CYBER SECURITY AND INTERNET OF THINGS

Muhammad Saad Department of Computer Science, SZABIST Dubai Campus and [1]Tariq Rahim Soomro, College of Computer Science & Information Systems, IoBM, Karachi

***Abstract*- Internet has become a vital part of our lives. The number of Internet connected devices are increasing every day and approximate there will be 34 billion IoT devices by 2020. It is observed that security is very weak in these devices and can be easily compromised by hackers as some manufactures failed to implement basic security. Current devices use standards that are easy to implement and works for most forms of communications and storage. There is no such standard solution that will work on every device within the Internet of Things, because of the varied constraints between different devices; resulting in classifications within the Internet of Things. This study addresses security challenges in the Internet of Things (IoT); first will discuss the IoT evolution, architecture and its applications in industries. Further, classify and examine privacy threats, including survey, and pointing out the challenges that need to be overcome to ensure that the Internet of Things becomes a reality.**

Keywords: Internet of Things, Cybersecurity, Cybersecurity Challenges.

I. INTRODUCTION

The Internet of things (IoT) period began from 2000 and onwards. In IoT everything is connected with the Internet, this concept changed the concept of everything. This concept will create ease in our life style. In IoT, things are interconnected and can be manage through other connected devices i.e. from office you can switch on and off your room temperature. Home, vehicle, workplace and even our shoes will be IoT connected. Although currently everything is not connected with IoT, but gradually as time is passing things are adding to the IoT. Data will generate by these connected devices. These devices will not only generate data, but also behave as well on the basis of collected information [1]. Things will be interconnected and ability to see everything in this life would be possible with just few clicks. This scenario raises the importance of security of data and connected things. If there are loopholes in the security, then malicious actors in society can see, access and misuse the same information too, for example Smart TV with camera, and there are cases that one's TV camera is hacked [2] [3]. By realizing the importance of IoT, investors are making huge investment in it but they are investing on the things that can be marketed and the can get quick return. There is not much or equal level of investment in security of IoT. As more things will add into IoT, concern about the things security will increase too.

[1] tariq.soomro@iobm.edu.pk

According to ITU, cybersecurity is “The collection of security principles, protection, guidelines, chance management processes, actions, education, practices, guarantee and technology that may be used to protect the cyber environment and organization and person's property” [4]. On the other hand according to IoT-SRA “The IoT is a large scale system with self-arranging abilities in view of standard and interoperable conventions and configurations which comprises of heterogeneous things that have characters, physical and virtual traits, and are flawlessly and safely integrated into the Internet” [5].

1.1. Evolution of IoT

The early period of IoT began with Machine-to-Machine (M2M). M2M once referred to communication between devices using any communications channel, including wired and wireless but currently it is typically use to refer machine communications using cellular or satellite networks. In telephony systems, information was exchanged through different end-points i.e. caller identity. This information was sent between the endpoints and no one required starting the transmission. M2M is still majorly wise used in the alarm panels, industrial sector and more. IoT is typically known as superset of M2M and currently overtaken the M2M market as shown in Figure 1 from Google.

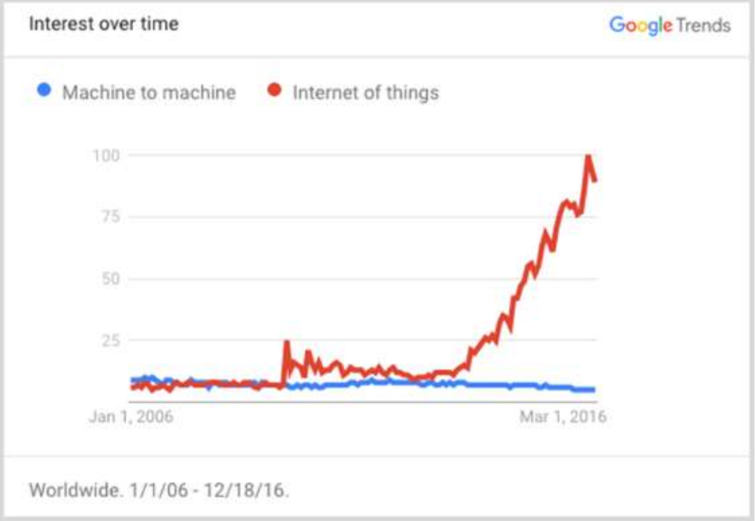


Figure 1: M2M to IoT - Interest over Time on Web Search [6]

Gartner highlight IoT as potential technology in 2013. Onwards from 2014 to 2016, it has been moved from initial stage to peak of inflated as shown in Figure 2 [7] [8] [9] [10].

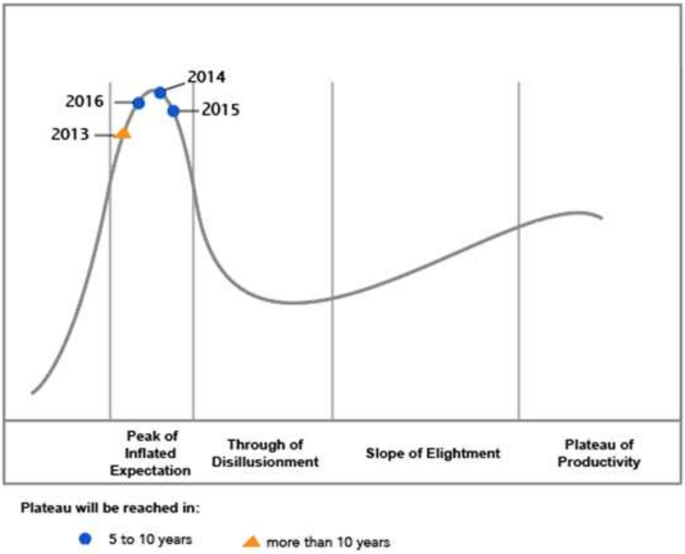


Figure 2: IoT Gartner's Hype Cycle from 2013-16

Everyday IoT umbrella is getting bigger as things are adding into it. According to Business Insider, there will be more than 24 billion IoT devices that mean everyone is going to keep more than 4 devices as shown in Figure 3 [11]. Gradually, this revolution will change everything from personal devices to smart cities.

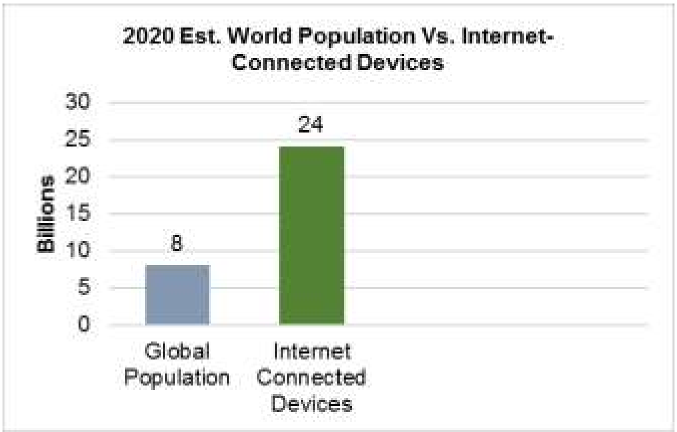


Figure 3: The IoT Growth Forecast

1.2. Cybersecurity in the Internet of Things

With IoT speedy growth, new security threats and challenges are rising in all industries. IoT is going the change the businesses and customer interaction with the world. IoT devices growth prediction is from 10 billion in 2016 to 24 billion in 2020 [11]. Sharing information with everything is an enormous cybersecurity challenge. When billions of IoT devices will connect to the other networks, malicious attacks will increased. Cyber criminals can use IoT devices as a door to enter business networks and cloud environment [12]. Cybersecurity is the primary challenge of IoT implementation. Cyber-attacks already have started on connected devices such as ability to hack connected vehicle. Nowadays, customers have realized their choices can be analyze by their information and they have started to think about who has access to their data and who is responsible to secure it. When different systems will interact, there will be fight among them on competitive intelligence. As it will create new cybersecurity challenges and these challenges will raise the importance of security. Also data security is a major concern for IoT devices and it should be taken seriously. Every second day, there is news about data breaches [13]. Every connected thing generates data and volume of generated data is in zeta bytes. Malicious actors can access this sensitive data. Let's take an example of thermostat data; it can be used to count total number of person and their availability. GPS can use to track your position and your availability at a certain position [14]. This information doesn't seem very important but it is enough for criminal to misuse it against anyone. Business data can misuse in the same way. Nowadays several companies are collecting social data i.e. Google, Yahoo and Facebook etc. and this data can be hacked by hackers. On 14 Dec 2016, Yahoo accepted their 1 billion accounts were compromised [15]. IoT Device manufactures need to understand that data privacy begins at the source. Information should not leave the sensor without protection. Data needs to be encrypted before moving to cloud for processing and storage.

This paper is organized as follows; section 2 will discuss IoT architecture, along with security attacks during 2015 to 2016; section 3 will explore the finding from literature; section 4 will discover the finding from survey done for this study; finally, discussion and future work will be covered.

II. IoT Architecture

IoT standard architecture consisting of things, local network, the Internet and back end services, as shown in Figure 4 below.

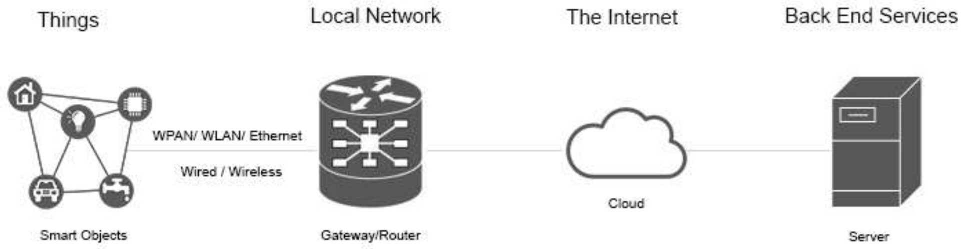


Figure 4: IoT Standard Architecture [16]

Following are the IoT architectures purposed by leading IT companies in the world.

2.1 IoT Architecture by Microsoft

Figure 5 shows the IoT architecture by Microsoft Azure [17]. There are three major areas in it:

- Device connectivity
- Data processing, analytics, and management
- Presentation and business connectivity

By using a gateway, devices can connect directly or indirectly. This architecture is designed for large-scale IoT environments.

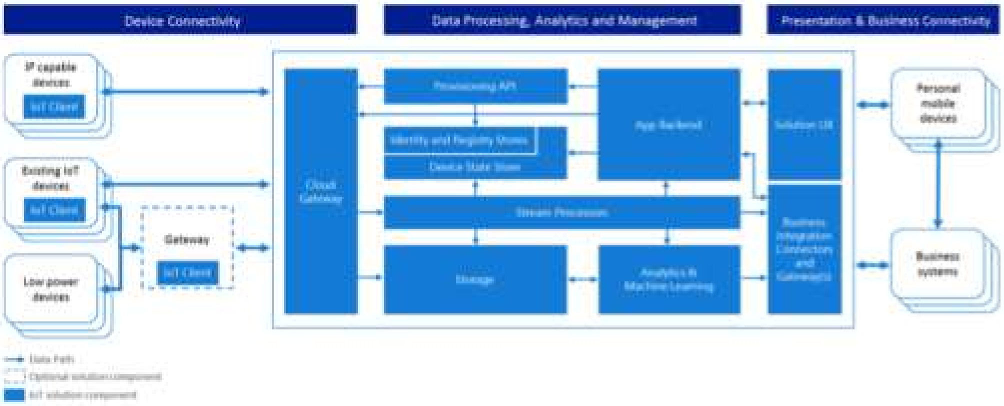


Figure 5: IoT Architecture by Microsoft [17]

2.2 IoT Architecture by Intel

Intel along with its ecosystem partners defined IoT architecture with name of system architecture specification (SAS) for all things whether they are connected with the Internet or not as shown in Figure 6 below. This architecture has 3 components:

- Things
- Network
- Cloud

Intel also released various IoT products along with ecosystem. This architecture provides data and device security [18].

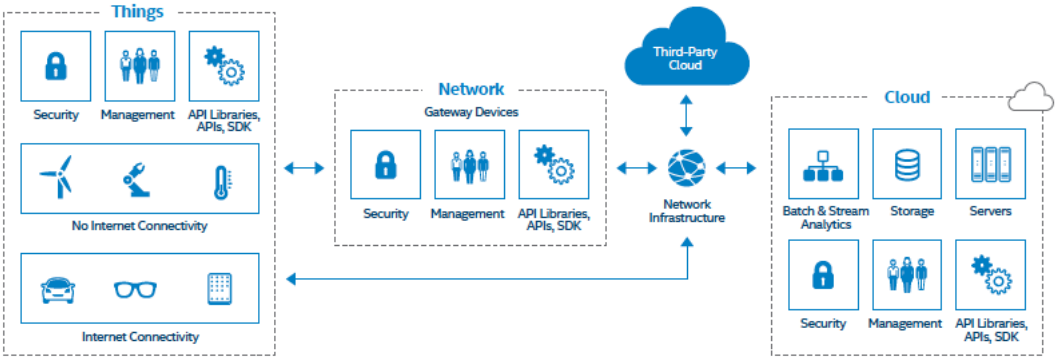


Figure 6: IoT Architecture by Intel [18]

2.3 IoT Architecture by Google

Google architecture is based on three main components.

- Device
- Gateway
- Cloud

Devices can communicate with other devices and these are Internet connected directly or indirectly. Devices, which do not have direct Internet connection, can be accessed by gateway [19]. Gateway also control network traffic that use various protocols. Cloud Platform is used to store, process and analyze data from all devices as shown in Figure 7 below.

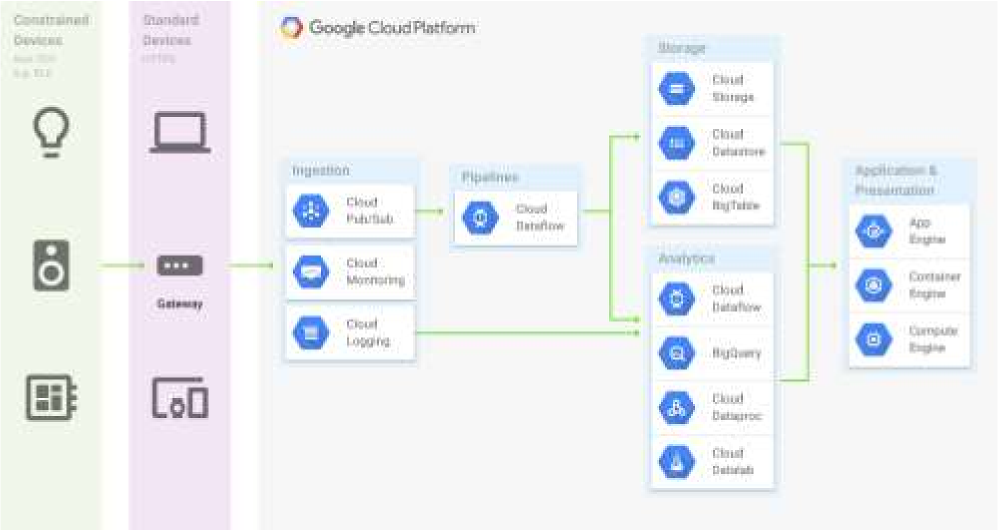


Figure 7: IoT Architecture by Google [19]

2.4 Exploitation of an IoT Device

Integrated circuit can be used as a gateway to control an IoT device. It has been observed from past, IC security is not strong. IoT device can also be accessed by insert-unauthorized device into the network. This technique has been applied to Google nest during a cyber security conference in US [20] [21]. IoT applications can be hacked by malicious code and gain access to device and server. Gateway/router can be used to gain access to network. By gaining network access, fake content can be published on devices as shown in Figure 8 below.

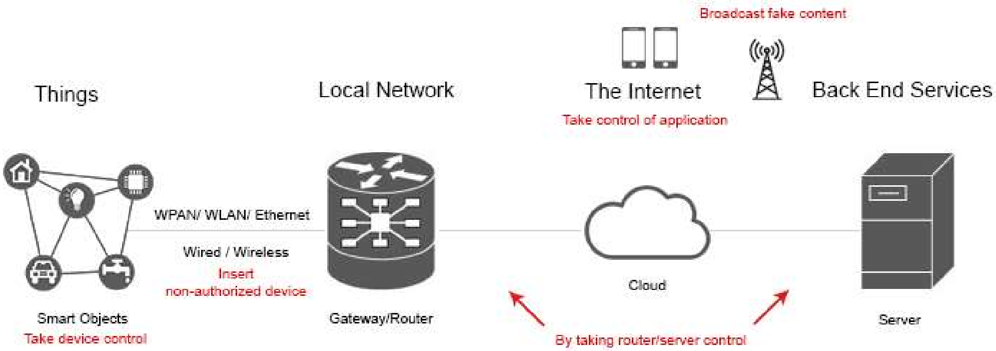


Figure 8: Exploitation of an IoT Device [20]

2.5 IoT Industries & Breach Incidents

IoT will cover everything in every industry [22]. Following are the possible major industries in IoT:

- Connected Home
- Food Services
- Utilities
- Hospitality
- Healthcare
- Government
- Transportation
- Defense
- Infrastructure
- Retail
- Logistics
- Banks
- Oil, gas, and mining
- Insurance
- Agriculture

Health industry is leading 1st half of 2016 with highest number of breaches 263. It has been observed that attacked on this industry has been increased from 2014 [23]. Next highest number breaches 137 happened in Government. Financial services were on third with 118 breaches. Retail, education, technology and other industries cited 102, 102, 90 and 162 respectively. Table 1 shows the breach incidents in IoT industries from 2013 to 1st half of 2016.

TABLE I
Breach Incidents in IoT Industries [23]

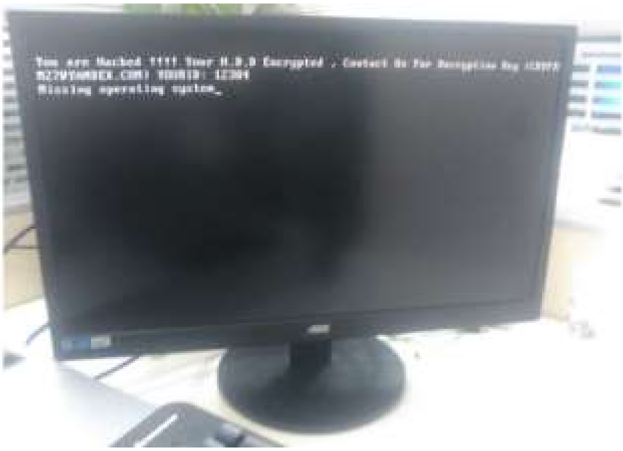
IoT Industries	**1st Half 2013**	**2nd Half 2013**	**1st Half 2014**	**2nd Half 2014**	**1st Half 2015**	**2nd Half 2015**	**1st Half 2016**
Healthcare	172	168	237	208	233	211	263
Finance	78	86	85	126	153	123	118
Government	127	64	109	180	161	135	137
Retail	56	41	81	113	130	108	102
Education	7	27	86	87	102	63	102
Technology	55	55	72	66	58	62	90
Other Fields	151	111	138	136	181	142	162

2.6 IoT Cyber Security Attacks from 2015-2016

As things are adding in IoT umbrella, numbers of breaches are increasing. Following are the 2015-2016 top cyber security attacks.

A. San Francisco's Railway System

On 29 Nov 2016, San Francisco Municipal Transportation Agency (SFMTA) system hacked by ransom-ware attack with a message: "You are hacked. All Data Encrypted". Cyber-criminal encrypted the data by ransom-ware as shown in Figure 9 below [24].



```
You are Hacked !!!! Your H.D.D Encrypted , Contact Us For Decryption Key (crypt
M27@YANDEX.COM) [illegible]: 12384
Missing operating system_
```

Figure 9: Hackers message on San Francisco's Railway System [24]

B. Ransomware hits Los Angeles hospital

Hollywood Presbyterian Medical Centre is one of the oldest private hospitals in Los Angeles, US. On 15 Feb 2016, a major cyber-attack happened and it blocked everything. This attack was very similar to ransom-ware. Medical staff were unable to access important patient data, which include medical reports and laboratory scan etc. Hackers asked 3 million dollars for this data [25]. On 04 Oct 2016, a name in medical Johnson & Johnson also warned customers that their diabetics insulin pumps can be hacked, which can cause an overdose [26].

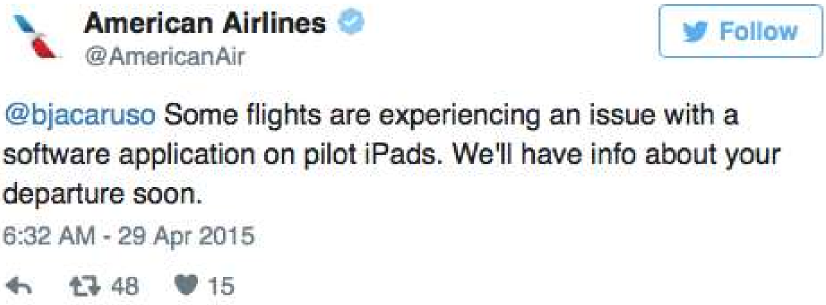
C. Security Researchers killed Jeep Cherokee 2014

In 2015, Charlie Miller and Chris Valasek demonstrated the vulnerabilities in connected vehicle Jeep Cherokee 2014 [27]. They were able to increase/decrease vehicle speed, switch on and off radio and stop it anywhere in mid. In past they have compromised other famous models Toyota Prius and

Ford Escape too. They are not the first one, in past University researchers also demonstrated their access to major components in vehicle [28].

D. Hacking in Aviation

The wave of cyber-crimes also hit aviation industry. On 29 Apr 2015, glitch in iPad app delayed more than fifty American Airlines flights. It is also informed to aviation authorities that flight Wi-Fi could leads to hijack a flight. Also passenger cabin and cockpit electronics use the same network as shown in Figure 10 [29].


American Airlines
@AmericanAir

@bjacaruso Some flights are experiencing an issue with a software application on pilot iPads. We'll have info about your departure soon.

6:32 AM - 29 Apr 2015

Figure 10: American Airlines Tweet About an Incident [29]

On Mar 2015 German Airbus A320 crashed. Aviation experts said this plane has vulnerabilities and could be electronically hacked. In past, criminal used fake boarding passes too. Air miles and loyalty programs are also soft target for cyber criminals [29] [30] [31].

E. ATM Skimming Attacks

ATM skimming attacks are rising worldwide. In 2015, 300 million euros were reported [32]. FICO Card Alert Service in US observed 546% increase in skimming attacks in 2015 and warned costumers about it. Usually these are happening in offsite ATMs as shown in Figure 11 below.

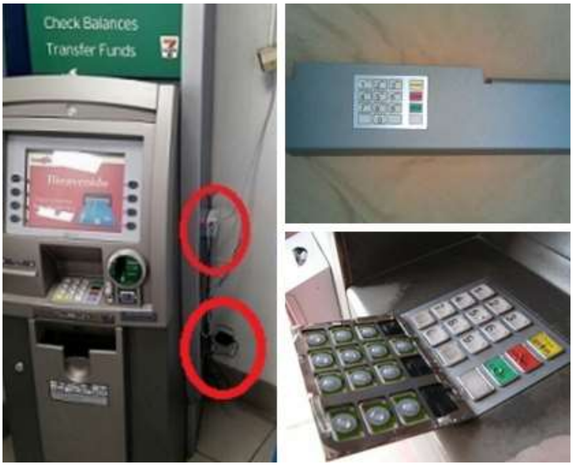


Figure 11: ATM Skimming Techniques [32]

2.7 Leading Sources of Data Breach Incident

Malicious outsiders are the biggest source of data breach incidents with 668 data breaches in 1st half of 2016 similar to previous periods as shown in Table 2 below. Malicious outsider is any unauthorized person in the organization who may or may not be recognizable [23]. Accidental loss cited second with 178 breaches in 1st half of 2016. When a person unintentionally shares important data is known as Accidental Loss. Malicious Insiders, hacktivist and state sponsored attacks cited 83, 29 and 14 breaches. Malicious Insider is a person in the organization, who has access to all confidential data. Hacktivist is a person who hacks system for social and political reasons while state sponsored attacks are govt. sponsored and supported attacks.

TABLE II
TABLE 2: LEADING SOURCES OF DATA BREACH INCIDENT [23]

Breach Sources	**1st Half 2013**	**2nd Half 2013**	**1st Half 2014**	**2nd Half 2014**	**1st Half 2015**	**2nd Half 2015**	**1st Half 2016**
Malicious Outsider	335	317	466	482	608	474	668
Accidental Loss	158	138	189	222	228	208	178
Malicious Insider	114	78	125	156	142	126	83
Hacktivist	20	7	4	16	18	18	29
State Sponsored	3	9	20	40	20	16	14

2.8 Cyber Security Challenges in IoT

Following are identified as cyber security challenges in IoT [33]:

- Insecure mobile & web interface
- Insufficient authentication/authorization
- Poor physical security and Insecure network services
- Lack of transport encryption
- Privacy concerns
- Insecure cloud interface
- Insufficient security configurability
- Insecure software/firmware

III. Findings From Literature

Following are the results and findings from literature:

3.1. Healthcare Industry is Top Target in 2016

The healthcare industry has been a big target of attackers in recent years and that did not change in the first half of 2016 [23]. Next highest in the number of breaches was in government with 137 breaches. Financial services were next with 118 data breaches. The retail and education sectors each had 102 data breaches and the technology industry experienced 90 data breaches, shown in Figure 12 below:

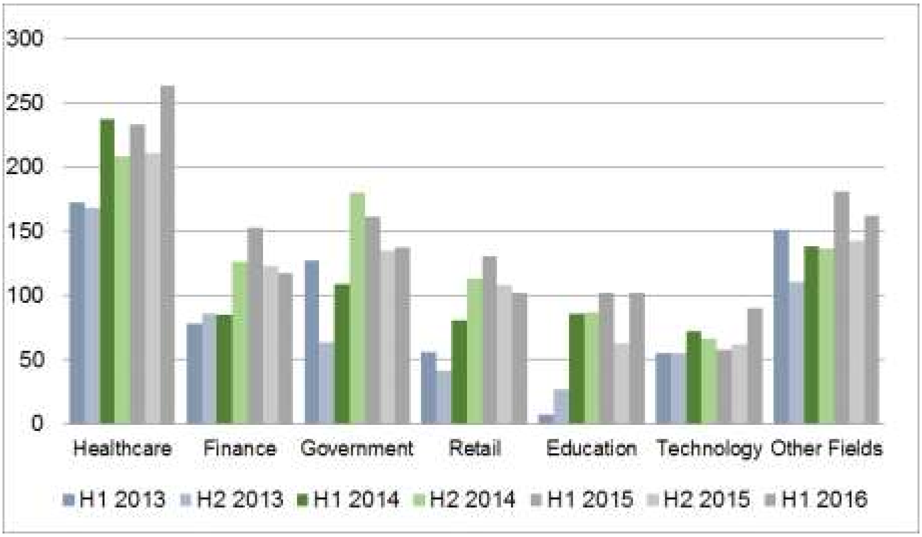


Figure 12: Cybersecurity incidents in different industries over time

3.2. Leading Sources of Data Breaches

Malicious outsiders were the biggest source of data breach incidents with 668 data breaches in 1st half of 2016 similar to previous periods as in Figure 13 below [23].

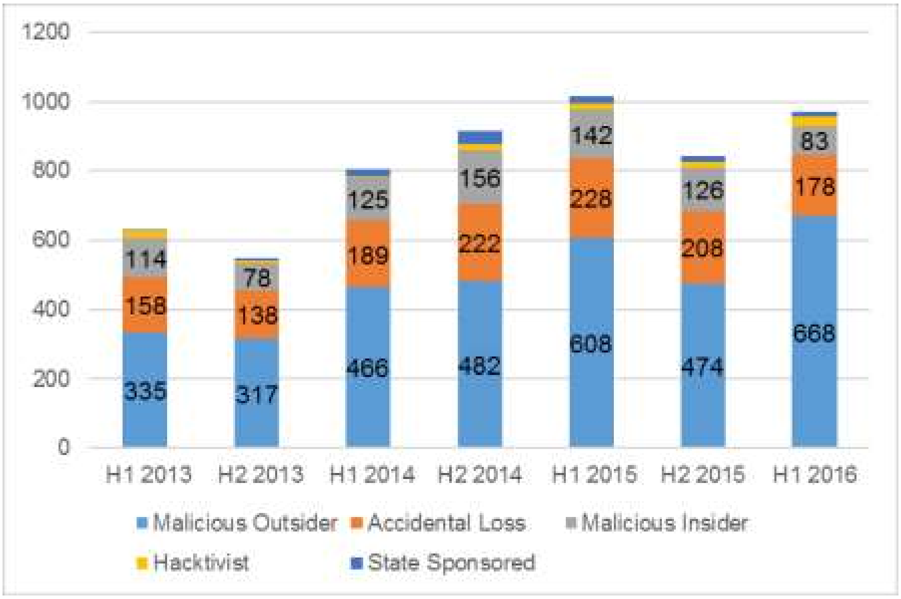


Figure 13: Leading Sources of Cybersecurity Threats from 2013 to 2016

IV. FINDINGS FROM SURVEY

Web based survey was conducted and 100 responses were received; sampling method was random. Survey study shows that the users have strong believe in the potential of IoT. Following are the key findings of this survey study.

4.1. Familiarity with IoT

Respondent’s knowledge about the survey technology is very important. 96.7% respondents were familiar and very small ratio, 3.3% had no idea about IoT at all.

4.2. Adaptors of IoT

The majority of the respondents were from North America 41.4% and Europe 31%. Some 17.2% were in Asia, 6.9% in Africa and 3.4% were in Australia as shown in Figure 14.

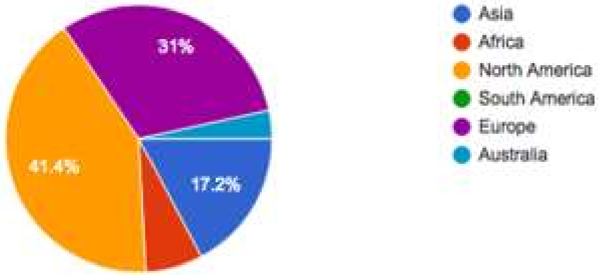


Figure 14: Survey Demographics

4.3. Survey Respondents

Survey respondents came from various industries, as shown in Figure 15. The single largest vertical was technology, at just over 48.3%.

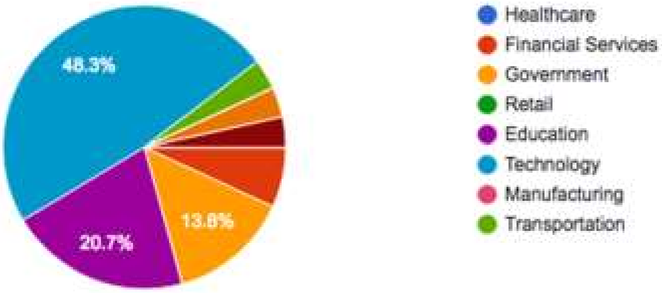


Figure 15: Survey Respondents

The next three largest verticals were education, government, financial services with 20.7%, 13.8% and 6.9% followed by equally spread transportation, hospitality and other fields cited 3.4%.

4.4. Lack of confidence in IoT device security

86.2% respondents feel that IoT devices security is weak. Only 13.8% are slightly more optimistic and satisfied with IoT devices security. Although cybersecurity in IoT is a big challenge but it is an opportunity as well for new ways of thinking.

4.5. Cybersecurity is important to business

Organizations were aware with vital importance of their data and concerned about cybersecurity. 90% respondents from major organizations think cybersecurity is more important than cost, data analytics, performance and integration with hardware as shown in Figure 16.

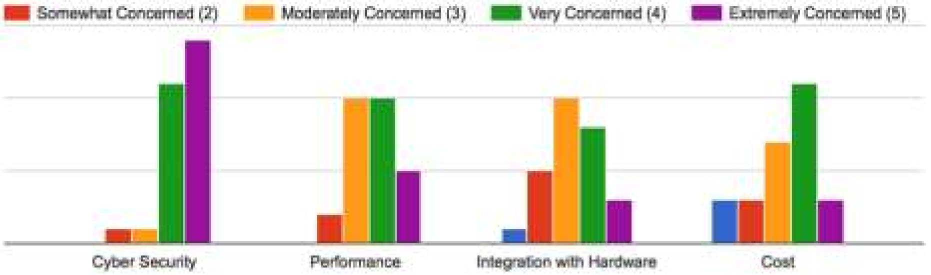


Figure 16: Cyber security is important to business

4.6. Impact of Cyber Security Concerns on Business

65.5% respondents indicate that cybersecurity concerns would discourage them from purchasing an IoT device while 34.5% respondents still want to use the latest technology products despite cyber security concern.

4.7. Awareness about Device Vulnerabilities

Cybersecurity concern is growing along with IoT growth. Only 3.7% are confident about IoT device security, rest 96.6% IoT devices are soft target for hackers.

4.8. Belief in the power of IoT

89.7% respondents have positive thoughts about IoT, they can feel the impact of IoT in their life, business and industries as compare 10.3%, who think IoT is not beneficial for them.

4.9. Most Popular IoT Devices

Smartphones, laptops and tablets were the most popular IoT devices in 2016 cited 100%, 97% and 83% respectively as shown in Figure 17. All respondents own a smartphone of some kind. Desktop computers and TV are the next-most popular devices among those measured cited 75% and 65%. Gaming consoles and wearable are the next with 31%. Rest of the devices popularity is low as compare to other devices that includes radio with 28%, health related devices 24%, kitchen appliances 7% and PDA 4%.

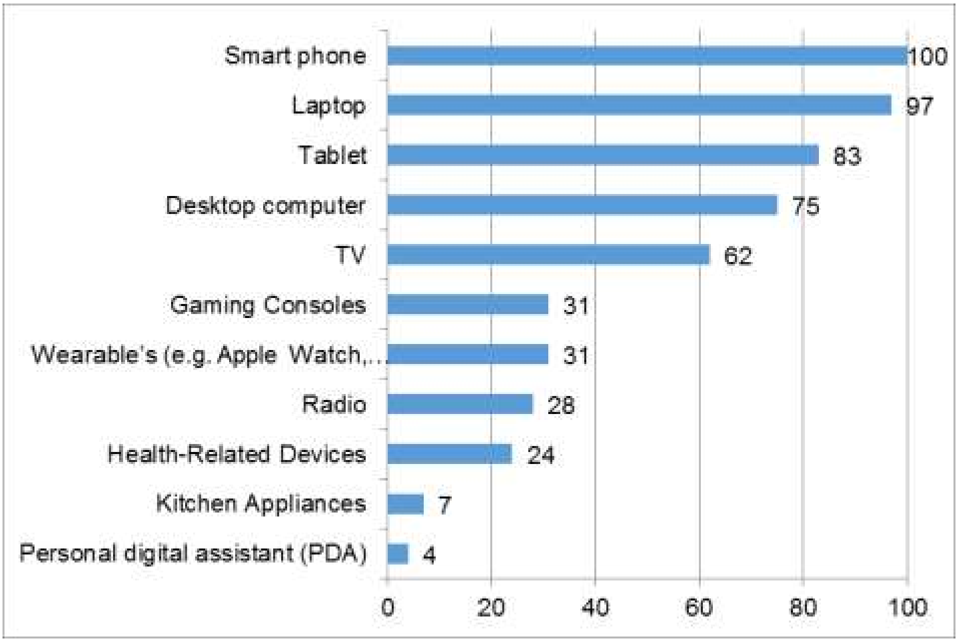


Figure 17: Most Used IoT Devices in 2016

4.10. Use of Credit/Debit Cards on Internet

58.6% respondents were willing to use debit/credit card during online or offline shopping because of ease in payment mode while 41.4% still don’t prefer online payments.

4.11. Public Awareness of Credit Card Breach

10.3% feel use of credit/debit cards is safe while 89.7% respondents are aware that their cards have the potential to be hacked. Credit/Debit card hacking is still an unsolved problem but good part in this problem is people awareness about the problem.

4.12. IoT Manufacturers Security Concerns

User awareness about cyber-crimes improved in recent years. 79.3% respondents think IoT manufactures can improve security in their devices, as they don’t provide enough security while only 20.7% are satisfied.

4.13. Most Sensitive Data in IoT

Everyone likes to keep personal things private. So, it isn't surprising that 62.1% of the respondents rated Personal data as the most sensitive in IoT as shown in Figure 18. Because so many devices will be connected with IoT and linked with password so passwords were next most frequently cited 24.1%, with concerns about Business data 10.3% and emails with 3.4% rounding out the list.

4.14. *Top Security Threat in IoT*

The vast majority with 51.7% of respondents felt the DDOS attack as the primary responsible party as shown in Figure 19. Phishing the next most highly cited selection with 48.3%. However, 31% respondents cited Ransom-ware is spreading across the organizations. Similarly, cyber espionage cited 27.6% while inside threats and nation state attacks were cited 20.7%.

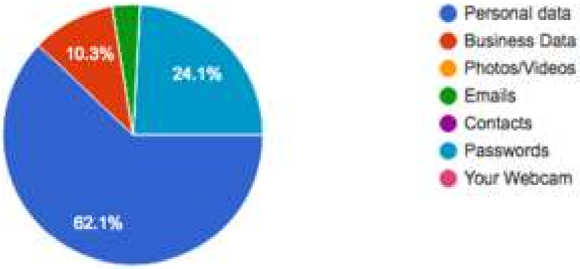


Figure 18: Most Sensitive Data in IoT

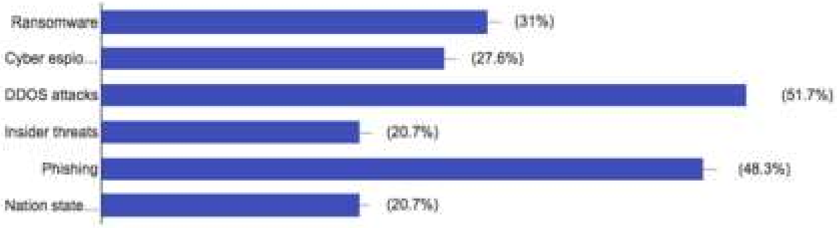


Figure 19: Top cybersecurity threats in IoT

4.15. *Leading Sources of Cyber Threats*

Malicious outsiders and accidental loss were the biggest sources of data breaches cited 31% and 17.2%. This finding is very close to literature finding. Next on the list of most common sources miscellaneous attacks, which cited for 17.2%? Malicious insiders were the next most common source of breaches, accounting for 13.8%. Hacktivists and state sponsored attacks were cited 10.3% as shown in figure 20.

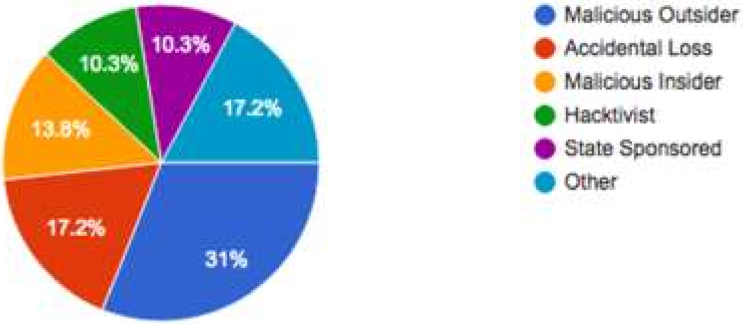


Figure 20: Leading Sources of Cybersecurity Threats in 2016

V. Discussion and Future Work

This study shows that IoT trends is growing up and 97% internet users already have awareness about it. 1st generation of connected things is already in the market and by passing everyday more devices are adding under IoT umbrella. Cybersecurity professional are already making strategies for IoT challenges. 89.7% survey respondents, think IoT will create ease in life and business. Almost majority of the IoT device users have high concerns about IoT device security. Furthermore, they believe it can be improve from manufacturer end; as they do not provide enough security. In recent year's cyber security attacks has been increased on the Internet connected medical devices. Healthcare industry faced 263 data breaches which is highest in all industries and it is 25% up as compare it with previous half [23]. Smart phone, iPad and laptops are the most popular devices while PDA, kitchen appliances and wearable are not much popular among users in 2016.

Cyber security is the main barrier for IoT, because of connected things; users have more awareness about everything that is happening in the world. IoT user awareness about device vulnerabilities is high. More than 90% feel IoT devices are soft target for hackers and 65% users indicate they will not purchase a device that have cybersecurity concerns. Organizations are aware with the impact of cybersecurity on their businesses. Survey results showed that cybersecurity more important than other issues i.e. cost, data analytics, performance and integration with hardware etc. Organizations should review their cybersecurity infrastructure that where they are lacking security measures and plan ahead of cyber-attacks. This study will help IoT manufacturers to use these results as a key to build more secure products in future.

5.1. Key Recommendations for IoT Users

Cyber security is heart of our devices [33]. Suggested security measures below will improve device security:

- Use HTTPS, two factor authentication option i.e. touch ID, firewall.
- Change or replace default name and password with strong characters and change them after every 30 days
- Don't share your personal information i.e. date of birth or home address unless it is very important.
- Activate pin or password on your device.
- Enable Logs on your device.
- Enable notifications for security alerts.
- Verify software and firmware update before install them on device.
- Disable unused physical ports.

REFERENCES

[1] Nermin Hajdarbegovic. (2014, Oct) https://www.toptal.com/i. [Online]. https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things
[2] Kristina Flüchter Felix Wortmann, "Internet of Things," Business & Information Systems Engineering, vol. 57, no. 3, pp. 221–224, June 2015.
[3] Jiafu Wan, Caifeng Zou, Jianqi Liu Hui Suo, "Security in the Internet of Things: A Review," in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, Hangzhou, China , 2012, pp. 648 - 651.
[4] ITU. itu.int. [Online]. http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
[5] Domenico Rotondi, Roberto Minerva Abyi Biru. (2015, Dec) http://iot.ieee.org. [Online]. http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf
[6] Google. (2016, Dec) https://www.google.com/trends/. [Online]. https://www.google.com/trends/explore?date=2006-01-01%202016-12-18&q=%2Fm%2F0b42qh,%2Fm%2F02vnd10&hl=en-US
[7] Ms. Fenn Mr. LeHong. (2013, Aug) http://www.gartner.com/. [Online]. http://www.gartner.com/newsroom/id/2575515
[8] Betsy Burton. (2014, Aug) http://www.gartner.com/. [Online]. http://www.gartner.com/newsroom/id/2819918?_ga=1.51071721.1904172021.1401730474
[9] Betsy Burton. (2015, Aug) http://www.gartner.com/. [Online]. http://www.gartner.com/newsroom/id/3114217
[10] Amy Ann Forni. (2016, Aug) http://www.gartner.com/. [Online]. http://www.gartner.com/newsroom/id/3412017
[11] BI Intelligence. (2016, June) http://www.businessinsider.com/. [Online]. http://www.businessinsider.com/there-will-be-34-billion-iot-devices-installed-on-earth-by-2020-2016-5
[12] W. David Stephenson Christopher J. Rezendes. (2013, June) https://hbr.org/. [Online]. https://hbr.org/2013/06/cyber-security-in-the-internet
[13] Hong Liu, Laurence T. Yang Huansheng Ning, "Cyberentity Security in the Internet of Things," Computer , vol. 46, no. 3, pp. 46 - 53, March 2013.
[14] C. Warren Axelrod, "Enforcing security, safety and privacy for the Internet of Things," in Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island, Farmingdale, NY, USA.

[15] NICOLE PERLROTH VINDU GOEL. (2016, Dec) http://www.nytimes.com. [Online]. http://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=

[16] (2014, Feb) http://architectcorner.yolasite.com. [Online]. http://architectcorner.yolasite.com/products.php

[17] Microsoft. (2016, Mar) https://azure.microsoft.com. [Online]. https://azure.microsoft.com/en-us/updates/microsoft-azure-iot-reference-architecture-available/

[18] Intel. (2016, Feb) http://www.intel.com/. [Online]. http://www.intel.com/content/www/us/en/internet-of-things/white-papers/iot-platform-reference-architecture-paper.html

[19] Google. (2016, Oct) https://cloud.google.com/. [Online]. https://cloud.google.com/solutions/iot-overview

[20] Lawrence Miller, IoT Security for Dummies, Carrie A. Johnson, Ed. Chichester, West Sussex, United Kingdom: John Wiley & Sons, Ltd, 2016.

[21] Eric Gross, Ryan Chinn, Samantha Forbis, Leon Walker, Hsinchun Chen Mark Patton, "Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT)," in Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint, The Hague, Netherlands , 2014, pp. 232 - 235.

[22] Andrew Meola. (2016, Aug) http://www.businessinsider.com. [Online]. http://www.businessinsider.com/internet-of-things-devices-applications-examples-2016-8?IR=T

[23] Gemalto. (2016) http://breachlevelindex.com. [Online]. http://breachlevelindex.com/assets/Breach-Level-Index-Report-H12016.pdf

[24] Krebs On Security. (2016, Nov) https://krebsonsecurity.com/. [Online]. https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/#more-37060

[25] Jason Murdock. (2016, Feb) http://www.ibtimes.co.uk/. [Online]. http://www.ibtimes.co.uk/los-angeles-hackers-demand-3m-ransom-hospital-unlock-vital-files-1543962

[26] BBC News. (2016, Oct) http://www.bbc.com. [Online]. http://www.bbc.com/news/business-37551633

[27] Andy Greenberg. (2015, Aug) https://www.wired.com. [Online]. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[28] Peter Mell and Tim Grance. (2009, July) www.nist.gov. [Online]. http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

[29] Adam Pasick. (2015, Apr) http://qz.com. [Online]. http://qz.com/393909/american-airlines-planes-are-grounded-because-their-pilots-ipads-have-crashed/

[30] SHAWN HELTON. (2015, April) http://21stcenturywire.com. [Online]. http://21stcenturywire.com/2015/04/13/remote-control-aviation-expert-says-germanwings-9525-could-have-been-hacked-electronically/

[31] Drew Harwell. (2015, May) https://www.washingtonpost.com/. [Online]. https://www.washingtonpost.com/business/economy/fbi-probe-of-plane-hack-sparks-worries-over-flight-safety/2015/05/18/8f75e662-fd69-11e4-805c-c3f407e5a9e9_story.html?utm_term=.66213252e33d

[32] Brian Krebs. (2016, Apr) https://krebsonsecurity.com/. [Online]. https://krebsonsecurity.com/2016/04/a-dramatic-rise-in-atm-skimming-attacks/#more-34596

[33] OWASP. (2014, Sep) https://www.owasp.org. [Online]. https://www.owasp.org/index.php/IoT_Security_Guidance

[34] Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg, Jon Shamah, Sławomir Górniak Charles Brookson Scott Cadzow. (2016, July) https://www.enisa.europa.eu/. [Online]. https://www.enisa.europa.eu/publications/definition-of-cybersecurity