IoT Security

With the growth of technology, IoT devices are being widely used in various industries ranging from home to offices. As of now there are over 25 billion devices [2] that are connected to the internet and are sharing their data in the cloud. Since the IoT devices have been introduced in the market, the standardization and steadiness of these devices have not been addressed. The alterations to the traditional network have been less, and this network is not capable of handling many connected devices. Because of this infrastructure, there are a lot of security threats which are currently being worked on.

Some major security issues which are being addressed now are hardware vulnerabilities, when IoT devices are developed on a commercial level, security is not being considered as a feature in hardware. Security features are added later depending on the need of the devices. This add-on feature can cause issue and will leave the device open for vulnerabilities.[1] Moreover, due to high demand of IoT devices, the developers are not testing the security component of the devices, which is increasing the security risks. Apart from the manufacturing issues, user awareness is also a big problem.[3] Users are not aware of the technologies they are using and the functionality it is providing. The users end up giving their personal information access to the cloud, which is also open to hackers.
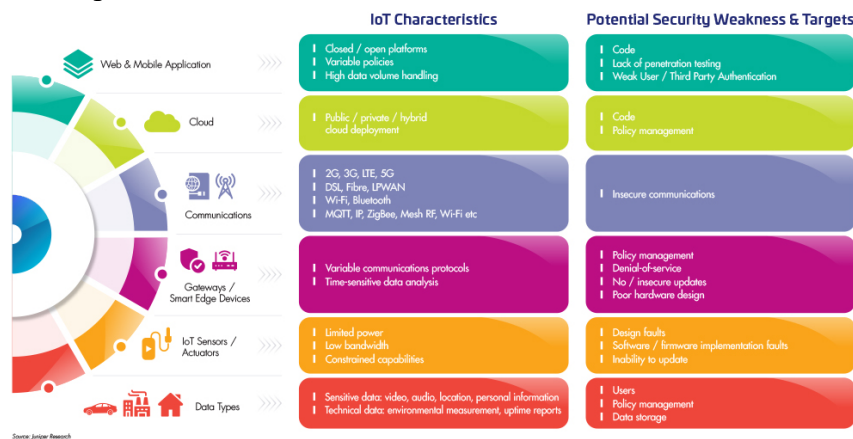

Fig. Security concerns at different stages of IoT devices.[5]

The main issue which the company should consider addressing is minimizing data and information leak. Since IoT devices are being used for personal use as well as medical use, there is a lot of personal information of users which is open to the hackers. This is an important issue as, if a hacker manages to get control of a house, he will be open to information such as who is at home and can lead to major issues such as kidnapping or black mailing. Moreover, if the hacker manages to get access to a medical device, he can alter things in the data collected from the device, which could lead to serious issues.[2] It is easy to do denial of service attack to a network if the hacker gains access to the IoT device. These serious issues need to be addressed on a priority.

It would be a benefit for the company if it focuses on addressing the need of universal standards to manage secure access and transportation of data collected from IoT devices. If the access is made secured, it would be safe to use the IoT devices and the applications where we can use such devices will increase. Moreover, technologies like big data could be used to monitor end to end security of internet connected IoT devices. [1]

REFERENCES

1. A. Roukounaki, S. Efremidis, J. Soldatos, J. Neises, T. Walloschke and N. Kefalakis, "Scalable and Configurable End-to-End Collection and Analysis of IoT Security Data : Towards End-to-End Security in IoT Systems," 2019 Global IoT Summit (GIoTS), 2019, pp. 1-6, doi: 10.1109/GIOTS.2019.8766407.

2. W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf and Y. A. Bangash, "An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10250-10276, Oct. 2020, doi: 10.1109/JIOT.2020.2997651.

3. N. M. Karie, N. M. Sahri, W. Yang, C. Valli and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," in IEEE Access, vol. 9, pp. 121975-121995, 2021, doi: 10.1109/ACCESS.2021.3109886.

4. P. Zhang, Y. Wang, N. Kumar, C. Jiang and G. Shi, "A Security- and Privacy-Preserving Approach Based on Data Disturbance for Collaborative Edge Computing in Social IoT Systems," in IEEE Transactions on Computational Social Systems, vol. 9, no. 1, pp. 97-108, Feb. 2022, doi: 10.1109/TCSS.2021.3092746.

5. "Building trust in IoT devices with powerful IoT security solutions," Thales Group. https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/iot-security (accessed Feb. 02, 2022).

https://iot-analytics.com/understanding-iot-security-part-1-iot-security-architecture/