Statement and Confirmation of Own Work

A signed copy of this form must be submitted with every assignment.
If the statement is missing your work may not be marked.

Student Declaration

I confirm the following details:

Student Name:	Johnson Kenisha Corera
Student ID Number:	c23020001@cicra.edu.lk
Qualification:	Bachelor in Cyber Security
Unit:	SIT325 Advanced Network Security
Centre:	CICRA Campus
Word Count:	983

I have read and understood both *Deakin Academic Misconduct Policy* and the *Referencing and Bibliographies* document. To the best of my knowledge my work has been accurately referenced and all sources cited correctly.

I confirm that I have not exceeded the stipulated word limit by more than 10%.

I confirm that this is my own work and that I have not colluded or plagiarized any part of it.

Candidate Signature:	J.
Date:	23/01/2025

Task 7.1P

Table of Content

Table of Acronyms

Acronyms	Meaning
IoT	Internet of Things
WSNs	Wireless Sensor Network
GPS	Global Positioning System
DoS	Denial of Service
CPS	Cyber-Physical system
eMBB	Enhanced Mobile Broadband
mMTC	Massive Machine-Type Communication
uRLLC	ultra-Reliable Low Latency Communication
CoAP	Constrained application protocol
MQTT	Message Queuing Telemetry Transport

Q1. What is IoT and how it is different from wireless sensor networks?

- Real-world objectsacobtain functionality when sensors, software, and connectivity unite with them to produce and transmit data for the Internet of Things (IoT). Everything that surrounds us now works smarter thanks to IoT. Both cars and technical equipment at factories as well as household appliances can connect to the worldwide web. WSNs are wireless sensor networks built to track environmental conditions by measuring multiple sensor inputs. Unlike WSN technology IoT connects to different platforms and uses automation in addition to sensor data and network connections. (Society, 2015)

Q2. Consider any 5 domains and discuss IoT use cases or applications in those domains.

- Applications of IoT are found in several fields: Everything in various sectors and fields can be utilized IoT for numerous applications.

  - ✓ **Agriculture**: Computerized watering system is one element of the modern watering system where water is delivered and applied through sophisticated management of the soil moisture status.

  - ✓ **Manufacturing**: These IoT sensors are employed by Predictive maintenance systems in order to monitor the condition of the machinery and therefore reduce the time the machinery is out of order.

  - ✓ **Healthcare**: Remote patient monitoring assists the practitioner to be sure that patients have their vital signs taken and that they are compliant with their medications.

  - ✓ **Transportation**: The majority of fleets use GPS which stands for global positioning systems to locate their vehicles, plot their routes and address fuel needs.

  - ✓ **Home Automation**: Some of the following are some of the smart home appliances and systems include: A smart thermostat for example is a gadget that regulates the climate in homes according to the users.

- These applications prove how Internet of Things makes automation and higher efficiency available in today's industries. (Rajkumar, 2001)

Q3. Illustrate three layered IoT architecture and identify at least 3 vulnerabilities in each layer.

- **Perception Layer**: Further, it has been tasked with the responsibility of using sensors to collect data.
  - ✓ **Vulnerabilities**: Assuming dominance, destruction, contribution, and deleting, modifying, and inserting data.

- **Network Layer**: Data sharing becomes feasible through its presence.
  - ✓ **Vulnerabilities:** Our network faces Denial of Service disruptions at the same time we need to guard against routing vulnerabilities and man in the middle threats.

- **Application Layer**: User applications send data to the server which performs basic preparation work before and after processing.
  - ✓ **Vulnerabilities:** The major privacy threats include unauthorized control of user data and its breaches alongside personal privacy violations. (Ericsson, 1876)

Q4. What is Cyber physical system?

- CPS systems serve as engineered systems that combine physical equipment with cyber controls to watch and manage objects between domains in real-time. CPS systems appear throughout smart grid facilities and business transportation while helping industrial environments when sensor output connects to processing systems for live operations. Real-time CPS systems work best when physics and computing elements team up to produce dependable systems that handle changes well. Industrial technology relies on CPSs today because these systems produce professional control and management solutions that benefit multiple industries. (Shelby, 2014)

Q5. Explain privacy concepts in IoT networks.

- In the Internet of Things era privacy means safely protecting your personal information during internet transmissions and making sure your data stays safe at all times. Our security methods include data minimization to stay away from data records, user approval before getting data, identity removal, and encrypted network security to protect user data privacy. The significant amount of personal information generated by IoT devices requires security measures to protect it which motivates us to build a secure Internet of Things framework. (ZigBee, 2004)

Q6. What is the impact of the launch of 5G technology on network architectures from security requirements context?

- The change 5G technology brings to network architecture creates new security challenges and benefits security solutions need to address. 5G technology offers fast delivery and low response times which connects more devices than before. The multiple virtual networks made possible by 5G network slicing expand the number of potential entry points into the system which must be tightly secured through robust access restrictions. Since 5G network systems run across many locations the technology must include advanced security tools such as intrusion protection systems and encryption to protect it against sophisticated cyber threats. For a 5G network to operate effectively security needs to become its core priority. (Gubbi, 2012)

Q7. 5G networks are expected to serve vertical markets with many distinct types of service, each with differing service requirement characteristics. Please broadly describe them (example Xmbb, Mmtc, and uMTC).

- eMBB stands as the main network focus to deliver exceptional data speed for VR virtual reality and 4K streaming.

- The term mMTC represents machine communication use on a large scale. A few of the applications include Smart cities: Baby symbols in industrial automation operate very efficiently with limited data flow.

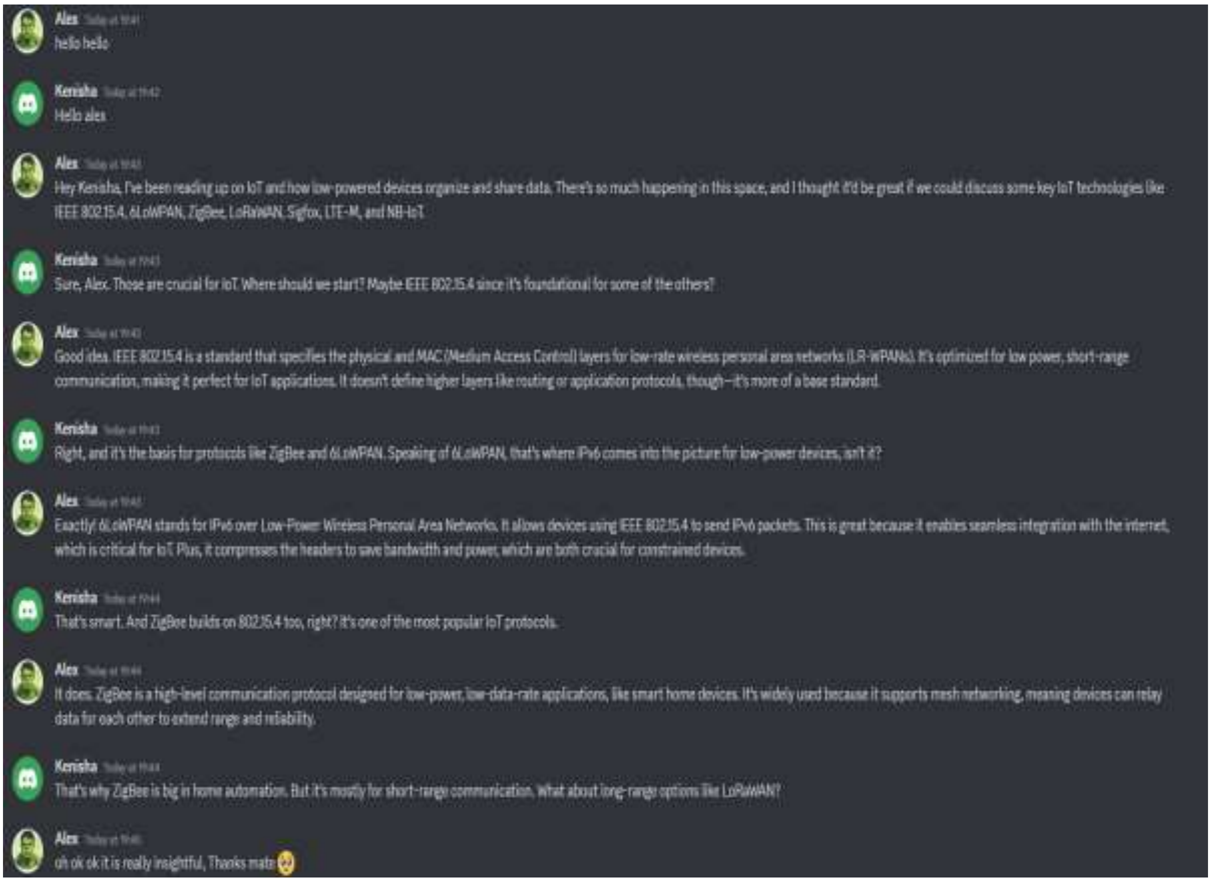
- The uRLLC system offers reliable low-latency performance which ensures seamless connections required for remote surgery and autonomous vehicle control. Due to its unique design capabilities a 5G network supports many types of applications that need this service. (Jing, 2014)

Q8. Explain CoAP and MQTT protocols.

- For basic operations on Internet of Things devices and environmental settings CoAP (Constrained Application Protocol) offers a light-weight but flexible alternative to standard networking protocols. Although designed to help devices with basic energy and processing limits COAP functions as a basic HTTP-style request-response system. Workers developed the MQTT messaging wire protocol for publish-subscribe usage in data systems that operate on networks with high delays and tight bandwidth. In contrast to direct broadcasting essential for industrial and medical applications to operate when power is available it offers a periodic signal system that matches specific needs. (Suo, 2014)

Q9. One of the fundamental aspects of the IoT is the manner low-powered devices self organise and share information (route and data information) among themselves. Even though these sensors are energy constrained, they need to store and process data, dynamically connect to the network, and possibly interoperate with other devices. Some of the devices may act as internal or border routers. Some proximity network protocols may connect devices directly to the access gateway, while some may connect via other devices. In this context discuss the following with your staff.

- **What is IEEE 802.15.4?**
- **6LoWPAN**
- **ZigBee**
- **LoRaWAN**
- **Sigfox**
- **LTE-M and NB-IoT**



Alex Today at 19:41
hello hello

Kenisha Today at 19:42
Hello alex

Alex Today at 19:43
Hey Kenisha, I've been reading up on IoT and how low-powered devices organize and share data. There's so much happening in this space, and I thought it'd be great if we could discuss some key IoT technologies like IEEE 802.15.4, 6LoWPAN, ZigBee, LoRaWAN, Sigfox, LTE-M, and NB-IoT.

Kenisha Today at 19:43
Sure, Alex. Those are crucial for IoT. Where should we start? Maybe IEEE 802.15.4 since it's foundational for some of the others?

Alex Today at 19:43
Good idea. IEEE 802.15.4 is a standard that specifies the physical and MAC (Medium Access Control) layers for low-rate wireless personal area networks (LR-WPANs). It's optimized for low power, short-range communication, making it perfect for IoT applications. It doesn't define higher layers like routing or application protocols, though—it's more of a base standard.

Kenisha Today at 19:43
Right, and it's the basis for protocols like ZigBee and 6LoWPAN. Speaking of 6LoWPAN, that's where IPv6 comes into the picture for low-power devices, isn't it?

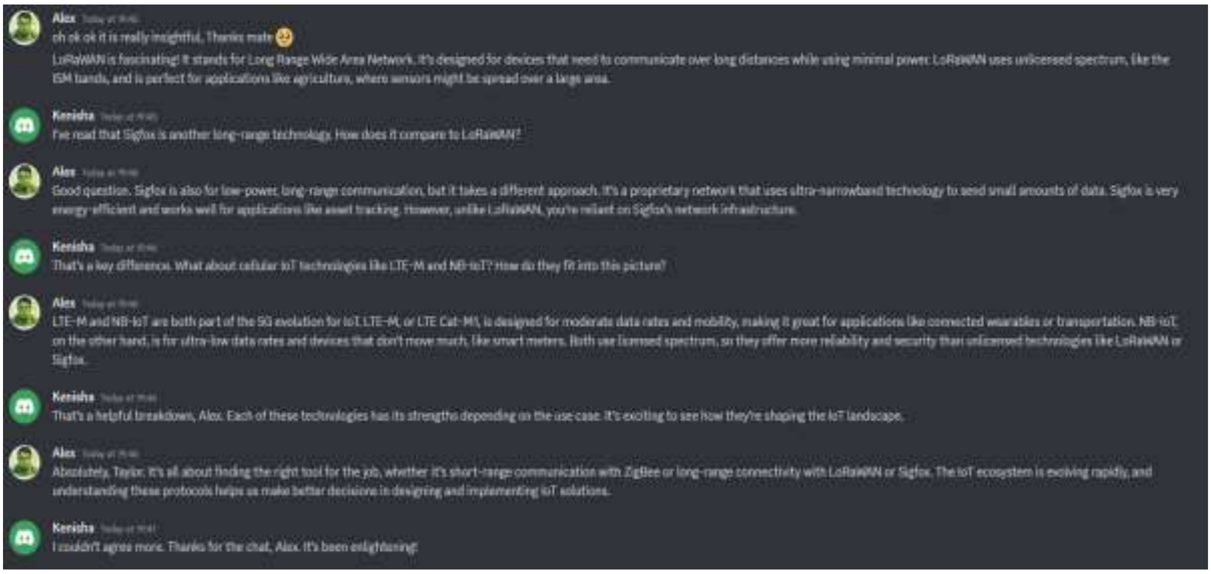
Alex Today at 19:43
Exactly! 6LoWPAN stands for IPv6 over Low-Power Wireless Personal Area Networks. It allows devices using IEEE 802.15.4 to send IPv6 packets. This is great because it enables seamless integration with the internet, which is critical for IoT. Plus, it compresses the headers to save bandwidth and power, which are both crucial for constrained devices.

Kenisha Today at 19:44
That's smart. And ZigBee builds on 802.15.4 too, right? It's one of the most popular IoT protocols.

Alex Today at 19:44
It does. ZigBee is a high-level communication protocol designed for low-power, low-data-rate applications, like smart home devices. It's widely used because it supports mesh networking, meaning devices can relay data for each other to extend range and reliability.

Kenisha Today at 19:44
That's why ZigBee is big in home automation. But it's mostly for short-range communication. What about long-range options like LoRaWAN?

Alex Today at 19:46
oh ok ok it is really insightful, Thanks mate 🥺



Alex Today at [illegible]

oh ok ok it is really insightful, Thanks mate 😊

LoRaWAN is fascinating! It stands for Long Range Wide Area Network. It's designed for devices that need to communicate over long distances while using minimal power. LoRaWAN uses unlicensed spectrum, like the ISM bands, and is perfect for applications like agriculture, where sensors might be spread over a large area.

Kenisha Today at [illegible]

I've read that Sigfox is another long-range technology. How does it compare to LoRaWAN?

Alex Today at [illegible]

Good question. Sigfox is also for low-power, long-range communication, but it takes a different approach. It's a proprietary network that uses ultra-narrowband technology to send small amounts of data. Sigfox is very energy-efficient and works well for applications like asset tracking. However, unlike LoRaWAN, you're reliant on Sigfox's network infrastructure.

Kenisha Today at [illegible]

That's a key difference. What about cellular IoT technologies like LTE-M and NB-IoT? How do they fit into this picture?

Alex Today at [illegible]

LTE-M and NB-IoT are both part of the 5G evolution for IoT. LTE-M, or LTE Cat-M1, is designed for moderate data rates and mobility, making it great for applications like connected wearables or transportation. NB-IoT, on the other hand, is for ultra-low data rates and devices that don't move much, like smart meters. Both use licensed spectrum, so they offer more reliability and security than unlicensed technologies like LoRaWAN or Sigfox.

Kenisha Today at [illegible]

That's a helpful breakdown, Alex. Each of these technologies has its strengths depending on the use case. It's exciting to see how they're shaping the IoT landscape.

Alex Today at [illegible]

Absolutely, Taylor. It's all about finding the right tool for the job, whether it's short-range communication with ZigBee or long-range connectivity with LoRaWAN or Sigfox. The IoT ecosystem is evolving rapidly, and understanding these protocols helps us make better decisions in designing and implementing IoT solutions.

Kenisha Today at [illegible]

I couldn't agree more. Thanks for the chat, Alex. It's been enlightening!

Q10. What do you mean by IoT node authentication?

- Correct node access to the Internet of Things network through authentication defines IoT node authentication. Strong security results from preventing devices that lack authorization from accessing the network because they cannot perform digital transactions with approved devices. Based on network standards and device features our authentication methods can use digital certificates pre-shared keys or biometric verification. Strong IoT node identification and authentication systems become fundamental in protecting against security risks when nodes operate in hard-to-reach and unpredictable locations with limited power supplies.

Reference

- Internet Society (2023) The Internet of Things (IoT) https://www.internetsociety.org/resources/doc/2015/iot-overview/

- Cyber-physical systems: The next computing revolution https://ieeexplore.ieee.org/document/5523280.

- A new reality for network deployment (2020) https://www.ericsson.com/en/network-services/deployment?gad_source=1&gclid=Cj0KCQjwz7C2BhDkARIsAA_SZKb9cP8-4l8mzYXvyP9MmYSusqy5hE84bZUt9z0CWV1nzH_dRzHtS1IaAk1_EALw_wcB&gclsrc=aw.ds

- The Constrained Application Protocol (COAP) https://datatracker.ietf.org/doc/html/rfc7252

- Getting Started with ZigBee and IEEE 802.15.4 (2010) https://www.science.smith.edu/~jcardell/Courses/EGR328/Readings/Zigbee%20GettingStarted.pdf

- Security in the Internet of Things: A review (2012) https://ieeexplore.ieee.org/document/6188257

- Gubbi, J. et al. (2012) Internet of Things (IoT) https://arxiv.org/abs/1207.0203

- Security of the Internet of Things: perspectives and challenges Security of the Internet of Things: perspectives and challenges | Wireless Networks