오픈 소스를 활용한 IoT 환경 관리 시스템

박재민[O], 김태욱[**], 최상용[*], 이종락[*], 김정삼[*]
[O]영남이공대학교 사이버보안학과,
[*]영남이공대학교 사이버보안학과,
[**]지피다
e-mail: tjrqhddl123@naver.com[O], tw.kim@zipida.com[**], csyong95@gmail.com[*],
jllee@ync.ac.kr[*], jskim@ync.ac.kr[*]

IoT Environment Management System Using Open Source

Jae-Min Park[O], Tae-Uk Kim[**], Sang-Yong Choi[*], Jong-Rak Lee[*], Jeung-Sam Kim[*]
[O]Dept. of Cyber security, Yeungnam University College,
[*]Dept. of Cyber security, Yeungnam University College,
[**]ZiPIDA

● 요 약 ●

스마트시티로 가는 첫걸음이자 핵심이라 할 수 있는 IoT 기술이 우리의 삶을 변화시키고 있다. 원격에서 집 내부의 상태를 확인하며 조정할 수 있고, 집 내부의 상황도 영상을 통해 확인할 수 있게 되었다. 이처럼 IoT 기술은 우리 삶의 편리함을 제공하고 중요한 요소가 되었지만, IoT 환경 관리의 주체가 사용자 개인이거나 IoT 환경상태를 모니터링하며 관리할 수 있는 수단이 없어 관리가 되지 않고 있고 공격을 받아도 사용자가 알 수 없다는 특성 때문에 IoT 보안에 있어 심각한 문제를 일으킬 수 있다. 이러한 문제에도 불구하고 IoT 보안에 대한 인식과 IoT 환경에 특화된 관리 시스템은 갖춰지지 않고 있다. 본 논문에서는 오픈 소스 데이터 분석 및 시각화 솔루션인 Elastic Stack을 활용하여 손쉽게 IoT 환경을 관리하고 상태를 시각화하여 제공하는 IoT 환경 관리 시스템을 제안한다.

키워드: 사물인터넷(Internet of Things), 엘라스틱스택(Elastic Stack), 시각화(Visualization)

I. Introduction

사물인터넷, IoT 디바이스를 우리 주변에 흔히 볼 수 있는 시대가 되었다. 도시의 범죄예방과 치안을 위한 CCTV와 가정의 각종 스마트 가전까지, 우리 생활 곳곳에 자리 잡은 IoT 기술은 우리 삶을 편리하고, 안전하게 만들어준다. 하지만 IoT 기술이 이점만 있는 것은 아니다. 기존의 우리 생활 속 여러 불편했던 부분들이 IoT 기술로 인해 편리해졌지만 그만큼 공격받기가 쉬워졌다. 기존의 물리적인 침입이나 공격이 아닌 인터넷을 통한 침입과 공격을 할 수 있게 되어 과거에 비해 공격과 침입이 간편해지고 은밀한 공격이 가능하게 되었다. 이러한 치명적인 문제점을 해결하기 위한 IoT 환경을 관리하는 시스템은 사용자들의 미흡한 보안 인식과 보안 개발사들의 소극적 태도로 인해 아직 자리 잡지 못하고 있다. 사용자들은 자신의 IoT 환경이 공격을 받아도 이 사실을 알 수 있는 수단이 없어 IoT 보안에 대한 필요성을 못 느끼고 있고 이러한 이유로 인해 개발사들도 IoT 환경 관리 시스템에 투자 및 개발을 하지 않고 있다. 그래서 본 논문에서 제안하는 IoT 환경 관리 시스템을 통해 사용자가 IoT 환경을 직접 관리 및 모니터링하고, IoT 보안에 관한 관심을 가질 수 있게끔 IoT 환경 맞춤형 시각화 도구를 제공한다. 이로 인해 사용자들은 IoT 디바이스들을 본래 목적에 맞게 안심하고 사용할 수 있으며 자신의 IoT 환경을 직접 관리하고 모니터링 할 수 있는 수단이 생기게 된다.

II. Preliminaries

1. Related works

1.1 Elastic Stack

Elastic Stack을 ESXi VMware 가상화 환경에 설치된 Ubuntu 운영체제에 구동시켜 Suricata에 의해 탐지된 IoT 홈캠 침입 로그 데이터를 수집하고 처리하여 최종적으로 시각화하는 데 사용하였다.

오픈 소스 기반 데이터 검색 및 분석 엔진인 Elastic Stack은 Suricata에서 침입을 탐지한 정보를 로그의 형태로 받아 이를 가공하여 대시보드로 시각화를 하는 역할을 한다. Elastic Stack은 총 4개의 요소로 구성되어 있다. 데이터를 수집하는 Filebeat, 다양한 플러그인을 이용하여 데이터 집계 및 보관, 서버 데이터 처리, 파이프라인으로 데이터를 변환 후 Elasticsearch로 전송하는 Logstash, Rest API를 이용해 전송받은 데이터를 분석하고 실시간으로 저장하는 Database기능을 하는 Elasticsearch, 처리된 데이터를 시각화해주는 Kibana로 구성되어 있다[1].

1.2 Filebeat

Filebeat는 로그 데이터를 전달하고 중앙 집중화하기 위한 데이터수집기이다. 지정한 로그 파일 또는 위치를 모니터링하고 로그 이벤트를 수집한 다음 인덱스를 위해 Elasticsearch 또는 Logstash로 전달한다. Filebeat를 시작하면 로그 데이터에 대해 지정한 위치에서 이벤트가 발생할 때마다 Filebeat는 데이터 수집기(Harvester)를 시작한다. 하나의 로그파일을 바라보는 각 데이터 수집기(Havester)는 새 로그의 데이터를 읽고 Libbeat로 보낸다. Libbeat는 이벤트를 집계하고 집계된 데이터를 Filebeat 설정에 구성된 출력으로 데이터를 보낸다[2].

1.3 Logstash

Logstash는 특정 장소에 저장되고 데이터를 읽어 분석이 가능한 포맷으로 정제한 뒤 Elasticsearch의 데이터 저장소로 전달하는 역할을 한다. Logstash에서 Elasticsearch로 각 시스템에서 발생한 다양한 형식의 데이터를 전달하기 전에 반드시 검색 및 분석을 위한 형태로 정제하는 과정을 거쳐야 한다. 데이터 정제는 JSON 형태로 입력(Input), 정제(Filter) 및 출력(Output)을 선언해 주기만 하면 된다. 입력 형태는 파일이나 TCP, UDP, S3 bucket(Amazon AWS), RabbitMQ, Redis 등을 지원하며, 많은 플러그인 방식으로 확장할 수 있으므로 다양한 기술과 함께 사용이 가능한 동적 데이터 수집 및 처리 파이프라인이다. 그리고 필터를 통해 데이터가 소스에서 저장소로 이동하는 과정에서 각 이벤트를 구문 분석을 하고 명명된 필드를 식별하여 구조를 도출한다. 구조 도출은 Grok을 통해 비정형 데이터에서 구조를 도출하거나 IP주소에서 위치 좌표 해독을 한다. 이를 통한 정보를 공통된 형식으로 변환하고 통합하여 더욱 빠르고 쉽게 분석한 후 원하는 곳으로 데이터를 라우팅하여 여러 저장소로 다운 스트림 한다[3].

1.4 Elasticsearch

Elasticsearch는 분산 환경을 지원하는 JAVA 기반의 오픈 소스 검색엔진 라이브러리인 Lucene을 기반으로 구현된 분산 검색엔진으로 설치와 서버 확장이 편리한 기술이다. Elasticsearch는 검색 기능뿐만 아니라 검색한 데이터를 집계할 수 있는 기능이 있어 분석 엔진으로도 활용할 수 있다. 여기서 검색, 집계 및 빠른 분석 기능을 정보보호 빅 데이터 분석에 활용한다. Elasticsearch 검색기술을 이용하여 Github, E-Bay, Gideon, Wikipedia, Netflix 등 많은 세계적 기업들이 구축하여 운영하고 있다. RESTful API2를 지원하기 때문에 다양한 환경에서 사용이 가능한 분산 검색엔진으로 Scale-out 확장성과 JSON 문서 기반으로 안정성과 관리의 편리성을 제공한다. Elasticsearch의 특징으로는 분산과 확장성, 고가용성, Multi-Tenancy, Full Text Search, JSON 문서 기반, schema Free와 같은 특징들이 있다[4].

1.5 Kibana

Kibana는 자바스크립트로 개발되었으며 내부에 웹 서버를 내장하고 있어 별도의 소프트웨어 설치는 필요 없다. 운영체제에 따라 다양하게 설치가 가능한 시각화 오픈소스도구이다. 검색엔진인 Elasticsearch를 통해 수집 된 데이터의 관계성을 히스토그램, 막대그래프, 파이 차트와 같이 시각적으로 보여주거나 시계열 데이터의 경우 시간을 기준으로 분석한 결과를 시각화하여 각 데이터의 시계열적인 연관성을 찾아내는 것이 가능하다. Geo location을 이용하여 지리적으로 특정 위치의 분포도를 지도상에 시각화함으로써 데이터의 상관관계도 보여준다. Kibana는 Elasticsearch에서 분석된 데이터를 시각화하여 텍스트 로그 상태에서는 볼 수 없었던 특이점을 찾아내거나, 과거 로그와 실시간으로 발생하는 로그를 동시에 시각적으로 보여줄 수 있기 때문에 누적된 과거 데이터로부터 얻을 수 있는 추이를 바탕으로 실시간 데이터를 분석하여 보여줌으로써 미래 예측을 할 수 있는 기반을 제공한다. Kibana는 시각화를 통해 가시성을 보장할 뿐만 아니라 Elastic Stack을 전체적으로 구성 및 기능을 통합 관리할 수 있고 확장 가능한 사용자 인터페이스 도구의 역할도 한다[5].

III. IoT Environment Management System Using Open Source

본 논문에서 제안하는 IoT 환경 관리 시스템은 사용자에게 IoT 환경을 직접 관리하고 상태를 모니터링 할 수 있는 수단의 제공이라는 목적이 있다. IoT 환경 관리 시스템은 사용자가 IoT 디바이스를 이용함으로써 로그 데이터가 생성되는 단계, 생성된 로그 데이터를 Filebeat와 Logstash가 수집 후 JSON 포맷으로 처리하여 Elasticsearch로 전송하는 단계, Filebeat와 Logstash로부터 전송받은 로그 데이터를 Elasticsearch가 인덱스 처리 및 분석하여 시각화를 위해 Kibana로 전송하는 단계, 최종적으로 Elasticseach로부터 전송받은 인덱스를 Kibana에서 사용자에게 대시보드를 통해 시각화하여 IoT 환경상태 정보를 제공하는 5가지 단계로 진행된다. IoT 환경 관리 시스템의 전체 아키텍처는 아래와 같다. 연구에서는 RaspberryPi를 IoT 디바이스로 활용하여 실험환경을 구성하였다.

Table 1. System Environment

Item	Value
Filebeat	Version 6.4.2
Logstash	Version 6.4.2
Elasticsearch	Version 6.4.2
Kibana	Version 6.4.2

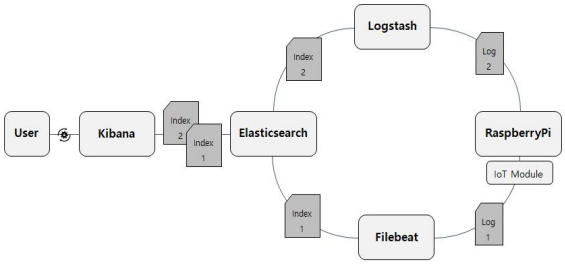

Fig. 1. System Architecture

1. Log Data

IoT 플랫폼으로 RaspberryPi를 사용한다. Raspbian 운영체제 설치와 초기 네트워크 설정 후 지원하는 모듈을 설치하여 IoT 디바이스로 활용한다. 사용자가 IoT 디바이스를 이용하면 IoT 디바이스에서는 상태정보 및 보안과 관련된 여러 타입의 로그가 생성된다. 기존의 IoT 환경에 맞는 관리 시스템이 없어 활용되지 않고 버려지던 로그들을 IoT 환경 관리 시스템에서 활용하여 IoT 환경상태와 보안 현황 정보를 대시보드를 통해 시각화하게 된다.

2. Data Collection

Filebeat가 RaspberryPi 로부터 가져온 로그 데이터를 수집하여 Elasticsearch로 전송을 하는 단계이다. 설치와 기본 설정을 끝내면 Filebeat.yml 파일에서 가져올 로그가 저장된 디렉터리와 파일명을 지정해주고 Elasticsearch의 주소로 전송 설정을 한다. Filebeat는 공식적으로 Suricata의 로그 포맷을 지원하기 때문에 Filebeat를 사용한다.

3. Data Aggregation & Parsing

Logstash가 RaspberryPi 로부터 가져온 로그 데이터를 수집하여 파싱하고 Elasticsearch로 전송하는 단계이다. 설치와 기본 설정을 끝내고 나면 Logstash.conf 설정 파일의 Input 설정에 가져올 로그가 저장된 디렉터리와 파일명을 지정해주고 Filter에서 시스템 로그를 JSON 포맷으로 파싱을 해준다. 그리고 Output 설정에서 Elasticsearch의 주소로 전송 설정을 한다.

4. Indexing & storage

IoT 환경 관리 시스템 아키텍처에서 Database기능을 수행하는 Elasticsearch는 Filebeat와 Logstash 에서 전송받은 JSON 포맷의 데이터를 Filebeat 인덱스와 Logstash 인덱스로 구분하여 저장하고 최종적으로 시각화하기 위해 Kibana로 전송하는 역할을 한다.

5. Analysis & visualization

Kibana에서 Elasticsearch으로부터 전송받은 두 종류의 인덱스를 전송받아 데이터를 최종적으로 대시보드를 통해 시각화한다. 여러 타입의 그래프와 지도로 사용자가 원하는 대시보드를 직접 제작할 수 있으며 이렇게 만들어진 대시보드는 Kibana의 설정 파일에 설정된 주소로 웹 접속을 하면 원격에서 IoT 환경 상태 현황을 대시보드를 통해 확인할 수 있다.

6. 결과 및 분석

RaspberryPi에 설치한 다양한 IoT 모듈을 통해 사용자의 목적에 맞는 IoT 환경을 구성하였고, Elastic Stack을 활용한 IoT 환경

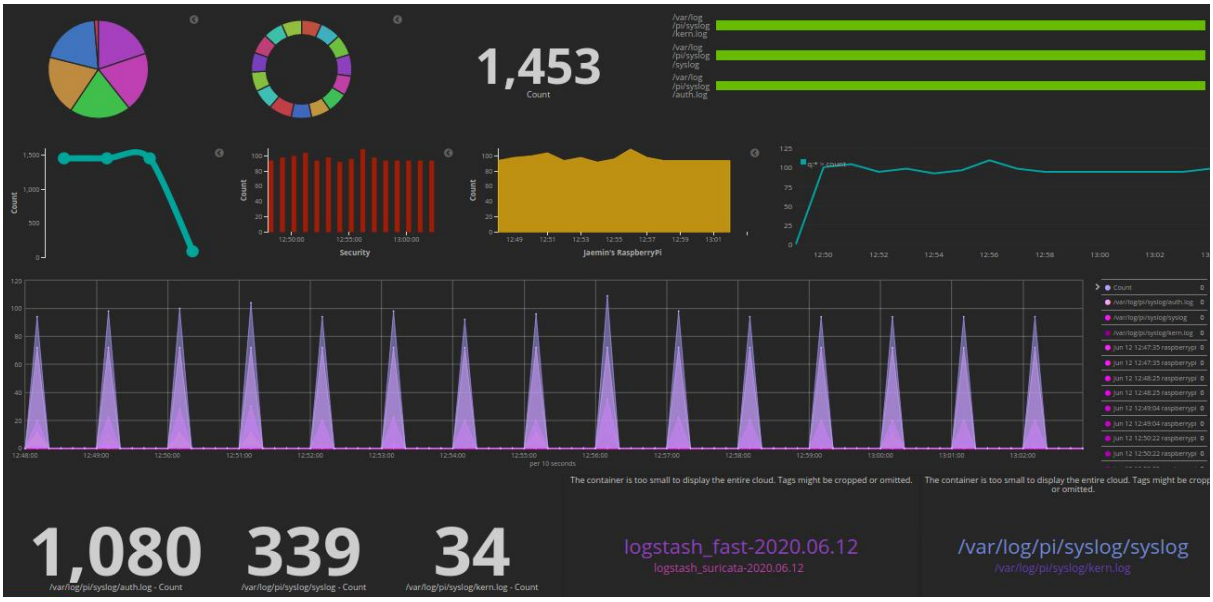

Fig. 2. IoT Management System. The pie chart at the top represents the ratio of each index, and the number at the top represents the total number of indexes. Each other item is a graph of the status and threat of each type.

관리 시스템을 구현하였다. 그 결과 외부에서 웹브라우저를 통해 IoT 환경 관리 시스템 서비스를 원활하게 이용하여 사용자의 IoT 환경의 전반적인 상태와 보안 현황을 모니터링 할 수 있었다. 해당 결과를 통해 사용자가 IoT 환경을 구성하여 IoT 기술을 이용하는 것도 중요하지만 자신의 IoT 환경을 관리하고 모니터링 할 수 있는 수단을 가지고 직접 관리하는 것이 향후 IoT 디바이스 시장 및 IoT 보안 시장의 안정적인 성장과 IoT 사용자의 성숙한 보안 인식 확립에 도움이 된다는 것을 확인하였다. 다만, 본 연구에서는 RaspberryPi를 활용하였기 때문에 상용 IoT 디바이스와는 기능과 성능상의 차이가 존재할 수 있다. 따라서 실제 본 시스템의 적용을 위해서는 다양한 IoT 디바이스가 제공하는 기능에 대한 분석이 이루어져야 한다.

Ⅳ. Conclusions

오픈 소스를 활용한 IoT 환경 관리 시스템을 제안하였다. 사용자에 특화된 IoT 환경, IoT 환경 관리 시스템 구성요소, 기반 운영체제 모두 오픈 소스들로만 구성되어 있고 초소형/초저가의 IoT 플랫폼을 도입하였다. IoT 디바이스들을 우리 주변에서 쉽게 접할 수 있지만 아직은 미흡한 부분이 많다. IoT 기술을 활용하는 사용자의 성숙한 보안 인식과 IoT 환경을 관리 및 모니터링 할 수 있는 수단의 부재가 있다. IoT 기술을 활용하는 것도 중요하지만 가장 중요한 것은 사용자의 성숙한 보안 인식과 IoT 환경을 직접 관리할 수 있는 관리 시스템을 통해 안전하게 IoT 기술을 이용하는 것이라 할 수 있다. 사용자들에 특화된 IoT 환경을 쉽게 구성하며 구성한 IoT 환경을 쉽게 관리 및 모니터링 할 수 있게 하는 것이 본 논문의 취지이다. 본 논문에서 제안하는 IoT 환경 관리 시스템을 통해 IoT 사용자들에게 관리 및 모니터링 수단을 제공하여 이를 통해 안전한 IoT 문화를 조성하면 IoT 보안 시장이 활성화되고 성장할 것이다. 향후 본 논문에서 제안하는 IoT 환경 관리 시스템을 더욱 발전시켜 오픈 소스 IDS인 Suricata를 도입하여 IoT 환경을 향한 위협을 세밀하게 탐지하여 공격자의 세부정보를 시각화할 수 있는 연구를 진행할 것이다.

REFERENCES

[1] Kleindienst, P. (2016). Building a real-world logging infrastructure with Logstash, Elasticsearch and Kibana.
[2] Elastic. (2020). https://www.elastic.co/kr/beats/
[3] Elastic. (2020). https://www.elastic.co/kr/logstash
[4] Andhavarapu, A. (2017). Learning Elasticsearch. Packt Publishing Ltd.
[5] Elastic. (2020). https://www.elastic.co/kr/kibana