International Journal of Multimedia and Ubiquitous Engineering
Vol.10, No.12 (2015), pp.61-66
http://dx.doi.org/10.14257/ijmue.2015.10.12.07

A Study on IP Exposure Notification System for IoT Devices Using IP Search Engine Shodan

Yun-Seong Ko[1], Il-Kyeun Ra[2] and Chang-Soo Kim[1*]

[1] Department of IT Convergence and Application Engineering, Pukyong National University, Busan, 608-737, Korea
[2]Department of Computer Science and Engineering, University of Colorado Denver, Denver, CO 80203, United States of America
*[kysung14@gmail.com, ilkyeun.ra@ucdenver.edu, *cskim@pknu.ac.kr]*

Abstract

As times become increasingly digitized and the importance of IoT_(Internet of Things) technology still growing, the number of IP-based IoT devices is also sharply increasing. This has the advantage of improving the quality of life because by increasing the numbers of IoT devices, but IP-related security threats are also increasing together while the system for preventing these threats is insufficient. In this paper, we study the IP exposure notification system for IoT devices using IP search engine 'Shodan'. First, we study the keywords to search the IP address of IoT devices. After that, we output the result file about those keywords using Shodan API. Finally, we develop a web-based IP exposure notification system for IoT devices using the output file and Google Map API. In the future, we can develop our system combining this study and the IP exposure threat level. It can also prevent the threat of countries or public institutions.

Keywords: *IoT (Internet of Things), IP Address, IP Search Engine Shodan, IP Exposure, Google Map*

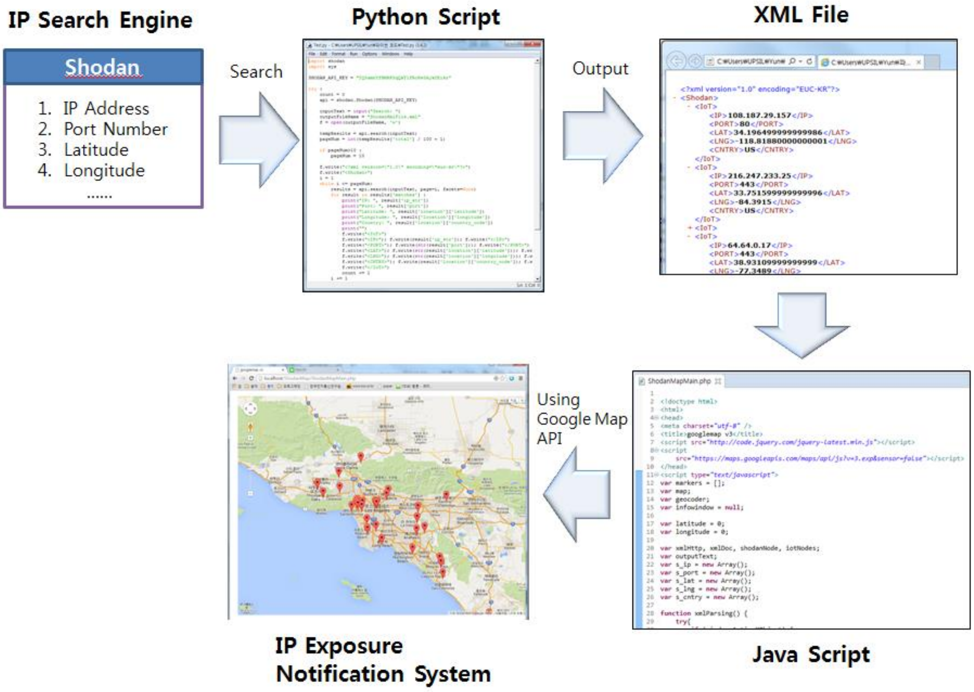
1. Introduction

As times become digitized and the IT technology is fused to devices, the number of IP-based IoT (Internet of Things) devices is sharply increasing. IoT is a promising technology that expected the economic effect of 1.9 trillion dollars and a market creation of 300 billion dollars. Development of IoT technology helps make life more convenient and increases national competitiveness, but it can also increase security threats of IP exposure at the same time. We can be threatened by invasion of privacy and system hacking of public organization. We can also be threatened by data leakage, data forgery/tampering, camera hacking, DoS (Denial of Service) attack, backdoors, *etc.* [1-4]. It is urgent that a countermeasure to these threats be created.

In this paper, we study an IP exposure notification system for IoT devices using IP search engine Shodan. First, we study the keyword for gathering IoT devices' information. After that, we search the IP address and some other information using that keyword, and output the results to XML file. Finally, we develop an IP exposure notification system using the extracted data and Google Map API. It displays how many exposed IoT devices exist in a certain area. Figure 1 shows the system diagram.

[*] Corresponding Author

ISSN: 1975-0080 IJMUE



```
<?xml version="1.0" encoding="EUC-KR"?>
- <Shodan>
  - <IoT>
      <IP>108.187.29.157</IP>
      <PORT>80</PORT>
      <LAT>34.196499999999986</LAT>
      <LNG>-118.81880000000001</LNG>
      <CNTRY>US</CNTRY>
    </IoT>
  - <IoT>
      <IP>216.247.233.25</IP>
      <PORT>443</PORT>
      <LAT>33.751599999999996</LAT>
      <LNG>-84.3915</LNG>
      <CNTRY>US</CNTRY>
    </IoT>
  + <IoT>
  - <IoT>
      <IP>64.64.0.17</IP>
      <PORT>443</PORT>
      <LAT>38.931099999999999</LAT>
      <LNG>-77.3489</LNG>
```

```
ShodanMapMain.php

<!doctype html>
<html>
<head>
<meta charset="utf-8" />
<title>googlemap v3</title>
<script src="http://code.jquery.com/jquery-latest.min.js"></script>
<script
    src="https://maps.googleapis.com/maps/api/js?v=3.exp&sensor=false"></script>
</head>
<script type="text/javascript">
var markers = [];
var map;
var geocoder;
var infowindow = null;

var latitude = 0;
var longitude = 0;

var xmlHttp, xmlDoc, shodanNode, iotNodes;
var outputText;
var s_ip = new Array();
var s_port = new Array();
var s_lat = new Array();
var s_lng = new Array();
var s_cntry = new Array();

function xmlParsing() {
    try{
```

Figure 1. System Diagram

2. Related Research

2.1. Internet of Things (IoT)

IoT is the network of physical objects or “things” embedded with electronics, software, sensors, and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices based on the infrastructure of International Telecommunication Union’s Global Standards Initiative. IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for a more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of almost 50 billion objects by 2020. IoT devices are used in various cases. It used in Smart Home System, Wearable Devices, Smart Car Devices, Living in Close Contact Devices, Smart Energy Devices, Industrial and Environmental Devices, *etc.* [5-7].

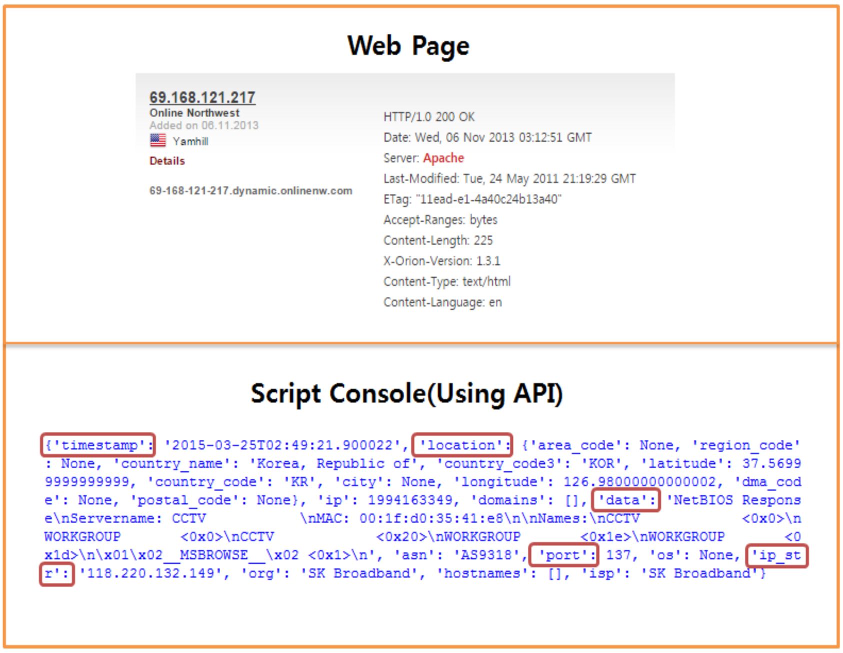
2.2. IP Search Engine ‘Shodan’

Shodan provides searching data for IP addresses and some other information. Although there are a lot of search engines nowadays, Shodan is the most powerful search engine as of now. Shodan lets the user find specific types of computers connected to the Internet using a variety of filters. Some have also described it as a search engine of service banners, which are meta-data that the server sends back to the client. This can be information about the server software, what options the service supports, a welcome message or anything else that the client can find out before interacting with the server. The Shodan IP search engine is designed to crawl the Internet and attempt to identify and index connected devices. Shodan engine collects more than 500 million IoT devices in one month. It also collects data mostly on web servers at the moment (HTTP port 80), but there are also some data from FTP (21), SSH (22), Telnet (23), SNMP (161) and SIP (5060) services. Using Shodan, researchers identified thousands of Internet-facing devices associated with industrial controls system [8-9].

3. Gathering Information from IoT Devices Using IP Search Engine Shodan

3.1. The Kinds of Information Provided by the IP Search Engine

The kinds of information that can be provided by Shodan search engine can be divided into two types. The first one is provided by the web page, and last one is provided by script console using IP search engine API. First, information provided by the web page has only basic data such as IP address, connected country, connected city, server name. But information provided by script console has more useful data than web pages such as port number, affiliation, latitude/longitude including the data of the web page. We compare the two types of this information in Figure 2.



Web Page

69.168.121.217
Online Northwest
Added on 06.11.2013
Yamhill
Details

69-168-121-217.dynamic.onlinenw.com

```
HTTP/1.0 200 OK
Date: Wed, 06 Nov 2013 03:12:51 GMT
Server: Apache
Last-Modified: Tue, 24 May 2011 21:19:29 GMT
ETag: "11ead-e1-4a40c24b13a40"
Accept-Ranges: bytes
Content-Length: 225
X-Orion-Version: 1.3.1
Content-Type: text/html
Content-Language: en
```

Script Console(Using API)

```
{'timestamp': '2015-03-25T02:49:21.900022', 'location': {'area_code': None, 'region_code'
: None, 'country_name': 'Korea, Republic of', 'country_code3': 'KOR', 'latitude': 37.5699
9999999999, 'country_code': 'KR', 'city': None, 'longitude': 126.98000000000002, 'dma_cod
e': None, 'postal_code': None}, 'ip': 1994163349, 'domains': [], 'data': 'NetBIOS Respons
e\nServername: CCTV            \nMAC: 00:1f:d0:35:41:e8\n\nNames:\nCCTV            <0x0>\n
WORKGROUP       <0x0>\nCCTV            <0x20>\nWORKGROUP       <0x1e>\nWORKGROUP       <0
x1d>\n\x01\x02__MSBROWSE__\x02 <0x1>\n', 'asn': 'AS9318', 'port': 137, 'os': None, 'ip_st
r': '118.220.132.149', 'org': 'SK Broadband', 'hostnames': [], 'isp': 'SK Broadband'}
```

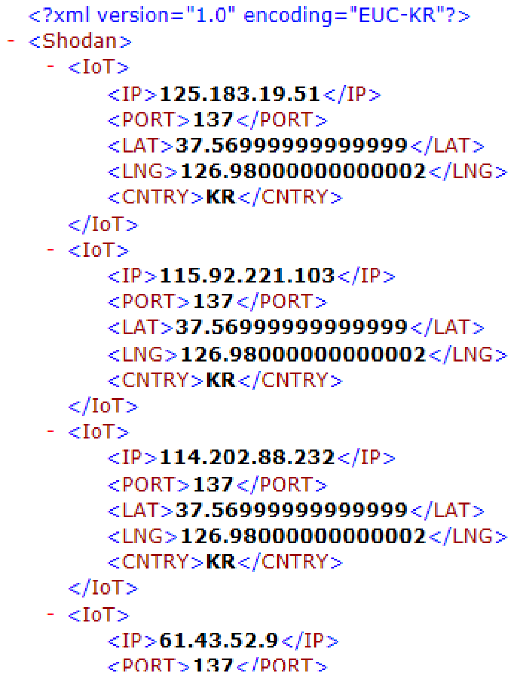
Figure 2. Compare Information between Web Page and Script API

Because information provided by web page can get only fragmentary data, it is difficult to use in this study. Information provided by script console can also get many useful data such as location information or port number, which makes it appropriate for use in our study. Also, it is appropriate to produce output using script programming, so we use script API for gathering information.

3.2. A Module Gathering Information from IoT Devices with Python

The script API of Shodan, an IP search engine, is used in three ways. The first way is using Python Language, the second way is using Ruby Language, and the final way is using Node.js Language. We use \ Python Language in order to take advantage of the result file variously because it’s very useful and makes it easy to interact on the web. In order to use Shodan API in Python, we purchased a Shodan license and input a license key to Python script. After that, we specified the XML file’s attributes to make a basic form of XML file. Then we input the query string, and we ran the query to get result data.

After we entered the information of IP address in the <IoT> tag in XML file, creates a XML file finally. Figure 3 is the contests of the resulting XML file. Many <IoT> tags are contained in <Shodan> tag, and <IP>, <PORT>, <LAT>, <LNG>, <CNTRY> tags are contained in each <IoT> tag. <IP> tag is information about IP address, <PORT> tag is information about port number, <LAT> tag is information about latitude, <LNG> tag is information about longitude, and <CNTRY> tag is information about country.



```
  <?xml version="1.0" encoding="EUC-KR"?>
- <Shodan>
  - <IoT>
      <IP>125.183.19.51</IP>
      <PORT>137</PORT>
      <LAT>37.56999999999999</LAT>
      <LNG>126.98000000000002</LNG>
      <CNTRY>KR</CNTRY>
    </IoT>
  - <IoT>
      <IP>115.92.221.103</IP>
      <PORT>137</PORT>
      <LAT>37.56999999999999</LAT>
      <LNG>126.98000000000002</LNG>
      <CNTRY>KR</CNTRY>
    </IoT>
  - <IoT>
      <IP>114.202.88.232</IP>
      <PORT>137</PORT>
      <LAT>37.56999999999999</LAT>
      <LNG>126.98000000000002</LNG>
      <CNTRY>KR</CNTRY>
    </IoT>
  - <IoT>
      <IP>61.43.52.9</IP>
      <PORT>137</PORT>
```

Figure 3. Result XML File

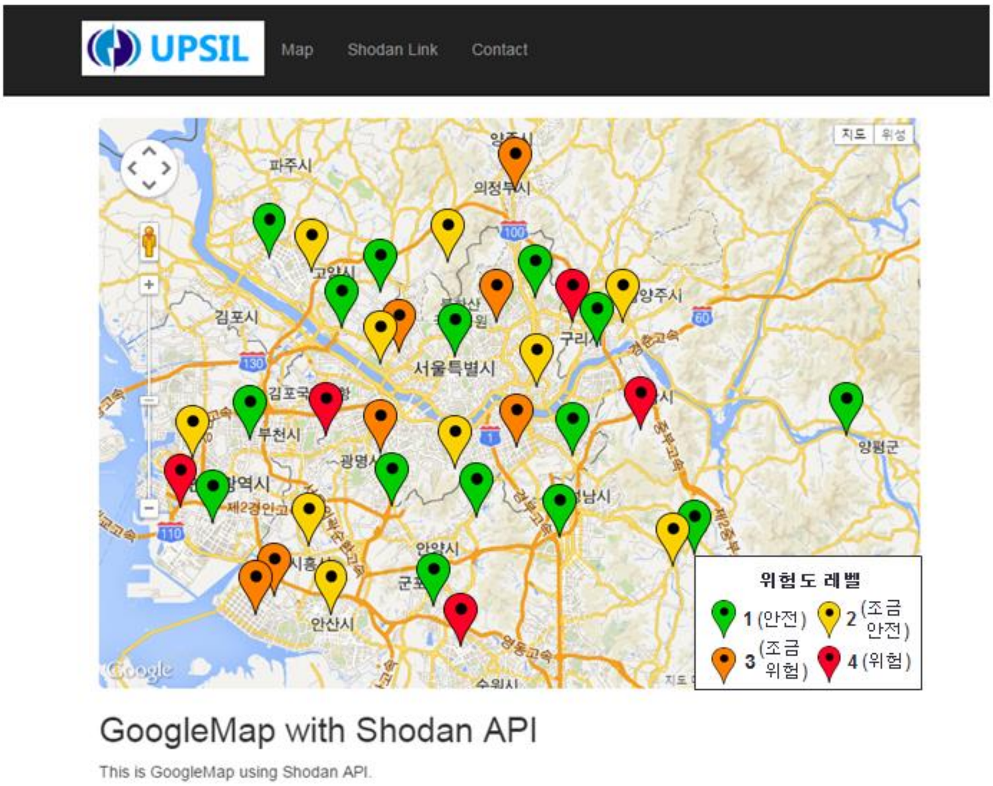
4. Developing an IP Exposure Notification System Using Information from IoT Devices and Google Map API

In order to develop the IP exposure notification system, we express information of the exposed IoT devices on Google Map using the resulting XML file as input. First, we enter the five attributes stored in the resulting XML file to array list. Information of IP address, port number, latitude, longitude, country is input into individual array. After that, we use this individual array in order to objectify the exposed IoT devices information. Table 1 is a configuration of that object. It has five attributes from Shodan API, which are IP Address, Port Number, Latitude, Longitude, and Country.

Table 1. Object of Exposed IoT Devices Information

No.	Attribute	Type	Description
1	IP Address	String	Exposed IoT device's IP address
2	Port Number	Integer	Exposed IoT device's port number
3	Latitude	Float	It is used for marking latitude in Google Map
4	Longitude	Float	It is used for marking longitude in Google Map
5	Country	String	Exposed IoT device's country

Using the latitude and longitude attributes of that object, we marked information of this object on Google Maps. Because of these marks that indicate the information on Google Maps, we can see how many IP exposures are within a certain area. If public authorities take advantage of that, they can be used as a way to warn that IP exposure is dangerous to that area. Because we also display their information, they will know which IoT devices are dangerous to exposure. Figure 4 is the result of executing this system.



GoogleMap with Shodan API

This is GoogleMap using Shodan API.

Figure 4. Execution Window of the IP Exposure Notification System

5. Discussion and Conclusion

Security threats posed by IP exposure of IoT devices have been appearing more often. Although large and small security threats such as hacking of personal web camera or national IP-based CCTVs are affecting our lives, the study for a system that radically prevents exposure of IP is still insufficient. It will become a major security threat of IoT devices.

In this paper, we studied an IP exposure notification system for prevent this threats. Through this study, we confirmed how many IP address are being exposed to the Internet, and we could see that access to the system with the exposed IP can be easily done. Because most of the exposed IP-based IoT devices can be easily accessed through their IP address and port number, it would be a big threat for IoT devices in the future.

In the future, integrated security management systems combined with IP exposure notification systems and IP exposure levels can be studied. Through this system, we can search the exposed IP address and estimate the IP exposure level to each IP address. Then we can measure the degree of risk of the IP exposure. Also, if you use this system in state institutions, you can reduce the threat in accordance with IP exposure ranging from personal to national.

References

[1] Y. H. Kim, J. G. Yang and H. B. Kim, “Trends and Threats of M2M/IoT”, Journal of Information Security, vol. 24, no. 6, **(2014)**.

[2] I. S. Lee, H. S. Kim and W. S. Yi, “u-City service information security threats and protective measures”, Journal of the Korea Institute of Information Security, vol. 18, no. 2, **(2008)**, pp. 67-75.

[3] H. W. Kim, “Security/Privacy Issues in the IoT Environment”, TTA Journal, **(2014)**

[4] D. H. Kim, S. W. Yoon and Y. P. Lee, “Security for IoT Services”, Journal of the Korean Communication(Information and Communication), vol. 30, no. 8, **(2013)**, pp.53-59.

[5] J. A. Jeon, N. S. Kim, J. K. Ko, T. J. Park, H. Y. Kang and C. S. Pyo, “IoT Devices Products and Technology Trends”, Journal of The Korean Institute of Communication Sciences, vol. 31, no. 4, **(2014)**, pp. 44-52.

[6] “Wikipedia: Internet of Things”.

[7] S. Husain, A. Prasad, A. Kunz, A. Papageorgiou and J. S. Song, “Recent Trends in Standards Related to the Internet of Things and Machine-to-Machine Communications”, Journal of Information and Communication Convergence Engineering, vol. 12, no. 4, **(2014)**, pp.228-236.

[8] “Wikipedia: Shodan”.

[9] R. Bodenheim, J. Butts, S. Dunlap and B; Mullins, “Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices”, International Journal of Critical Infrastructure Protection, vol. 7, no. 2, **(2014)**, pp. 114-123.

Authors

Yun-Seong Ko, He received his B.S. degree in Computer Multimedia Engineering from Pukyong National University, Korea in 2014. He is in a master course in Pukyong National University. His current research interests are disaster prevention, Internet of Things, Cloud Service, GIS and u-prevention system.

Il-Kyeun Ra, He holds a Ph.D. degree in Computer and Information Science from Syracuse University in 2001, a M.S. degree in Computer Science from University of Colorado Boulder, and B.S. degree and M.S. degree in Computer Science from Sogang University. He was a Research Staff Member at the LG Information and Communications Research Center. He joined the department of Computer Science and Engineering at the University of Colorado Denver 2001. His main research interests include computer networks, developing adaptive distributed system software and high speed communication system software to support High Performance Distributed Computing Applications.

Chang-Soo Kim, He received a B.S degree in Computer Science from Ulsan University, Korea, in 1979, and a M.S. degree in Computer Engineering and Ph.D. degree in Computer Engineering from Chungang University, Korea, in 1984 and 1991 respectively. He has been a professor at the department of IT Convergence and Application Engineering, Pukyong National University, Korea, since 1992. His research interests are operation system, LBS/GIS, WSN and urban disaster prevention system.