Unit 11: Future Trends in Secure Software Development

1. **Give examples of fog computing, IoT and Cyber Physical System components and solutions.**

Fog computing:

Fog computing is a decentralised computing infrastructure that optimises resource utilisation by bringing computation, storage, and communication closer to the network's edge. It reduces energy usage, traffic congestion, and latency, making it a popular solution for various applications, including smart grids, smart cities, intelligent buildings, vehicle networks, and software-defined networks (Mukherjee et al. N.D.).

As Posey et al. (N.D.) explain, fog computing brings the benefits of the cloud closer to where data is generated and utilised. It works with cloud computing, allowing for short-term analysis at the edge while the cloud handles more resource-intensive, long-term study.

Furthermore, as Yi (2015) highlights, fog computing enables computing at the network's edge through fog nodes like set-top boxes, access points, routers, switches, base stations, and end devices or resource-rich machines. These nodes can be resource-poor or resource-rich, like Cloudlet and IOx. IOx is a fog device from Cisco that hosts applications in a Guest Operating System (GOS) running in a hypervisor on the Connected Grid Router (CGR).

According to Mohanakrishnan (2022), there are various implementation methods of fog computing, as Mohanakrishnan notes, but they all share components in their architecture. End devices serve as conduits to the physical world, while fog nodes, classified as fog devices, servers, and gateways, gather the generated data. Monitoring services oversee the system's performance and resources, and data processors sift through and repair faulty data. The resource manager handles resource

allocation and data transfer scheduling. The system includes built-in security tools, and applications offer services to end-users.

Fog computing is an emerging technology that effectively tackles IoT devices' latency challenges, as Mohanakrishnan (2022) points out. It has been widely applied across smart homes, smart cities, healthcare, video surveillance, and more sectors. Additionally, it offers real-time solutions to enterprises and can become vital in many industry verticals, including retail, oil & gas, government & military, and hospitality.

Clancy (2023) describes four types of fog computing components: device-level, edge-level, gateway-level, and cloud-level. Fog computing can benefit connected cars, smart cities, industrial IoT, connected health, and AR/VR. By moving compute resources closer to data sources, fog computing can improve performance and reduce costs.

IoT components:

The Internet of Things (IoT) is a sophisticated ecosystem connecting devices, machines, objects, and people. It allows them to communicate and exchange data seamlessly over a network without needing human-to-human or human-to-computer interaction. IoT utilises a combination of sensors/devices, connectivity, data processing, and user interface to gather, process, and present data in a user-friendly manner. It facilitates real-time system monitoring and alerts and the ability to initiate and execute actions remotely. By harnessing the power of IoT, industries can reap the benefits of improved decision-making, superior customer service, and enhanced operational efficiency (Duggal, 2021).

The Internet of Things (IoT) is a vast network of physical devices that can seamlessly exchange data without human intervention. IoT devices are equipped with sensors and unique identifiers (UID), which allow them to self-report and communicate with other

devices and users in real time. IoT devices have become increasingly ubiquitous daily, from smart home gadgets like thermostats and security systems to wearable technologies like smartwatches and personal medical devices like pacemakers (Coursera, 2023).

As Duggal (2021) highlights, IoT has become more practical due to recent advancements in affordable sensors, cloud computing, machine learning, and artificial intelligence. This ecosystem of devices, machines, objects, and people enables them to communicate and exchange data seamlessly over a network without human-to-human or human-to-computer interaction. IoT utilises a combination of sensors/devices, connectivity, data processing, and user interface to gather, process, and present data in a user-friendly manner. It facilitates real-time system monitoring and alerts and the ability to initiate and execute actions remotely. By harnessing the power of IoT, industries can reap the benefits of improved decision-making, superior customer service, and enhanced operational efficiency.

According to Bring IT On NI (2022), IoT has four main components - sensors/devices, connectivity, data processing, and user interface. Sensors collect data from connected environments and deposit it into the cloud. The data is then sent to the cloud through various connectivity options. The cloud processes the data for the end-user, and a user interface prepares the information for consumption. The user can review ongoing processes and perform actions remotely. As IoT grows, securing it becomes increasingly important.

IoT represents a sophisticated ecosystem that connects devices, machines, objects, and people. IoT devices are prevalent across diverse industries, from household appliances and automobiles to security systems and healthcare monitors. As

projected, connected devices will exceed 27 billion by 2025, and IoT will continue revolutionising how we live and work (Thomas, 2022).

Cyber-Physical System:

Cyber-Physical Systems (CPS) integrate hardware, software, and potentially other systems. They can be found in various domains such as healthcare, agriculture, transport, energy, etc. These systems can help monitor patients' health, provide safe and efficient road traffic systems, secure food supplies, and provide energy-optimized buildings and sustainable energy. Designing and building secure CPSs that deliver consistent and dependable emergent behaviour is essential (NCU, N.D).

As we continue to enjoy the benefits of intelligent living, safeguarding data authentication is becoming a growing challenge. Multi-factor authentication is a highly effective solution to ensure security in this era of IoT and IoE. Cyber-physical systems use advanced computing, communication, and control to enable cutting-edge technology and have become integral to numerous fields, including energy, transportation, the environment, and healthcare (Tyagi & Sreenath, 2021).

Cyber-Physical Systems (CPS) enhance the operation of physical systems by integrating computational and physical subsystems. These systems are safe and interoperable, interacting with the physical world and human users in real-time. Sensors convert real-world phenomena into signals that can be processed, stored, visualised, and acted upon in the cyber world. Embedded systems perform specific tasks with tightly coupled physical and cyber components. Networked control systems exchange information with distributed sensors and actuators over communication networks (Jahromi & Kundur, 2020).

2. Describe some of the security issues with the above-mentioned systems.

Security poses a significant challenge in Fog Computing, IoT (Internet of Things), and Cyber-Physical Systems (CPS) since the consequences of breaches can be devastating. Breaches can cause financial loss, impact safety and privacy, and disrupt operational integrity. As Jang-Jaccard & Nepal (2014) pointed out, the interconnected nature of these systems means that a security breach in one component can bring down the whole system.

According to Tariq et al. (2019), below are some of the most significant challenges associated with Fog computing, the Internet of Things (IoT), and Cyber-Physical Systems (CPS):

- Lack of centralised security controls. These systems are usually distributed, with various devices and components located in different geographical locations, which makes it challenging to implement and manage centralised security measures. Due to this decentralised nature, managing security controls becomes complex, and ensuring that all the devices and components are adequately protected against cyber threats becomes challenging. As a result, implementing robust security measures becomes crucial to mitigate the risks of potential security breaches and data loss.
- Fog computing, the Internet of Things (IoT), and Cyber-Physical Systems (CPS) often comprise a diverse range of devices sourced from different manufacturers, resulting in a complex and heterogeneous ecosystem. This heterogeneity poses significant challenges in implementing consistent and standardised security measures across all devices. For instance, the devices' varying processing capabilities, communication protocols, and security configurations make it difficult to effectively develop a uniform security framework to mitigate potential vulnerabilities across the entire system. Therefore, it is crucial to address the heterogeneity issue to ensure that the devices' security remains robust and reliable and that the system's integrity and confidentiality are upheld.
- Physical vulnerabilities concerning fog computing, IoT, and CPS devices are a significant concern. These devices are often physically exposed and may be difficult to protect from tampering or theft. Physical attacks can cause considerable damage to the device, resulting in system downtime, data loss, and even financial losses. Physical access to these devices can also allow attackers to install malicious software or extract sensitive data. As a result, it is crucial to implement robust physical security measures to safeguard these devices from unauthorised access and physical damage. These measures can include physical locks, surveillance systems, and access controls.

- Limited resources, such as processing power and battery life, often characterise these devices. As a result, implementing complex security measures on these devices can be a significant challenge. The limited resources of these devices make it difficult to support advanced cryptographic algorithms, perform regular software updates, and run security scans, which can leave them vulnerable to cyber-attacks. Additionally, the lack of resources on these devices can make it challenging to implement security mechanisms that do not compromise their performance or functionality. Therefore, addressing the security challenges posed by limited resources is critical to ensure these devices safe and secure operation and the systems they are connected to.

The Federal Trade Commission advises companies to prioritise security measures that minimise the risks associated with IoT devices. While fog computing can benefit data storage, it poses potential privacy and security concerns. Fortunately, blockchain technology provides a reliable and streamlined solution for addressing these challenges. To bolster system defences against potential threats and vulnerabilities, it is crucial to implement strict authentication and authorisation controls, encryption protocols, regular vulnerability patching, system monitoring, physical security measures, and security frameworks (Tariq et al., 2019).

3. Recommend emerging technologies and solutions to investigate.

Technology has transformed how we work, and the next wave of innovation centres around how technology can augment our capabilities. Combining people and technology can bring more significant gains, as seen in examples like upskilled finance pros using automation to take on data tasks and robots designed to work alongside nurses. However, we must address trust-related challenges, including equity, ethics, data privacy, and security (PWC, N.D.).

Several emerging technologies and solutions are worth investigating for various applications. Here are some that caught my attention:

Generative AI:

Generative AI is artificial intelligence that can produce text, images, and audio. Using GANs can create realistic media. It has many applications, including educational content, deepfakes, and movie dubbing (Lawton, 2023). Transformative advancements in transformers and large language models have enabled generative AI to write engaging text and photorealistic images. However, there are still issues with accuracy, bias, and hallucinations. Generative AI has the potential to automate tasks and optimise supply chains, revolutionising businesses. For example, it could help the medical industry identify drug candidates more efficiently.

Quantum computing:

Quantum computing is a field that uses quantum mechanics to solve complex problems faster than classical computers. It is a multidisciplinary field that leverages effects such as superposition and quantum interference. Quantum computers can solve currently impossible issues for even the most powerful supercomputers. They have applications in machine learning, optimisation, and simulation of physical systems. Due to their potential, the use cases for quantum computing are vast and far-reaching (AWS, N.D.).

Martin (2023) suggests that quantum computing can solve problems beyond the reach of classical computers, such as breaking encryption, designing new drugs, and simulating molecule behaviour.

Metaverse:

The Metaverse is a groundbreaking idea that blends the physical and virtual worlds, creating a lasting multiuser realm. Users can engage with digital products, virtual environments, and individuals through various modes of interaction. The Metaverse is

a connected network of interactive and social platforms that remain permanent (Simplilearn, 2023). One critical application of this technology is its potential to create novel educational and training experiences.

Blockchain:

Blockchain technology offers a secure and transparent method for tracking assets and recording transactions on a shared ledger. It instils greater confidence, reduces costs, and gives permission network members real-time access to accurate information (IBM, 2023). Blockchain benefits include enhanced security, greater transparency, instant traceability, increased efficiency and speed, and automation through intelligent contracts (IBM, (2022).

References:

Mukherjee, M., Shu & L., Wang, D. (N.D.). *Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges*. [online] Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8314121.

Posey, B., Shea, S. & Wigmore, I. (N.D.). *What is Fog Computing? - Definition from IoTAgenda*. [online] Available at: https://www.techtarget.com/iotagenda/definition/fog-computing-fogging.

Yi, S., Li, C. & Li, Q. (2015). A Survey of Fog Computing. *Proceedings of the 2015 Workshop on Mobile Big Data*. doi:https://doi.org/10.1145/2757384.2757397.

Mohanakrishnan, R. (2022). *What Is Fog Computing? Components, Examples, and Best Practices*. [online] Available at: https://www.spiceworks.com/tech/edge-computing/articles/what-is-fog-computing/.

Clancy, R. (2023). *What Is Fog Computing? definition, Applications, Everything to Know*. [online] Cybersecurity Exchange. Available at: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/fog-computing-everything-to-know/.

Duggal, N. (2021). *What Are IoT Devices : Definition, Types, and 5 Most Popular Ones for 2021*. [online] Simplilearn.com. Available at: https://www.simplilearn.com/iot-devices-article.

Coursera (2023). *What is the Internet of Things (IoT)? With Examples*. [online] Coursera. Available at: https://www.coursera.org/articles/internet-of-things.

Bring IT On NI. (2022). *What are the 4 components of Internet of Things (IoT)?* [online] Available at: https://bringitonni.co.uk/technology/what-are-the-4-components-of-internet-of-things-iot-bring-it-on/.

PROLIM. (N.D). *IoT Solutions | Industrial IoT*. [online] Available at: https://www.prolim.com/iot/iot-solutions/.

NCU (N.D). *Cyber-Physical Lab - Newcastle University*. [online] Available at: https://research.ncl.ac.uk/cplab/aboutthelab/whatarecyber-physicalsystems/.

Tyagi, A.K. & Sreenath, N. (2021). Cyber physical systems: Analyses, challenges and possible solutions. *Internet of Things and Cyber-Physical Systems*. doi:https://doi.org/10.1016/j.iotcps.2021.12.002.

Jahromi, A.A. & Kundur, D. (2020). Fundamentals of Cyber-Physical Systems. *Cyber-Physical Systems in the Built Environment*, [online] pp.1–13. doi:https://doi.org/10.1007/978-3-030-41560-0_1.

Jang-Jaccard, J. & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, [online] 80(5), pp.973–993. doi:https://doi.org/10.1016/j.jcss.2014.02.005.

Tariq, N., Asim, M., Al-Obeidat, F., Zubair Farooqi, M., Baker, T., Hammoudeh, M. & Ghafir, I. (2019). The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey. *Sensors*, 19(8), p.1788. doi:https://doi.org/10.3390/s19081788.

PWC (N.D.). *What happens when you harness digital convergence*. [online] PwC. Available at: https://www.pwc.com/us/en/tech-effect/emerging-tech/convergent-technologies.html.

Lawton, G. (2023). *What is Generative AI? Everything You Need to Know*. [online] Enterprise AI. Available at: https://www.techtarget.com/searchenterpriseai/definition/generative-AI.

AWS (N.D.). *What is Quantum Computing? Quantum Computing Explained - AWS*. [online] Available at: https://aws.amazon.com/what-is/quantum-computing/.

Martin, J. (2023). *Quantum Computing? What is that?* [online] Available at: https://www.linkedin.com/pulse/quantum-computing-what-jonathan-martin/.

Simplilearn (2023). *What Is Metaverse Technology?: An In-Depth Guide To Its Potential* | *Simplilearn*. [online] Available at: https://www.simplilearn.com/what-is-metaverse-technology-article.

IBM (2023). *What Is Blockchain Technology*. [online] www.ibm.com. Available at: https://www.ibm.com/topics/blockchain.

IBM (2022). *Benefits of blockchain*. [online] www.ibm.com. Available at: https://www.ibm.com/topics/benefits-of-blockchain.