IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Review of Computer Engineering Studies
Vol. 5, No. 1, March, 2018, pp. 17-22
Journal homepage: http://iieta.org/Journals/RCES

Cyber security in internet of things

Asim Ismail[1*], Muhammad Saad[1], Robert Abbas[2]

[1] Shaheed Zulfikar Ali Bhutto Institute of Science & Technology Dubai Campus 345004, United Arab Emirates
[2] Macquarie University Sydney NSW 2109, Australia

Corresponding Author Email: asimismail7@gmail.com

https://doi.org/10.18280/rces.050104

Received: 20 January 2018
Accepted: 29 March 2018

Keywords:
Internet of things, cybersecurity, cybersecurity challenges and recommendations.

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 they can be easily compromised by hacker 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 research addresses security challenges in the Internet of Things (IoT). To this end, it's the discussions of the IoT evolution, architecture and its applications in industries. Secondly, it classifies and examines privacy threats by survey, pointing out the challenges that need to be overcome to ensure that the Internet of Things becomes a reality.

1. INTRODUCTION

In a very short time period computer systems size has been reduced from main frames to personal computer and from pc to smart phones. The Internet of things (IoT) period began from 2000 and onwards. In IoT everything is connected with 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 managed 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. There are other examples of IoT as well i.e. smart thermostat, smart locks and smart health devices etc. 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].

As things will be interconnected, we will be able to see everything in our life on 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. 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 in IoT, concern about the things security will increase too.

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. Gradually, this revolution will change everything from personal devices to smart cities.

2. THE IMPORTANCE OF IOT DATA

Data security is a major concern for IoT devices and it should be taken seriously. Every second day, there is news about data breaches. 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. This information doesn't seem very important but it is enough for criminal to misuse it against you. Business data can misuse in the same way.

Nowadays several companies are collecting our data i.e. Google, Yahoo and Facebook etc. and our data can be hacked by hackers. On 14 Dec 2016, Yahoo accepted their 1 billion accounts were compromised [2]. IoT Device manufactures need to understand that data privacy begins at the source. Information shouldn't leave the sensor without protection. At very least, data needs to be encrypted before moving for processing on cloud. IoT standard architecture consisting of things, local network, the Internet and back end services.

3. MATERIAL AND METHODS

This discusses the methods that have been used in the collection and analysis of data for research. Both qualitative and quantitative research methods have been used in carrying out this research. Qualitative research involves the use and study of a variety of empirical materials i.e. case study and visuals etc. while quantitative research is the systematic empirical investigation of noticeable phenomena by means of factual, numerical or computational procedure [3] [4].

The literature study was done with the research questions in mind when searching databases for similar work. Google Scholar used as a main search tool. Google Scholar is a freely accessible web search engine that lists the metadata of scholarly articles and papers across an array of publishing formats and disciplines. The second search tool that was used is Google. Google was mostly used in order to identify both scientific and non-scientific information. The search terms used in this process were based on the questions written and the results were analyzed and evaluated through literature review and online survey.

3.1 Survey study

The survey study is split into two parts. The first part insures that if a user has IoT knowledge; if participant don't know about IoT, survey will be ended without moving to next part. In second part the IoT-environment and security were analyzed to verify the literature findings. All responses were recorded and then analyzed in order to summarize their content.

3.2 Survey questions

Online Survey method is used to for this survey. Google Forms used as a tool to conduct it. Survey responses can be found under the following link:

Link: https://goo.gl/forms/uO3XEyThcE1K6yuh2

Following questions were asked in this survey:

1) Are you familiar with Internet of Things?
2) Which continent do you belong to?
3) Which job industry do you belong to?
4) Are you confident that IoT devices are safe, secure and protect personal information?
5) How much you/ your organization is concern about following?
6) If there are concerns about the cyber security of an IoT device, would you like to purchase that device?
7) Do you think that hackers could access data on IoT devices?
8) Do you think IoT will create ease in life and business?
9) Which of the following devices do you use that are Internet-connected?
10) Are you willing to use debit/credit card on a connected device?
11) Do you have fear that your debit/credit card or connected device could be hacked?
12) Do you think IoT device manufacturers do not provide enough security?
13) According to you, what is most sensitive?
14) What are the top two security threats your organization faces?
15) If any breach happened in your organization, what was the source?

3.3 Survey audience

This survey covers a large sample of people covering a wide geographical area. It was posted on the following groups using LinkedIn social groups.

•Internet of Things
•Media & Marketing Professionals Worldwide
•Information Security Community
•Telecoms Professionals
•Cyber Security Forum Initiative
•Technology Leadership
•IoT – Internet of Things, M2M, Smart Cities
•IoT Security
•Healthcare IT World

3.4 Survey length

Population: Professionals from different industries who use Internet

Sampling Frame: Top Linked Groups from different industries

Date: 4 Weeks

Sampling Method: Random Sampling

Survey method: Web based survey (Questionnaires)

Response: 100 respondents.

4. RESULT AND FINDINGS

4.1 Key findings of literature review

Following are the results and findings of literature review:

4.1.1 Healthcare industry is top target in 2017

The healthcare industry has been a big target of attackers in recent years and that did not change in 2017. 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.

4.1.2 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 shown in Figure 4.2. Malicious outsider is any unauthorized person in the organization who may or may not be recognizable [5]. 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.

4.2 Key findings of survey study

This survey study shows that the users have strong believe in the potential of IoT. Following are the key findings of this survey study.

4.2.1 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 as shown in Figure 1. Gartner hype cycle shows the hype about IoT.

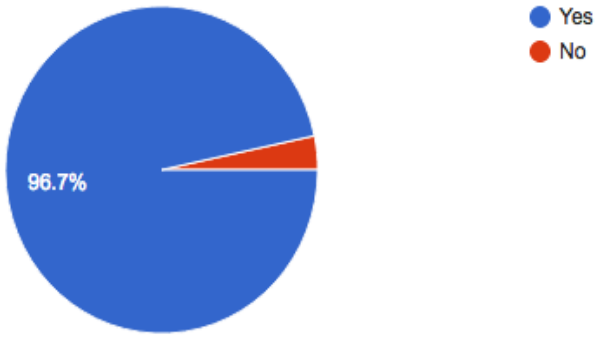

Figure 1. Familiarity about IoT

4.2.2 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 2.

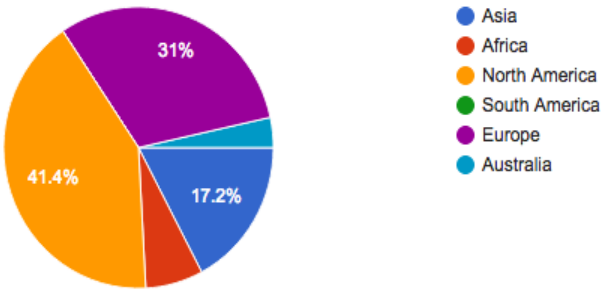

Figure 2. Survey demographics

4.2.3 Survey respondents

Survey respondents came from various industries, as shown in Figure 3. The single largest vertical was technology, at just over 48.3%.

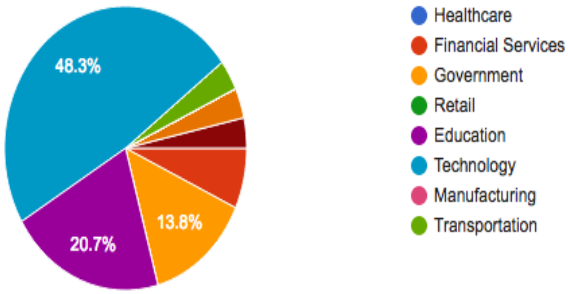

Figure 3. Survey Respondents

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%.

4.2.4 Lack of confidence in IoT device security

86.2% respondents feel IoT devices security is weak as shown in Figure 4. Only 13.8% are slightly more optimistic and satisfied with IoT devices security. Although cyber security in IoT is a big challenge but it is an opportunity as well for new ways of thinking.

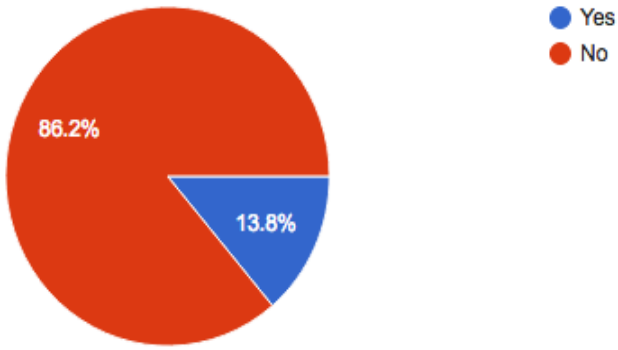

Figure 4. Perceptions about IoT device security

4.2.5 Cyber security is important to business

Organizations were aware with vital importance of their data and concerned about cyber security. 90% respondents from major organizations think cyber security is more important than cost, data analytics, performance and integration with hardware as shown in Figure 5.

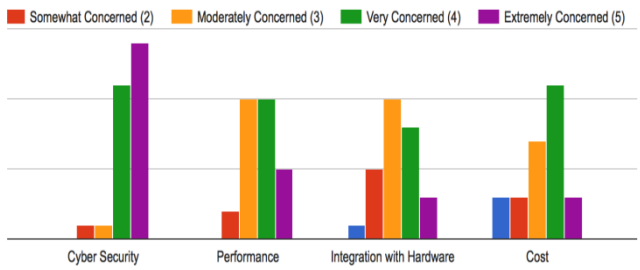

Figure 5. Cyber security is important to business

4.2.6 Impact of cyber security concerns on business

65.5% respondents indicate that cyber security 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 as shown in Figure 6.

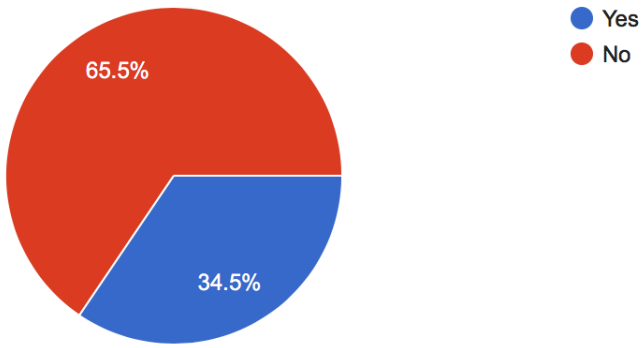

Figure 6. Impact of cyber security concerns

4.2.7 Awareness about device vulnerabilities

Cyber security 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 as shown in Figure 7.

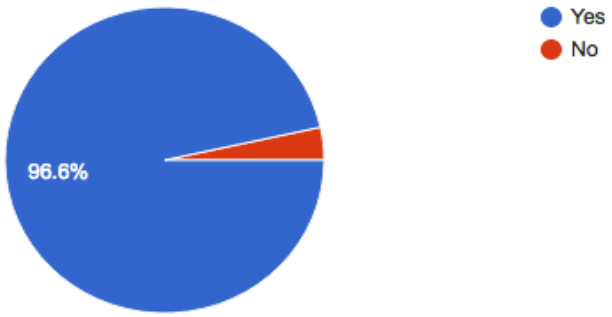

Figure 7. Awareness about IoT device vulnerabilities

4.2.8 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 as shown in Figure 8.

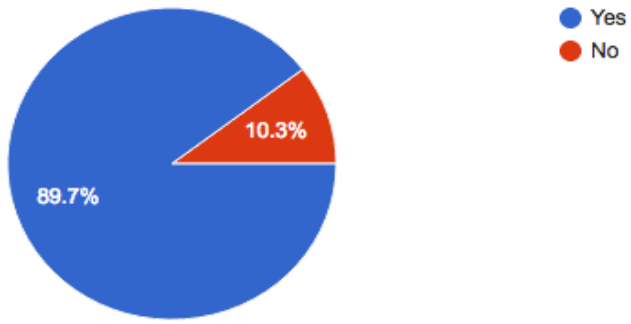

Figure 8. Belief in the Power of IoT

4.2.9 Most popular IoT devices

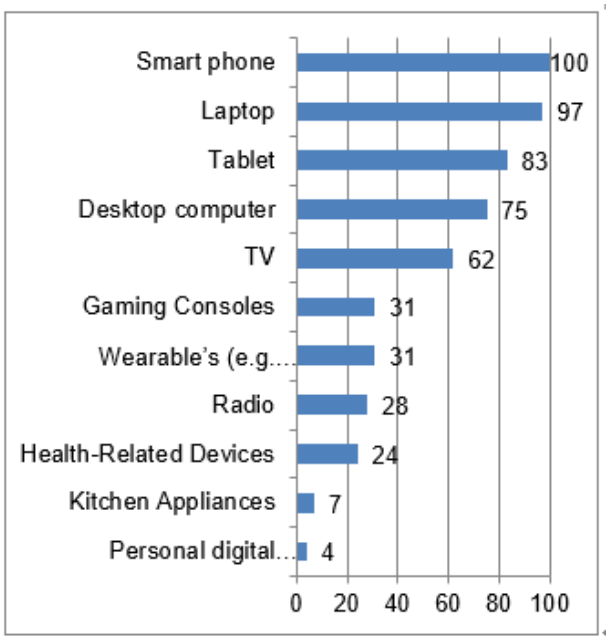

Figure 9. Most used IoT devices in 2017

Smartphones, laptops and tablets were the most popular IoT devices in 2016 cited 100%, 97% and 83% respectively as shown in Figure 9. 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%.

4.2.10 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 as shown in Figure 10.

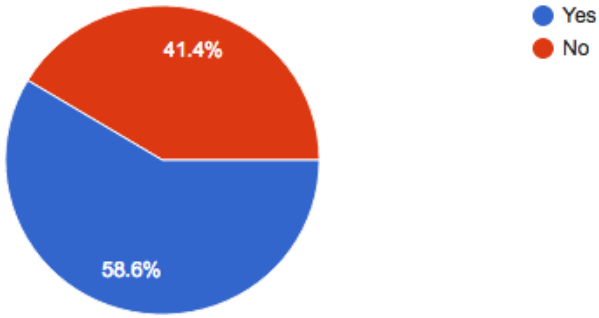

Figure 10. Use of debit/credit card on IoT devices

4.2.11 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 as shown in Figure 11. Credit/Debit card hacking is still an unsolved problem but good part in this problem is people awareness about the problem.

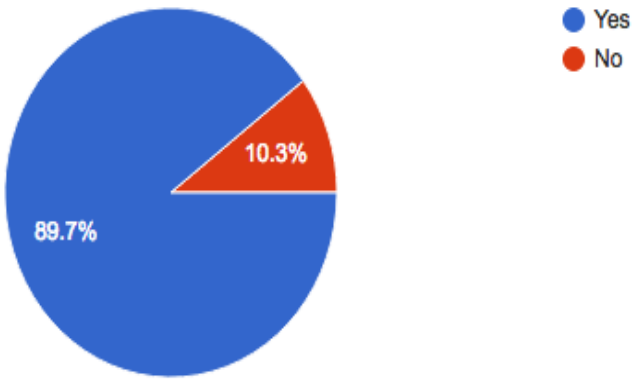

Figure 11. Public Awareness about cyber security breach

4.2.12 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 as shown in Figure 12.

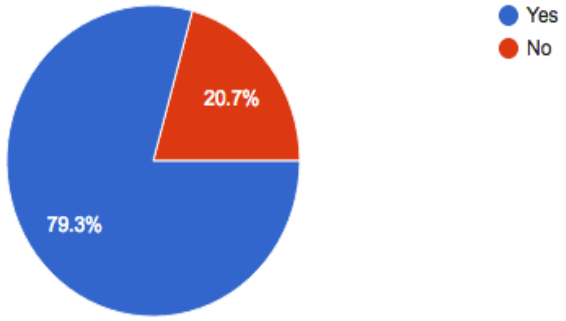

Figure 12. IoT Device Manufacturers Should Improve Security

4.2.13 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 4.15. 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.

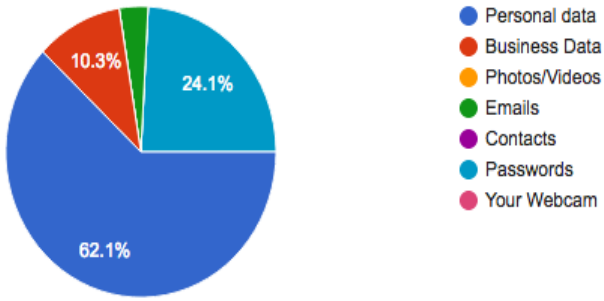

Figure 13. Most sensitive data in IoT

4.2.14 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 14. 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%.

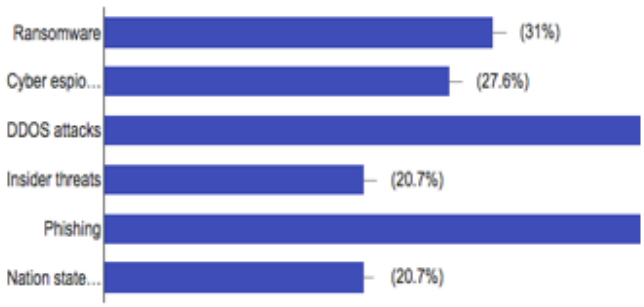

Figure 14. Top cyber security threats in IoT

4.2.15 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, this 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 15.

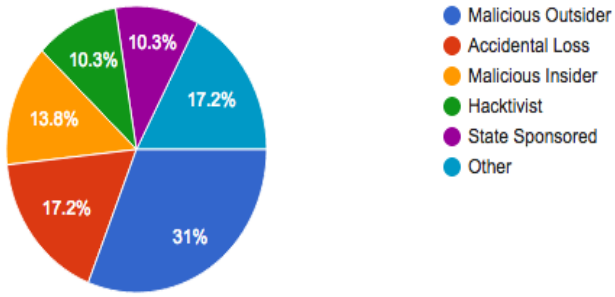

Figure 15. Leading sources of cyber security threats

4.3 Comparison of key findings in literature and survey study

Survey and literature results were very similar as show in Figure 16. Malicious outsiders are the main source of cyber security attacks with 69% data breaches of the total as per literature study and 31% data breaches as per survey study. Accidental loss is the second main source with 18% in literature study and 17.2% in survey study. Accidental loss survey study result is very close with literature study. Third main source is malicious insider cited 9% in literature study while 13.8% in survey study which is bit high as compare to literature study but both ranked them as 3rd main source of attacks. Hacktivist cited 3% in literature while 10.3% in survey. Although survey figure is high but literature and survey ranked them on number 4. State sponsored attacks are the 5th main leading source of attack cited 1% in literature as they are very specific to the target and cited 10.3% during survey. Despite higher figure, both evaluated them as 5th source.

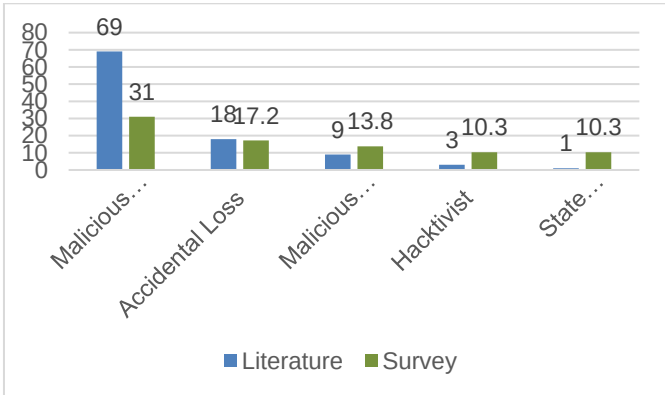

Figure 16. Comparison of literature and survey study

Secondly, key finding of in literature study was hype about of IoT is on peak and it is also very similar to the survey

study. 96.7% survey respondents were familiar with IoT which shows literature studies are true.

Furthermore, IoT growth is forecasted till 2020 which predicted that by everyone will keep 4 devices. Survey shows more 80% users have smart phone, tablet and laptop, 3 devices which depicts that target is very close and very much achievable.

5. 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. cyber security professional is 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 improved from manufacturer end as they don't provide enough security.

In recent year's cyber security attacks has been increased on 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 [5]. Smart phone, iPad and laptops are the most popular devices while PDA, kitchen appliances and wearable are not much popular among users in 2018.

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 cyber security concerns. Organizations are aware with the impact of cyber security on their businesses. Survey results showed that cyber security more important than other issues i.e. cost, data analytics, performance and integration with hardware etc. Organizations should review their cyber security 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 very important. Suggested security measures 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 updates before install them on device.

•Disable unused physical ports.

REFERENCES

[1] Nermin Hajdarbegovic, Toptal. (2014). https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things, accessed on Jan. 17, 2018.

[2] NICOLE PERLROTH VINDU GOEL. (2016). http://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=0, accessed on Jan. 29, 2018.

[3] Johnson RW. (2006). http://www.qualres.org/HomeWhat-3513.html, accessed on Feb. 10, 2018.

[4] Given LM. (2008). The SAGE Encyclopedia of Qualitative Research Methods, 2nd ed. Charles Sturt University, Australia: SAGE Publications, Inc. https://en.wikipedia.org/wiki/Quantitative_research, accessed on Feb. 10, 2018.

[5] Gemalto. (2016). http://breachlevelindex.com/assets/Breach-Level-Index-Report-H12016.pdf, accessed on Jan. 10, 2018.