한국컴퓨터정보학회지
제26권 제2호, 2018. 12.

사물인터넷 보안을 위한 IP 카메라에 관한 연구

(A Study on the Effective Identification of IP Cameras)

• 박재경 (한국폴리텍대학 서울강서캠퍼스 정보보안과 교수)
• 김현우 (한국폴리텍대학 서울강서캠퍼스 정보보안과 교수)

I. Introduction

4차 산업혁명에서 사물과 인터넷, 인공지능이 연결된 초 지능화된 시스템 중 IoT, MSA, CPS, 인공지능, IP 카메라 등 다양한 신기술들이 개발되고 있으며, 특히 IP 카메라는 4차 산업혁명 기술이 축약된 영상보안 장비로, 폭행이나, 사고 등이 발생했을 경우 이를 자동으로 인지 및 실시간 대응할 수 있는 기술로 중요성이 부각되고 있다. IP 카메라 기술의 발전은 우리의 생활을 편리하게 하는 긍정적인 측면이 있는 반면, 개인정보 침해 및 이로 인하여 금전적 피해를 입을 수 있는 부정적인 측면도 있다. 특히, IP 카메라 특성상 기업의 내부 네트워크와 연결되어 있어 공격자가 IP 카메라를 통하여 기업의 내부 네트워크로 접근하여 개인정보 및 중요 기밀문서 등이 유출될 수 있다. 이와 같은 IP 카메라의 위협은 통신 구간에서의 도청, 데이터 변조가 있으며 공격자가 정상으로 위장한 IP 카메라로 교체하여 내부 네트워크로 접근하는 진위 판단 우회 등이 있다. 이러한 위협이 발생되는 이유는 IP 카메라가 IP 기반으로 통신을 수행하며 기업에서 IP 카메라에 대하여 단순히 IP 주소와 MAC 주소를 매칭 시켜 진위 판단을 수행하기 때문이다. 따라서 IP 카메라의 운영환경이 안전하고 보안신뢰도가 높은 환경이 되기 위해서는 기존 IP 주소와 MAC 주소 진위 판단방식에서 보다 효과적이고 안정적으로 적용할 수 있는 진위 판단 기술을 연구할 필요가 있다.

II. Preliminaries

1. Definition of IP Camera System

IP 카메라란 카메라 본체, 카메라 모듈, CPU, 디코더, 영상 압축 칩, 네트워크 전송 칩으로 구성된 디지털 비디오카메라의 일종으로, 기존 사용되던 IP 카메라의 단점인 저 화질, 배선 작업, 신호 손상률, 비용 문제 등을 극복한 카메라이다. 이는 네트워크 환경을 이용하기 때문에 어느 공간에서든 네트워크에 연결되어 있다면 실시간으로 영상을 모니터링 및 제어가 가능하며, 별도의 DVR이 없더라도 손쉽게 영상 녹화 및 캡처 역시 가능하다. Fig. 1은 IP 카메라 의 개념을 나타낸 것이다[1].

Fig. 1. IP Camera System Diagram

IP 카메라는 다양한 유형이 있으며, 고정형, 돔 카메라, 돔 적외선 카메라, 적외선 카메라, 하우징 일체형 카메라, 스피드 돔 카메라로 분류할 수 있다.

IP 카메라는 기술이 발전할수록 인간의 안전 및 범죄예방, 편의성 증대를 목적으로 다양한 분야에서 사용되고 있다. 미국 센트라케어 병원에서도 의료 서비스의 향상 및 병원의 보안 강화를 위해 IP 카메라를 도입하였다. 센트라케어 병원은 보안의 강화를 위해서 기존의 노후된 아날로그 카메라와 DVR을 교체하는 프로젝트를 진행했으며, 병원 내 주요 시설들에 IP 카메라를 설치하여, 중앙의 통합 관제실에서 보안강화 및 실시간 모니터링을 수행할 수 있도록 활용되고 있다[2].

이처럼 다양한 분야에 IP 카메라를 사용하고 있으나 외부에서 IP 카메라를 해킹하는 등 위협이 끊이질 않고 있는 상황이다. 이러한 문제를 해결하기 위해 기존의 IP 카메라 진위 여부

판단하는 기술들에 대해 살펴보고 이러한 기존 기술의 한계점을 극복하기 위해 새로운 방식의 방안을 제시하도록 한다.

2. MAC 주소 기반 진위 판단 기술

MAC은 통신을 하는 디바이스에 저장된 OSI 2계층에서 사용하는 하드웨어 주소로 총 Fig. 2와 같이 48비트로 구성되어 있다[3].

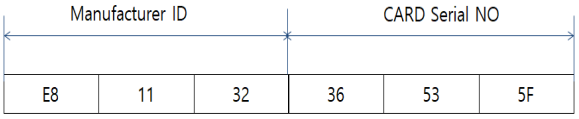

Fig. 2. MAC Address Configuration

Fig. 2는 Filtering System에서 MAC 주소를 이용하여 IP 카메라 진위 판단기술을 나타낸 것이다. 사용자는 Filtering System에서 허용할 IP 카메라의 MAC 주소를 등록한다. MAC 주소가 등록된 IP 카메라는 Filtering System을 통과하여 서버에 접근할 수 있으며, MAC 주소가 등록되지 않은 IP 카메라는 Filtering System에서 차단을 수행한다. Fig. 3의 네트워크 환경에서 IP 카메라 1은 MAC 주소가 AAA로 설정되어 있으며 IP 카메라 2는 MAC 주소가 BBB로 설정되어 있다. IP 카메라1 번과 2번이 서버로 네트워크 접근을 수행할 때 Filtering System은 통과하려는 네트워크 패킷의 MAC 주소를 확인한다. Filtering system에 IP 카메라 1번과 2번의 MAC 주소가 등록되어져 있으므로 Filtering System은 서버로의 접근을 허용한다. 만약 등록되지 않은 MAC 주소를 가진 노트북이 서버로 접근 시 Filtering System에 MAC 주소가 등록되어져 있지 않으므로 접근을 차단한다.

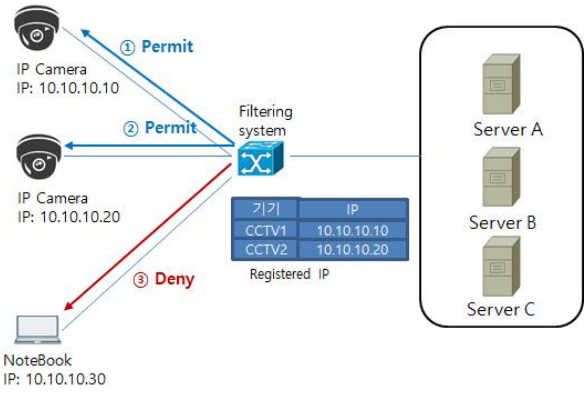

Fig. 3. Camera Verify With MAC Address

3. IP 주소 기반 진위 판단 기술

IP 주소는 컴퓨터 네트워크에서 장치들이 서로를 인식하고 통신을 하기 위해서 사용하는 특수한 번호이다. IPv4 주소는 오늘날 일반적으로 사용하는 IP 주소로써 이 주소의 범위는 32비트로 보통 0~255 사이의 십진수 넷을 쓰고 콤마로 구분하여 나타낸다.

IP 주소 기반 진위 판단기술은 MAC 주소 진위 판단과 동일하게 사용자에 의해 등록되어진 IP를 매칭 하여 진위 판단을 수행한다. Filtering System은 IP 카메라와 서버 사이에 위치하며 서버로 접근하는 네트워크 패킷을 분석하고 확인하여 패킷의 허용 및 차단을 수행한다[4]. 사용자는 접근 통제를 수행하기 위해 서버에 접속을 허용 할 IP 주소를 Filtering System의 접근통제 DB에 등록한다. 접근통제 DB에 IP 주소가 등록된 카메라가 서버에 접근을 수행할 때 Filtering System은 네트워크 패킷을 확인하여 패킷의 IP를 도출하고 Filtering System의 정책 DB에 저장되어 있는 IP와 비교하여 동일한 IP가 저장되어 있으면 허용하고, 도출된 IP가 정책 DB에 없으면 차단을 수행한다.

4. 전자서명을 이용한 진위 판단 기술

전자서명은 인터넷 환경에서 특정 사용자를 진위 판단을 수행하기 위하여 사용한다. Fig. 4.는 전자 서명의 원리를 설명한다. 일반적으로 전자 서명의 진위 판단 과정은 RSA 알고리즘과는 반대 원리며 비공개키 알고리즘과 공개키 알고리즘의 조합을 사용한다. 전자 서명은 자신을 다수의 타인에게 증명하는 기능이므로, 암호화 과정에서 자신만 아는 비공개키를 사용한다. 암호화한 전자 서명은 다수의 타인이 확인하므로 해독 과정에서는 공개키를 사용한다[5].

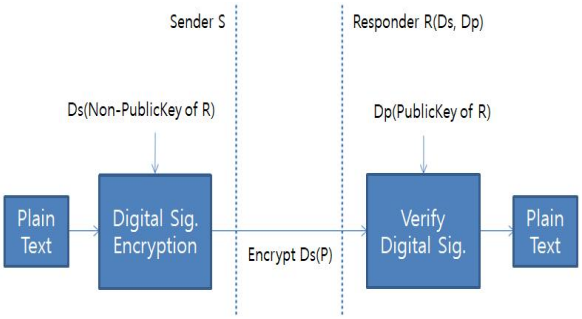

Fig. 4. Digital Signature Method

전자서명을 이용한 진위 판단기술은 전자서명 방식을 사용한 진위 판단 기법으로 공개키와 비공개키를 기반으로 진위를 판단한다. Filtering System은 IP 카메라를 진위 판단하기 위하여 IP 카메라에 전자서명과 IP 카메라의 공개키를 요구한다. IP 카메라는 등록되어 있는 개인키를 이용하여 전자서명을 수행한 후에 전자서명과 공개키를 Filtering System에 전달한다. Filtering System은 IP 카메라의 공개키를 이용하여 복호화 및 IP 카메라의 진위 판단을 수행한다. 전자서명을 이용한 방식은 진위 판단을 수행하기에 강력한 방법이나 각 IP 카메라 마다 공개키와 개인키를 등록해야 함으로써 실제 적용하기에는 문제가 있다. 또한 IP 카메라 마다 공개키와 개인키를 다르게 등록을 해야 하기 때문에 관리에 대한 문제도 있으며 진위 판단 방식이 다른 진위 판단 방식보다 복잡하기에 시스템 부하에 대한 문제도 발생할 수 있다.

5. IP 카메라 진위 판단기술 한계 및 개선

앞 절에서 살펴본 바와 같이 IP 카메라 진위를 판단하는데 사용될 수 있는 여러 가지 기술이 제안되었지만 한계점 또한 존재한다. IP 및 MAC 주소 기반의 진위를 판단하는 기술은 주소변조를 통한 위장공격에 취약하다. Fig. 5는 MAC 주소로 IP 카메라의 진위를 판단할 때 문제점을 나타낸다.

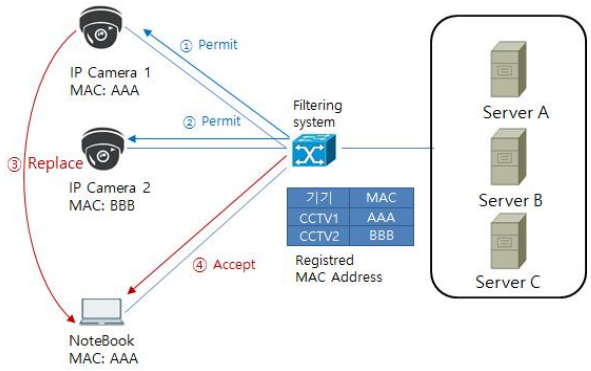

Fig. 5. Avoid of MAC Address Verify

Fig. 5는 공격자가 MAC 주소 진위 판단기술을 우회하여 서버로 접근하는 네트워크 환경을 나타낸 것이다. 네트워크 환경은 IP 카메라와 서버, 서버로의 네트워크 접근을 통제하는 Filtering System, 공격자가 MAC 주소 진위 판단기술을 우회하기 위한 노트북으로 구성되어 있으며, 공격자가 MAC 주소 진위 판단기술을 우회하기 위한 절차는 다음과 같다.

첫 번째, 공격자는 악의적인 행위를 수행하기 위하여 TcpDump 와 같은 패킷 모니터링 도구를 이용하여 1차적으로 IP 카메라 1의 MAC 주소를 알아낸다. 두 번째, 공격자는 IP 카메라 1을 제거한 후에 공격자가 준비한 악성코드가 심어져 있는 IP 카메라 또는 노트북으로 교체를 수행한다. 세 번째, 공격자는 교체한 기기를 IP 및 MAC 주소를 변경할 수 있는 소프트웨어를 이용하여 IP 카메라 1의 MAC 주소와 동일하게 설정을 변경한다. 네 번째, 공격자는 교체한 기기를 이용하여 서버로 접근을 수행한다. 다섯 번째, Filtering System은 IP 카메라 1로 위장한 공격자의 노트북이 서버에 접근 시 패킷을 분석한다. 이 때, MAC 주소 정보를 도출하기 위하여 네트워크 Packet 정보 중 OSI 7 Layer의 Layer2 헤더를 분석하며, MAC주소를 도출한 후에 Filtering System에 사용자가 정상으로 판단하기 위하여 저장했던 MAC 주소와 비교를 수행한다. 다섯 번째, 공격자가 교체한 기기가 IP 카메라 1과 MAC 주소가 동일함으로 Filtering System은 공격자가 교체한 기기를 사용자가 등록한 기기로 판단하여 서버로의 접근을 허용하는 문제가 생긴다.

위와 같은 문제를 해결하기 위하여 전자서명을 이용한 진위 판단 기술이 등장하였다. 전자서명을 이용한 진위 판단 기술은 공개키와 비공개키를 이용하여 IP카메라의 진위를 판단한다.

본 연구에서는 IP와 MAC기반, 전자서명을 이용한 진위 판단 기술의 한계점을 개선하기 위해 다음과 같은 방법을 연구하였다. 먼저 IP 카메라에 설치되어 있는 운영환경에서 필수기능으로 적용되어진 네트워크 통신의 특성과 IP 카메라 고유의 특성을 추출하고 이를 이용하여 특정한 고유의 값을 생성하여 기존 진위 판단기술 보다 정확성을 향상 시킨다. 또한 진위 판단 시 위장공격을 탐지하기 위하여 임의값인 nonce 값을 이용한다. 진위 판단 시스템은 임의적 nonce값을 생성하여 IP 카메라에 전달하고 IP 카메라는 해당 값을 해시 알고리즘을 이용하여 값을 도출한다. 도출된 값을 통하여 진위 판단 시스템은 정상 및 비정상을 판단하는 연구를 소개한다.

III. Effective IP Camera Verification

1. System Architecture

본 연구에서 제안하는 IP 카메라 진위 판단 시스템은 기존 진위 판단기술인 IP 주소 방식과 MAC 주소 방식, 전자서명

의 진위 판단 방식에서 진위 판단우회의 한계점을 개선한 방법으로 등록된 IP 카메라의 진위를 판단할 수 있다. 첫 번째 가설은 '동일한 장비라면 매 질문 시 장비에서 응답하는 장비의 정보가 동일할 것'이라는 것이다. 즉, 장비에서 응답하는 정보가 상이하다면 동일한 장비가 아니므로 식별이 가능하다. 하지만 첫 번째 가설은 쉽지는 않지만 재전송 공격으로 우회가 가능하다. 본 연구에서 제안하는 두 번째 가설은 '동일한 장비라도 IP 카메라와 진위 판단 시스템에 저장 되어 있는 해시 알고리즘이 동일하지 않을 것'이라는 것이다. 즉, IP 카메라가 변경되었다 해도 해시 알고리즘이 동일하지 않기 때문에 진위 판단우회가 힘들다는 가설을 설정한다.

2. System Diagram

본 연구에서 제안하는 IP 카메라의 진위를 판단하는 시스템의 아키텍처는 Fig. 6과 같다. IP 카메라 진위 판단 시스템 아키텍처는 사용자가 네트워크 패킷을 허용할 IP 카메라를 등록하는 IP 카메라 등록 모듈과 네트워크 통신과 IP 카메라의 특징을 조합하여 검사를 수행하는 1차 검사 모듈, IP 카메라와 진위 판단 시스템간의 동일한 nonce 값을 이용하여 진위를 판단하는 2차 검사 모듈과 IP 카메라 등록정보, 시간정보, IP 카메라 상태등을 저장하는 데이터베이스, 진위 판단 시스템의 상태 정보 및 검사정보를 저장하는 로그가 있으며, 사용자가 실시간 정보를 확인할 수 있는 시스템 모니터링 모듈로 구성되어 있다.

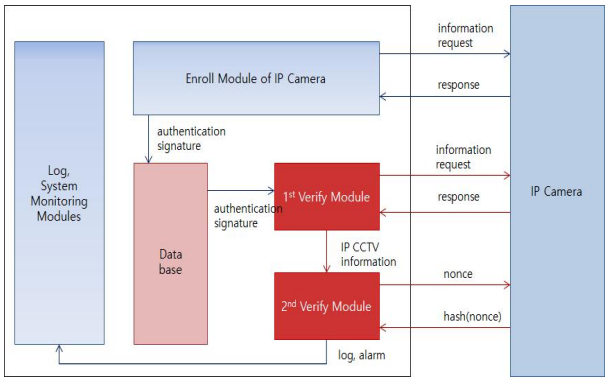

Fig. 6. IP Camera system Architecture

등록이 완료되면 등록된 IP 카메라의 진위를 판단하기 위해 주기적으로 1차 검사와 2차 검사를 수행한다. 1차 검사에서 IP 카메라의 정보를 통해 만들어진 시그니쳐를 이용하여 진위 여부를 판단하며, 비정상으로 판단되면 사용자에게 알람을 전송하고 정상으로 판단되면 2차 검사를 수행한다. 2차 검사는 nonce 값을 생성하여 해시 알고리즘을 통해 값을 도출하고 비교하여 IP 카메라의 진위 여부를 판단 한다. 1차 검사와 동일하게 2차 검사 수행 결과가 비정상으로 판단되면 사용자에게 알람을 전송한다. 등록 모듈 및 1차 검사 모듈에서는 사용되는 시그니쳐를 생성하기 위하여 IP 카메라 진위 판단 시스템은 다양한 정보를 IP 카메라에 요청한다. 먼저 IP 카메라의 열려있는 포트와 닫혀 있는 포트에 대한 정보를 사용하고, 시스템의 통신 특성으로 TTL, 응답 패킷의 옵션정보(Tcp Mass, Windows Scale, Windows Size, Tcp Syn Size)등을 사용한다. 이러한 정보는 운영체제의 커널에 따라 조금씩 달라지는 정보로써 유사한 제품이라 하더라도 상이한 정보가 생성되며, 해당 정보를 이용해 시그니쳐를 생성한다.

3. System Function

본 연구에서 제안하는 IP 카메라 진위 판단 시스템의 모듈별 동작절차는 다음과 같이 이루어진다.

등록된 IP 카메라의 진위를 판단하기 위해서는 IP 카메라 등록 모듈에 검사를 수행할 IP 카메라를 등록해야 한다. IP 카메라 등록 모듈은 IP 카메라의 진위를 판단하기 위하여 IP 카메라의 정보를 수집하고, 수집된 정보를 통하여 진위 판단에 필요한 시그니처를 생성한다.

사용자는 IP 카메라를 검사를 수행하기 위하여 IP 카메라 진위 판단 시스템에 등록할 IP 주소를 입력한다. IP 주소를 사용자에게 입력받은 진위 판단 시스템은 ICMP 프로토콜을 사용하는 리눅스 명령어인 PING 을 이용해 네트워크의 연결 상태 및 TTL 값을 수집한다. TTL값이 OS 마다 다르기 때문에 IP 카메라의 진위를 판단하기 위해 시스템별 정보를 미리 파악해야 한다.

Fig. 7은 IP 카메라 등록모듈에서 IP 카메라 등록을 하기 위한 절차를 나타낸 것이다. IP 카메라가 정상적으로 네트워크에 연결되어 있다면 등록 모듈은 1차 검사모듈에서 사용할 시그니처를 생성하기 위하여 IP 카메라의 시스템 정보 및 네트워크 통신 정보를 수집한다. 시그니처를 생성하기 위하여 사용하는 IP 카메라의 정보를 살펴보면 진위 판단 대상인 IP 카메라의 열려 있거나 닫혀 있는 포트를 점검하는 것이다. 즉, 일반적인 윈도우 시스템의 경우 135/TCP, 445/TCP 등 넷 바이오스와 관련된 포트가 열려있는 경우가 많으며,

80/TCP, 443/TCP, 22/TCP 등 서비스에 관련된 포트는 닫혀있는 경우가 많다. 반면 리눅스나 유닉스 시스템의 경우는 22/TCP와 같은 SSH 또는 23/TCP와 같은 원격접속 서비스 등이 열려있는 경우가 많다.

진위 판단을 수행할 IP 카메라의 경우 영상정보를 전송하기 때문에 스트리밍에 관련된 포트가 열려 있지만 이는 일반적인 윈도우나 유닉스 단말기에는 열려있지 않은 포트이다. 이러한 가정에 따라 진위 판단을 수행할 IP 카메라를 등록할 때 열려있는 포트와 닫혀있는 포트의 정보를 수집하게 된다. 이와 같은 정보는 IP 카메라가 달라질 경우 정보가 달라질 수 있으며, 동일 제조사의 IP 카메라라 하더라도 설정에 따라 다를 수 있다. 그 외에 OS 정보인 WINDOW SIZE값과 TCP MSS 정보를 수집한다. 두 번째는 통신의 특성이다. ICMP TTL 값은 OS를 비교하기 위해서 사용 및 시그니쳐 생성에도 사용된다. 이는 시스템의 커널의 종류에 따라 달라지는 것으로 만약 다른 시스템이라면 운영체제 또한 달라질 것이고 이는 응답되는 정보가 달라질 수 있다.

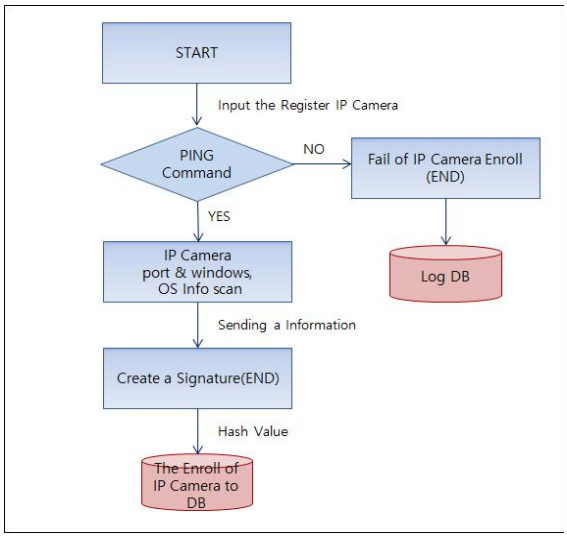

Fig. 7. Enroll Process of IP Camera

4. 1st IP Camera Verification Module

IP 카메라 1차 진위 판단모듈은 등록되어진 IP 카메라를 진위 판단하기 위한 첫 번째 진위 판단 기능이다. 1차 진위 판단 모듈은 프로세스가 실행이 되면 데이터베이스에서 등록된 IP 정보를 수집하고, 연결리스트로 구현하여 메모리에 적재한 후에 적재된 IP 정보를 하나씩 읽어와 1차 진위를 판단메커니즘을 수행한다.

IP 카메라의 IP 정보를 입력받으면 1차 진위 판단 모듈은 PING 명령어를 이용하여 TTL 값을 추출한다. 등록 모듈에 수집한 TTL 값과 추출된 TTL 값을 비교하여 값이 다르면 등록되지 않은 IP 카메라로 판단하고 사용자에게 알람을 전송한다. TTL 값이 동일하면 등록 모듈에서 수행했던 방식과 동일하게 시그니쳐를 생성하기 위하여 IP 카메라의 열려있는 Port와 닫혀있는 Port 정보, TCP Window Mss, TCP Window Scale, IP 주소와 MAC 주소, IP 카메라 OS 정보, IP 카메라 TTL 값을 추출한다. 추출된 정보는 해시 알고리즘을 이용하여 시그니쳐를 생성하며, IP 카메라 등록 모듈에서 생성된 시그니쳐 값을 데이터베이스에서 수집하여 1차 진위 판단 모듈에서 생성한 시그니쳐와 등록모듈에서 생성된 시그니쳐를 비교한다. 값이 동일하면 사용자가 등록한 IP 카메라로 판단하게 되며 2차 진위 판단을 위해 해당 IP를 2차 진위 판단 모듈에게 전달한다.

Fig. 8.은 IP 카메라 1차 진위 판단모듈의 절차를 나타낸 것이다.

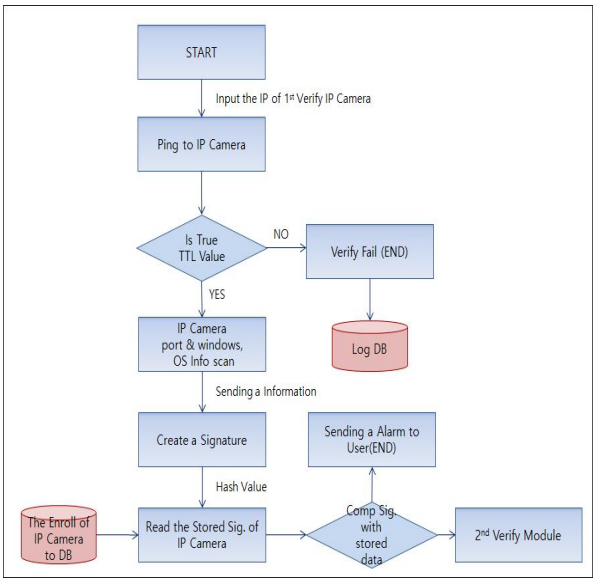

Fig. 8. A Process of 1st Verify Module of IP Camera

5. 2nd IP Camera Verification Module

IP 카메라 2차 진위 판단모듈은 1차 진위 판단모듈을 통과한 IP 카메라를 추가적으로 진위 판단을 수행하기 위한 기능이다. 1차 진위 판단모듈에서 진위 판단을 수행하기 위하여

생성한 시그니처는 값이 항상 동일하기 때문에 재전송 공격을 통하여 진위 판단 우회가 가능하다. 진위 판단우회에 대한 문제를 해결하기 위하여 2차 진위 판단모듈을 수행한다. IP 카메라 2차 진위 판단모듈의 프로세스는 Fig. 9와 같다.

IP 카메라 2차 진위 판단 모듈은 랜덤한 수인 nonce 값을 생성하여 진위를 판단하는 방식이다. 1차 진위 판단 모듈은 2차 진위 판단 모듈을 수행하기 위해 1차 진위 판단 모듈에서 정상으로 판단되어진 IP를 수집하여 2차 진위 판단 모듈에게 전달한다. 진위 판단을 수행 할 IP를 입력받은 2차 진위 판단 모듈은 먼저 랜덤한 값인 nonce 값을 생성한 후 입력받은 IP를 통하여 해당 카메라에 nonce값을 전달한다. IP 카메라는 IP 카메라 진위 판단 시스템에서 전달받은 nonce 값을 저장한 후 nonce 값을 단방향 암호화인 해시 알고리즘을 이용하여 값을 추출한다.

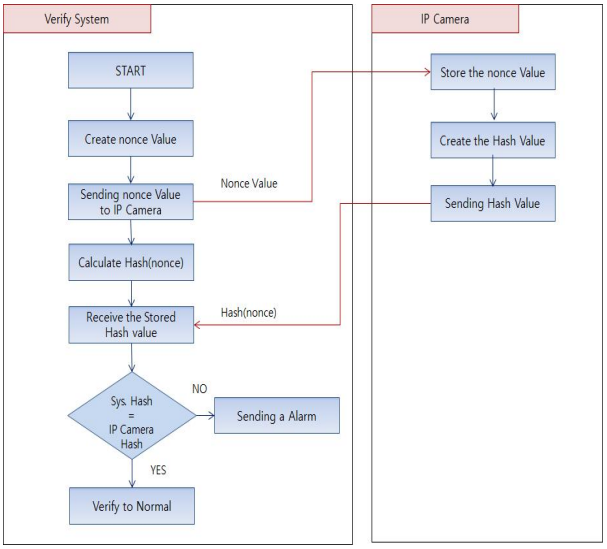

Fig. 9. A Process of 2nd Verify Module of IP Camera

IP 카메라 진위 판단 시스템은 IP 카메라에서 보내온 해시 값을 전달받으면 현재 추출 되어진 해시 값과 IP 카메라에서 보내온 해시 값을 비교하여 최종 IP 카메라의 진위여부를 판단한다.

Ⅳ. Conclusions

본 연구에서는 IP 카메라 진위여부를 확인하기 위하여 IP 카메라를 주기적으로 진위 여부를 판단하는 IP 카메라 진위 판단 시스템을 제시하였다. 이 연구에서는 IP 카메라 환경의 특성과 위협, 그리고 이미 연구자들에 의해 연구되고 있는 진위 판단기술을 살펴보고, 현재 진위 판단기술의 한계점을 분석하며, 한계점 해결을 위한 접근 방향을 제시하였다. 본 연구의 결과로 현재 활성화 되고 있는 IP 카메라 환경에서 보안 위협의 근간이 되는 진위 여부를 판단하는 기능이 개선되어 보다 안전하고 신뢰성 있는 IP 카메라 사용이 가능해질 수 있다.

향후, 본 연구를 확장하여 IP 카메라를 포함한 다양한 기기에서 사용이 가능하도록 지속적으로 연구를 진행할 계획이며, 보다 안정적이고 보안성이 강화된 모델을 만들어 체계적으로 연구를 확장해 나갈 계획이다.

REFERENCES

[1] SunYoung Heo, TaeHeon Moon, “An Analysis on the CCTV Location Appropriateness and Effectiveness for the Crime Prevention”, KARG, Vol.21, pp. 739-750, 2015.
[2] http://www.ciokorea.com/news/25488.
[3] http://www.aitimes.kr/news/articleView.html
[4] https://ko.wikipedia.org/wiki/IP_주소
[5] Tae Woon Seo, Sung Ryoul Lee, “An Analysis of Vulnerabilities and Performance on the CCTV Security Monitoring and Control”, JKMS, Vol.15, pp, 93-100, 2012.
[6] YoungJin Chae,. “Design and implement enhanced user authentication system based on ID/PW using smart phones”. PCU Master, 2016.

저 자 소 개

Jae-Kyung Park

1993: BS, Department of Computer Engineering, Dongguk University

1996: MS, Department of Computer Science, Hongik University

2002: PhD, Department of Computer Science, Hongik University

He is interested in Network security, cyber security.Areas

Hyun-Woo Kim

2018: MS, Department of Information Security, Sungkyunkwan university

He is interested in System security, cyber security.Areas