Security and Privacy in the Internet of Things (IoT)

(A summary of the lecture by Dr. Elisa Bertino)

The lecture starts with the introduction to IoT and its usage in various domains. The purpose of IoT is briefly explained and then it dwelled into the topic of its usage in industries and business. This covered the areas of the evolution of IoT, the generic and privacy risks that come along with the usage of IoT devices, and also the security measures that are being taken to ensure the safety and confidentiality of the system. The latter part of the lecture touched the topics of communication architecture, and it also gave a brief idea of where the future research direction of IoT headed to.

When you try to see the relationship between the IoT and the information security you will obviously come to know about the **confidentiality** of data. In IoT, maintaining the confidentiality of the data is difficult, also opposite to the fact, obtaining information from devices without the user's authorization is very easy. Be it whether the personal devices such as the health monitoring system or the public devices that monitor the agricultural growth they can be easily hacked. In other words, the data which are collected by them are not secure, they can be exposed to any of the third party without the user's notice. As per the Dr. Elisa Bertino's research on the application of IoT on agricultural welfare, farmers don't feel good about letting others know about the fertility of the soil, then how will people feel about the exposure of information about personal health to others. This shows that to completely integrate the IoT into every nuke and corner, domain, sectors, areas then it should have the ability to mediate data only with user's authorization or permission.

The lecture made me understand how IoT can evolve and what all are the risks that might accompany its evolution. I have always limited my vision of usage of IoT up to the automation level. But now, I have come to know that artificial intelligence can also be implemented in the collection, processing, and analysis of data through IoT. It also made me realize how the implementation can expose the private data to the third party members without any authorization. The lecture also introduced me to the topic of **Mirai Botnet,** which is a particularly designed malware that can launch multiple DDOS attacks. And this also shed some light on designing defense mechanism against botnet attacks and challenges present in them. The topic which piqued me is the **Heimdall**, which is a whitelist based anomaly detection defense mechanism for IoT routers. This method uses the DNS and the IP addresses of the devices connected to the router to detect the botnets or any user who creates DOS or DDOS.

Altogether I feel like the lecture has shown me the sides of security concerns in IoT which I haven't got to know or haven't seen before.

College of Science
ILLINOIS INSTITUTE OF TECHNOLOGY

Vignesh Kumar Karthikeyan Rajalakshmi
A20424508