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

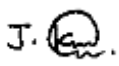
I confirm the following details:

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:	920

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:	
Date:	20/01/2025

Task 8.1P
Table of Content

Table of Content

Acronyms	Meaning
IoT	Internet of Things
DC	Drought Code
DMC	Duff Moisture Code
ISI	Initial spread index
XML	Extensible Markup Language
FFMC	Fine Fuel Moisture Code

Q1. Explain IoT's applications in precision farming sector.

- The use of IoT is crucial to achieving precision farming, because owing to advancements in technology, crop health and status of the soil as well as other environmental factors can be monitored on real time basis. The major technologies used in IoT technology include sensors and drones to capture data on moisture, heat, humidity, and fertilizers for irrigation, nutritive and sickness management. Thus, sustainability is enhanced, there is a reduction in impacts to resources, and in particular, an increase in food production. In addition, precision farming incorporates complex automation to all the operational activities on the field such harvesting, planting, and other tasks through mechanized planters and harvesters, GPS controlled among other things. Hence, the application of Iot in agriculture has enabled them to increase on the amount of produce while at the same time cutting down on costs by using real time data to make these choices.

Q2. What are the three main scenarios, discussed by the authors in [1], in which the IoT sensors may generate faulty and compromised malicious sensor streams?

- There are three primary ways that IoT sensors can break down or be compromised: One must understand that incorrect data can stem from the following: Brief malfunctioning of the various constituent parts of the sensor that is made of hardware; wrong data which can be as a result of software hitches that reduce the quality of data pulled from the data sensor; and lastly, emanates from malicious attacks that can alter the functionality of the sensor and thus provide incorrect data. Such scenarios complicate the assessment of a wise decision concerning the security and reliability of IoT devices. On the one hand, they might be designed to deceive automation systems or even compromise them, which leads to wasting the resources. (Sood, 2017)

Q3. Explain in your own words the research problem tackled by the authors of [1].

- In their work, Sood et al. address the research issue of accurately recognizing and differentiating between the normal, hacked, and faulty sensor behavior of IoT devices. This is required to ensure that the IoT systems do not break down or fail in relation to the things they are measuring such as when sensors are placed in strategic/farf flated areas such as government facilities or corporate institutions. Thus, the authors employ a machine learning and spatial correlation analysis based approach to develop a fresh method for detecting anomalies in data from sensors. This makes it easier to detect errors and failings as well as security breaches in good time.

Q4. What is spatial-correlation approach used by the authors for anomaly detection in IoTs?

- This is evident from the authors' spatial-correlation method in which they endeavored to detect abnormalities through the type of spatial correlations that exist in the received sensor data. The method can also reveal gaps that can mean some sensors may be either bad or not working well because the distances between the sensors enable the algorithm to notice how the different sensor data may be connected. This technique exploits the fact that proximate sensors should change in a similar manner under normal operating conditions. In simplest terms, when the level of interaction is off the predicted correlation, an alert is flagged, which is helpful in defining problems and possible invasions into IoT networks ahead of time. (HaddadPajouh, 2021)

Q5. What is Moran's I index and how it is related to spatial-correlation approach?

- The Moran's I index shows the extent of spatial autocorality while the arrangement of spatial data is done based on how related it is. E-statistic Moran's I indicates how sensor measurements reflecting of spatial structure is used to detect unusual patterns in context of Internet of Things. In other words, when the recorded sensor value is closer to or equal to the one then it implies that the relation of the corresponding sensor is high the neighboring sensors. On the other hand a low number is indicative of anomalies or values out of the norm which mean that perhaps some of the sensors are faulty or damaged. This index is very useful for searching for anomalies in IoT data applying the spatial-correlation method.

Q6. Give details about Forest Fire data set.

- This paper focuses on the Forest Fire data set available in the UCI machine learning data base which has information about forest fire including those which occurred in northeast Portugal. The weather, FFMC (Fine Fuel Moisture Code), DMC (Duff Moisture Code), DC (Drought Code), and ISI (Initial Spread Index) are some of the characteristics and 13 such characteristics have 517 instances which determine the amount of fire flames. Therefore, the value of the dataset is seen in its application toward assessing what fire does to the environment or in improving means to deal with fire. Regression assignments are often attempted to solve this problem by predicting the area going to be burnt by a forest fire. (GmbH, 2020)

Q7. Identify at least 3 limitations of the work given in [1].

- Some of the ways that Sood et al.'s work is limited are as follows: The approach can be disadvantageous in the sense that it is less efficient in identifying changes especially in a situation where the rates of change of its corresponding sensors are very high. A minimum level of sensors is required for the inherent use of space correlation and sometimes it is not possible in Internet of Things. This is the case as the model may be comprised by a growing number of compromised or adversarial sensors as the measure of potential threat is directly related to the proportion of true sensors in the system.

Q8. What are the different forms of data used in data analytics and based on your data analytics understanding list 2 critical challenges in the received data for analytics?

- Most types of data in use are employed in data analytics; these include: Semi-structured data (like XML files), unstructured Data (like texts and photos), and Organized data (like data bases). Data heterogeneity affects IoT data integration and analysis because data sources and their formats are diverse, and poor quality data cause low forecasting and conformance. These form hard tasks which in reality must undergo basic transformations and data cleaning techniques so as to make them more insightful and truly analytical. (Cortez, 2008)

Reference

- Accurate detection of IoT sensor behaviors in legitimate https://ieeexplore.ieee.org/document/9632348.

- A survey on internet of things security: Requirements, challenges, and solutions https://doi.org/10.1016/j.iot.2019.100129.

- IoT Analytics Definition https://www.softwareag.com/en_corporate/resources/iot/article/iot-analytics.html

- UCI Machine Learning Repository. https://archive.ics.uci.edu/dataset/162/forest+fires.