Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.1, Feb. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.1.229

AHP를 활용한 IP-CCTV 위험 결정 모델 (클라우드 컴퓨팅 기반으로)

정 성 후,† 이 경 호‡
고려대학교 정보보호대학원

IP-CCTV Risk Decision Model Using AHP (Cloud Computing Based)

Sung-hoo Jung,† Kyung-ho Lee‡
Institute of Cyber Security & Privacy (ICSP), Korea University

요 약

본 논문은 기존의 CCTV가 가진 문제점을 분석하고, 클라우드 컴퓨팅 환경에서의 IP-CCTV를 사용할 때, 보안 문제점에 대하여 논한다. 클라우드 서비스 제공과 관련된 보안 위험을 단순히 위험 현상만 제거하는 실수를 줄이기 위해서는 위험 분석과 조치에 대한 효과적인 수행 방법이 필요하다. 이에 따라, Threat Risk Modeling의 STRIDE 모델을 통하여 위협 분석을 하고, 위협 분석된 내용을 토대로 Analytic Hierarchy Process(AHP) 방법론을 사용하여 위험 우선순위를 측정하였으며, 우선순위에 대한 적절한 해결방법이 무엇인지를 분석하였다.

ABSTRACT

This paper analyzes the problems of existing CCTV and discusses cyber security problems of IP-CCTV in cloud computing environment. In order to reduce the risk of simply removing the risk associated with the provision of cloud services, the risk analysis and counter-measures need to be carried out effectively. Therefore, the STRIDE model as the Threat Risk Modeling is used to analyze the risk factors, and Analytic Hierarchy Process(AHP) is used to measure risk priorities based on the analyzed threats.

Keywords: IP-CCTV, Cloud Computing, Threat Risk Modeling, Analytic Hierarchy Process(AHP)

I. 서 론

1.1 연구배경 및 목적

CCTV는 교육용, 의료용, 교통관제, 감시용, 방재용등으로 모든 산업에 걸쳐 사용되고 있으며, 보안에 있어 매우 중요한 물리적인 수단으로 사용된다. 범죄의 예방과 시설 안전 및 교통 정보 수집을 목적으로 중앙 행정기관 및 지방자치단체 및 그 소속 기관이 설치한 CCTV 대수는 전국에 65만 여대(2014년도 기준)가 운영되고 있고, 그 이외 민간에서 운영하는 것도 496만대(2013년도기준)가 있다.[1]

기존의 CCTV 영상정보는 유선(동축)케이블을 이용하여, DVR(Digital Video Recorder)등에 저장이 되었으나, DVR 내의 하드디스크(HDD) 고장 등으로 인하여, 많은 불편함이 제기되었다.

이런 이유로 네트워크 기반의 영상저장 장치인 NVR(Network Video Recorder)을 이용하게 되었고, NVR은 여러 형태로 진화를 하게 된다. NVR은 주로 IP를 기반으로 하여 카메라를 사용을 하며, 카메라에서 데이터를 압축하고, NVR로 전송한 후, 다시 압축된 데이터를 풀며, 영상을 보이는 일련의

Received(11. 13. 2017), Modified(12. 11. 2017), Accepted(01. 05. 2018)
† 주저자, 2001240326@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

과정에서 시간이 필요하고, 이로 인하여 NVR은 시간 지연 현상이 발생한다. 시간지연 현상은 사건의 파악이나, 원격지에서 현장을 관리 감독할 때, 치명적인 단점으로 작용을 한다.

이러한 기존의 CCTV가 가진 문제점을 해결하기 위하여, 클라우드 컴퓨팅을 활용한 CCTV 서비스가 점차 늘어나고 있는 추세이다. 클라우드 서비스 환경에서 새롭게 부각되는 보안 문제점이 어떤 것들이 있는지 알아보고 해결방안이 무엇인지 분석해본다.

1.2 연구방법 및 구성

본 연구는 클라우드 컴퓨팅 기반에서 IP-CCTV에 대한 위협을 분석하기 위하여 2가지 방법론을 사용한다. 첫 번째로, Threat Risk Modeling 방법론을 사용을 하여 위협을 분석하고, 그 위협들이 논리적으로 타당성을 갖는지 여부를 Analytic Hierarchy Process(AHP) 방법론으로 입증한다.

Threat Risk Modeling은 일반적으로 5단계로 이루어지며, 본 연구에서는 좀 더 명확한 결론을 얻기 위하여 Treat Risk Modeling 4단계까지 진행하여 위협 분석을 하고, 마지막 5단계의 위협 우선순위 및 가중치에 대한 내용은 AHP 방법론을 사용하여, 전문가들의 설문을 통하여 진행이 되었다. AHP 방법론은 클라우드 환경에서 IP-CCTV를 운영해 본 관리자 그룹, 정보보호 경력 10년 이상의 보안 전문가 그룹, 실제 IP-CCTV를 사용해 본 사용자 그룹으로 총 3개의 단위 그룹으로 나누어 설문의 신뢰도를 높였으며, 본 연구의 구성은 다음과 같다. 제Ⅰ장 서론에서는 연구의 배경 및 목적, 연구방법 및 구성에 대하여 기술한다. 제Ⅱ장에서는 선행연구로 클라우드 컴퓨팅 연구, Threat Risk Modeling 연구, AHP 방법론 연구를 기술하였고, 최근 IP-CCTV의 사고에 따른 공격 시나리오를 기술한다. 제Ⅲ장에서는 Threat Risk Modeling 방법론을 사용하여, 클라우드 컴퓨팅 기반 IP-CCTV의 위협들을 분석하여 기술한다. 제Ⅳ장에서는 AHP 방법론을 사용하여, Ⅲ장에서 도출된 위협을 논리적 타당성을 얻기 위하여 위험 결정요인을 기술한다. 그리고 마지막 제Ⅴ장 결론에서는 본 연구의 시사점에 대하여 기술한다.

Ⅱ. 선행연구

2.1 클라우드 컴퓨팅 연구

클라우드 컴퓨팅이란 인터넷 기술을 활용하여, 가상화(Virtualization) 형태로 서버, 스토리지, 네트워크 등의 자원을 필요한 만큼 사용하고 비용을 지불하는 종량제 형태의 컴퓨팅을 의미한다. 클라우드 컴퓨팅을 이루는 대표적인 기술은 가상화 기술과 대용량 분산처리기술로 클라우드 컴퓨팅의 핵심을 이룬다.[2]

많은 기업들이 기존의 IDC 환경에서의 제약조건 없이, 빠르고, 능동적으로 시스템을 구성하기 위하여 클라우드 컴퓨팅 환경을 선택한다.

클라우드 컴퓨팅 구성 요소는 서버, 소프트웨어, 스토리지, 네트워크, 단말로 나누어 볼 수 있다. 각 구성 요소별로 보안 기술이 필요한데, 서버에는 운영체제 및 Hypervisor 보안 기술이, 소프트웨어에는 응용프로그램 인증, 사용자 인증 및 결재 기술이, 스토리지에는 접근제어 및 암호화 기술이, 네트워크에는 암호화 및 DDoS 공격 방어 기술이, 단말에는 악성코드 방지 및 개인정보 보호 기술이 필요하다.[3]

서비스 기준으로 클라우드 컴퓨팅은 프라이빗 클라우드(Private Cloud), 퍼블릭 클라우드(Public Cloud), 하이브리드 클라우드(Hybrid Cloud) 등으로 나누어지는데, 본 연구는 퍼블릭 클라우드(Public Cloud) 기준으로 연구를 진행을 하였다. 퍼블릭 클라우드(Public Cloud)는 2017년 현재 기준으로, 글로벌 대기업 인 아마존의 아마존웹서비스(Amazone Web Service), 마이크로소프트 애져(Microsoft Azure), IBM의 소프트레이어(SoftLayer), VMware, AlertLogic 등이 있으며, 가장 많은 고객 클라이언트를 가지고 있는 아마존웹서비스(Amazon Web Service) 플랫폼 환경에서 연구를 진행하였다.

2.2 Threat Risk Modeling 연구

Threat Risk Modeling이란, 하나의 시스템에서 가장 중요한 보안 위협을 결정하기 위하여 보안 분석을 하는 기법이다.

Threat Risk Modeling을 하는 방법은 Fig. 1과 같이 5가지 절차로 분류가 된다.

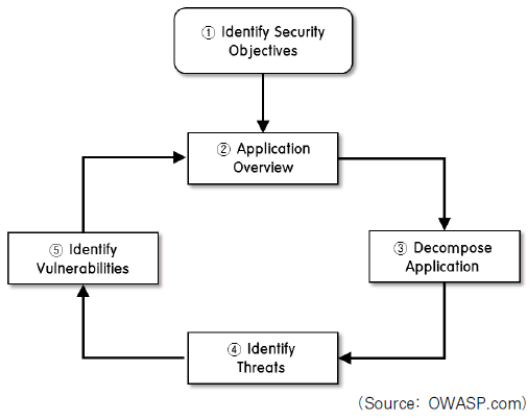

Fig. 1. Threat Risk Modeling 5 Procedures

각 단계별로 ① Identify Security Objectives 단계에서는 보안의 객체(Objective), 즉, 시스템의 구성요소와 자산을 식별한다. ② Application Overview 단계에서는 식별된 보안 객체에 대하여 구성요소(Components), 데이터 흐름(Data flows), 신뢰 경계(Trust boundaries)를 식별하기 위해 DFD(Data Flow Diagram)를 작성한다. ③ Decompose Application 단계에서는 분석된 Application 구조를 통해 평가할 필요가 있는 보안에 영향을 미치는 요소들을 확인하고 분석한다. 구체적인 방법으로 STRIDE 기법을 통해 공격자의 입장에서 어떠한 방법으로 공격할 수 있는지 식별하는 단계이다. ④ Identify Threats 단계에서는 현재까지 알려진 다양한 위협을 기술하고, 이때, 구조화된 Attack Tree를 사용한다. ⑤ Identify Vulnerabilities 단계에서는 분석된 위협을 평가하고 관련된 취약점을 검토한다. 확인된 위협과 취약점을 통해 위험을 측정하는 단계로서 DREAD 모델을 사용한다. 이를 통하여 각각의 위협에 등급을 부여하고 이를 종합하여 위험을 측정한다.[4]

2.3 AHP 방법론 연구

보안 위협의 가정과 자산의 특성을 연결하여 위험을 분류한다. 보안 위협의 가정에 대한 논리적 타당성 검증을 위하여, AHP를 활용하였다.

Tomas L. Saaty에 의해 개발된 AHP는 복수의 대안에 대한 복수의 평가 기준이 존재하는 다기준의 의사결정 문제를 해결하기 위한 대표적인 기법으로 다양한 유형의 의사결정 문제에 활용되어 왔다[5]. AHP는 주어진 의사결정 문제를 목표, 평가요인, 대안으로 구성되는 계층(Hierarchy)으로 Fig. 2 와 같이 모형화 하고, 각 계층 내 의사결정 요소들 간의 쌍대비교(Pairwise Comparison)를 수행하여 최종 우선순위를 도출한다.

AHP 기법은 의사결정 요소들 간에 상대적 가중치를 추정하여 사용한다. $A \cdot w = \lambda max \cdot w$. 여기서 A는 쌍대비교로 얻어진 정방행렬식으로부터 고유벡터 값을 구한 후 고유벡터 W의 각 요소를 ΣWi로 나눔으로써 표준화된 가중치를 구한다. 일관성 지수(Consistency Index, C.I)는 $C.I=(\lambda-N)/(N-1)$를 통해 산출하며, 여기서 N은 쌍대비교의 대상수이다. 일관성 정도(Consistency Ration, C.R.)는 $C.R.=C.I/R.I$로 산출한다. 또한 무작위 지수(Random Index, R.I.)는 경험적 자료로 얻어진 행렬의 차원별 평균무작위 지수이다[6].

AHP 기법은 다양한 유형의 MCDM 문제해결에 효과적으로 연구되고 있으며, 이석원 등[7]은 AHP 기법을 사용하여 금융회사 서버 Privilege 계정 운영방식 결정 모델을 분석하고 Windows Privilege 계정 관리강화를 위한 4가지 개선방안을 제시하는 연구를 진행하였다. 성기훈 등[8]은 AHP를 기반으로 SNS 제공환경에서 정보보호의 중요 위협요인을 분석하고, 정보보호 투자 결정 기준을 도출하는 연구를 진행하였다. 연구 결과에 따르면, 의사결정 수립을 위한 가장 중요한 기준이 목표 설정을 하는 부분인데, AHP 방법론을 사용하여 논리적 타당성을 증명하는 기준이 되었다.

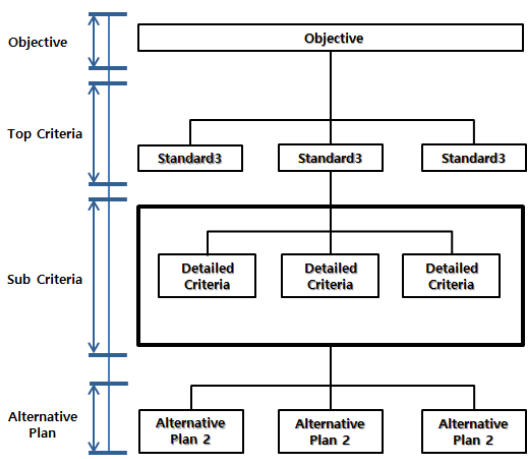

Fig. 2. AHP hierarchical model example

III. 연구대상

연구대상으로는 클라우드 환경에 연결되어 있는 가정용 IP-CCTV를 대상 모델로 선정을 하였으며, 선정 사유는 최근 들어 해킹을 통한 IP-CCTV 사고가 빈번히 발생하고 있기 때문이다. 최근 5개년도 IP-CCTV 사고사례를 보면 Table 1과 같다.

2015년 130건에서 2016년 362건을 2.7배 상승하였으며, 올해도 2분기 기준으로 이미 200여건이 신고 되었다고 밝힌 바 있다.

또한 한국은 2016년 말 전 세계에서 미국에 이어 두 번째로 많은 CCTV가 해킹되어 전 세계로 생방송 중계되기도 하였다. 해당 사이트는 러시아에 서버를 둔 인세캠(http://www.insecam.org)이라는 사이트로 전 세계 265국의 7만 3천대의 CCTV를 생중계하였다. 미국은 1만1천개로 1위, 한국은 6536개로 2위를 차지하는 불명예를 겪기도 하였다.

이 사이트는 쇼단(https://shodan.io)과 지맵(https://zmap.io)등을 이용하여, 인터넷에 연결된 IP기반 CCTV를 찾은 다음, CCTV의 비밀번호를 해킹하여 영상을 재생하는 방법으로 운영된다.

일반적으로 IP 기반의 CCTV는 네트워크 통신을 하기 때문에 많은 기업에서 클라우드 컴퓨팅을 도입하고 있는 추세이다. 클라우드 컴퓨팅 환경에서 IP-CCTV의 시스템 설계는 어떻게 되는지와 그로 인하여 발생되는 위협은 어떤 것들이 있는지 알아보고, 해결방안을 모색해본다.

Table 1. 2013~2017 IP-CCTV related reports

Year	2013	2014	2015	2016	2017 (Q2)
Calls	4	6	130	362	199

3.1 (1단계) 자산식별 및 구성요소

위협분석을 수행하기 위한 첫 단계로 클라우드 컴퓨팅 환경에서 IP-CCTV가 어떻게 구성이 되어 있는지를 알기 위하여, 자산식별 단계를 수립한다.

IP-CCTV 가 서비스를 하기 위한 구성요소로는 사용자(User), 사용자 기기(PC, Mobile기기), 통신수단(Web browser, Mobile APP), 인터넷(Internet, Wireless network), 서버(Web, TURN, XMPP Server), 인증 데이터 서버를 식별 할 수 있다.

3.2 (2단계) DFD 구성

클라우드 컴퓨팅 기반의 IP-CCTV 시스템은 데이터의 전송과정에 따라, Trust bound(신뢰경계도)로 보안의 경계선(점선)을 나눈다. User Device(PC, Mobile) 등은 Web Server를 통해서 접근하여, IP-CCTV의 Camera는 TURN Server를 통하여 접근 하므로 크게 외부 환경과 클라우드 서버가 설치된 내부 환경, 그리고 사용자 인증 데이터를 저장한 인증 데이터 서버 환경으로 아래 Fig. 3과 같이 표현할 수 있다.

클라우드 컴퓨팅 기반 IP-CCTV를 설계할 때는

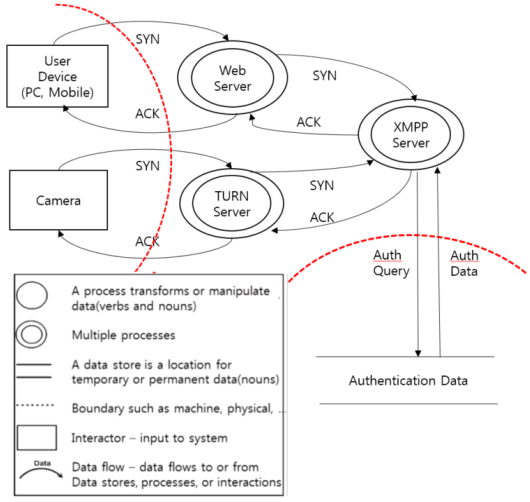

Fig. 3. Cloud computing based IP-CCTV DFD configuration diagram

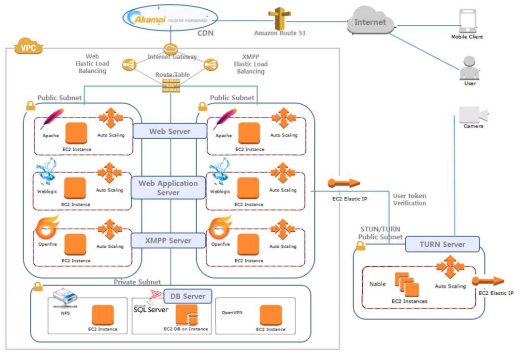

Fig. 4. IP-CCTV System Configuration based on Cloud computing

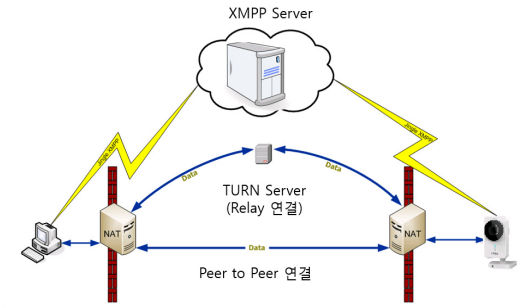

Fig. 5. XMPP, TURN-Relay Server Architecture

대체로 아래 Fig 4.와 같이 구성된다.

WEB, WAS, DB 서버 등의 전통적인 구성과 IP-CCTV 시스템을 구성하기 위하여 XMPP, TURN 서버가 더해졌다. CCTV의 영상을 송출하기 위하여, XMPP(Extensible Messaging and Presence Protocol) 서버가 구성된다.

TURN(Traversal Using Relays around NAT) 서버란, 그 이름에서 알 수 있듯이 NAT 환경에서 서비스가 제대로 동작할 수 있도록 CCTV 카메라와 서버를 연계시켜주는 기능을 의미한다.

3.3 (3단계) STRIDE를 활용한 위협 분석

STRIDE 모델은 공격의 종류에 따라 알려진 위협의 특성에 대한 분류체계로서, S는 인증정보를 속이는 행위, T는 인가받지 않은 수정, R은 행위 부인, I는 정보 유출, D는 서비스의 거부, E는 부정한 권한의 상승을 나타낸다.[9]

IP-CCTV의 사용자와 시스템 관리자 계정을 활용하여 인증정보를 속이는 행위(Spoofing)를 할 수 있다. 인터넷과 무선인터넷 등으로 연결되기 때문에, 인가 받지 않은 수정행위(Tampering with data)를 할 수 있다. 사용자와 시스템 관리자 계정으로 로그인을 하여, 접속 IP주소의 변경 및 로그 수정으로 행위 부인(Repudiation)을 할 수 있으며, 인터넷과 무선인터넷으로 개인정보를 유출(Information disclosure)을 할 수 있다.

또한 DDoS 공격을 감행할 경우, 영상정보를 제대로 가용하지 못하는 점이 있다. 사용자 또는 시스템 관리자 계정을 통하여 시스템의 특권권한(Elevation of privilege) 을 얻을 수 있다. 이러한 위협들을 전제로 상세한 공격이 어떻게 이루어지는 지를 알기위하여, 4단계에서 Attack Tree를 활용한 공격 모델을 알아본다.

Table 2. Classification by IP-CCTV STRIDE model

Category	Threat target(s)
Spoofing identity	user, user device, root account
Tampering with data	internet, wireless network
Repudiation	user, user device, root account
Information disclosure	internet, wireless network, personal data
Denial of Service	internet, wireless network, web server
Elevation of privilege	user, user device, root account

3.4 (4단계) 위협의 구조화된 분석(Attack Tree)

STRIDE를 통하여, IP-CCTV에서 위협이 발생할 수 있는 요인들에 대하여 정리를 하였다.

이러한 분류들을 좀 더 세분화하기 위하여 Fig. 6과 같이 구조화된 분석을 Attack Tree[10]를 활용하여 분석을 한다. 실질적인 위협이 어디에서 어떠한 방법으로 공격이 될지 가능성을 예측하는 단계이다. 클라우드 컴퓨팅 환경에서 IP-CCTV를 공격 할 경우 Table 3과 같은 공격 기법들이 수행된다.

해커들은 CCTV를 해킹하기 위하여 쇼단(https://shodan.io)과 지맵(https://zmap.io) 등의 사이트를 활용하여, 먼저 해킹을 위한 대상을 물색한다. 그 대상을 확인한 후, Password sniffing, Password guessing, Social engineering, Brute-force attack 등의 공격을 통하여 계정을 얻고, 계정이 맞는지 검증을 하여, 공격자는 개인의 사생활이 담겨있는 영상을 언제 어디서든지 볼 수 있는 환경이 제공이 되는 것이다. 공격자는 쇼단과 지맵 사이트를 사용하지 않고 단독 공격을 수행할 경우에는 인터넷 상에 열려 있는 포트를 찾기 위하여, Port scanning을 활용하여 열려있는 Port를 찾고, 공격자 자신의 IP를 노출시키지 않기 위하여 IP Spoofing 기술등을 사용할 수 있다. 또한, 공격자는 한번 해킹한 대상에 대하여서는 단 한번의 공격으로 끝내지 않고, 지속적인 공격을 위하여 Back door를 심어두어 추후 공격이 쉽게 이루어질

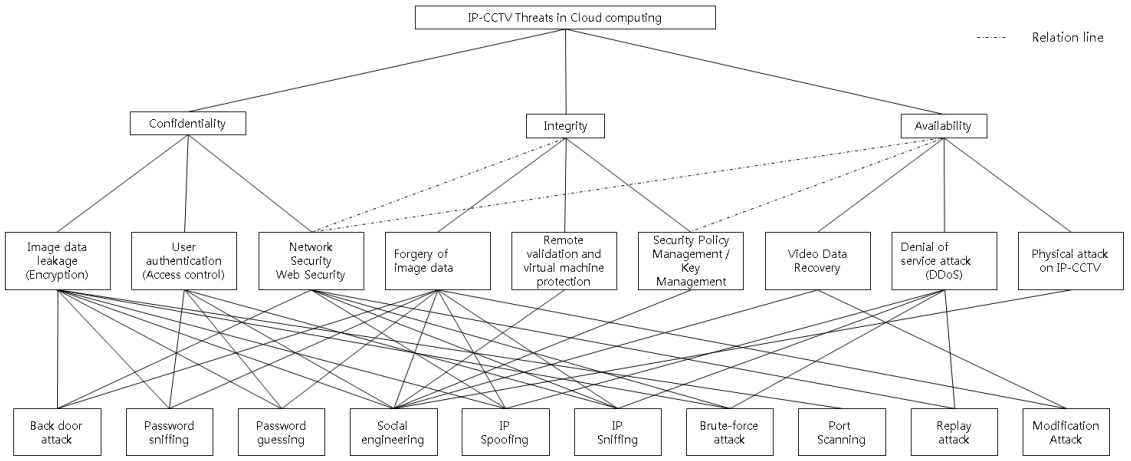

Fig. 6. IP-CCTV Attack Tree

Table 3. IP-CCTV major Cyber attack techniques

No.	Cyber Attack	Contents
1	Back door attack	Actions to re-invade a self-inflicted system in general
2	Password sniffing	Accessing the system by secretly acquiring online passwords
3	Password guessing	Accessing the system by estimating the default password when manufacturing the product
4	Social engineering	Acquiring confidential information by tricking people based on basic trust among people, not in a technical way
5	IP spoofing	Accessing the system by fabricating an Internet address by acting as an authorized user
6	IP sniffing	Stealing Internet addresses (IP) by reading packets
7	Brute-force attack	Assigning all possible values to solve a specific password
8	Port scanning	Retrieving open TCP / UDP ports on an active server.
9	Replay attack	Stealing and replaying authentication information when using cookies or sessions
10	Modification attack	If an attacker modifies illegal data sent or received in the middle attack

수 있도록 공격자만의 비밀의 문을 만드는 공격도 수행 할 수 있다. 이렇듯 공격자들은 한번에 하나의 공격을 하지 않고, 여러 공격을 섞어 지능적 공격을 수행하기도 한다.

IV. AHP 기법을 활용한 클라우드 컴퓨팅 기반 IP-CCTV 위험 결정 모델

3장에서와 같이 이러한 위협 분석을 통하여, 위협의 우선순위 선정을 위하여 4장에서 AHP 방법론을 사용하였다.

4.1 IP-CCTV 위험 결정 요인을 위한 절차

AHP는 계층 모델 구축, 쌍대비교, 부분 우선순위 도출, 일관성 평가, 최종 우선순위 도출 및 대안 선택의 5단계로 이루어진다.[11]

① 사전 분석 및 평가 요인 선정
: 효과적인 위험 결정요인을 위한 선행 연구 및 평가요소 선별 , 사전 분석 결과를 바탕으로 최종 평가 기준(요인) 선정
② 계층 모델 수립
: AHP를 이용한 계층 모델의 수립
③ 설문조사 및 유효성 평가
: 이전 단계에서 수립된 AHP 계층 모델을 바탕으로 설문 조사를 실시하고, 결과 데이터의 유효성을 평가
④ 평가 요인 별, 대안별 우선순위도출

: 사용자 유형에 따라 3개 그룹으로 나누어 각각의 평가 요인별, 대안별 중요도를 평가하여 최종 가중치를 도출

⑤ IP-CCTV 위험 결정요인을 위한 방안 선정

: 최종 도출된 결과 값을 이용하여 중요 평가 요인 및 대안을 바탕으로 IP-CCTV의 위험에 따른 대응 방안을 선정

4.2 사전 분석 및 평가 요인 선정

3.3절의 STRIDE를 활용한 위협 분석을 통하여, 클라우드 환경에서 IP-CCTV 취약점에 대해 분석을 하였다. 10가지의 위협들을 AHP 기법을 활용하기 위하여, 각 부분들을 보안 3요소(기밀성, 무결성, 가용성)로 Top Criteria 정리를 하였으며, 일반적인 10가지 위협들은 IP-CCTV의 각 기능들의 위협에 귀결이 되며, 이 부분들은 Sub Criteria로 일반화 하였다. IP-CCTV 의 기밀성에는 자산이 유출 또는 외부에 공개되었을 경우에 미치는 영향도를 기준으로 선정하였으며, 무결성에는 자산(정보)이 변조 되었을 경우에 미치는 영향도를 기준으로 선정하였고, 가용성에 있어서는 자산을 사용/이용할 수 없을 경우에 미치는 영향도에 따라 Sub Criteria를 선정하였다.

Top Criteria에 따른 Sub Criteria는 3장에서의 Threat Risk Modeling의 위협요인을 기준으로 선정하였다. 또한, 클라우드 컴퓨팅 보안 요소기술 내역[12] 과 한국정보통신기술협회(TTA) 표준으로 지정된 영상감시 시스템 보안 요구사항[13] 자료를 참고하여 작성되었다.

4.3 AHP 계층 모델 수립

4.3절의 클라우드 컴퓨팅 기반 IP-CCTV 사전분석을 토대로 AHP 계층 모델을 Fig.7과 같이 수립하였다. 기밀성, 무결성, 가용성의 보안 3요소를 기준으로 작성되었다. AHP를 이용한 분석은 3개의 상위평가 기준 간 쌍대비교, 각 상위평가 기준에 해당하는 하위평가 기준간의 쌍대비교를 통하여 평가요인별 최종 가중치를 도출하였다.

4.4 설문 조사 및 유효성 평가

Table. 4의 평가요인 선정 지표와 Fig. 7 의 AHP 계층 모델을 기반으로 설문지를 작성하였고,

Table 4. Selection of IP-CCTV AHP evaluation factor

Top Criteria	Sub Criteria	Definition
Confidentiality	Image data leakage / encryption	A serious problem concerning the leakage of image data and the corresponding encryption method
	User authentication / access control	Authentication for accessible users
	Network security / web Security	SSL / TLS-based threats using web-based interfaces
Integrity	Forgery of image data	Error checking for messages exchanged with stored data
	Remote validation and virtual machine protection	Support for remote executable code and virtual machine program execution area and memory protection
	Security policy management / key management	Security policy and user key management for information security management plan
Availability	Video data recovery	Failure durability and data recovery to prevent service disruption or data loss
	Denial of service attack	Cloud computing IP-CCTV denial of service attack
	Physical attack on IP-CCTV	Threats due to direct physical attacks on IP-CCTV cameras

(1) 가중치 산정 결과

					Consistency Index				0.0401
	Factor 01	Factor 02	Factor 03	Factor 04	Factor 05	Factor 06	Factor 07	Factor 08	Factor 09
Weight	0.092	0.177	0.170	0.071	0.051	0.159	0.056	0.169	0.054
Priority	5	1	2	6	9	4	7	3	8

(2) 비교 행렬

	Factor 01	Factor 02	Factor 03	Factor 04	Factor 05	Factor 06	Factor 07	Factor 08	Factor 09
Factor 01	1.0	0.5	0.5	1.0	2.0	0.5	3.0	0.3	2.0
Factor 02	2.0	1.0	2.0	2.0	3.0	1.0	3.0	1.0	3.0
Factor 03	2.0	0.5	1.0	3.0	3.0	1.0	2.0	2.0	3.0
Factor 04	1.0	0.5	0.3	1.0	1.0	0.5	2.0	0.3	1.0
Factor 05	0.5	0.3	0.3	1.0	1.0	0.3	0.5	0.3	1.0
Factor 06	2.0	1.0	1.0	2.0	3.0	1.0	3.0	1.0	3.0
Factor 07	0.3	0.3	0.5	0.5	2.0	0.3	1.0	0.3	1.0
Factor 08	3.0	1.0	0.5	3.0	3.0	1.0	3.0	1.0	3.0
Factor 09	0.5	0.3	0.3	1.0	1.0	0.3	1.0	0.3	1.0

Fig. 7. Prioritizing IP-CCTV risk factors using AHP

평가 대상은 시스템 운영을 담당하는 관리자 그룹 , 보안업무 10년 이상 경력을 가진 전문가 그룹 , 실제 IP-CCTV를 사용하는 사용자 그룹으로 총 3개의 그룹으로 나누어 진행하였다.

Satty[9]는 일관성 비율이 0.1 이하일 때 쌍대비교 행렬이 일관성이 있다고 하였다. 설문 결과, 일관성 비율이 0.1 미만일 경우 일관성 유지한다고 판단하여 분석대상에 포함하였고, 일관성 비율이 0.1 이상인 설문의 경우에는 일관성이 결여되어 합리적 판단에 적합하지 않으므로 분석대상에서 제외하였다.

전체 분석 설문에 응답한 25부 중에서 분석에서 제외된 설문은 총 4부로 일관성 비율이 0.1 미만으로 평가된 설문은 총 21부에 해당한다. 3개의 그룹을 기준으로 관리자 그룹 8부, 전문가 그룹 6부, 사용자 그룹 7부가 유효한 설문으로 나누어졌다.

설문의 평가는 5점 척도로 평가되었고, 각 항목별 점수는 쌍대비교를 통하여, 매우중요(3점), 중요(2점), 보통(1점), 중요하지 않음(0.5점), 전혀 중요하지 않음(0.3점)으로 계량화 하였다.

4.5 평가 요인별 가중치 및 우선순위 도출

그룹별로 나누어 운영자 그룹, 보안 전문가 그룹, 사용자 그룹 등 기밀성, 무결성, 가용성 중에서 기밀성을 토대로 한 사용자 인증/ 접근제어가 가장 높은 가중치를 기록을 하였고, 두 번째로 네트워크 보안/웹 보안이 중요하다는 결론을 얻었다. 그 외에도 클라우드 환경에서 네트워크 및 웹 보안이 취약하여 생기는 영상 데이터 유출, 암호화가 그 뒤를 이루었다.

설문의 일관성 면에 있어서는 C.I(Consistency Index)와 C.R(Consistency Ratio)값으로 측정하였다. C.I는 비교 수행자가 얼마나 일관성을 가지고 결과를 적었는지 보여주는 지표로써, C.I 값은 Fig.8 과 같이 0.0401로 나타났으며, C.R 값은 C.I값에다 R.I(Random Consistency Index) 즉, 무작위로 추출한 표본값을 나누어 비율로 계산하는 방식이다. R.I값은 Saaty가 9가지 속성 값을 정해두어 Factor 9개의 수치는 고정값 1.45로 나눠주면 최종적으로 C.R값은 0.0276이라는 값을 얻을 수 있었다.

IP-CCTV 위험에 따른 대책방안은 AHP 방법론의 가중치 및 우선순위를 기준으로 선정을 하였으며, 관리자, 보안전문가, 사용자의 가중치와 우선순위는 Fig. 9 와 같이 나타났다.

관리자 그룹은 사용자 인증/접근제어(0.177), 네트워크 보안/웹 보안(0.170), 서비스 거부 공격

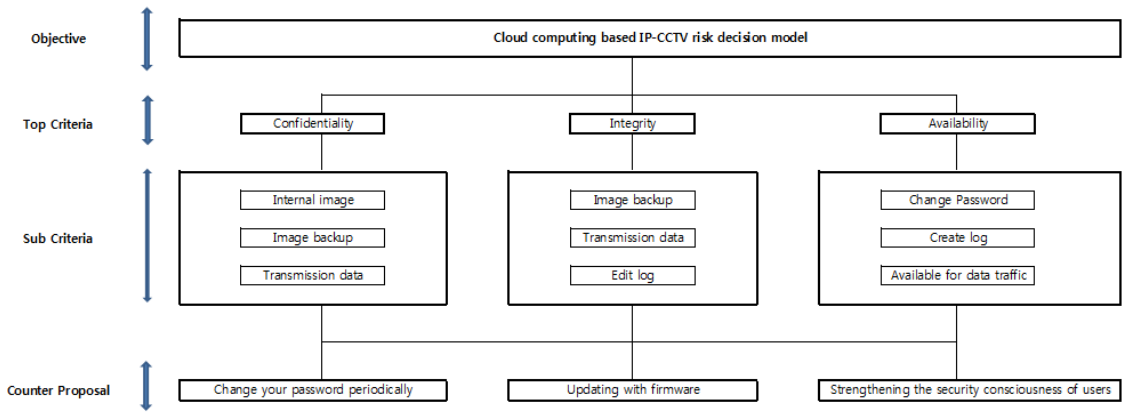

Fig. 8. risk factor results matrix using AHP

Group			Managers		Technicals		Users	
Criteria	Sub Criteria	Factor	Weigt	Priority	Weigt	Priority	Weigt	Priority
Confidentiality	Video data leakage / encryption	Factor 01	0.092	5	0.182	1	0.129	4
	User authentication / access control	Factor 02	0.177	1	0.179	2	0.152	1
	Network Security / Web Security	Factor 03	0.170	2	0.125	4	0.144	2
Integrity	Forgery of Video data	Factor 04	0.071	6	0.092	6	0.118	5
	Remote validation and virtual machine protection	Factor 05	0.051	9	0.062	7	0.085	7
	Security Policy Management / Key Management	Factor 06	0.159	4	0.169	3	0.135	3
Availability	Video Data Recovery	Factor 07	0.056	7	0.054	8	0.079	8
	Denial of service attack	Factor 08	0.169	3	0.116	5	0.092	6
	Physical attack on camera	Factor 09	0.054	8	0.021	9	0.066	9

Fig. 9. risk factors using AHP weights and priorities by group

(0.169), 보안정책 관리/키 관리(0.159), 영상 데이터 유출/암호화(0.092), 영상데이터 위변조(0.071), 영상데이터 복구(0.056), 카메라에 대한 물리적 공격(0.054), 원격 확인 및 가상머신 보호(0.051) 순으로 결과가 나타났고, 관리자그룹에서는 IP-CCTV가 외부 공격자로부터 사용자 인증과 접근제어가 클라우드 환경에서 IP-CCTV의 가장 큰 위협이라고 AHP 통계를 통하여 결과가 도출되었다.

전문가 그룹은 영상데이터 유출/암호화(0.182), 사용자 인증/접근제어(0.179), 보안정책 관리/키 관리(0.169), 네트워크 보안/웹 보안(0.125), 영상데이터 유출/암호화(0.092), 영상데이터 위변조(0.092), 원격 확인 및 가상머신 보호(0.062), 영상 데이터 복구(0.054), 카메라에 대한 물리적 공격(0.021) 순으로 나타났다. 전문가 그룹은 사용자 인증/접근제어 보다는 영상데이터의 유출과 그에 따른 암호화 방법이 중요하다고 나타났다.

사용자 그룹은 사용자 인증/접근제어(0.152), 네트워크 보안/웹 보안(0.144),보안정책 관리/키 관리(0.135), 영상데이터 유출/암호화(0.129), 영상데이터 위변조(0.118), 서비스 거부 공격(0.092), 원격 확인 및 가상머신 보호(0.085), 영상데이터 복구(0.079), 카메라에 대한 물리적 공격(0.066)으로 운영자 그룹에서와 같이 사용자의 인증과 접근제어가 가장 큰 위협이며, 중요도가 높게 결과가 나타났다.

4.6 IP-CCTV 위험 결정요인을 위한 대안 선정

IP-CCTV 위험에 따른 대안은 AHP 방법론의 가중치 및 우선순위를 기준으로 선정을 하였다. 관리자, 보안전문가, 사용자의 가중치 별 합계와 내림차

Sub Criteria	Factor No.	Weigt	Priority
Video data leakage / encryption	Factor 02	0.508	1
User authentication / access control	Factor 06	0.463	2
Network Security / Web Security	Factor 03	0.439	3
Forgery of Video data	Factor 01	0.403	4
Remote validation and virtual machine protection	Factor 08	0.377	5
Security Policy Management / Key Management	Factor 04	0.281	6
Video Data Recovery	Factor 05	0.198	7
Denial of service attack	Factor 07	0.189	8
Physical attack on camera	Factor 09	0.141	9

Fig. 10. Priority based on IP-CCTV risk factors weighted using AHP

순 별 우선순위는 Fig.10 과 같이 도출이 되었다.

세 그룹의 보안식별 요인에 미치는 영향력은 상대적으로 다를 수 있으나, IP-CCTV의 위험 순위에 대한 많은 인원 수에 따른 조금 더 명확한 우선순위를 나타내기 위하여 그룹별 가중치 합으로 나타내었다. 이러한 결과를 기반으로 기밀성, 무결성, 가용성에 대한 모델을 생성한다면 Table.5 와 같이 나타낼 수 있다. 기밀성의 경우를 예를 든다면, 기밀성에 포함된 영상데이터 유출/암호화, 사용자 인증/접근제어, 네트워크 보안/웹 보안의 항목들을 각 가중치를 곱한 값을 각 항목들의 합으로 표현하였다. 무결성, 가용성도 기밀성과 같이 각 항목들을 가중치를 곱한 값에 각 항목의 합으로 나타내었다.

사용자 인증과 접근제어를 해결하기 위해서는 IP-CCTV 제품 출시가 될 때 기본적인 Default 패스워드를 사용자 관점에서 패스워드 변경이 쉬워야 하며, 접근제어를 위한 SSL 인증서 암호화 등의 방법이 필요할 것이다.

보안정책 관리 / 키 관리는 IP-CCTV 출시하는 각 회사마다 정보보호 정책 수준 및 개인정보보호법, PCI, HIPPA, 바젤II 및 CJIS 등 여러 법제 및 관련 제도가 시행되면서 CCTV 영상 정보의 보안을

Table 5. Cloud computing based IP-CCTV risk decision model

Criteria	Formula
Confidentiality	(Factor01×0.403)+(Factor02×0.508)+(Factor03×0.439)
Integrity	(Factor04×0.281)+(Factor05×0.198)+(Factor06×0.463)
Availability	(Factor07×0.189)+(Factor08×0.377)+(Factor09×0.141)

강화할 수 있는 암호화 기술 등에 초점을 맞추고 있다.

네트워크 보안 및 웹 보안은 클라우드 컴퓨팅 환경에서 아마존웹서비스(AWS) 내의 방화벽정책 설정과 같은 기능을 하는 Security Group을 사용하여, 특정 IP만 접근이 가능할 수 있도록 설계할 수 있다. 보안성 강화를 위하여 IAM을 사용하는데, 리소스에 대한 접근정책을 활용할 수 있다. IAM을 이용하여, AWS 리소스를 사용할 수 있는 사람(인증)과 이들이 사용할 수 있는 리소스 및 사용방법(권한부여)을 제어할 수 있는 방법이 있다.

4.7 위험 결정 모델

IP-CCTV의 위험 요인을 결정하기 위하여 정리를 한다면 Fig.11과 같은 모델로 도식화 할 수 있다. 자산을 식별하고, Threat Risk Modeling의 STRIDE를 통하여 위협을 분석하여 그 위협에 따른 AHP 방법론으로 가중치를 선정하고, 가중치별로 위협 우선순위를 나타내어 전체적인 대안을 선정하는 방법이 위험의 결정요인이라 할 수 있겠다.

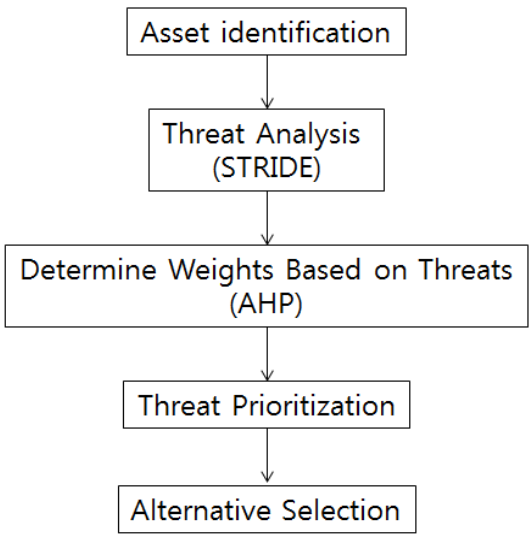

Fig. 11. Risk decision model

V. 결론 및 한계사항, 발전방향

클라우드 환경에서의 IP-CCTV 위험 결정요인에 대하여 분석을 하였으며, AHP 방법론의 가중치에 있어 0.01 차이의 오차가 발생할 경우, 위험에 따른 지표가 달라질 수 있는 부분은 명확히 존재한다. 그러나 전문가로 하여금 다수의 인원들에 대한 설문을 통한 부분이 타당성이 반영된 부분이라 생각을 한다.

또한 IP-CCTV 뿐만 아니라, 클라우드 환경에서의 모든 IoT 기기들이 인터넷과 연결이 되어 있어, 언제 어디서든 심각한 보안문제가 발생할 수 있다는 보안인식 제고가 필요하다. 시스템의 설계부터 보안에 대한 부분을 고려를 한다면 신뢰성 높은 제품을 출시할 수 있을 것이다.

References

[1] A Public institutions cctv installation status, Ministry of the Interior, 2016.
[2] Choon-Sik Park, "Study on Security considerations in the Cloud Computing", Journal of the Korea Academia-Industrial cooperation Society, Vol.12, No.3 pp.1408-1416, Mar. 2011.
[3] Sung-Kyong Un, "Trend of Cloud Computing Security Technology", Review of KIISC(Korea Institute of Information Security and Cryptology) Vol.20, No.2, pp.27-31. Apr. 2010.
[4] Dae Yong Jeong, "A Study on Risk Analysis and Countermeasures of Electronic Financial Fraud", KIISC (Korea Institute of Information Security and Cryptology), Vol.27 No.1 [2017], pp. 118-119, Feb. 2017.
[5] Saaty T. L., "The Analytic Hierarchy ro-cess," McGraw-Hill, New York, 1980.
[6] Sang-Pil Shin, "An analytic hierarchy process (AHP) approach to selection of implementation mode of mobile office system," Seoul National Univetsity of Science and Technology, July. 2013.
[7] Suk-Won Lee, "Decision Making Model for Selecting Financial Company Server Privilege Account Operations". KIISC(Korea Institute of

Information Security and Cryptology),Vol.25, No.6, p1607-1620, Dec, 2014.
〔8〕 Kihoon Sung, "A Study on Threat factors of Information Security in Social Network Service by Analytic Hierarchy Process," Journal of The Korea Institute of Information Security & Cryptology, Vol.20. no.6. pp.261-270, Dec. 2010.
〔9〕 Microsoft, "The STRIDE Threat Model" available https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx
〔10〕 Schneier, Bruce, "Attack Trees," Dr. Dobb's Journal of Software Tools, 24(12), pp. 21-29. Dec. 1999.
〔11〕 Min-Sun Lee, "Decision Model of the Effectiveness for Advanced that Security Visualization", KIISC(Korea Institute of Information Security and Cryptology), Vol.27, p154-5 Feb. 2017.
〔12〕 Jae-Gyu Choi, "Security Technology Research in Cloud Computing Environment", JSE(Journal of Security Engineering), Vol.8 No.3, p371-384, Jun. 2011.
〔13〕 "Security Requirements of the Video Surveillance System", Telecommunications Technology Association, Dec. 2012.

〈저자소개〉

정 성 후 (Sung-hoo Jung) 정회원
2008년 8월: 고려대학교 과학기술대학 전산학과 학사
2018년 2월: 고려대학교 정보보호대학원 정보보호학과 석사
2008년 8월~2014년 2월: 롯데정보통신 IDC센터
2014년 3월~현재: 한화테크윈(판교R&D센터) 책임연구원
〈관심분야〉 클라우드 시스템 아키텍쳐, 클라우드 컴퓨팅 보안, 정보보호정책
E-mail: 2001240326@korea.ac.kr

이 경 호 (Kyung-ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사
2009년 8월: 고려대학교 정보보호대학원 박사
1994년 2월 삼성그룹 네이버주, 시큐베이스등 근무
2011년 9월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 위험관리, 정보보호컨설팅, 정보보호 및 개인정보보호정책
E-mail: kevinlee@korea.ac.kr