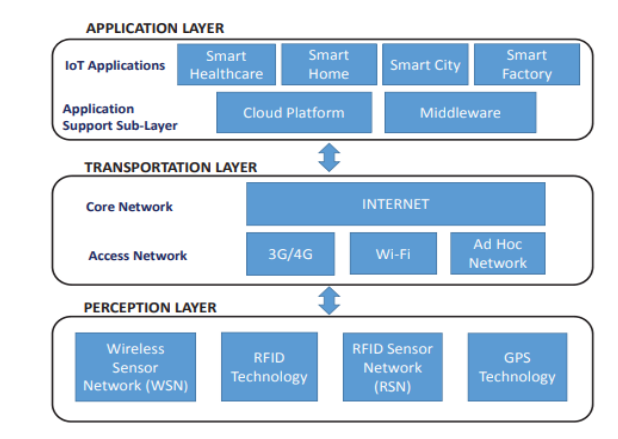
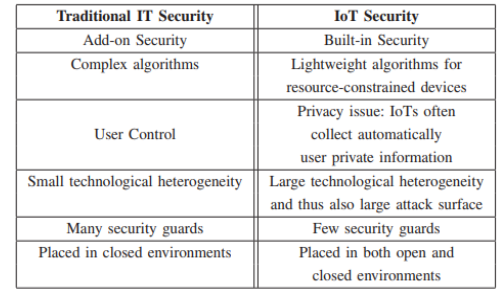
**ISTE 782: Assignment 4: Technology 1 - Internet of Things (IoT) Security**

Over the past few years Iot has been one of the most emerging technologies of recent times. According to a report there are more than 10 billion connected Iot devices today. Regular commodities like as household items, automobiles, indoor regulators, and child screens can now be linked to the web via implanted gadgets, allowing for continual communication between people, cycles, and things. [1] Specialist says that this will increase up to 20 billion by 2025. Even tough Iot received acceptance from all over the world. There were few security challenges that were ignored.

**Figure 1: Iot infrastructure model Figure 2: Security differences**

As we can see from figure 1 Iot infrastructure model consists of three layers. And each of these layers are exposed to vulnerability [2]. The vital problem associated with Iot security is that very less importance is given to security component by the developers resulting in cost saving. [1] Top most importance is given to the software whereas on the other hand hardware devices are left unsecured resulting in the security threats to the devices. Overall security in the figure 1 can be addressed by following the three major security pillars such as Confidentiality, Integrity and Availability. Figure 2 represents the difference between traditional security vs Iot security. Considering the current state of Iot it can be noticed that our personal devices such as tablets, mobile phones, laptops are exposed to high risks. Following the three pillars of security, confidentiality provides the client with a certainty of their own information insurance which can be potentially done by information encryption methods or other access control systems. Which will on the other hand prevent any illegal access into the users personal and private data. [3] According to the security perspective in IoT framework, it should be equipped for adding security to the currently functional framework for example advanced mobile phones, tablets etc. [5] Best procedure to upgrade the security of IoT framework is to consider the solid conventions that are utilized for the transmission process.

Of the major challenge that a company should consider addressing is long term evaluation (LTE) which is widely used procedure in mobile phones. There are few algorithms that already exists such as stream cipher cryptography and block cipher cartography. However, companies should aim focusing at the key principal which was constructed from core stream cipher cartography called as ZUC [4]. After reviewing the findings of the study, it is evident that AES and ZUC are far superior encryption standards to the others.

**Bibliography**

|  |  |
| --- | --- |
| [1] | R. B. Sulaiman, "Future Threats to internet of things (Iot) Security and privacy," *School of Computer Science and Technology Univeristy of Bedfordshire Vicarage St , Luton LU1 3JU,* p. 12, 2017. |
| [2] | A. V. V. J. W. J. L. a. D. Q. Qi Jing, "Security of internet things : perspective and challenges," *Wireless Networks, ,* vol. 20, p. 8, 2018. |
| [3] | L. B. A. T. L. F. P. G. R. G. A. V. L. P. M.Di Felice, "Smartphones like stem cells: Cooperation and evolution for emergency communication in post disasters scenarios," *IEEE BlackSeaComm ,* p. 20, 2017. |
| [4] | A. a. I. F. T. A. Ghanim, "Comparative study on 4G/LTE Cryptographic ALgorithms Based on different factors," *IJCST,* 2019. |
| [5] | C. C. G. Tanganelli, "Coapthon : Easy develpoment of coap-based Iot applications with python," *Internet of things (WFoT) IEEE 2nd World Forum on,* vol. 63, 2019. |

|  |  |
| --- | --- |
|  |  |