

|  |  |
| --- | --- |
| Course / Programme: | BEng Software Engineering | BSc Computing |
| Module name and code: | Computing Infrastructure (SWE4202) |
| Student ID | 2224755 |
| Tutor: | Francis Morrissey | Dr Mohammed Benmubarak |
| Assignment Number: | 1 |
| Assignment Title: | Infrastructure Proposal for Suretide |
| Weighting | 40% of overall module grade |
| Issue Date: | 03/03/2023 |
| Submission Deadline: | 31/03/2023@ 2355 |
| Learning Outcomes assessed:   1. Explain the features of systems hardware and software in addition to services provided. 2. Apply networking principles and protocols to solve a given problem. | |

# FIGURES

[Figure 1 16](#_Toc131191810)

Contents

[FIGURES 2](#_Toc131192729)

[INTRODUCTION 1](#_Toc131192730)

[INFRASTRUCTURE MODELS 2](#_Toc131192731)

[PROPOSAL 7](#_Toc131192732)

[NETWORKING SOLUTION 9](#_Toc131192733)

[CONCLUSION 18](#_Toc131192734)

[REFERENCES 19](#_Toc131192735)

[BIBLIOGRAPHY 22](#_Toc131192736)

# INTRODUCTION

The United Kingdom (UK) has been particularly affected by an over reliance on fossil fuels in comparison to its neighbours in Europe (Guardian, 2022). According to Statista.com (2023), gas was used to create 41.9% of the power produced in the previous year and 78% of homes' central heating systems (grid.iamkate.com, 2023). In the UK, homes lose heat "three times faster than those in Norway and Germany" (tado.com, 2022), which has made the issue worse and increased energy expenditures.

The UK government has promoted the use of renewable energy sources and has offered significant incentives to companies in this sector. According to their predictions, renewable energy sources would overtake fossil fuels as the country's main energy source by 2030. The following report provides networking solutions and explanations in detail for the leading company offices that are responsible to deal with the matter above.

Assumptions

Within three months, the network infrastructure must be in place. This indicates that the infrastructure's design and implementation must be finished by the deadline.

To manage the massive amount of data the company generates, a data lake will be needed. It is necessary to plan the network architecture to accommodate significant data transmission and storage needs.

The network infrastructure will need to be built from scratch because the organisation currently has no IT infrastructure. The entire network must be secure and easy to maintain, and each office location's demands must be taken into consideration by the network design.

Both tailored Red Hat Linux distributions for specialised apps and standard productivity tools like email and word processing must be supported by the network infrastructure.

# INFRASTRUCTURE MODELS

Comparing and contrasting the two main options: On-prem and Cloud

On-prem.

On-premises software or IT systems are installed and maintained on the organization's own physical infrastructure rather than being hosted in the cloud or delivered as a software-as-a-service (SaaS) solution (Rittinghouse, 2010)*.* This indicates that the organisation owns the servers, data centres, and other infrastructure required to run the programme or system. On-premises solutions provide organisations complete control over their data and applications, but they need more investment in hardware, maintenance, and IT personnel to operate and defend the systems. On-premises solutions are typically used in industries with strict regulatory requirements, such as healthcare or finance, where the company must keep complete control over its data and equipment. On-premises solutions differ from cloud-based solutions in several aspects, including advantages and disadvantages.

Hardware, software and services necessary for On-prem solutions.

Physical Infrastructure

To support the software, on-premises solutions require an organisation's own hardware infrastructure. This infrastructure may contain servers, storage, networking equipment, and other devices.

Control and security

On-premises solutions provide companies complete control over their data and applications, including where and how they are stored and accessed. This capability also enables businesses to develop their own data security practises.

Customisation

On-premises solutions may be adjusted to a company's specific demands and requirements, giving the programme more flexibility and control. On-premises solutions need a significant initial investment in hardware, software licencing, and IT personnel to operate and maintain the infrastructure Blythe, M. (2020).

What is Cloud.

Cloud computing (Wang, L. and Al, E. 2012)is the delivery of online services such as servers, storage, databases, software, analytics, and more. The online servers allow individuals and organizations to access these resources on a pay-as-you-go basis from various cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP).

Definition for Cloud Computing.

Cloud computing is a technology that involves a network of remote servers hosted on the internet for storing, managing, and processing data. With cloud computing, users can easily access computing resources such as applications, storage, and processing power on-demand, without the need for local hardware or infrastructure. According to the National Institute of Standards and Technology (NIST), a cloud is defined as a model that enables convenient, ubiquitous, and on-demand network access to a shared pool of computing resources that can be quickly provisioned and released with minimal service provider interaction. The popularity of cloud computing has increased significantly in recent years, mainly due to its scalability, flexibility, and cost-effectiveness. By outsourcing IT infrastructure and services to cloud service providers, businesses can concentrate on their core competencies and allow service providers to manage the technical aspects.

Main characteristics of Cloud Computing.

Cloud computing has several key characteristics that differentiate it from traditional on-premises computing. These characteristics include:

1. On-demand self-service: Users may rapidly and simply provide cloud computing resources without the assistance of service providers' employees.
2. Wide network access: Any device with an internet connection may be used to access cloud services at any time and from any location.
3. Resource pooling: By distributing cloud computing resources across many users, it is possible to save money and operate more effectively.
4. Quick elasticity allows for flexibility and cost savings since cloud resources may be swiftly scaled up or down to suit changing demands.
5. Measured service: Cloud providers track resource utilisation using metering and billing systems, enabling precise and open charging.
6. Security: To safeguard the data and systems of their clients, cloud service providers substantially invest in security measures.

These characteristics make cloud computing an attractive option for businesses of all sizes looking for flexible and cost-effective IT solutions.

Benefits and Drawbacks of Cloud Computing.

Benefits

Scalability – Easily scale computing resources depending on what is needed.

Employ cloud computing for scalability: The ability to scale is one of the major advantages of cloud computing. Businesses may rapidly and simply scale up their cloud resources as needed to keep up with demand as they expand. Compared to needing to spend money on pricey gear and software, this can result in significant financial savings.

Cost-effectiveness – Only pay for the service you need (time, usage).

Cloud computing limits users from overspending and helps paying solely for the service used while being effective while taking into consideration the accuracy of the task at the same time*.*

Flexibility – Data and application access anytime from anywhere with basic internet connection which makes remote work a leading choice.

(Er, G. S., & Pal, P. 2017) (Aljabri, 2021)

Drawbacks

Dependence on Internet Access: Cloud computing is very reliant on Internet Access. The functionality and accessibility of cloud-based apps and services may be impacted if the internet connection is weak or disrupted.

Dependency on the provider: Because users of cloud computing depend on the provider's services and infrastructure, any failures or issues with the provider might influence the customers' businesses.

Cloud Deployment models

Public Cloud

In this kind of deployment, the cloud provider makes their services accessible to everyone online. Clients just need to pay for the resources they use; they are not required to purchase or maintain any hardware. The most often used deployment technique, public cloud provides the most scalability and affordability (Erl, Puttini and Mahmood, 2013).

Private Cloud

Under this deployment method, a single business receives exclusive access to the cloud infrastructure. Either a third-party supplier or on-site hosting are both options. Private clouds are frequently utilised for extremely sensitive data or regulatory compliance since they provide users more control over the infrastructure (Linthicum, 2009).

Hybrid Cloud

To maximise workload distribution, this deployment method combines public and private clouds. For instance, a business may maintain sensitive data on a private cloud while using the public cloud for non-critical activities (Arundel and Domingus, 2019).

Cloud Service models.

With the infrastructure as a service (IaaS) concept, the cloud provider provides virtualized computer resources including servers, storage, and networking. Customers can create their own virtual data centres and install applications using these resources. The maximum flexibility and control over the infrastructure are offered by IaaS (Comer, D. 2021).

Platform as a Service (PaaS): Under this business model, the cloud provider provides clients with a platform on which they may create, run, and maintain their applications. The operating system, programming languages, and other tools required for application development are included in the platform. PaaS offers a higher degree of abstraction, streamlining the process of developing applications (Rhoton, 2013).

Software as a Service (SaaS): Under this paradigm, the cloud provider provides access to online software applications. Clients may use the application using a web browser without having to install or maintain any software. SaaS offers the greatest level of abstraction and is the most user-friendly (Rittinghouse, 2010)*.*

# PROPOSAL

Cloud on-premises is the version used for this project. This version is a hybrid computing model that combines the benefits of both cloud computing and on-premises infrastructure. In this model, some applications and data are hosted in the cloud, while others are kept on local servers or data centres that are owned and managed by the organization. With cloud on prem, the organisation can leverage the scalability and flexibility of the cloud while maintaining control over their data and applications. This allows them to choose the best platform for each specific workload, based on factors such as performance requirements, security needs, and compliance regulations.

Cloud on prem can also help the organisation avoid the high upfront costs associated with building and maintaining their own data centres in various cities around the UK while still maintaining control over their infrastructure. This hybrid model can also help meet regulatory compliance requirements, such as HIPAA or GDPR, by allowing them to keep sensitive data on-premises while leveraging the cloud for less sensitive workloads.

Overall, cloud on prem provides a flexible and cost-effective approach to IT infrastructure that allows organisations to balance the benefits of cloud computing with their own security and control requirements.

Alternative strategies.

Full cloud option

Suretide can leverage cloud-based solutions to take advantage of their flexibility, scalability, and cost-effectiveness, while reducing their reliance on-premises infrastructure and maintenance costs. Furthermore, cloud-based solutions can guarantee exceptional availability and performance, which are fundamental to the success of Suretide's operations.

Suretide can utilize a blend of Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) cloud offerings to cater to its hardware and software needs. The hardware component would consist of virtual machines provided by the cloud vendor, on which the software would be installed.

Full on-prem solution

For Suretide to implement an on-premises solution, an IT infrastructure would need to be built and maintained inside the company's offices in key UK cities including London, Manchester, Leeds, Liverpool, Bristol, Cardiff, Edinburgh, and Belfast. Establishing this infrastructure to support sixty systems per office for usage by scientists, data analysts, and administrators is the responsibility of the SysOps Lead. The procedure has a three-month time limit, and employees who cannot commute to the stated cities must have remote access to all systems and data. Each office will also feature a conference room for guests who do not need access to the business's systems and data.

# NETWORKING SOLUTION

Services required for the offices based on the scenario details and assumptions made; this includes connectivity to each workstation, wireless access for tablets and other mobile devices and connectivity to networked phones – also includes assumptions.

1. To ensure that all sixty workstations used by scientists, data analysts, and administrators in each office have access to a fast and dependable network connection, it is necessary to provide a network infrastructure that can support high-bandwidth activities such as data analysis, machine learning, and visualization.
2. To keep up with the increasing trend of using mobile devices in workplaces, each office must be equipped with wireless access points to ensure uninterrupted wireless connectivity to tablets and other mobile devices used by employees and visiting consultants.
3. To ensure effective communication between the office, employees, clients, and stakeholders, a dependable phone system is necessary. This includes networked phones that are connected to the office network to support both voice and video calls.
4. Employees who are unable to physically work in the office must have a secure and reliable remote access system to all systems and data required to carry out their job responsibilities. The remote access system should enable employees to access systems and data from any location.
5. The smooth running of the company's digital business processes is crucial; thus, the infrastructure must ensure high availability and operational performance to support these functions effectively.
6. The company's unique applications for statistical analyses, visualization, and machine learning are developed using the Red Hat Linux distribution. Hence, the infrastructure should be compatible with this customized distribution.
7. Aside from customized applications, basic software tools like email and word processing are necessary for everyday operations of the office.
8. To identify the optimal locations for positioning turbines around the British Isles, a large amount of data will be generated and stored in a data lake. The infrastructure needs to be capable of managing and storing the data efficiently as the volume of data is expected to increase considerably over time.

Assumptions

1. The infrastructure will be cloud on premises to enable remote access and high availability and better data access.
2. A reliable internet connection will be available in each office.
3. Each office will have a server room or space to include on-premises equipment.
4. A unified communication system will be used to provide voice and video communication.
5. The infrastructure will be designed with security as a top priority, and appropriate measures such as firewalls and encryption will be implemented.

Networking Topology.

Networking topology refers to the physical or logical arrangement of network devices and their interconnections. It defines the way in which computers, servers, printers, and other network devices are connected to each other to create a network. The topology determines the flow of data between devices, the reliability of the network, and the ease of maintenance (Tanenbaum, 2011).

Bus Topology

In a bus topology, all devices are connected to a single cable. The cable acts as a shared communication medium, and data is transmitted in both directions along the cable. This type of topology is simple and inexpensive, but it can be prone to data collisions and is not very scalable (Pearl, 2011).

Benefits of Bus Topology

1. Cost-effective: Since bus topology uses less cabling than other topologies, it is a cost-effective alternative for small networks.
2. Bus topology is extremely simple to set up and maintain because there is just one wire to take care of.
3. High data transmission rate: Because the bandwidth is not shared by the nodes, bus architecture offers a high data transfer rate.

Forouzan, B. A. (2013), Stallings, W. (2016)

Drawbacks of Bus Topology

1. One single point of failure exists in the bus topology. The entire network may be unavailable if the main cable is destroyed.
2. Distance restriction: In a bus topology, the signal's intensity determines how far the cable may run. The signal may deteriorate, and data loss may occur if the distance between nodes is too great.
3. Tough to troubleshoot: Bus topology problems might be difficult to diagnose. As the wire passes through every node, pinpointing the exact location of the issue might be challenging.

Techopedia (n.d.), TechTarget (n.d.)

Star Topology

According to Cisco (n.d.) In a star topology, all devices are connected to a central hub or switch. Data is transmitted from one device to the hub, and then from the hub to the destination device. This type of topology is easy to install and maintain, and it provides good performance and scalability.

Benefits of Star Topology

1. Scalability: Star Topology is highly scalable as new devices can be easily added to the network without affecting the performance of other devices.
2. High reliability: If one device fails, it does not affect the rest of the network. Also, the central hub or switch acts as a backup, so if one link fails, the data can be rerouted through another link.
3. Fast data transfer: Each device has its own dedicated link to the central hub or switch, which ensures fast data transfer rates.

Tanenbaum and Wetherall (2011), Stallings (2016)

Drawbacks of Star Topology

1. Dependency on the central hub or switch: Star Topology is heavily dependent on the central hub or switch. If the hub or switch fails, the entire network will be affected.
2. Cost: As each device requires a dedicated point-to-point connection to the central hub or switch, the cost of cabling and network equipment can be higher than other topologies.
3. Security: As all devices are connected to a central point, it can be easier for unauthorized users to access any private source or information.
4. Limited Bandwidth: In a star topology, the bandwidth is shared among all the nodes. If too many nodes are connected to the hub, the network's performance may be affected.

(Rendell, 2013), (Ondieki, M., 2017)

Ring Topology

In a ring topology, all devices are connected in a closed loop. Data is transmitted from one device to the next in a sequential fashion until it reaches the destination device. This type of topology is reliable and provides good performance, but it can be expensive to install and maintain (GeeksforGeeks, 2020).

Benefits of Ring Topology

1. Cost-effective: For smaller networks, a ring topology is a good option. This is because it needs less cabling than other topologies, such as the star topology.
2. Data Transmission: Data transmission in a ring architecture is unidirectional. Data collisions are reduced as a result, and network performance is enhanced.
3. Tolerant to certain faults: The ring topology is tolerable to some faults. The network can continue to operate even if one node fails since the data may be transferred in the other way.

Uyless (2007)

Drawbacks of Ring Topology

1. Single Point of Failure: If one node fails in a ring topology, the entire network might be brought to a halt.
2. Limited Number: The signal's intensity determines the maximum number of nodes that may be included in a ring topology. The signal may deteriorate, and data loss may occur if the distance between nodes is too great.
3. Limitations on bandwidth: With a ring architecture, the network's nodes share the available bandwidth equally. The network's performance may suffer if there are too many nodes added.

Forouzan, B. A. (2013)

Mesh Topology

In a mesh topology, all devices are connected to every other device in the network. This type of topology provides the highest level of redundancy and reliability, but it can be expensive and difficult to manage.

Benefits of Mesh Topology

1. Because there is no single point of failure, mesh topology is very reliable. The network can continue to operate even if one node fails since there are several pathways for data transmission.
2. Mesh architecture can handle many nodes without degrading network speed, making it very scalable.
3. High data transfer rate: Unlike other topologies where the bandwidth is shared, mesh topology allows each node to transmit data concurrently, resulting in a high data transfer rate.

Drawbacks of Mesh Topology

1. Cost: Mesh topology requires a lot of cabling, making its implementation and maintenance costly.
2. Complexity: Because every node in a mesh topology is linked to every other node, mesh topology is difficult to design, construct, and administer.
3. Harder to troubleshoot: Because of the complexity of a mesh architecture, troubleshooting problems can be difficult. Finding the issue's root cause might be challenging, and finding a solution could involve a large investment of time and money.

Best Topology for Suretide.

Overall, choosing the right topology for a network depends on factors such as the size of the network, the level of reliability required, and the cost of installation and maintenance. The Topology that suits Suretide best is the Star Topology. It provides each device a separate link to the central hub which increases the speed of data transfer. This could also result in a downside as the system is dependent on the switch. Which means if the central hub fails to operate then the system collapses. However, Star Topology is easy to manage and provides high level of scalability and reliability. It allows new systems to join without affecting the already existing devices while ensuring reliable data transfer from one end to the other.

Importance of subnetting.

Subnetting is a technique used in computer networking to divide a larger network into smaller subnetworks, or subnets, which can improve network performance, security, and manageability. There are several subnetting strategies that can be used, depending on the specific requirements of the network.

Use of subnetting strategy.

When choosing a subnetting strategy, it's important to consider the specific requirements of the network, such as the number of hosts that need to be accommodated which in Suretide’s case are 60 in each office, the amount of traffic that will be transmitted, the level of security needed, and the overall manageability of the network. A network administrator should also consider the potential for future growth and expansion when designing the subnetting scheme (Tanenbaum & Wetherall, 2011).

IPv4 private networks are reserved for use within an organization or a local area network (LAN) and are not accessible from the internet. There are three classes of IPv4 private networks: Class A, Class B, and Class C. Each class provides a different range of IP addresses and can support a different number of hosts.

When deciding which class of IPv4 private network to use, several factors should be considered, including the size of the network, the number of hosts, and the level of network security required. Here are some reasons why each class may be appropriate for different scenarios:

Class A:

A Class A private network provides a large range of IP addresses and can support up to 16,777,214 hosts. This class is suitable for large organizations that require a vast number of IP addresses. However, it may not be suitable for smaller organizations or those that require higher levels of network security. Using a Class A private network may result in unused IP addresses and higher complexity in managing the network (Smith, 2009).

Class B:

A Class B private network provides a moderate range of IP addresses and can support up to 65,534 hosts. This class is suitable for mid-sized organizations that require a moderate number of IP addresses. Using a Class B private network may result in some unused IP addresses, but it is a good balance between network size and manageability (Johnson, 2010).

Class C:

A Class C private network provides a small range of IP addresses and can support up to 254 hosts. This class is suitable for smaller organizations that require a limited number of IP addresses. Using a Class C private network is a good option for organizations that require higher levels of network security because it allows for more efficient use of IP addresses and easier network management (Lee, 2012).

In summary, the choice of which class of IPv4 private network to use depends on the organisation's size, the number of hosts, and the level of network security required. Ultimately the network suitable for Suretide is the Class B network which is more than enough number of networks in this case scenario.

Assuming we use a subnet mask of 255.255.255.0 (which provides for 256 hosts), we can use the following formula to determine the number of subnets:

2^(n) >= number of subnets, where n is the number of bits used for subnetting.

Since we need to build offices in eight major cities across the United Kingdom, we can use three bits for subnetting, which gives us a total of eight subnets:

So 2^(3) = 8

To calculate the number of hosts needed for each subnet, we deduct two from the total number of hosts for each subnet. This is because one address is reserved for the network address and another for the broadcast address.

So, for each office, we need to provision a subnet with 62 hosts:

256 - 2 = 254

254 - 192 = 62

Hence, to meet the infrastructure requirements, set out by Suretide, we can make use of a Class B network address and a subnet mask of 255.255.192.0. This will meet the requirements, as it allows for 64 subnets, each with the ability to accommodate 62 hosts. This capacity is sufficient to allocate 60 systems per office and permit remote workers to access all systems and data.

One common subnetting strategy is to use a Classless Inter-Domain Routing (CIDR) scheme. With CIDR, a network administrator can allocate a block of IP addresses, such as a Class B network (16 bits for the network portion and 16 bits for the host portion), and then divide that block into smaller subnets by borrowing bits from the host portion. For example, if we borrow 3 bits from the host portion, we can create 8 subnets with 2^13 (8192) addresses in each subnet.

Cisco Packet Tracer

To create a Cisco Packet Tracer model for 60 systems in a small office, one would need to follow several steps. Firstly, the network topology to be used should be determined based on the office size, number of devices, and network requirements.

Next, the Packet Tracer model can be built by creating a new network and adding the necessary devices such as switches, routers etc. Devices can be connected to the network and configured by using the configuration tabs. This may include setting IP addresses, configuring routing protocols, and configuring security settings.

Finally, the network should be tested using the simulation mode in Packet Tracer. This will help to check connectivity, simulate traffic between devices, and troubleshoot any issues. By following these steps, a reliable and functional network that meets the needs of the office can be created, although the process may be complex.

A picture containing map

Description automatically generated

Figure

Assuming each office has 60 systems, the network solution could utilize the Class B network address range of 172.16.0.0/16 for this scenario. This address range can support up to 65,536 hosts, which is sufficient for the requirements of each office. To accommodate future growth and ensure scalability, the range can be divided into smaller subnets using variable-length subnet masks.

As there are eight offices to provision, at least eight subnets are required. This will ensure that the network can accommodate the necessary number of hosts for each office and allow for future expansion.

# CONCLUSION

To summarize, the recommended infrastructure solution for Suretide involves a combination of on-premises and cloud services. This approach provides reliable performance, scalability, and availability, as well as addressing data security and regulatory compliance issues. The solution will include security measures such as access controls, encryption, and network security to prevent unauthorized access and protect against cyber threats. The report underscores the necessity of having a data lake to accommodate the vast amounts of data generated for identifying optimal locations to install turbines around the British Isles. As the volume of data is anticipated to increase significantly throughout the project's lifespan, a scalable solution is provided.

# REFERENCES

Wang, L. and Al, E. (2012). *Cloud computing: methodology, system, and applications*. [online] Boca Raton, Fl: Crc Press. Available at: <https://publications.csiro.au/rpr/pub?pid=nicta:4686>.

‌ Rhoton, J. (2013). Cloud computing explained. London: Recursive Press.

Kurose, J. F., & Ross, K. W. (2017). Computer networking: a top-down approach (7th ed.). Pearson. (p. 389-395)

Rittinghouse, J.W. (2010). Cloud computing: implementation, management, and security. Florida: Taylor & Francis.

Erl, T., Puttini, R. and Mahmood, Z. (2013). Cloud computing: concepts, technology, & architecture. Upper Saddle River, Nj: Prentice Hall.

Linthicum, D.S. (2009). Cloud Computing and SOA Convergence in Your Enterprise. Pearson Education.

Arundel, J. and Domingus, J. (2019). Cloud Native DevOps with Kubernetes: building, deploying, and scaling modern applications in the cloud. Sebastopol, CA: O’Reilly Media.

Er, G. S., & Pal, P. (2017). Cloud computing risks and benefits. International Journal of Advanced Research in Computer Science, 8(4) Retrieved from <https://login.ezproxy.bolton.ac.uk/login?url=https://www.proquest.com/scholarly-journals/cloud-computing-risks-benefits/docview/1912629080/se-2>.

Tanenbaum, A. (2011). Computer Networks. Pearson Education India.

Pearl, E.M. (2011). Open Problems in Topology II. Elsevier.

Forouzan, B. A. (2013). Data Communications and Networking. McGraw-Hill Education.

Stallings, W. (2016). Data and Computer Communications. Pearson.

Techopedia. (n.d.). Bus Topology. Retrieved from <https://www.techopedia.com/definition/2431/bus-topology>

TechTarget. (n.d.). Bus Network. Retrieved from <https://searchnetworking.techtarget.com/definition/bus-network>

Cisco. (n.d.). Star Topology. Retrieved from <https://www.cisco.com/c/en/us/support/docs/optical/sdh-synchronous-digital-hierarchy/13939-star-topology.html>

Tanenbaum, A. S., & Wetherall, D. (2011). Computer Networks. Pearson. (Chapter 5 covers the benefits of star topology, such as easy fault isolation and the ability to add or remove devices without affecting the rest of the network.)

Stallings, W. (2016). Data and Computer Communications. Pearson. (Chapter 6 explains the advantages of star topology, such as centralization of network management, easier troubleshooting, and the ability to handle heavy network traffic.)

Rendell, C. (2013). Network topologies: types, performance impact, and advantages/disadvantages. New York: Novinka.

GeeksforGeeks (2020). Advantages and Disadvantages of ring topology. [online] GeeksforGeeks. Available at: <https://www.geeksforgeeks.org/advantages-and-disadvantages-of-ring-topology/>.

Uyless, B. (2007). Computer Networks. PHI Learning Pvt. Ltd. (Chapter 8 covers the advantages of ring topology, such as the ability to handle heavy network traffic and the efficient use of network bandwidth.)

Aljabri, S. (2021). Advantages and Disadvantages of Cloud Computing. International Journal of Advanced Computer Science and Applications, 12(3), 236-240.

Blythe, M. (2020). Cloud Computing vs On-Premises Servers: Which is Best for Your Business? Tech.co. Retrieved from <https://tech.co/cloud-computing-vs-on-premises-servers-which-is-best-for-your-business-2020-02>

Ondieki, M. (2017). The disadvantages of a star topology network. International Journal of Scientific and Research Publications, 7(9), 114-118. Retrieved from https://www.ijsrp.org/research-paper-0917/ijsrp-p7019.pdf

Forouzan, B. A. (2013). Data communications and networking (5th ed.). McGraw-Hill. (p. 233-234)

Smith, J. (2009). Introduction to Computer Networking. Boston: Pearson Education.

Johnson, R. (2010). Computer Networking for Small and Medium-Sized Businesses. New York: McGraw-Hill.

Lee, K. (2012). Fundamentals of Computer Networking. San Francisco: Wiley.

Tanenbaum, A. S., & Wetherall, D. (2011). Computer Networks (5th ed.). Boston: Pearson.

# BIBLIOGRAPHY

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. Decision Support Systems, 51(1), 176-189

Kshetri, N. (2010). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 34(5-6), 605-617.

Mell, P., & Grance, T. (2009). The NIST definition of cloud computing. National Institute of Standards and Technology, 53(6), 50.

Duan, Y., Xiong, H., Zhang, X., Huang, G., & Wang, W. (2017). A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.

Eckerson, W. W. (2010). Performance dashboards: measuring, monitoring, and managing your business. John Wiley & Sons.

Han, J., Pei, J., & Kamber, M. (2011). Data mining: concepts and techniques. Elsevier.

Hwang, K., Kim, H., Kim, D., Lee, K., Lee, K., Lee, J., ... & Kwon, O. (2014). On-premises public cloud: A survey. Journal of Network and Computer Applications, 44, 148-159.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

Bianchi, G. (2000). Performance analysis of the IEEE 802.11 distributed coordination function. IEEE Journal on selected areas in communications, 18(3), 535-547.