The Rise of Internet of Things (IoT) and its Security Challenges

Gajendra Sharma and Saugat Acharya

School of Engineering, Department of Computer Science and Engineering
Kathmandu University (Email: gajendra.sharma@ku.edu.np)

Abstract**:** *Internet of Things (IoT) is on the rise, around 8 billion devices are connected to the internet worldwide. Around 20 billion devices will be connected to the internet by 2020. With these many connected devices, a huge amount of data is being transferred online. These IoT-enabled devices produce massive data which needs to be securely transferred and protected. Securing these data at scale is a major issue. Recently, there has been an increase in IoT devices being hacked. IoT devices often store sensitive user data that hackers may try to steal. Sensitive information combined with weak infrastructure makes IoT devices vulnerable to hackers and criminals. The primary challenge for the IoT ecosystem right now is to secure IoT devices and its communication protocols. This will help protect user's private information, the number one security concern amongst IoT manufacturers and its users.*

Keywords: *IoT, Connected Devices, Security, Connectivity, Communication, Internet*

1. Introduction

The Internet of Things (IoT) is an emerging topic of high significance. It is the inter-networking of physical devices, vehicles, buildings (also referred as "connected devices") embedded with electronics, software, sensors and network activity that enable these objects to collect and exchange information. As the size and cost of wireless radios have dropped tremendously, more and more devices are connected to the internet. Projections for the impact of IoT and economy are impressive. The term IoT generally refers to scenarios where network connectivity and computing capability extends to objects, sensors, and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention (Rose, Eldridge, & Chapin, 2015, p. 5). ¬¬IoT devices will soon become essential, in our daily lives. The concept of IoT may be convenient, but there are also huge challenges and security risks involved. This paper examines what are the risks and challenges associated with IoT.

IoT represents the next evolution of the internet, taking a huge leap in its ability to gather, analyze, and distribute data that we can turn into information, knowledge, and, ultimately wisdom (Evans, 2011, p. 2). Since IoT is rapidly growing, most major companies are seeking to get involved, there are enormous efforts to trigger this trend as something positive in the forthcoming future. IoT devices are already under way to improve the distribution of the world's resources and provide powerful creations in human history. Gartner, Inc. forecasts that 8.4 billion connected things will be in use worldwide in 2017, up 31 percent from 2016, and will reach 20.4 billion by 2020 (Table 1). According to (Cisco Global Cloud Index, 2016), the data created by Internet of Everything (IoE) devices will reach 507.5 ZB per year (42.3 ZB per month) by 2019, up from 134.5 ZB per year (11.2 ZB per month) in 2014. Generally, the data created by IoE devices will be 269 times higher than the amount of data being transmitted to data centers from end-user devices and 49 times higher than total data center traffic by 2019.

To handle these huge amounts of data in real time can be a big challenge. Processing large quantities of IoT data in real time will increase workloads of data centers, leading data center providers with different challenges in security, capacity, and analytics. There will also be huge amounts of data providing information on user's personal use of devices that, if not secured, can give rise to breaches of privacy. Another challenge will be the increasing demand for storage capacity and scalability. How will all this data be stored? How will it be

https://doi.org/10.15242/DiRPUB.DIR1017015

transported and analyzed? How will it be kept secure and private? These questions loom large around the IoT ecosystem.

Security and scalability are the main challenges facing IoT. Recently, a major 1distributed denial-of-service (DDoS) attack on Internet domain service provider Dyn disrupted many websites. The magnitude of the attack was so huge, it is claimed to be the largest DDoS attack to date. A 2malware named Mirai exploited poorly secured and vulnerable IoT devices all over the world to be used as part of a botnet in large-scale network attack. These kinds of attacks are on the rise making security one of the most vital challenge for the IoT ecosystem. A report by (HP Inc., 2014) revealed that “70 percent of the most commonly used Internet of Things (IoT) devices contain vulnerabilities, including password security, encryption and general lack of granular user access permissions.”

The research question for this study are as follows:

1) Why is security an emerging issue for IoT?
2) What challenges under security are the primary concerns for IoT

The purpose of this research is to identify challenges in the IoT ecosystem, mostly related to security and privacy. The paper will also determine why security is one of the main challenges for IoT

2. Methodology

The research methodology for this paper includes a study of secondary data obtained from various sources. The various sources include statistics from the web and other research papers related to IoT. Analysis of the secondary data gives us a clear view of what security challenges lies ahead for IoT in the coming days.

2.1. Analysis

According to a recent survey by (Eclipse Foundation, 2016, p. 15), the top two concerns related to IoT are Security and Interoperability. This survey was mostly focused on organizations and people developing IoT solutions. 47.4% of the respondents answered security as the number one concern when developing IoT solutions (Figure 1). With 29.4% interoperability came in second place. This shows that even developers and tech enthusiasts who are developing IoT solutions are not yet sure how to secure the communication and data transfer channels between IoT devices. A similar survey was carried out by Eclipse Foundation in 2015 where security was ranked number one as well. This clearly shows that people are still skeptical about IoT and its security.

When it comes to IoT, there are many challenges related to security. The data from (Tarzey & Fernandes, 2015, p. 9) shows the number one security concern among users as privacy/data protection (Figure 2). The next concern is expanded attack surface which means that more IoT deployments mean more devices on the network for attackers to probe as possible entry points to an organization’s network infrastructure. Similarly, attacks on IoT-enabled processes to disrupt business activities is amongst the key concerns for users.

As stated by the (Internet Society, 2015, p. 23) “Many IoT deployments will consist of collections of identical or near identical devices. This homogeneity magnifies the potential impact of any single security vulnerability by the sheer number of devices that have all the same characteristics.” This means that the vulnerability in one company’s brand of IoT devices could be the same across all its devices that uses the same protocol or manufacturing characteristics. The report also raises a concern on privacy aspect of IoT. Most IoT devices collect data about their environment, which frequently includes data related to people. This data could be beneficial to the device’s owner and the device manufacturer. The user might not be aware of the fact that the IoT device is collecting data about the individual and potentially sharing it with third parties. “The Internet of Things can threaten a person’s expectations of privacy in common situations. There are social norms and expectations of privacy that differ in public spaces versus private spaces, and IoT devices challenge these norms.” states the report. Another report from (Hewlett Packard Enterprise, 2015) showed that 80% of devices that they reviewed raised privacy concerns. More so, 70% of the devices did not encrypt communications to the

https://doi.org/10.15242/DiRPUB.DIR1017015

Internet and local network and 80% of the devices had authentication issues and failed to require passwords of sufficient complexity and length.

“IoT devices often lack stringent security measures. If a device can be hacked, it likely will be.” says (Symantec, 2016, p. 16) in its Internet Security report. More connected devices mean more security challenges. The future of cloud-based security services is in part linked with the future of IoT. Thus, more and more funds are being spent on the security side of IoT infrastructure. Spending on IoT is expected to reach $547 million in 2018 (Table 2). No one is really safe, “Security researchers explain that hacking oil rigs, pipelines, water pumps, industrial facilities, and the power grid are not myths born in the cyber-mist, but realities.” (Symantec, 2016)

3. Results and Discussion

Due to the rise of internet and connectivity in the past few years, more and more devices are being connected to the internet. This overwhelming rise of connected devices (IoT) brings a lot of challenges regarding security, privacy and safety. When we talk about internet we generally talk about data. IoT devices generate a lot of data and are a prime hacking target. The biggest worry is that someone can remotely disable your “smart” home security system, or hack into your car or your health monitoring device. Thus, securing user privacy/confidentiality is the number one security challenge in the IoT ecosystem right now. The scale of growth of IoT doesn’t really help in securing these devices connected to the internet. Every year there’s a significant rise in number of IoT attacks. ***(Symantec, 2016, p. 16)***

Due to the disperse set of global standards and regulations across different sectors like health and transportation. There seems to be no default security standard in place for the IoT ecosystem. There is an 3Open Connectivity Foundation (previously referred as Open Internet Consortium) in place which includes major corporations to establish a common standard for a robust and secure method to connect IoT devices, but it is far from promising and is still in a very early stage.

Connecting everything to each other via the internet exposes new vulnerabilities. On the internet attack is easier than defense. To stop IoT threats from happening regularly a global trust model should be in place. Data shared among IoT devices needs proper encryption and communication protocols so that user’s private information doesn’t get jeopardized.

4. Conclusion

The study clearly shows that security is the primary concern for the IoT ecosystem. There are large voids to fill regarding security in IoT. Given the poor state of security on connected devices, the IoT ecosystem is an increasingly attractive target for hackers and criminals. Security is not only the number one concern among end-users but also amongst organizations involved in making these devices. Securing data privacy/confidentiality of users is the top priority in terms of securing the IoT infrastructure.

5. References

[1] Cisco Global Cloud Index. (2016). Forecast and Methodology, 2015–2020. Cisco.

[2] Eclipse Foundation. (2016). IoT Developer Survey. IEEE IoT.

[3] Evans, D. (2011). The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. Cisco IBSG. Cisco Internet Business Solutions Group (IBSG).

[4] Gartner Inc. (2016, April 25). Gartner Says Worldwide IoT Security Spending to Reach $348 Million in 2016. Retrieved from Newsroom: http://www.gartner.com/newsroom/id/3291817

[5] Gartner Inc. (2017, February 7). Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. Retrieved from Newsroom: http://www.gartner.com/newsroom/id/3598917

[6] Hewlett Packard Enterprise. (2015). Internet of Things Research Study. Hewlett Packard Enterprise.

https://doi.org/10.15242/DiRPUB.DIR1017015

[7] HP Inc. (2014, July 29). Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack. Retrieved from http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WQRJMYmGPfb

[8] Internet Society. (2015). Understanding the Issues and Challenges of a More Connected World. Internet Society.

[9] Rose, K., Eldridge, S., & Chapin, L. (2015). The Internet of Things: An Overview.

[10] Symantec. (2016). An Internet of Things Reference Architecture. Symantec.

[11] Symantec. (2016). Internet Security Threat Report. Symantec.

[12] Tarzey, B., & Fernandes, L. (2015). The Many Guises of the IoT. Quocirca Ltd.

6. Footnotes

[1] A denial-of-service attack (DoS attack) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

[2] Malware, short for malicious software, is any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

[3] The Open Connectivity Foundation is an industry group whose stated mission is to develop specification standards, promote a set of interoperability guidelines, and provide a certification program for devices involved in the Internet of Things.

Table 1: IoT Units Installed Base by Category (Millions of Units)

Category	2016	2017	2018	2020
Consumer	3,963.0	5,244.3	7,036.3	12,863.0
Business: Cross-Industry	1,102.1	1,501.0	2,132.6	4,381.4
Business: Vertical-Specific	1,316.6	1,635.4	2,027.7	3,171.0
Grand Total	6,381.8	8,380.6	11,196.6	20,415.4

Note. From (Gartner Inc., 2017)

Table 2: Worldwide IoT Security Spending Forecast (Millions of Dollars)

Year	2014	2015	2016	2017	2018
Spending	**231.86**	**281.54**	**348.32**	**433.95**	**547.20**

Note. From (Gartner Inc., 2016)

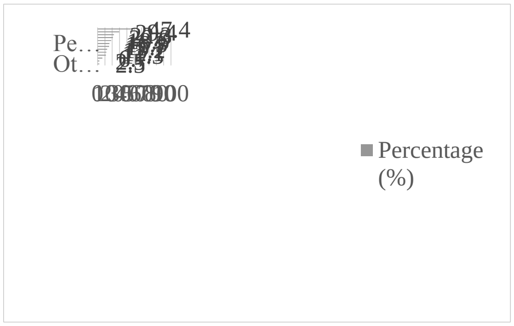

Fig 1: Top concerns for developing IoT solutions. A total of 528 individuals participated in the survey, most of the participants were developers who built IoT solutions in their organizations. Adapted from (*Eclipse Foundation, 2016*)

https://doi.org/10.15242/DiRPUB.DIR1017015

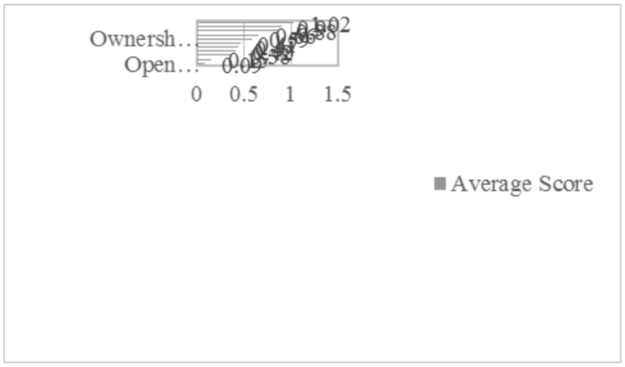

Fig:2. IoT security concerns on the scale of 0 - 3. Users were asked to select and rank their top 3 of 7 general and 11 security specific concerns. To derive a weighted average for each concern, each instance of a top rating was scored 3, a second rating 2, a third rating 1 and unrated 0. *Adapted from* (Tarzey & Fernandes, 2015, p. 9)

https://doi.org/10.15242/DiRPUB.DIR1017015