2024

# DNCT702 Internet of Things

# Assessment 1

1 – REPORT AND PRESENTATION

MURACHI, TAKASHI

ID# 850000605 | DANCT7124C-E/OL

Diploma in Applied Network and Cloud Technology (Level 7)

**Cover Sheet and Student Declaration**

This sheet must be signed by the student and attached to the submitted assessment.

| | | | |
|---|---|---|---|
| **Course Title:** | **DNCT702 – Internet of Things** | **Course code:** | **DNCT702** |
| **Student Name:** | **Takashi Murachi** | **Student ID:** | 850000605 |
| **Assessment No & Type:** | Theory/Practical | **Cohort:** | DANCT7124C-E/OL |
| **Due Date:** | 8/11/2024 | **Date Submitted:** | 8/11/2024 |
| **Tutor's Name:** | Vaibhav Fanibhare | | |
| **Assessment Weighting** | 40% | | |
| **Total Marks** | 100 | | |

**Student Declaration:**

I declare that:

I have read the New Zealand School of Education Ltd policies and regulations on assessments and understand what plagiarism is.

I am aware of the penalties for cheating and plagiarism as laid down by the New Zealand School of Education Ltd.

This is an original assessment and is entirely my own work.

Where I have quoted or made use of the ideas of other writers, I have acknowledged the source.

This assessment has been prepared exclusively for this course and has not been or will not be submitted as assessed work in any other course.

It has been explained to me that this assessment may be used by NZSE Ltd, for internal and/or external moderation.

If I am late in handing in this assessment without prior approval (see student regulations in handbook), marks will be deducted, to a maximum of 50%.

**Student signature:**

**Date: 08/11/2024**

| | | |
|---|---|---|
| **Tutor only to complete** | | |
| **Assessment result:** | **Mark /100** | **Grade** |

## Table of Contents

# “Smart World’s IoT System Analysis

# and Recommendations for SDN Integration”

## Introduction

This report examines current offered IoT solution for smart homes and offices in New Zealand. The analysis focuses on the value chain structure, communication models, and protocols, as well as scalability considerations for their initial 50,000 users. The report suggests improving system performance, security, and cost-effectiveness to meet the initial target of 50,000 users. The goal is to create adaptable solutions for smart devices, such as internal home sensors and actuators that can alert and monitor the billing system in real time. The proposed architecture also improves network security in cloud connectivity for edge and core servers. The report also emphasizes the importance of usability in mobile and web applications. The new network's integration with software-defined networking (SDN) allows for more flexible solutions for smart devices. Personal related private information data will be encrypted for safety in scenarios that occur less than 30 kilometres away in Christchurch, New Zealand. The report also informs residents about the cloud platform's automation, high availability, and scalability, which ensure a long-term business strategy.

## Main body

### 1. Value Chain Structure Analysis and Recommendations

### 1.1 Current Value Chain Structure

The aim of this critical analysis is to evaluate the IoT value chain which consists of various stages and components, illustrating how different entities interact to deliver IoT products and services in smart home and office service to target initial 50,000 users.

Following components were identified and also depicted in the IoT value chain layout.
1.Hardware device layer: Ideally compatible sensors, actuator, and smart devices.
2.Connectivity network layer: ensure the secure data transmission by TCP/IP between nodes.
3.Data Processing layer: Data collection, processing, filtering, sorting, mining, and visualisation.
4.Application layer: Provide the user-interface by API between device and application or end users.

1. **Hardware device layer**
   **Current structure issue:**
   Current 2G IoT sensors and devises in home has limited amount of data transmission and low speed. Therefore, this 2G technology is not cost effective. For example, smart lights, thermostats, central heating systems, meters, fridges, and doors are some examples of smart devices that can control indoor temperatures, make reports on energy consumption usages, send alerts when food is purchased, and warn users if someone breaks in without permission.

   **Recommendation:**

Edge computing can increase the transmitted data and reducing the security risk. Such smart home sensors inside home can be controlled by threshold of their setting through actuators relate to home appliances with higher secure protocol. However, the compatibility of each home appliance and security setting levels are different.

**Justification:**

Reducing the unmeaning variable of topics of each sensor parameter can reduce the number of traffic flows and improves the RTT time, therefore the performance of traffic flow will be increased and wastages of unmeaning topic as variables are minimised to save the cost. The actuator operates under a set of thresholds. If the data exceeds the threshold, proceed to the next stage; if not, return to the sensors.

2. **Connectivity Network layer**

**Current structure:** GSM(2G) technology has limited capability to transfer the data to cloud and At least 4G and 5G high bandwidths Wi-Fi are required but current 2G bandwidths Wi-Fi are not enough capability to transmit for the large number of at least 50,000 users. Due to short battery life span, LPWAN can lead to lower cost of power consumption by sleeping only specific time such as everyone hours as activate over on and off time in total

**Recommendations:**

Each device sends its IP addresses through a multi-layered switch (MLS) gateway using 5G Wi-Fi at home to another network node. Each message travels from the multiple-cell tower to the cloud.

**Justifications:** Rather than setting up multiple switches, a multilayer switch gateway can manage various VLANs using routing and security protocols. It can also integrate with virtual switches, tailoring them for future scalable network extensions. This approach reduces repair and overhead costs while also enhancing the performance of larger networking systems. The Virtual Network Function (VNF), a type 1 hypervisor in Azure, controls the multi-layered switch (MLS). This lets physical MLS and virtual multi-layer switches work together to add more devices.

3. **Data processing layer**

**Current structure**:

There are only one central cloud processing unit which could be slower the performance of traffic flows, resulting in congested in one cloud computing because initial 50,000 users are expecting to start the project. Real time processing is expected with data visualisation under secured and private management systems are expected.

**Recommendation**:

Parallel distributed processing architecture by the used of load balancer can distribute the equal amount of traffic flows in both physical and virtual machines if it is required scalable networking. AI can predict the ratio or classify the objects class from large number of historical collected data. This data processing layer in analysing data to provide insights and actionable intelligence to accumulate and manage all data streams, using tools like data analytics platforms like Power BI, machine learning algorithms, and artificial intelligence systems to identify patterns, trends, and anomalies for informed decision-making for customer applications. This process entails combining data from multiple sources, reconciling formats, and aggregating data in one place or accessible through data virtualization. The application layer reformats the data collected for physical-level transmission. The data accumulation and abstraction stages improve the interoperability of smart devices, allowing software developers to focus on specific business tasks by redundant multivariable to predict the target probability of regression if the p-value is to be set as more than either 0.05 or 0.03, and classification by separating from multiple categorical data rather than delving into device specifications from different vendors.

**Justification**:
Improved performance and reduced latency using artificial intelligence can contribute to reduce the human error and repeated works which will take time and costs. Business intelligence (BI) comprises tools and methodologies employed to analyse business data for informed decision-making. It entails extracting raw data from its source, transforming it, loading it into a consolidated storage system, and presenting it to the user. The foundational infrastructure, referred to as a data pipeline, encompasses the Extract, Transform, Load (ETL) process and its associated tools. A BI system's frontend serves as the user interface, displaying data visually. This data visualization software tools, and techniques are well contributed to decision making within the context of business intelligence (*Data Visualization in Business Intelligence*, 2022).

4. **Software Application layer**
**Current structure**:
Only one user of mobile application is the current diagram. User interface for having the usage power consumption by monitoring the statues and optimise by automated configuration are limited because of processing capability and storage when it comes to showing the dashboard with alerts system under secure authorised users only, however authentication and of user encryption has also not implemented yet.

**Recommendation**:
Microservices have many advantages, such as being flexible, having small, focused teams, a small code base, a mix of platforms, failure isolation, the ability to grow, and data separation. Independent rollout enables the addition of bug fixes and new features without the need to redeploy the entire application. They also cut down on connections so that service teams can pick the technology that works best for them (RobBagby, n.d.).

**Justification**:
The microservices architecture provides flexibility, agility, and accelerated development cycles. It facilitates scalability, provides fault isolation, boosts team efficiency, and enables expedited deployment time. The compartmentalized architecture enables specialized teams to concentrate on certain services, minimizing the risk of coordinating modifications across the entire application(Atlassian, n.d.).The application layer of the Internet of Things includes software applications that use data to provide value to end users, such as mobile apps, web apps, and dashboards. These API-based applications provide user-friendly interfaces for data visualisation and reporting. IoT applications can analyse data to answer business questions using a variety of technology stacks and operating systems. Examples include device monitoring software, mobile apps, business intelligence services, and machine learning analytics solutions.

5. **User Interface Layer**
**Current structure:**
This user interface layer describes user interaction with IoT applications and devices, including mobile applications, web dashboards, and voice interfaces. It provides an intuitive experience for device control, analytics viewing, and notifications via API.
**Recommendation and Justification:**
For instance, setting the threshold to the maximum or minimum amount of network traffic or CPU usage sends an alert text or email message to a registered cell phone and email account. If the billing was not completed last month on time, it automatically turns back on to notify the billing amount and send an alert message for users.

6. **System Integration Layer**

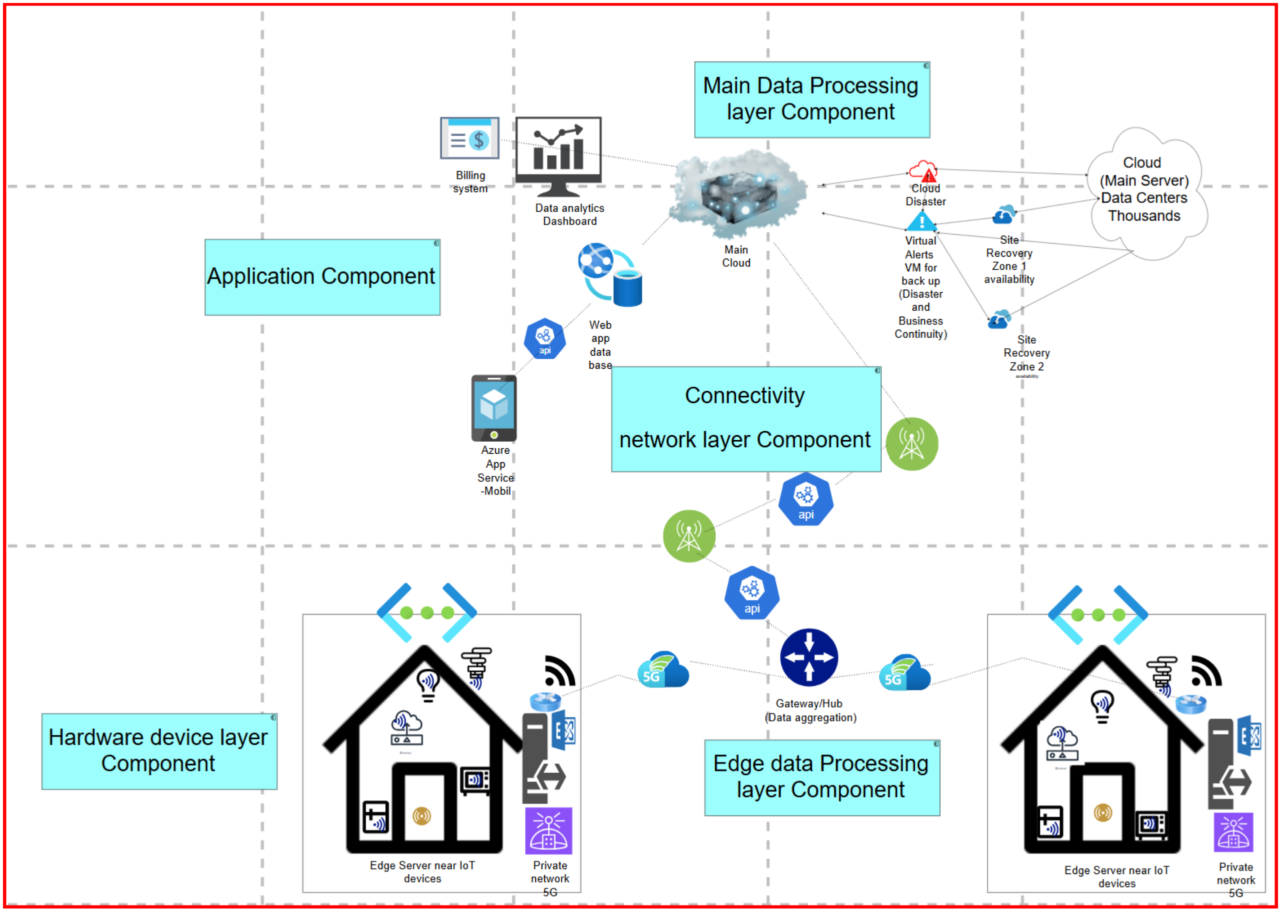
**Current Structure:**

This component of the ecosystem and relationships encompasses users within the IoT ecosystem, such as manufacturers, service providers, and developers, and involves the integration of essential network components with backend systems.

**Recommendation and Justification:**

The design specifically addresses compatibility, automation, and the industrial sector's use of the HART wireless protocol in IoT networks, aiming to optimise power consumption and enhance scalability. It operates at the Medium Access Control (MAC) and Network layers, each possessing unique security characteristics. The network layer uses cryptographic keys to guarantee data integrity and confidentiality, while the public key generates a message integrity code. The network key permits authentication among shared devices, whereas the join key allows individual devices to connect to the network(*Wireless Hart: DNCT702 - Internet of Things*, n.d.). The main purpose is to implement data-driven solutions for business challenges in near real time. When other networks are integrated with nodes, they can share the common information and reduce the initial investment to only one cloud user under a restriction share holder like Z folder.

Examples include IoT platform providers, telecom companies, cloud service providers, and third-party developers, collaborating to create a comprehensive IoT solution in Figure1.


Main Data Processing layer Component
Billing system
Data analytics Dashboard
Main Cloud
Cloud Disaster
Virtual Alerts VM for back up (Disaster and Business Continuity)
Site Recovery Zone 1 availability
Cloud (Main Server) Data Centers Thousands
Site Recovery Zone 2 availability
Application Component
Web app data base
api
Azure App Service -Mobil
Connectivity network layer Component
api
api
Gateway/Hub (Data aggregation)
5G
5G
Hardware device layer Component
Edge Server near IoT devices
Private network 5G
Edge data Processing layer Component
Edge Server near IoT devices
Private network 5G

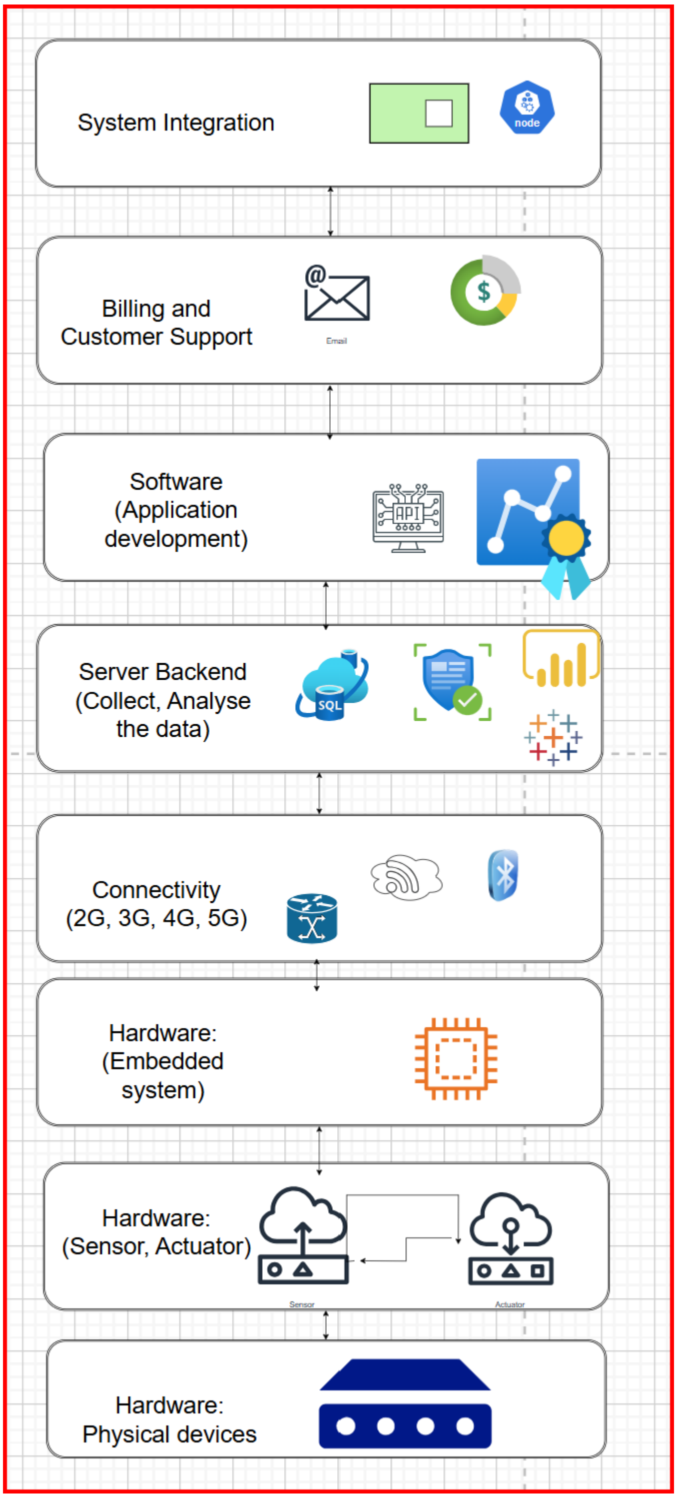

System Integration
node
Billing and Customer Support
Email
Software (Application development)
API
Server Backend (Collect, Analyse the data)
SQL
Connectivity (2G, 3G, 4G, 5G)
Hardware: (Embedded system)
Hardware: (Sensor, Actuator)
Sensor
Actuator
Hardware: Physical devices

*Figure 1: the proposed components of the IoT value chain structure*

## 2. Communication Models and Protocols Evaluation in relation to cloud connectivity

### 2.1 Three Communication Models

**Request & Response Model:**

In a client-server design, such as the Request & Response Model in figure 2, the client like mobile application users at home asks the central cloud server for information in an encoded manner that converts categorical string data to numerical digital data. This model's status indicates that it handles each request on its own and does not keep data between requests. The server sorts the request into the right category, gets data from the database, changes it into an answer, and sends it to the client. According to the request-answer communication model, the client sends a request to the server(Communication Models in IoT (Internet of Things ), 2021). Why this model is used as one of proposed model out of 3 models is that this model is very simple and easy to understand requests and answer between clients and server. The server is generalised between clients of app users and devises sensor at each home, so it is easy to maintain the secured data and consistent data. However, if the one server itself is broken down, entire system will not work. If the traffic flow is so congested and processing queue and stored in buffered storage, then reach to the limit then data loss and response tie will be delayed. As resolutions, high availability of servers as back up (alternative server) can mitigate the risk of centred one server to avoid the risk of crashing the entire server. Adding load balancer can increase the performance the traffic load by receiving the requests messages from devises to server enables to reduce the heavy traffic flows into the server.

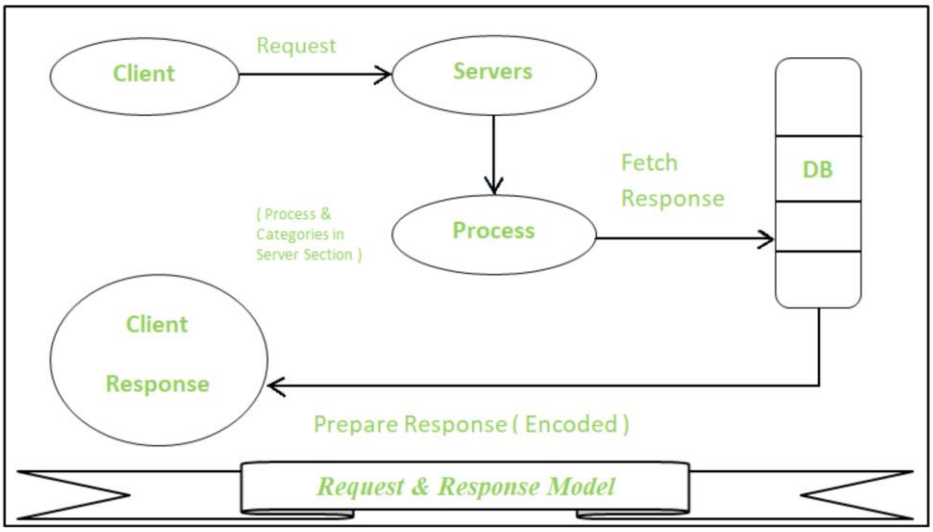


*Figure 2: Request & Response Model. Source:(*Communication Models in IoT (Internet of Things )*, 2021)*

**Publisher-Subscriber Model:**
The model comprises publishers, brokers, and consumers in figure 3. Publishers serve as the topic (unique name of parameter), payload(value), QoS and retain or not. The broker's duty is to receive data from publishers and transmit it to the relevant customers. The broker only has information about the customer associated with a certain issue, and the publisher remains uninformed(Communication Models in IoT (Internet of Things ), 2021).

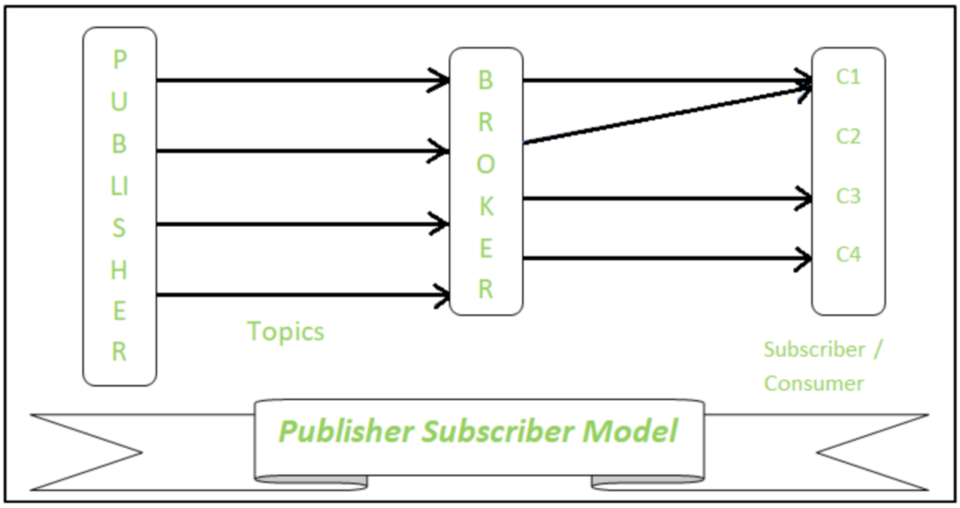


*Figure 3: Publisher-Subscriber Model. Source: (*Communication Models in IoT (Internet of Things )*, 2021)*

**The back-end data-sharing communication model:**
Device sensors, such as thermostats, smart fridges, and smart doors in this case, can aggregate all collected data from smart devices to each node and transfer to the central cloud. This improves data validation and error handling. RESTful API and GraphQL enable users to share data between devices and clients of web or mobile applications in a proper format and protocol in Figure-4. XML and JSON formats facilitate the creation of dictionary types, where topics serve as IDs and payloads as values, allowing users to easily extract and store data. By offering a customized small cloud, users can avoid conflicts with other users by standardizing their data with multiple values ranging from 0 to 1 or -1 to 1. Small clouds synchronize changes to the user's cloud server upon updating sensor data by setting a unique username or key value and a specific protocol port number. Setting up their own cloud allows them to avoid queuing and processing delays, achieving enough bandwidth and low latency.

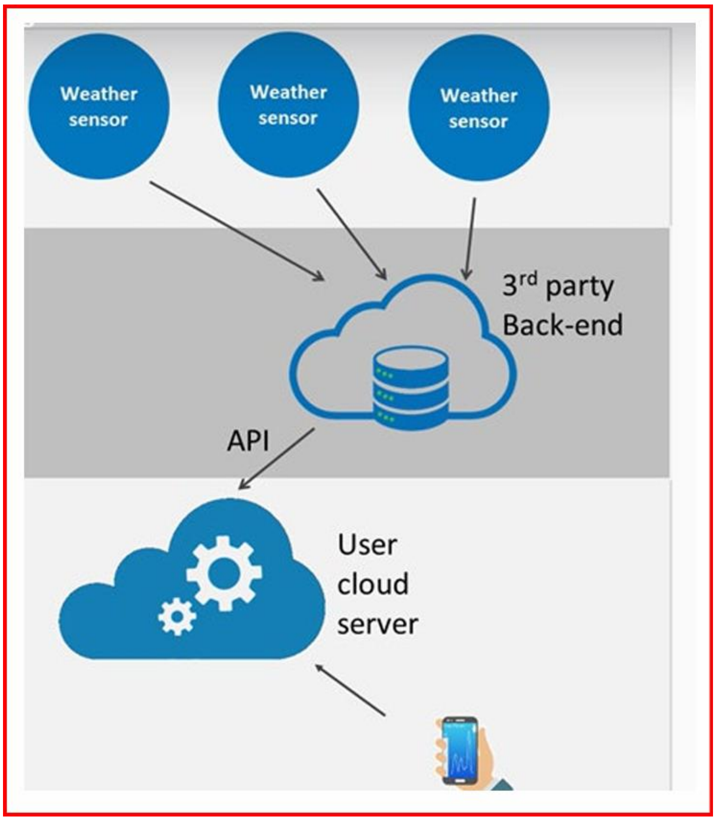


*Figure 4: Back-End Data Sharing model. Source: (5. IoT Communication Models.Pdf: DNCT702 - Internet of Things, n.d.)*

## 2.2 Four Communication Protocols

**Message Queue Telemetry Transport (MQTT)**
MQTT architecture in figure 5 is a lightweight protocol that enables communication between nodes in both reliable and unreliable networks. It follows a publish/subscribe architecture, with brokers making available information and clients accessing it after subscribing. An example of an MQTT architecture is in a smart factory with temperature sensors. The sensors connect to the MQTT broker, publishing data within sensor topics. MQTT clients then subscribe to the same topic to read the data. This architecture is suitable for low-bandwidth networks and unreliable networks(*IoT Communication Protocols—IoT Data Protocols - Technical Articles*, n.d.). MQTT is a service quality mechanism that classifies messages into three tiers depending on reliability: Level 0 (no assurance of message delivery), Level 1 (assured delivery, but potential duplicates), and Level 2 (certain delivery without duplicates).

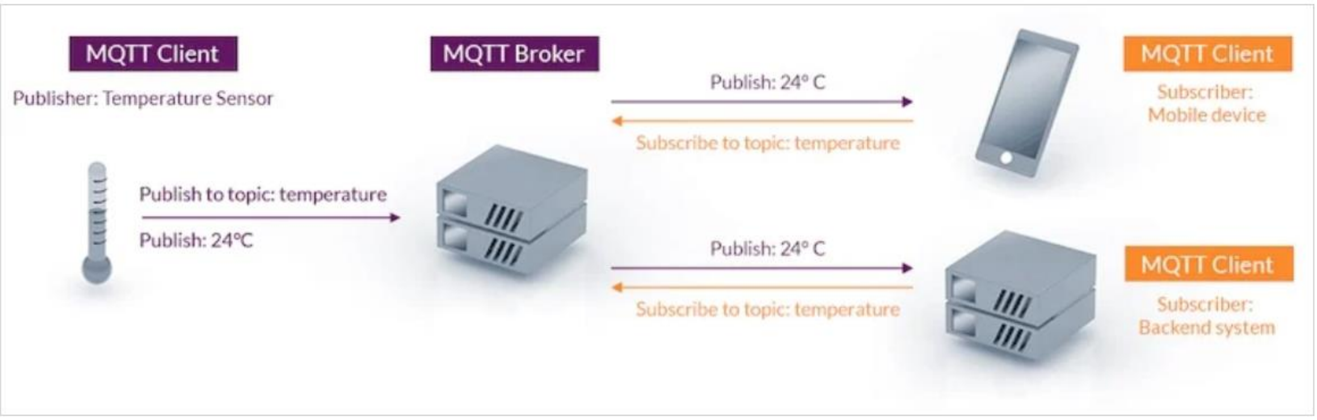

MQTT Client
Publisher: Temperature Sensor
Publish to topic: temperature
Publish: 24°C
MQTT Broker
Publish: 24° C
Subscribe to topic: temperature
Publish: 24° C
Subscribe to topic: temperature
MQTT Client
Subscriber: Mobile device
MQTT Client
Subscriber: Backend system

*Figure 5: MQTT's publish/subscribe architecture. Source: (*IoT Communication Protocols—IoT Data Protocols - Technical Articles*, n.d.).*

**Data Distribution Service (**DDS)
DDS in figure 6 uses MQTT, a publish-subscribe framework, to link all publishers (temperature sensors) and subscribers (mobile devices) to the same Global Data Space (GDS) network, thereby facilitating interconnection across nodes to prevent bottlenecks. The DDS GDS network facilitates rapid communication and data sharing across devices, minimising reliance on brokers(*IoT Communication Protocols—IoT Data Protocols - Technical Articles*, n.d.).

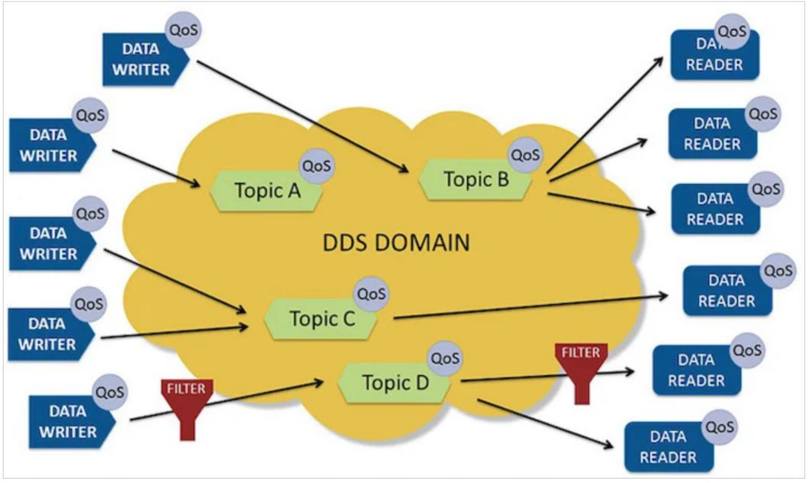


*Figure 6: A DDS Global Data Space. Image used courtesy of the DDS Foundation. Source: (*IoT Communication Protocols—IoT Data Protocols - Technical Articles*, n.d.)*

**WebSocket and HTTP**
Figure 11 illustrates how WebSocket technology establishes a TCP connection between a browser and a server, allowing for continuous information flow until the connection terminates. Despite its advancements over HTTP connections, the WebSocket remains cumbersome and resource-intensive for IoT applications (*IoT Communication Protocols—IoT Data Protocols - Technical Articles*, n.d.)**.**

For example, With Software as a Service (SaaS), users can run web apps directly in their web browsers from any internet-connected computer. This has fundamentally transformed the way web apps operate. Users no longer must download and install software, address dependencies and issues, and make sure they are up to date on changes and updates. On the other hand, web computers struggle to run apps because their design solely focuses on "talking" HTTP, a feature not always suitable for web apps. The request/response model underpins HTTP, but WebSocket's step in when a SaaS app utilizes a service that either doesn't "talk" HTTP or doesn't align with this model. This means that users can run many different apps right on their computer without having to download or install them first. Because it's not always right for web apps, the HTTP standard has some problems, even though web sockets are convenient(Rowena, 2022).

The World Wide Web Consortium (W3C) created Web Sockets in 2008 to combine the advantages of HTTP at the application layer with TCP's numerous features at the transport layer in figure 7. TCP establishes connections between addresses and maintains them open until applications have finished exchanging messages. This facilitates the transmission of HTTP requests and replies. Web apps can initiate a TCP-like link with an initial HTTP request, which they can later upgrade to a web socket. We can now use the current TCP/IP link as a WebSocket connection, enabling bidirectional data transfer without the need for HTTP's request and answer system. When both the client and the server agree to end it. The Scale way IoT Hub has built-in Web Sockets, making it easier for web apps to connect to the Hub. By default, a Hub establishes two networks: an MQTT network, which allows limited devices to send and receive messages with the Hub, and a WebSocket network, also referred to as an MQTT-over-Web socket network, enabling direct message transmission and reception in a browser. This lets web apps connect to the Hub without using middleware or APIs (Rowena, 2022).

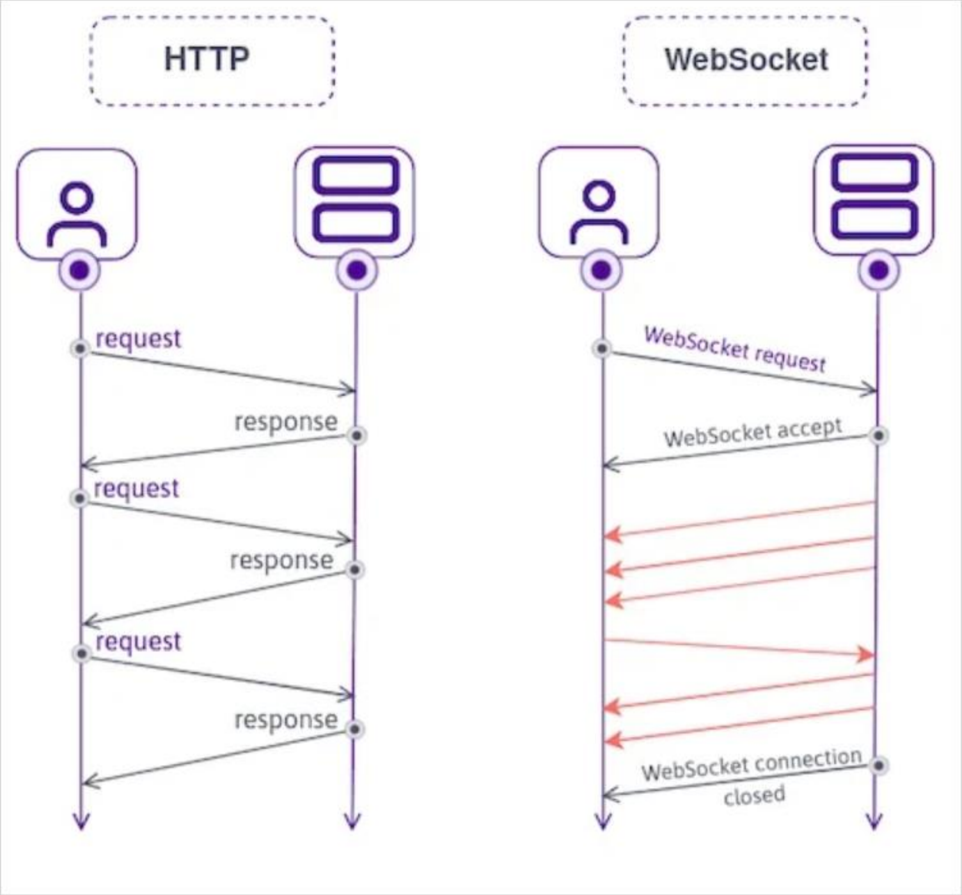


*Figure 7: Comparison between HTTP and WebSocket. Source:(*IoT Communication Protocols—IoT Data Protocols - Technical Articles*, n.d.)*

## 3. Recommended Communication Model and Protocol

Based on Smart World's requirements and the evaluation of various options, the following recommendations are made as justification:

**The back-end data-sharing communication model** improves the scalability of the number of publishers by connecting each sensor and actuator device to a central unit of a third-party cloud. In this scenario, we target the initial 50,000 users, but as each user increases the number of IP addresses, we shift from IPv4 to IPv6 addresses. For instance, ArcGIS Enterprise on Kubernetes, in conjunction with

Microsoft Azure, provides an excellent model for sharing large data sets, as well as for storing and mining large datasets. ArcGIS Online (*ArcGIS Enterprise Administrator API | ArcGIS REST APIs | ArcGIS Developers*, n.d.) provides a RESTful Application Program Interface (API) that serves as a useful tool for extracting the key topic, payload, and timestamp in a customized, small cloud. This allows for the display of real-time graphical maps and analytical results in time series. During the processing time, third-party apps can gain limited access to HTTPS, a secure protocol, instead of HTTP. HTTPS can convey heavy traffic bandwidth in near real time with secure protocols and a faster process than HTTP (To, 2020, pp. 34–35). Each user can use a small cloud to reduce heavy traffic instead of relying on a large central cloud. Users can download either CSV or Json format to analyse the result.

**WebSocket** is the best communication protocol, enabling two-way communications between several clients and servers for the real time data, in the dashboard that is expected to be used for 50,000 users initially. For example, in this given case, real time transaction within 1 seconds as well as high security measurements are key points. Regarding the security components, WebSocket can prevent from security issues like cross-site scripting (XSS) vulnerabilities and offers some methods for connecting protection.

With low latency protocols enabling high performance and real-time applications, the Internet of Things (IoT) is growingly popular for uses. This work compares Message Queue Telemetry Transport (MQTT) and WebSocket, which use Node.js servers for data sharing, with ESP8266. Experimental studies computed packet times differences between servers and ESP8266 using both protocols to assess latency. Based on the data and circumstances provided in the paper, the results showed that WebSocket is more suitable than MQTT for applications with a round-trip time (RTT) of at least 1 millisecond(Oliveira et al., 2018). Due to its lightweight nature, testing and development primarily use the MQTT protocol, which is not suitable for heavy traffic flows. Due to the expected heavy traffic from the initial 50,000 users and the need for low latency and high bandwidth, the MQTT protocol is not suitable for HTTP. While it may be suitable due to its lightweight nature, it consumes a significant amount of energy, is unsecured, and requires care for each end point, making scaling to 50,000 users initially challenging initially.

DDS (Data Distribution Service) has several disadvantages, such as complex setup and maintenance, significant resource usage, compatibility challenges, a steep learning curve, communication overhead, and debugging difficulties. The multifunctionality and adaptability of DDS may pose challenges for novices, and the extensive array of QoS policy options may complicate the user experience. Interoperability challenges may occur owing to varying suppliers, and troubleshooting might be difficult because of network latency or packet loss. Consequently, meticulous selection is essential for certain applications and system specifications(*Advantages of DDS Protocol | Disadvantages of DDS Protocol*, n.d.).

## 4. Improve the scalability of the system

The existing suggested IoT solutions provide challenges regarding the expansion of IoT devices in many aspects.

Performance testing is the evaluation of a network's data transmission speed and efficiency. It involves evaluating connections, timing, and transmitting specific data. The time measurement test assesses latency, while the transmit test entails transmitting data from a computer or smartphone across the network. The load test assesses the network's capability by transmitting a substantial volume of data simultaneously.

We can rectify issues if the network is sluggish or defective. To transmit more data simultaneously, it may be necessary to examine network configurations, modify the data flow, or include additional devices. These modifications will enhance the overall functionality of the network. Performance testing is a crucial tool for assessing the speed and efficiency of a network, as well as for identifying any issues or delays.

The proposed IoT architecture includes a singular IoT hub functioning as a broker, which may result in considerable traffic congestion among newly added nodes and those at the central cloud computing unit due to the addition of new IP addresses for each device. This could adversely impact network performance, leading to slower speeds, diminished user satisfaction, loss of customers, and a decline in trust and profitability. The intricacy of this centralized code unit may endanger the entire IoT hub, since alterations to different libraries might affect other components as well. The lack of standardized communication protocols, together with diverse data formats and reading durations, might create compatibility issues, leading to inconsistent delays due to varied processing speeds across devices.

The microservice design may improve scalability by enabling a fridge sensor to detect rapid, extreme changes and autonomously adjust the quantity of an increase or reduction via the API gateway. When incorporating new devices, we may easily integrate additional scandalised API keys to establish connections from the primary core cloud to each autonomous database storage as a minor cloud server. Containerization enables the use of one service independently without affecting other services. Microservice architectures with deep learning methods can achieve compatibility by decoupling services (independently separating components), implementing an API service gateway (facilitating endpoint-to-endpoint communication within the network, using load balancer), utilising protocol adapters (transforming various protocol payload messages into a uniform format), and adopting an event-driven architecture (enabling communication with other devices via alerts sent through message brokers) to address issues related to disparate communication protocols. This method facilitates communication between devices that use different protocols by establishing a standard interface. It also employs version control identifiers, such as versioned API keys, to simplify communication among device sensors, manage minor protocol changes over time without disrupting compatibility, and regularly monitor and test network traffic to identify potential problems or issues(Gupta et al., 2020).

Edge computing shifts data handling from the cloud to the network's edge, closer to the data's creation location. This lets processing and study of data happen in real time close to the source of the data, which improves flexibility. Edge computing lowers the amount of data sent to the cloud. This lowers network traffic and the stress on cloud resources. It also supports low-latency communication, which lets us make decisions in real time, use resources efficiently, allocate them dynamically, and set up an organizational structure. This method facilitates the addition of more IoT end devices, thereby enhancing the system's efficiency and meeting the growing needs of businesses(*Towards Smart Home Automation*

*Using IoT-Enabled Edge-Computing Paradigm*, n.d.).

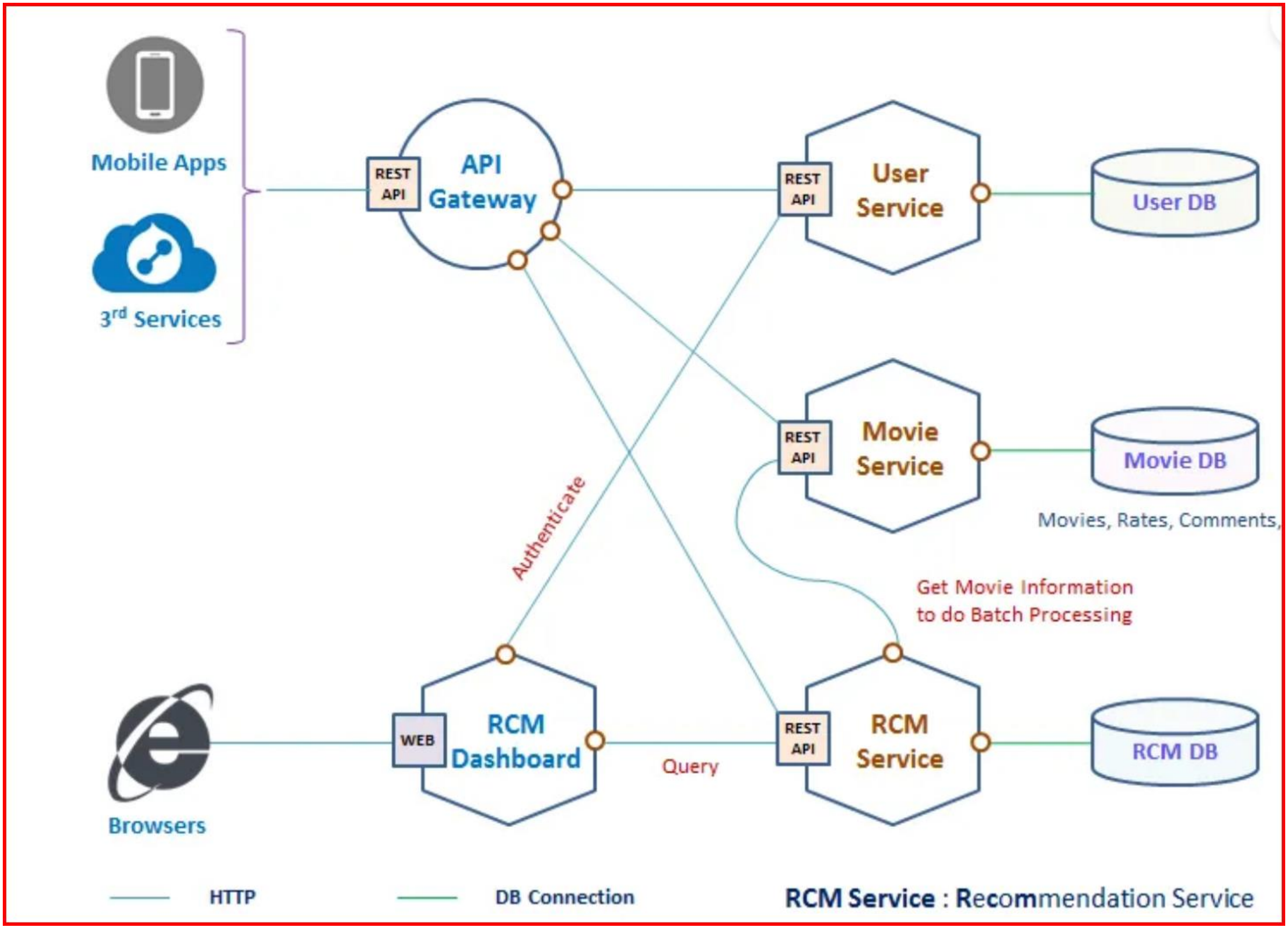


*Figure 8: Microservices-based recommendation system cited from (Raycad, 2018)*

## 5. Analyse the application of Software Defined Networking in an IoT framework

This research investigates the implementation of Software Defined Networking (SDN) inside the current IoT framework, emphasizing its advantages and possible problems, as well as its capacity to improve connections, flexibility, and scalability in the projected IoT system for a "Smart World."

SDN, or software-defined networking, simplifies contemporary networking by enabling visualization and programming, such as Python, on Linux systems. Following advantages can support current proposed IoT solutions.

The existing IoT system, consisting of interconnected devices like sensors, actuators, and gateways, communicates with cloud services for data processing and application delivery. However, it may face challenges like limited bandwidth, latency issues, and managing diverse devices and protocols.

For example, the deployment of smart data networks (SDN) is complicated and labour-intensive, requiring careful design and execution specifying targeting 50,000 users initially. It could involve substantial expenses and a considerable time commitment for hiring and IT specialised training and infrastructure renovation. Inadequate handling of such centralised control in SDN could lead to a single point of failure, necessitating the establishment of redundancy and failover solutions. A gradual approach may facilitate the integration with older systems, such as gateways or middleware. However, centralisation introduces security risks, such as the risk of infiltration by central controllers. Stringent access controls, encryption, and regular security assessments are crucial for protecting the SDN infrastructure. Following advantages of SDN can resolve challenging in current 5 situations as follows.

**1.Efficient traffic flow controls**

SDN is a system that lets administrators control all of a network's devices and connections from a single location. This simplifies the process of making changes to the network's settings, monitoring it, and resolving issues in the "Smart World" IoT system, as it eliminates the need for manual reconfiguration of each device. SDN effectively manages and regulates traffic flows to transmit encrypted data from multiple sensors, regardless of their proximity or far distance from the devices having Ip address.

**2.Enhancement security**

The Smart World IoT system uses SDN's advanced security methods to protect private devices. These include tracking odd traffic trends in real time, automatic protocol changes, and network division. This lowers the risks that come with IoT bugs. At the point where communication protocols meet network connections, SDN can find malware threats. It now works with AI to instantly change traffic networking under Quality of Service.

**3. Scalability**

The flexible design of SDN makes it simple to add new devices and services, which is why it is essential for the future growth of Smart World's IoT services. It adapts to the linking of more devices without requiring significant system changes. Cloud companies offer VNF type 1 Hyper-V, compatible with SDN, as part of their service agreements. The SDN controller can manage the infrastructure layer on top of the Hyper-V layer and link new devices to the IoT hub in the Azure cloud service.

**4. Interoperability among diverse devices by automated operation**

Traditional configuration by human's manual configuration in different VLAN networking, it will make time consume and replacement cost by human and go and visit to repair and do maintenance as operational cost and capitalisation cost. It will be very difficult to manage large asset networking in the case of initial 50,000 users. If one user has at least 2 IP addresses like their mobile phone and personal laptop, the number of Ip address are double. Therefore, SDN controller can be used in Ryu. Ryu applications provide the scandalised result, such as traffic management, load balancing, and real-time security policy administration. They oversee network traffic, enhance routing, and use multiple routes for better performance. Furthermore, they identify network risks and implement security rules in real-time.

At the end, less investment for dynamic large scales of network can make more profitable in expanding the business.

**5.Increasing the latency**

Due to heavy traffic flow are expecting in complexed networking by newly created new IP address, there are soe possibility to decrease the performance and if VNF in Azure is not working due to misconducted by cloud providers, such as malware attack or unknow reason, infrastructure layer will be significantly impacted when running the SDN controller by automated system and implement security policy.

## 6. Revised diagram for modified IoT architecture with integrated SDN

Provided a redesigned IoT architectural diagram with SDN that is clear, unambiguous, and labelled with the right terminology in Figure 9.

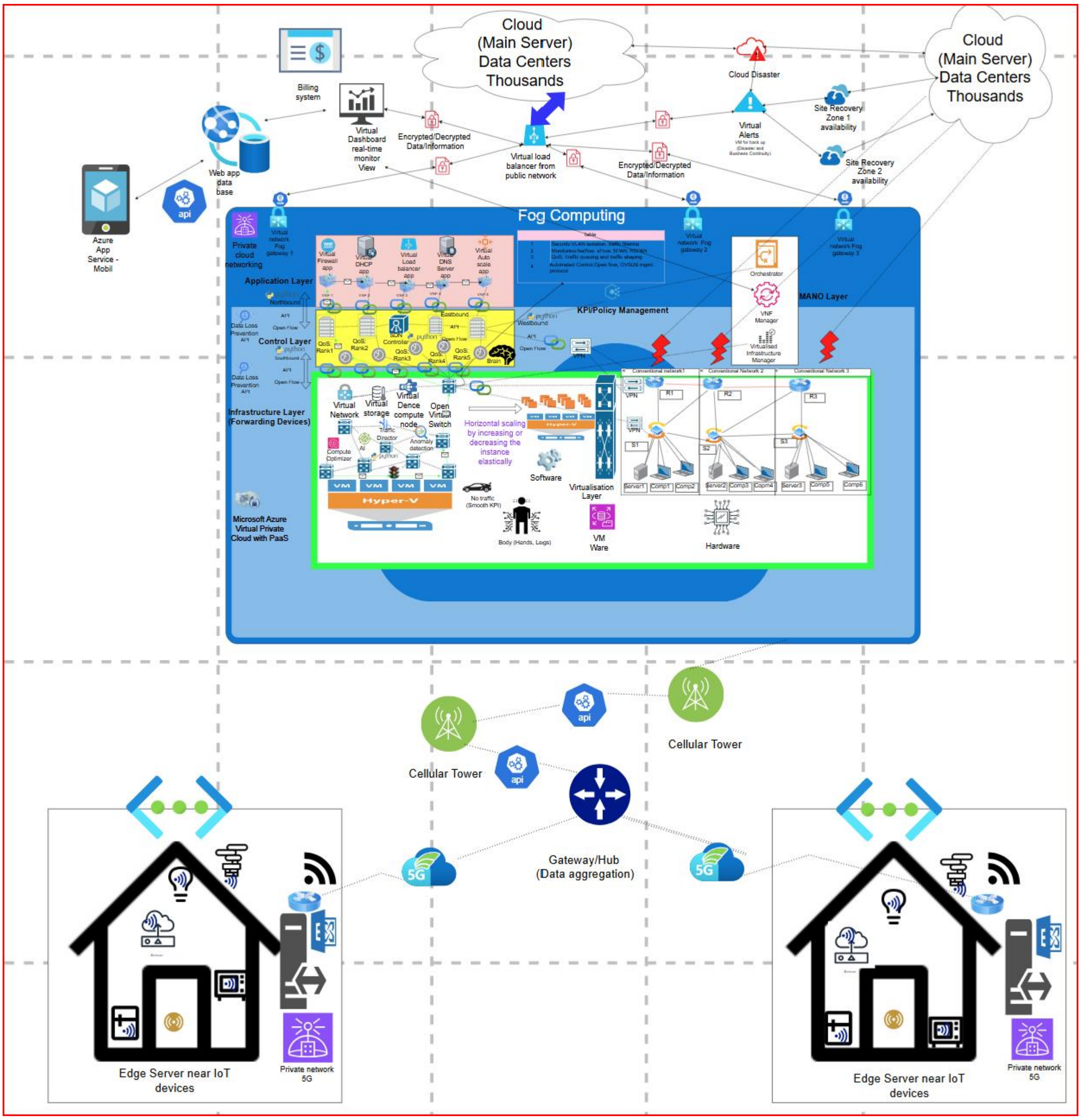


*Figure 9: The proposed components of the IoT value chain structure incorporate the modified IoT architecture, including the integration of SDN*

## 7. Explains how factor of SDN enhances the flexibility of network management.

The study examined five aspects of service delivery networks (SDN) to improve flexibility and network administration. SDN improves flexibility and management via centralized controls, programmable networks, open protocols, dynamic traffic management, and automation, enabling swift adjustments to growing business needs and enhancing network performance.

### SDN（Software-Defined Networking）

SDN consists of three layers in the architectures, which is application layer, control layer and infrastructure layer. SDN's main brain in control layer are separate from infrastructure layer because the main purpose of this SDN is to control the traffic flow.

### Encapsulating SDNs

**1.Traffic separation to sort different types of traffic flow**

When SDN are encountered into different types of traffic flow of live video, voice, text and numerical data in both structure unstructured, it is easy to manage and adjust the bandwidth and QoS. For example, video and voice is UDP format in transport layer that is forces on continuous data transition while TCP format in text by email are well protected with less priority on the latency. Therefore, what is the purpose and what is the criteria of each performance are important aspects in separating the traffic flow behaviour. Due to central controller in SDN, we can easily control one of devices from far distance from the central main controller so security camera in smart door and smart light can easily change configuration and ser different actuator setting from remote controller, so it is easy to set alert and easy to install new devises. SDN can create emerging traffic routing route in the case of emergency analyse the traffic outages. The research indicated that the cloud-local topology exhibited the lowest packet loss ratio of 1.4%, followed by local and cloud topologies at 1.9% and 2.3%, respectively(Gilani et al., 2024).

**2.Uniform communication protocol**

In the large network, each family has different router and switches from different vendors with different communication protocols as communication connectivity as their own rules. However, such different protocol can make same protocol by encapsulating in SDN frameworks. This is like our different language like speaking English, Japanese and Hindi, but translator like SDN can make our same uniform language. SDN can contribute such compatibility issue into smooth traffic flow.

**3.Enhancement of security**

Each different VLAN in their internal organisation and WLAN in their external organisation network are integrate, VPN, peering are important security protocol to make sure all traffic packets are smoothly gone through their tunnel; therefore, each traffic flow's encapsulation is important factor. Other than this encryption can convert plaintext into ciphertext in unreadable format like Arabic words by using different algorithms like ACE (Advanced Cryptographic Encryption) and AES (Advanced Encryption Standard). When updating the latest application and software, new security feature is installed as additional security measures. Heavy weight protocol is now Https are more recommended than http especially video and imagery than just simple text and numerical values nowadays. Authentication is important process because only authorised person who are given the permission to access the site for user who are giving ID and password with **Multi-Factor Authentication (MFA)** by global owner. At each node of network can be equipped with network security group (NSG) as firewall can only accept the specific agreed port number so than we can prevent malware attacks as unauthorised attacker in both incoming and outcoming traffic. Advantage of peering is to cut the extra budget of broker because direct communication between different WAN and low latency because of direct connection even if different regions if the smart homes are located such as smart home 1(New Zealand) and smart home 2(USA).

**4.Flexible network structure by automation**

In this scenario, there are several equipment, such as smart light, smoke sensor, smart fridge, smart door sensors and smart microwave. If each smart home owner has bought additional equipment like smart speaker and adding extra smart tools and more number of new joined smart home owner, then encapsulated techniques can normalise their new feature and tools in the same network of this IoT infrastructure so that a company can provide new service and introduce applications for user to receive the notification when they subscribe the specific their interest variables (e.g. Smart speaker)in their agreed cloud broker like IoT Hub in Microsoft Azure. In the case of changing the setting of smart sensor light at night, or one particular time to be heater up in a room before arriving at home can easily programme by python.

**5. Scalability by installing new service**

SDN provides network managers with improved visibility and monitoring via the aggregation of data from the whole network. This facilitates real-time analysis, enabling proactive resource management, rapid problem discovery, and informed decision-making. This allows managers to promptly address network alterations and failures, hence improving network dependability. For example, By encapsulating the data in each networking or different networking, each information such as source of node and destination node such as protocols are encapsulated each packet like putting in the envelop or box to be secured, therefore different service and different devises are mutually interacted each other on the demand. In the case of installing new devises in the smart speaker, we can easily configure and listen to the music due to the same configuration in protocols under flexible cloud VNF type 1 hypervisor resources.

## 8. Hinderance to performance and implementation while encapsulating SDN

Extensively detail the five obstacles that the suggested IoT system encounters while incorporating SDN, which hinder its performance and deployment.

**1.Scalability issues:**
The organization intends to initially provide access to 50,000 individuals, with each user assigning several IP addresses as an endpoint. This presents significant challenges in terms of performance and data translation. Initially, we establish the equilibrium of supply and demand, but the rising demand puts pressure on providers like SDN controllers to effectively manage and allocate traffic. The growing number of IoT devices within the network may pose scalability challenges for the SDN controller, as the architecture of SDN could potentially hinder performance as the network grows. This may result in communication delays, data loss, and diminished performance of real-time IoT applications. If the controller has inadequate computing power, it may jeopardize its ability to monitor devices, evaluate network conditions, and enforce appropriate regulations.

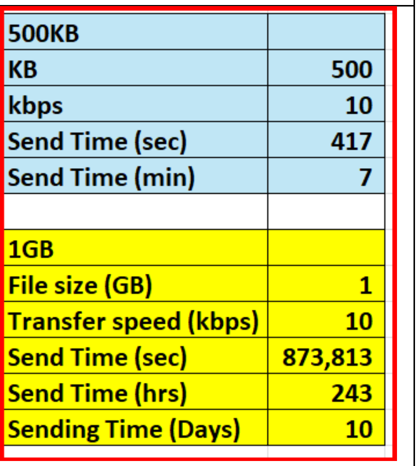
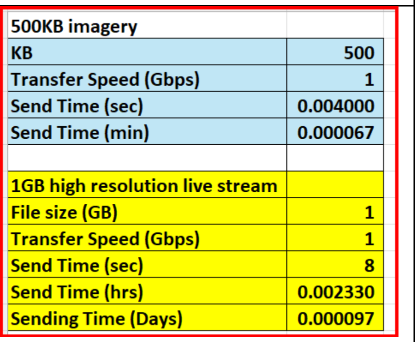
**2. Security vulnerability issue:**
The centralized management approach to SDN renders controllers susceptible to assaults, but most IoT devices possess insufficient security protections. This increases the potential for unauthorized access or data breaches, resulting in diminished confidence in the overall IoT system and threatening user privacy. The separated design of SDN exposes each segment of the network to potential attacks, especially because of the constrained resources and insufficient security protocols of IoT devices.

**3. Different protocol issue:**
IoT devices use various communication protocols and have varying security levels, whereas SDN primarily relies on IP-based communication, which can lead to interoperability issues across multiple protocols. This could potentially lead to network inconsistencies and uneven connectivity among devices. The complexity of facilitating interoperability between IoT devices and SDN frameworks stems from the various manufacturer standards, such as those of Apple versus Android products and the varying communication protocols in terms of distance coverage. Lack of standards leads to compatibility issues that complicate the process of connecting devices and establishing an SDN management network. This makes it harder to use IoT solutions. The need for additional adapters and protocol translations, which necessitate additional configuration and costs to ensure compatibility across diverse devices, limits the implementation of IoT systems. This is because SDN, a commonly standardized open flow protocol, may not be suitable for all IoT devices.

**4.Guarantee of real time data transmission issue:**
IoT apps often need to process and respond to data in real time. However, centralised management models of smart data networks (SDN) can lead to communication issues, thereby reducing performance

in safety-critical areas such as guaranteeing the presence of all 50,000 users initially and subsequently expanding the user base. If the centralized controller managing the network has latency concerns, it can significantly impair system performance. The inclusion of SDN in IoT systems complicates network administration, particularly in settings characterized by frequent device additions, removals, and configuration changes. This elevates administrative burdens and increases the possibility of operational mistakes and misconfigurations, thereby diminishing network dependability and adversely impacting system performance.

*Table 1: Comparative Analysis of 2G and 5G: Transmission Speed, Connectivity Delay, Connectivity Capacity, and Data Storage*

<table>
<tr><th>Criteria</th><th>Transmission speed</th><th>Connectivity delay</th><th>Number of connectivity</th><th>Data storages capacity</th></tr>
<tr><td>2G</td><td>Max 9.6kbps：High latency affects smart lock in door sensors, impossible massive amount of streaming live video of camera and big data in real time.</td><td>High latency between devices-to-devices control in real time can make challenging to control such as light, fridge, microwave,</td><td>Approximately 2,000 to 3,000 devices per square kilometre. Due to limitation of number of devises are connected all together, traffic flow will be congested.</td><td>
<table>
<tr><td>500KB</td><td></td></tr>
<tr><td>KB</td><td>500</td></tr>
<tr><td>kbps</td><td>10</td></tr>
<tr><td>Send Time (sec)</td><td>417</td></tr>
<tr><td>Send Time (min)</td><td>7</td></tr>
<tr><td></td><td></td></tr>
<tr><td>1GB</td><td></td></tr>
<tr><td>File size (GB)</td><td>1</td></tr>
<tr><td>Transfer speed (kbps)</td><td>10</td></tr>
<tr><td>Send Time (sec)</td><td>873,813</td></tr>
<tr><td>Send Time (hrs)</td><td>243</td></tr>
<tr><td>Sending Time (Days)</td><td>10</td></tr>
</table></td></tr>
<tr><td>5G</td><td>Gigabits per seconds speed can transfer the high spatial resolution and streaming video data.</td><td>Targeting less than 1 mm per second can transit low latency traffic flow are possible.</td><td>Up to approximately 1,000,000 devices per square kilometre. Due to the large number of connectivity are promising all together, smooth traffic flow is expecting. Regardless of increasing sudden changes, it is smoothly controlling smart home devises.</td><td>
<table>
<tr><td>500KB imagery</td><td></td></tr>
<tr><td>KB</td><td>500</td></tr>
<tr><td>Transfer Speed (Gbps)</td><td>1</td></tr>
<tr><td>Send Time (sec)</td><td>0.004000</td></tr>
<tr><td>Send Time (min)</td><td>0.000067</td></tr>
<tr><td></td><td></td></tr>
<tr><td>1GB high resolution live stream</td><td></td></tr>
<tr><td>File size (GB)</td><td>1</td></tr>
<tr><td>Transfer Speed (Gbps)</td><td>1</td></tr>
<tr><td>Send Time (sec)</td><td>8</td></tr>
<tr><td>Send Time (hrs)</td><td>0.002330</td></tr>
<tr><td>Sending Time (Days)</td><td>0.000097</td></tr>
</table></td></tr>
</table>

Another limitation is that it supports mobility. If the cloud broker subscriber uses the app while driving, connectivity is poor because an urban city may have all the devices to connect a cellular tower near the default gateway if the person is in the office, but remote country areas are out of range. The current planned IoT solution for smart homes does not meet the criteria for big data from the following perspective.

2G, the second generation of cellular network standards, is being used as the Global System for Mobile Communication (GSM). GSM is a communication technology used in cell phones to locate the closest cellular network station. Each mobile phone must have a SIM card inserted; hence, the GSM system is inoperative without a SIM card for each device. GSM is limited to transmitting voice and brief text messages, with a maximum data transmission rate of 9.6 kbps, resulting in significant traffic congestion due to distance and speed constraints.

**5.Limited resources issue:**

Limited processing power and battery life issues in hardware can significantly impact the cost and energy consumption of various devices. Each device's insufficient resources can result in shorter battery lifespans and, ultimately, lower reliability for end users. The high cost of battery replacements poses a significant problem for individuals with high expectations for return on investment, particularly when they anticipate high network performance. If the company monitors performance more frequently, controlling all traffic flow in the central unit of cloud servers can naturally increase power usage, leading to high energy consumption and shorter battery life. Expectation of duty cycle is always high frequency as per customer demands, but limitation is that high frequency of duty cycle, such as every 1-minute active mode overactive and off time to measure how much percentage can activate to use power, because lower activation can last longer battery life. Therefore, this expectation of each home user may be different because of high power consumption and the high replacement cost of the battery, which is not economical for the low-budget users.

# Conclusion

The analysis of Smart World's suggested IoT solution indicates its capacity to enhance smart home and workplace settings via advanced connection and data management. The structure of the IoT value chain is essential, including vital elements such as cloud services and data privacy protocols. Selecting appropriate communication models and protocols enhances the system's performance and effectiveness. We propose combining the Back-End Data Sharing communication paradigm with the WebSocket protocol to enhance flexibility and ensure reliable device connections. The incorporation of Software Defined Networking (SDN) has strategic benefits; nevertheless, issues such as security risks and operational intricacies need resolution. The effective implementation of Smart World's IoT system relies on a meticulously organized strategy, which creates a resilient and scalable IoT ecosystem that satisfies user requirements and facilitates future innovations in smart technology.

# Reference lists:

*Advantages of DDS protocol | disadvantages of DDS protocol*. (n.d.). Retrieved 8 November 2024, from https://www.rfwireless-world.com/Terminology/Advantages-and-Disadvantages-of-DDS-protocol.html

*ArcGIS Enterprise Administrator API | ArcGIS REST APIs | ArcGIS Developers*. (n.d.). ArcGIS REST APIs. Retrieved 4 November 2024, from https://developers.arcgis.com/rest/enterprise-administration/enterprise/overview-of-the-arcgis-enterprise-admin-api/

Atlassian. (n.d.). *5 Advantages of Microservices [+ Disadvantages]*. Atlassian. Retrieved 8 November 2024, from https://www.atlassian.com/microservices/cloud-computing/advantages-of-microservices

*Communication Models in IoT (Internet of Things )*. (2021, March 1). GeeksforGeeks. https://www.geeksforgeeks.org/communication-models-in-iot-internet-of-things/

*Data Visualization in Business Intelligence*. (2022, March 11). AltexSoft. https://www.altexsoft.com/blog/data-visualization-tools-types-techniques/

Gilani, S. M. M., Usman, M., Daud, S., Kabir, A., Nawaz, Q., & Judit, O. (2024). SDN-based multi-level framework for smart home services. *Multimedia Tools and Applications*, *83*(1), 327–347. https://doi.org/10.1007/s11042-023-15678-2

Gupta, N., Anantharaj, K., & Subramani, K. (2020). Containerized Architecture for Edge Computing in Smart Home: A consistent architecture for model deployment. *2020 International Conference on Computer Communication and Informatics (ICCCI)*, 1–8. https://doi.org/10.1109/ICCCI48352.2020.9104073

*IoT Communication Protocols—IoT Data Protocols—Technical Articles*. (n.d.). Retrieved 21 September 2024, from https://www.allaboutcircuits.com/technical-articles/internet-of-things-communication-protocols-iot-data-protocols/

Oliveira, G., Costa, D., Cavalcanti, R., Oliveira, J., Silva, D., Nogueira, M., & Rodrigues, M. (2018). *Comparison Between MQTT and WebSocket Protocols for IoT Applications Using ESP8266*. 236–241. https://doi.org/10.1109/METROI4.2018.8428348

RobBagby. (n.d.). *Microservice architecture style—Azure Architecture Center*. Retrieved 2 November 2024, from https://learn.microsoft.com/en-us/azure/architecture/guide/architecture-styles/microservices

Rowena, J. (2022, July 21). *IoT Hub: What Use Case for WebSockets?* Scaleway. https://www.scaleway.com/en/blog/iot-hub-what-use-case-for-websockets/

To, T. H. (2020). *Energy Saving Protocols for the Internet of Things* [Phdthesis, Université Grenoble Alpes [2020-....]]. https://theses.hal.science/tel-03041561

*Towards Smart Home Automation Using IoT-Enabled Edge-Computing Paradigm*. (n.d.). Retrieved 8 November 2024, from https://www.mdpi.com/1424-8220/21/14/4932

*Wireless Hart: DNCT702—Internet of Things*. (n.d.). Retrieved 21 September 2024, from https://nzseg.instructure.com/courses/1196/pages/wireless-hart?module_item_id=59752