











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](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](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.