할 수 있는 취약점을 갖는다.

이에 따라, 본 논문은 데이터 센터와 물리 서버 간 TOTP를 이용하여 상호인증 및 세션키 공유방안을 제안함으로써 세션 보호를 가능하게 하였다. 따라서, 이 과정에서 공격자가 TOTP 또는 인증과정에서 전달되는 메시지를 탈취하더라도 다음의 마이그레이션 과정에 해당 데이터들을 사용할 수 없도록 한다.

Step 3. 물리 서버 간 가상머신 데이터 전송

6. 근원 데이터 센터의 물리 서버는 SK로 암호화

1. K is a secret key
2. C is a counter
3. $HMAC(K,C) = SHA1(K \oplus 0x5c5c... \| SHA1(K \oplus 0x3636... \| C)$
4. $HOTP(K,C) = Truncate(HMAC(K,C))$ & 0x7FFFFFFF

Fig. 7. HOTP Algorithm

1. $TC = (time\,now - time(TO))/TS$
2. $TOTP$ is computed as follows:
   $TOTP = HOTP(\mathrm{secret}key(K), TC)$
   $TOTP\,value = TOTP \bmod 10^d$

Fig. 8. TOTP calculation process

된 가상머신의 데이터 VM_Data_Tran을 목적 데이터 센터의 물리 서버로 전송한다. 이때, VM_Data는 전송하고자 하는 실제 데이터이고, $Hash(VM_Data)$는 SHA와 같은 해쉬함수로 VM_Data를 해쉬한 값이다.

$$VM\_Data\_Tran = [E_{SK}(VM\_Data \| Hash(VM\_Data))] \quad (9)$$

7. 목적 데이터 센터의 물리 서버는 SK로 VM_Data_Tran을 복호화 하여 VM_Data를 얻는다. 더불어, 근원 데이터 센터 물리 서버와 동일한 해쉬함수로 VM_Data를 해쉬하여 해쉬 값을 얻고, 계산한 해쉬 값과 근원 데이터 센터 물리 서버로부터 전달받은 해쉬 값을 비교함으로써 데이터에 대한 무결성을 확인 할 수 있다.

4.4 안전성 분석

본 논문은 2.1장에서 분석한 기존 마이그레이션을 위한 인증 기법[2,6,9]에서 분석한 안전성을 토대로 제안하는 동적인증 프레임워크에 적용하여 비교 및 분석한다. 더불어, 2.2.2장에서 언급한 Sheren A. El-Booz 등[5]의 TOTP 기반의 동적인증 기법에 따른 안전성 또한 적용하여 분석하였다.

결과적으로, 제안하는 동적인증 프레임워크는 기존의 마이그레이션을 위한 인증 방식이 만족하는 안전성을 모두 만족한다. 더불어, 동적인증 기술의 도입을 통해 동적인증이 갖는 추가적인 안전성을 만족할 수 있다. 이에 따라, 제안하는 OTP 기반 동적인증 프레임워크가 만족하는 안전성은 아래와 같다.

● 상호인증

물리 서버와 데이터 센터는 각각 생성한 TOTP를 이용해 물리 서버의 PID 및 데이터 센터가 생성한 $nance_2$를 상호 암호화하여 전송하고, 복호화 하여 해당 값을 확인함으로써 상호인증이 가능하다.

● 재생 공격 방지

인증 과정에서 OTP 및 TOTP를 사용하여 암호화된 메시지를 전송함으로써, 공격자가 인증과정에서 전송되는 메시지를 탈취하더라도 세션마다 암호화 및 복호화하는 키가 다르기 때문에 재생 공격이 불가능하다.

● 기밀성

마이그레이션 과정에서 근원 물리 서버와 대상 물리 서버간 전송되는 데이터는 SPEKE 알고리즘으로 생성 및 교환된 세션키 SK를 통해 암호화 되어 전송된다. 따라서, 공격자가 전송되는 데이터를 탈취하더라도 암호화된 데이터를 해독할 수 없으며, 이를 통해 기밀성을 보장할 수 있다.

● 무결성

마이그레이션 과정에서 전송되는 데이터는 해쉬함수로 암호화된 값과 함께 SK로 암호화 되어 전송된다. 대상 물리 서버는 동일한 SK로 복호화 하여 해당 데이터를 해쉬 하고, 이를 받은 해쉬 값과 비교함으로써 데이터에 대한 무결성을 보장할 수 있다.

● 중간자 공격 방지

일반적으로 마이그레이션을 위해 근원지와 목적지 서버 간 세션키 공유는 Diffie-Hellman 키 교환 알고리즘을 이용한다. 이는 Diffie-Hellman의 알려진 취약점에 의해 중간자 공격에 취약하다.

본 논문은 근원 물리 서버와 대상 물리 서버 간 SK를 공유 과정에서 중간자 공격에 강하도록 Diffie-Hellman을 변형한 알고리즘인 SPEKE 도입함으로써 중간자 공격을 막을 수 있다.

● 계정 도용 방지

공격자는 사용자의 계정을 도용하여 클라우드 서비스에 대한 권한 탈취를 시도한다. 이때, 사용자가 마이그레이션 서비스를 요청할 때 마다 인증서버로부터 부여받은 OTP를 이용해 인증함으로써 막을 수 있다. 이는 공격자가 사용자 계정을 탈취하여 로그인을 하더라도 마이그레이션 서비스를 이용하지 못하도록 한다.

● 세션 보호

마이그레이션은 근원 물리 서버의 VM이 다른 물리 서버의 VM으로 복제되는 과정으로, 물리 서버에 대한 인증이 필요하다. 이때, 제안하는 프로토콜은 사용자가 접근 및 마이그레이션을 요청한 데이터 센터에서 해당 물리 서버를 인증하는 과정을 포함한다.

이때, 공격자가 기존의 탈취한 TOTP 또는 인증과정에서의 메시지를 탈취하여 하더라도 TOTP는 물리 서버와 데이터 센터 간 한 세션 동안만 사용이 가능하므로 세션을 보호할 수 있다.

Table. 1.은 앞서 분석한 기존 가상머신 마이그레이션 인증 방안[2,6,9]과 본 논문에서 제안하는 방안이 각각 만족하는 안전성을 분석한 표이다. 해당 안전성을 제공하는 경우 '○'로 표기하며, 제공하지 않는 경우 '×'로 표기한다. 단, 안전성 제공의 여부를 확인 불가한 경우 '-'로 표기한다.

Table. 1. Security comparison and analysis result

	[2]	[6]	[9]	proposed technique
Mutual Authentication	○	○	×	○
Prevention of Replay Attack	○	○	○	○
Confidentiality	○	○	○	○
Integrity	○	○	○	○
Prevention of Man-in-the-middle Attack	×	-	○	○
Prevention of Account hijacking	×	×	×	○
Session protection	×	×	×	○

V. 결 론

본 논문은 기존의 가상머신 마이그레이션을 위한 인증 방식의 취약점과 현재 사용 가능한 OTP 기반의 동적인증 기술을 분석하였다. 이를 통해 기존의 취약점을 개선하여 안전한 가상머신 마이그레이션을 위한 OTP 기반의 동적인증 프레임워크를 제안하였다. 제안한 프레임워크는 가상머신 마이그레이션을 요청하는 사용자에 대한 동적인증과 데이터 센터와 물리 서버 간 TOTP 기반의 상호인증 프로토콜을 포함한다. 더불어, 마이그레이션의 세션키 교환 과정에서 발생하는 취약점을 분석하고 이를 개선하기 위한 방안을 모색하였다. 또한, 제안한 방안에 대하여 기존 방안과 안전성을 비교 분석 함으로써, 기존 방안 보다 높은 안전성을 갖음을 보였다.

최근 클라우드 서비스 사용자가 급증함에 따라 사용자의 프라이버시와 같은 사용자 데이터 보호의 중요성이 대두되고 있다. 이러한 이유로 사용자의 주요 데이터 및 중요 인프라를 이동해야하는 마이그레이션 과정에서 발생하는 무단 접근과 같은 보안 위협은 사용자에게 치명적일 수 있다. 따라서, 안전한 마이그레이션을 위한 강력한 인증 기술이 필요하다. 이에 따라, 본 논문에서 제안하는 동적인증 방안의 개선 및 강화된 안전성을 고려하여 추후 안전한 마이그레이션을 위한 인증 기술 개발에 활용될 것으로 기대한다.

References

[1] Devi, Y., Aruna, P., Sudha, D. "Security in virtual machine live migration for KVM" International Conference on Process Automation, Control and Computing (PACC), Aug. 2011

[2] Tayyaba Zeb, Abdul Ghafoor, Awais Shibli, Muhammad Yousaf, "A Secure Architecture for Inter-cloud Virtual Machine Migration", International Conference on Security and Privacy in Communication Networks Volume 152 of the series Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp.24-35, Nov. 2015

[3] CH. Venkateswara Rao, G. Varaprasad Rao, "Dynamic Authentication for Data Sharing in Multiple Clouds ", International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), Volume 1, pp.6-11, Nov. 2014

[4] Wei Peng, Feng Li, and Xukai Zou, "Moving Target Defense for Cloud Infrastructures: Lessons from Botnets", High Performance Cloud Auditing and Applications, Springer Science+Business Media New York 2014, pp.35-64, 2014

[5] Vikas Malik, C. R. Barde, "Live migration of Virtual Machines in Cloud Environment using Prediction of CPU Usage", International Journal of Computer Applications, Volume 117, No. 23, May. 2015

[6] Santosh Kumar Majhi, Sunil Kumar Dhal, "An Authentication Framework for

Securing Virtual Machine Migration", Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept. 21-24, 2016
〔7〕 Sarbjeet Singh, "cloud computing using virtualization", May. 2015
〔8〕 Misbah Liaqat, Shalini Ninoriya, Junaid Shuja, Raja Wasim Ahmad, Abdullah Gani, "Virtual Machine Migration Enabled Cloud Resource Management: A Challenging Task", Distrib, Parallel, and Cluster Computing, Jan. 2016
〔9〕 Issa Khalil, Ismail Hababeh, Abdallah Khreishah, "Secure Inter Cloud Data Migration", Information and Communication Systems (ICICS), Apr. 5-7, 2016
〔10〕 Rakel Haakegaard, Joanna Lang, "The Elliptic Curve Diffie-Hellman (ECDH)", Dec. 2015
〔11〕 Jing-Chiou Liou, "Performance Measures for Evaluating the Dynamic Authentication Techniques", International Journal of Cyber-Security and Digital Forensics (IJCSDF), Jan. 2016
〔12〕 Sheren A. El-Booz, Gamal Attiya, Nawal El-Fishawy, "A secure cloud storage system combining time-based one-time password and automatic blocker protocol", International Computer Engineering Conference (ICENCO), Dec. 2015

〈저자소개〉

이 은 지 (Eun-ji Lee) 학생회원
2016년 2월: 공주대학교 정보통신공학과 학사
2016년 3월~현재: 아주대학교 컴퓨터공학과 석사과정
〈관심분야〉 제어시스템 보안, 클라우드 컴퓨팅 보안, 암호프로토콜, 사물인터넷 보안

박 춘 식 (Choon-Sik Park) 종신회원
1995년: 일본동경공업대 공학박사
1982년~1999년: 한국전자통신연구원 책임연구원
2000년~2008년: 국가보안기술연구소 책임연구원
2009년 3월~현재: 서울여자대학교정보보호학과 교수
〈관심분야〉 사이버보안, 클라우드컴퓨팅보안, 개인정보보호기술

곽 진 (Jin Kwak) 종신회원
2000년 8월: 성균관대학교 학사
2003년 2월: 성균관대학교 석사
2006년 2월: 성균관대학교 박사
2006년 4월~2006년 11월: 일본 큐슈대학교 방문연구원
2006년 8월~2006년 11월: 일본 큐슈시스템정보기술연구소 특별연구원
2006년 11월~2007년 2월: 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 3월~2015년 2월: 순천향대학교 정보보호학과 교수
2008년 1월~현재: 한국정보보호학회 상임이사
2011년 1월~현재: 한국정보처리학회 이사
2015년 3월~현재: 아주대학교 사이버보안학과 교수
〈관심분야〉 자동차 보안, 암호프로토콜, 응용시스템보안, 클라우드 컴퓨팅 보안, 개인정보보호, 정보보호제품평가