**Unit 5: Future trends in Secure Software Development**

**Objectives:**

* Discuss future trends in the areas of secure design, development, programming languages and operating systems.
* Explain what is meant by Fog Computing, the Internet of Things and Cyber Physical Systems.
* Explore systems and solutions that can be investigated as possible research topics or fields.

**Outcomes:**

* Give examples of fog computing, IoT and Cyber Physical System components and solutions.
* Describe some of the security issues with the above-mentioned systems.
* Recommend emerging technologies and solutions to investigate.

**Reflection:**

When data, compute, storage, and applications are dispersed between on-premises servers and cloud servers in a "fog" environment, it's called "fog computing." Edge computing, like fog computing, brings the benefits and energy of the cloud closer towards where information is formed and acted upon. Fog computing. In order to perform complex computations and processing, fog computing is required on all devices. For example, the Car-to-Car Consortium (Europe) and other IoT devices (such as devices with sensors and cameras) are examples of fog computing being used in the real world. In a manufacturing line, an embedded application with a temperature sensor connected to an edge server measures the temperature every moment. This is an excellent example of fog computing in action. It would then be sent to the cloud application, which monitors temperatures, for this data to be analysed. As there are numerous devices connected to fog nodes and gateways, security concerns arise. Any hacker can gain access to your personal information stored in that fog node by faking your IP address, which is unique to each device (Posey, n.d.).

Internet of Things (IoT) refers to a network of material things  that are equipped with sensors, software, and other innovations for the aim of integrating and swapping information between computers and systems over the Internet. On the market, you'll find a slew of high-quality products. Several examples of Internet of Things (IoT) products include smart phones, smart fridges, smart watches, smart fire alarms, smart locks, smart bicycles, medical sensors, fitness trackers, and smart security systems.

The following are some of the most common reasons for IoT systems to be vulnerable to attack: Poor built-in security due to a lack of computing resources Inadequate security measures in IoT systems. Lack of resources for comprehensive firmware security testing and improvement (Gillis, 2022).

Connecting physical objects to the Internet and each other is the goal of cyber-physical systems that incorporate sensors, computation, and control into the physical world. integration, across technologies, industries, and the entire life cycle, and "smartness" characterize CPSs. CPS can be seen in a variety of forms, such as autonomous vehicles, intelligent buildings, implantable medical devices, self-driving cars, and planes that operate within a predetermined airspace (Monostori, 2018).

These are some trends in software development that will have a high impact on the broad IT industry.

There is a growing reliance on artificial intelligence, progressive web apps, and server less computing, as well as a rise in the Internet of Things.

**References**

Gillis, A. (2022). *What is IoT (Internet of Things) and How Does it Work? - Definition from TechTarget.com*. [online] IoT Agenda. Available at: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT [Accessed 12 July. 2022].

Monostori, L. (2018). Cyber-Physical Systems. *CIRP Encyclopedia of Production Engineering*, [online] pp.1–8. doi:10.1007/978-3-642-35950-7\_16790-1.

Posey, B. (n.d.). *What is Fog Computing? - Definition from IoTAgenda*. [online] IoT Agenda. Available at: https://www.techtarget.com/iotagenda/definition/fog-computing-fogging [Accessed 12 July. 2022].