클라우드를 활용한 IoT 스마트 홈 침입탐지 모니터링 시스템

김동주 [1], 최민주 [1], 이현경 [1], 정혜주 [1], 김성욱 [2]
[1] 서울여자대학교 정보보호학과 학부생
[2] 서울여자대학교 정보보호학과 교수

rlaehdehd20@swu.ac.kr, swu89mj@swu.ac.kr, hk0305@swu.ac.kr, jhj0912@swu.ac.kr, kim.sungwook@swu.ac.kr

Cloud-based IoT Smart Home Intrusion Detection and Monitoring System

Dong-Ju Kim[1], Min-Ju Choi[1], Hyeon-Kyeong Lee[1], Hye-Ju Jeong[1], Sung-Wook Kim[2]
[1]Dept. of Information Security, Seoul Women's University
[2]Dept. of Information Security, Seoul Women's University

요 약

홈 IoT 사용의 확대로 우리의 생활이 편리해진 반면, 보안 취약점을 통해 사생활을 침해하는 문제가 다수 발생하고 있다. 따라서 사용자들이 안전하게 사용할 수 있는 스마트 홈 보안 시스템이 필수적이다. 본 논문에서는 웹 페이지에 홈 IoT 환경을 구성한 후, AWS 서비스를 활용하여 로그를 수집하고 이상 징후를 찾는다. 침입 및 공격이 탐지되면 웹 페이지를 통해 사용자에게 알림을 전송한다. 사용자에게 경고와 조치 안내를 제공하여 빠른 대응이 가능하도록 한다.

1. 서론

현대의 디지털 시대에 IoT(Internet of Things) 기술과 기기들은 사용자들의 일상생활을 보다 더 편리하게 변화시키고 있다. 특히 스마트 홈은 센서와 카메라 등을 직접 제어할 수 있어, 사용자들의 생활에 편의성을 높이는 데 도움이 된다. 하지만 최근 보안 취약점을 통해 월패드 해킹 등 사생활을 침해하는 문제도 함께 발생하고 있다. [1]

스마트 홈 시스템을 안전하게 사용하기 위해선 외부 침입자나 악의적인 공격으로부터 사용자의 개인 정보와 시스템을 보호해야 한다. 해킹이 시도되어도 사용자들은 상황을 신속하게 파악하기란 어렵다.

사물인터넷 환경에서의 보안 문제에 대응하기 위해 악성 트래픽을 감지하고 사용자에게 실시간 경고를 제공하는 시스템이 필요하다. 따라서 본 논문에서는 사용자들의 개인정보 유출과 사생활 침해까지 이어지는 사태를 방지하고 안전한 사물인터넷 환경을 제공하기 위해 모니터링 대시보드를 제공하고 사용자에게 알림을 전송하는 시스템을 구현하고자 한다.[2]

2. 에이전트 개발도구의 요구사항

2.1. 관련 연구와의 차별성

본 시스템은 사용자와 관리자에게 실시간 경고 알림과 함께 모니터링 대시보드를 제공하여 사용자가 보안 상태를 쉽게 확인할 수 있도록 설계되었다. 모니터링 대시보드는 AWS 의 CloudWatch 를 활용하였다. CloudWatch 는 각 사용자가 구동 중인 가상머신의 자원 사용량을 모니터링하고, 자원 사용량이 급증하면 경고 메시지를 통해 사용자에게 알려주는 기능을 제공한다.[3] 본 연구에서는 네트워크 트래픽의 사용량을 대시보드 형태로 제공하고 있으며 설정한 네트워크 트래픽 임계치에 따라 웹 앱에 알림을 전송한다.

2.2. 프로그램 주요 기능

2.2.1. IoT 기기 제어

사용자는 웹 앱을 통해 다양한 IoT 기기를 제어할 수 있다. 언제 어디서나 전등 스위치, 멀티탭, 도어락,

카메라 등의 스마트 홈 기기들을 간편하게 제어할 수 있다.

2.2.2. 회원가입과 로그인

사용자는 회원가입을 통해 개인 정보를 입력하고, 자신의 IoT 기기를 시스템에 등록할 수 있다. 권한이 있는 기기에만 접근이 가능하며 관리자 계정이 사용자 계정들을 관리하여 보안을 강화할 수 있다.

2.2.3. 침입탐지 모니터링 대시보드

사용자는 웹 앱의 실시간 탐지 결과를 대시보드로 확인할 수 있다. 관리자가 설정한 탐지 규칙에 따라 악성 트래픽이 발생할 때, 시스템은 푸시 알림과 메일을 통해 사용자와 관리자에게 경고를 전달하여 공격에 신속하게 대응할 수 있다.

2.3. 프로그램 구현

프로그램은 React.js(프론트엔드), Spring boot(백엔드)를 활용하여 개발하였다. 계정 정보 및 IoT 기기 정보는 MySQL 데이터베이스에 저장했으며, 이를 AWS RDS 인스턴스에 연결하여 활용하였다.

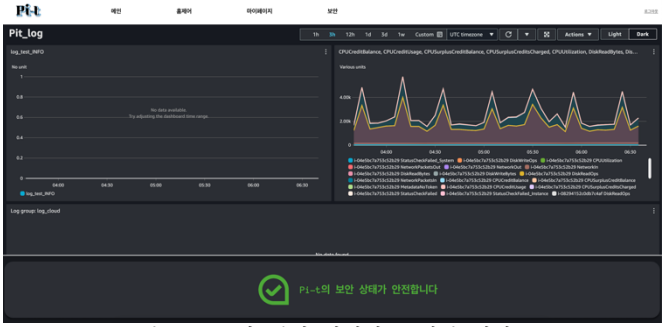
라즈베리파이 4 대와 아두이노 2 대를 사용하여 IoT 기기(카메라, 멀티탭, 도어락, 전등)를 개발하고 미니 스마트홈 환경을 구축하였다. IoT 기기와 웹 앱 간의 통신은 Microsoft Azure 의 IoT Hub 를 활용하였다.

AWS CloudWatch 로 웹 앱에 발생하는 로그를 수집하고 탐지규칙을 설정하여 경고 알림을 생성하였다. 이어서 실시간 탐지결과를 대시보드화 하여 웹 앱에 탑재하였다.

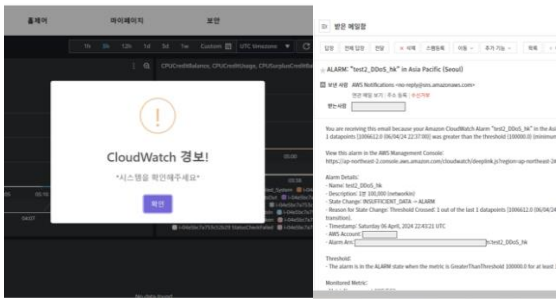
2.4. 공격 탐지 규칙 설정

관리자가 디도스 공격을 실시간으로 인지할 수 있게 함으로써 공격에 즉각적인 대응을 할 수 있도록 하였다. AWS CloudWatch 에 디도스 공격을 의심할 수 있는 네트워크 트래픽의 임계치를 설정하여 경보를 등록하였다. 해당 경보는 Simple Notification Service(SNS) 토픽에 등록되어 있으며, 해당 SNS 토픽을 Simple Queue Service(SQS)가 구독한다. 이를 통해 백엔드에서 주기적으로 SQS 를 확인하여 메시지를 처리하고 메시지를 프론트엔드로 전달하여 알림을 제공한다.

마지막으로 AWS CloudWatch 의 대시보드 공유 기능을 활용하여 설정한 네트워크 트래픽 임계치를 시각화하여 웹 앱 보안 탭에 대시보드로 제공하였다.



<그림 1>. 보안 탭의 실시간 트래픽 대시보드



<그림 2>. 악성 트래픽 경고 알림 및 메일

2.5. 결과

본 연구에서 개발한 클라우드 기반 IoT 스마트 홈 침입 탐지 모니터링 시스템은 스마트 홈 환경에서의 보안 위협에 대응하는 신속하고 효과적인 솔루션을 제공한다. AWS CloudWatch 를 활용한 로그 수집 및 분석을 통해, 사용자는 실시간으로 보안 위협을 인지하고 적절한 조치를 취할 수 있게 되었다.[4] 이 시스템은 사용자가 언제 어디서나 자신의 집 보안 상태를 모니터링할 수 있도록 하여, 스마트 홈 기기 사용의 안전성을 크게 향상시킨다.

본 연구에서 개발된 시스템의 소스 코드 및 관련 자료는 다음 GitHub 리포지터리에서 확인할 수 있다.
https://github.com/PiT-HOME/PiT-HOME_WEBAPP

참고문헌

[1] 장나래, (2022 년 12 월 20 일), '거실 인터폰' 아닌 '해킹 월패드', 40 만 가구 사생활이 유출됐다, 한겨레,https://www.hani.co.kr/arti/society/society_general/1072351.html

[2] 전정훈, 스마트 홈 공격에 대한 대응 방안의 연구, 융복합지식학회논문지, 제 10 권, 제 2 호, pg109-118, 2022

[3] 최상훈, 클라우드 컴퓨팅의 미시적 분석을 위한 메모리 덤프 및 덤프기록 고속화 기법 연구, 석사학위논문, 2016

[4] 김수정, 악성코드 및 로그 분석을 이용한 엔드포인트 위협탐지 기술 연구, 석사학위논문, 2020