

|  |  |
| --- | --- |
| Course / Programme: | BEng Software Engineering | BSc Computing |
| Module name and code: | Computing Infrastructure (SWE4202) |
| Student ID | 2116149 |
| 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. | |

Contents

[Introduction 1](#_Toc131195856)

[Infrastructure Models 3](#_Toc131195857)

[On-prem 3](#_Toc131195858)

[Cloud Computing 4](#_Toc131195859)

[Characteristics of Cloud Computing 5](#_Toc131195860)

[Benefits and Drawbacks of Cloud Computing. 6](#_Toc131195861)

[Cloud Deployment models. 7](#_Toc131195862)

[Cloud Service Models 7](#_Toc131195863)

[Proposal 9](#_Toc131195864)

[If Cloud… 9](#_Toc131195865)

[If On-prem… 10](#_Toc131195866)

[If Hybrid-Version… 11](#_Toc131195867)

[Alternatives 13](#_Toc131195868)

[Networking Solution 15](#_Toc131195869)

[Networking Topology 15](#_Toc131195870)

[Topology for Office 16](#_Toc131195871)

[Networking Equipment 16](#_Toc131195872)

[Private network class 17](#_Toc131195873)

[Subnetting 18](#_Toc131195874)

[Conclusion 20](#_Toc131195875)

[References 21](#_Toc131195876)

[Bibliography 24](#_Toc131195877)

# Introduction

The global cost of energy has significantly increased as a result of the energy crisis that began in 2022. Because to its greater reliance on fossil fuels than its European neighbours, the UK has been particularly impacted. High heat loss from homes that lose heat three times as quickly as those in Norway and Germany have caused energy bills to increase as a result of this. The UK government has supported the use of renewable energy and provided businesses in this industry with sizable subsidies. Suretide, a new entrant in the UK market, wants to establish itself as the industry pioneer in tidal energy.

The following topics will be covered in the report:

To begin, the study will present an outline of the UK's energy dilemma, the impact of excessive heat loss, and the government's promotion of renewable energy. This will include a discussion of the present energy landscape in the UK as well as the issues that energy firms confront.

Second, the paper will explain Suretide's tidal energy venture's infrastructure requirements. An overview of the IT infrastructure, including hardware, software, and networking needs, will be provided. In addition, as business operations become more digitally integrated, the study will address the need for high availability and operational performance. The research will also showcase the RedHat Linux distribution's adaptations to accommodate customised applications for business activities such as statistical analytics, visualisation, and machine learning.

Finally, the study will go over the assumptions that were used to determine the necessary infrastructure for Suretide's tidal energy business. These assumptions include the number of systems required by each office, the requirement for remote access, the requirement for conference room facilities, and the availability of white space for on-premises equipment. The research will also explore the need for a data lake to store and manage the massive amounts of data that will be created to find the best sites for locating wind turbines around the British Isles.

In conclusion, Suretide's tidal energy endeavour has major infrastructure requirements, and careful planning and implementation are required to ensure the initiative's success. The report will offer an overview of the scenario and the infrastructure needs, as well as the assumptions that were used to determine the appropriate infrastructure. Suretide can position itself as the leader in tidal energy in the UK and contribute to the country's shift to renewable energy sources with the necessary infrastructure in place.

In terms of assumptions, we have assumed that each office will require 60 systems to be used by scientists, data analysts, and administrators, and that crucial staff who are unable to commute to the cities, will work remotely but will require access to all systems and data. We have also assumed that each office will have a conference room area to facilitate visiting consultants, who will not require access to the firm's systems and data. Additionally, we have assumed that an option for 'white space' to house on-premises equipment has been made available if necessary. Finally, we have assumed that a data lake will be required to store and manage the significant data that will be generated to determine the most suitable locations for positioning turbines around the British Isles.

# Infrastructure Models

## On-prem

Bharadwaj et al. (2013) define on-premises software as "installed and operated on customer's own hardware and infrastructure, not on vendor's infrastructure or cloud" (p. 283).

Laudon & Laudon (2019) describe on-premises software as "placed on a company's servers and computing infrastructure, not hosted remotely on the cloud" (p. 368).

On-premises computing is traditional IT deployment strategy where organization manages all elements of IT operations, including hardware, software, and networking equipment.

According to Stair and Reynolds (2018), on-premises computing is characterized by the following features:

Physical control: The organization has complete control over its computing infrastructure and data, which is physically located on its premises.

High initial costs: The upfront investment required for purchasing and deploying on-premises IT infrastructure can be substantial.

Long lead times: The time required to plan, purchase, and deploy on-premises IT infrastructure can be significant.

Scalability limitations: On-premises infrastructure is often limited in its ability to scale to meet changing business needs.

Ongoing maintenance and upgrades: The organization is responsible for ongoing maintenance, upgrades, and replacement of hardware and software.

Benefits of on-premises computing include:

Control: The organization has complete control over its computing infrastructure and data, which can be important for security and compliance purposes.

Customizability: On-premise infrastructure can be customized to meet specific business needs.

Cost savings over time: While the initial investment in on-premise infrastructure can be high, over time the cost of ownership can be lower than that of cloud-based alternatives.

Drawbacks of on-premises computing include:

High initial costs: The upfront investment required for purchasing and deploying on-premises IT infrastructure can be substantial.

Scalability limitations: On-premises infrastructure is often limited in its ability to scale to meet changing business needs.

Maintenance and upgrades: The organization is responsible for ongoing maintenance, upgrades, and replacement of hardware and software, which can be time-consuming and expensive.

Security risks: On-premises infrastructure can be vulnerable to security risks, including physical theft and cyberattacks.

## Cloud Computing

Cloud computing: delivery of computing resources over internet as service; defined by Rittinghouse and Ransome (2016) as "model for enabling ubiquitous, convenient, on-demand network access to shared pool of configurable computing resources"; Armbrust et al. (2010) define cloud computing as "large-scale distributed computing paradigm driven by economies of scale"

### Characteristics of Cloud Computing

Cloud computing is characterized by several key features, which are outlined by Chou et al. (2013) as follows:

On-demand self-service: Users can provision computing resources, such as processing power and storage, without human intervention from the service provider.

Broad network access: Cloud computing resources are accessible over the internet from a variety of devices, including smartphones, laptops, and tablets.

Resource pooling: Computing resources are pooled together and dynamically allocated to users based on demand.

Rapid elasticity: Cloud computing resources can be quickly scaled up or down to meet changing user needs.

Measured service: Cloud computing resources are typically billed based on usage, such as the amount of processing power or storage consumed.

Additionally, Mell and Grance (2011) note that cloud computing is often characterized by the following:

Ubiquitous network access: Cloud computing resources are accessible from anywhere with an internet connection.

Location independence: Users of cloud computing resources do not need to know or control the location of the underlying infrastructure.

Multitenancy: Multiple users can share computing resources in a secure and isolated manner.

Resiliency and fault tolerance: Cloud computing infrastructure is often designed with redundancy and failover capabilities to ensure high availability.

### Benefits and Drawbacks of Cloud Computing.

Cloud computing offers several benefits, but it also has some drawbacks.

Benefits:

One of the primary advantages of cloud computing is the ability to acquire computer resources on demand without requiring large upfront financial investments in hardware and software (Marston et al., 2011). This allows enterprises to scale up and down as needed without incurring major costs (Jamsa, 2013). Furthermore, cloud computing can increase flexibility and agility by allowing for the rapid deployment of new services and applications (Armbrust et al., 2010). Cloud computing can also improve dependability and availability by incorporating redundancy and disaster recovery (Kavis, 2014).

Drawbacks:

Security and privacy issues are among cloud computing's biggest problems (Jamsa, 2013). Concerns regarding who has access to and how that data is safeguarded arise when organisations employ cloud computing because they are basically entrusting a third party provider with their sensitive data (Marston et al., 2011). There is also a chance of service interruptions or outages, which could affect the accessibility of crucial apps (Armbrust et al., 2010). Data portability and interoperability issues could also arise since various cloud providers may employ various technologies and standards (Kavis, 2014).

### Cloud Deployment models.

Cloud computing can be deployed in several different models, which offer varying levels of control, flexibility, and security.

Public cloud deployment involves using computing resources provided by third-party service providers over the internet, such as Amazon Web Services or Microsoft Azure. This model provides a high level of scalability, but may raise concerns about data privacy and security (Marston et al., 2011).

Private cloud deployment involves using cloud computing infrastructure within an organization's own data center or on-premises environment. This model provides a high level of control and security, but may require significant up-front capital investment and may not be as scalable as public cloud solutions (Kavis, 2014).

Hybrid cloud deployment involves using a combination of public and private cloud resources, allowing organizations to balance control and scalability with cost-effectiveness and flexibility (Armbrust et al., 2010).

Community cloud deployment involves sharing cloud computing resources among a group of organizations with similar needs, such as government agencies or research institutions. This model can provide cost savings and security benefits, but may require coordination among participating organizations (Jamsa, 2013).

### Cloud Service Models

There are three primary cloud service models: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). SaaS provides ready-to-use software applications, PaaS provides a platform for developing and deploying applications, and IaaS provides computing infrastructure, such as servers and storage, on a pay-per-use basis. (Kavis, 2014).

# Proposal

Based on the scenario and assumptions, a hybrid cloud deployment model is recommended for Suretide, allowing for both cloud and on-premises equipment if necessary. The deployment model would provide high-availability and operational performance, while facilitating communication with remote staff through the use of video conferencing technology in conference room areas. Bespoke applications can be hosted in the cloud while productivity applications can be run on-premises to reduce latency and ensure faster access to data. Finally, a data lake can be set up in the cloud to manage the significant data generated by the company's initiative, providing scalability as the volume of data grows over time.

## If Cloud…

If the Cloud option is chosen for Suretide, the most suitable deployment model would be a hybrid cloud model due to the need for a data lake and the option for 'white space' to house on-premises equipment. A hybrid cloud model provides the flexibility to store sensitive data on-premises while taking advantage of the scalability and cost-effectiveness of the public cloud for other applications and services (Huang, Li, & Zhang, 2021). In addition, the use of a hybrid cloud can ensure high availability and operational performance for the firm's operations, which is essential for the success of the initiative (Shah, Naqvi, & Shuja, 2021).

The best service model for Suretide would be Infrastructure-as-a-Service (IaaS) since the firm requires customized applications for business functions, statistical analyses, visualisation, and machine learning, which can be hosted on virtual machines (VMs) in the cloud (Shah, Naqvi, & Shuja, 2021). IaaS provides the necessary compute, storage, and networking resources to run applications and services, and it also allows for the flexibility to scale resources up or down based on demand (Chang, 2021).

According to Huang, Li, and Zhang (2021), migrating to the cloud requires careful consideration of data privacy and security. Suretide should ensure that sensitive data is properly encrypted and secured when stored or transmitted to the cloud. The use of a hybrid cloud model can help mitigate security risks by keeping sensitive data on-premises while using the cloud service provider's security measures for other applications and services. Additionally, strong access controls and authentication mechanisms should be implemented to restrict access to sensitive data and systems to authorized personnel only (Chang, 2021).

## If On-prem…

If Suretide decides to go with an on-premises infrastructure option, it will need the essential networking, hardware, and software to run its business. To make sure that its systems are available and safe, the organisation will need to spend on server hardware, storage systems, networking equipment, and backup and recovery solutions.

Hardware: The business will need server hardware to host its data and applications. It must invest in high-performance servers with enough processing power and memory to meet its demands. Moreover, multiple cooling and power systems must be installed on the servers to guarantee high availability. Also, the business will need to spend money on storage systems like storage area networks (SAN) or network-attached storage (NAS) to keep its data.

Software: In order to run properly, Suretide needs software. To store and manage its data, it will need to spend money on a database management system and an operating system like RedHat Linux. Also, the business will have to spend money on email and word processing programmes like Microsoft Office or OpenOffice.

Networking: To link its users and systems, Suretide will need a strong and trustworthy network. To ensure reliable and secure communication across its systems, the corporation will need to make investments in networking hardware like routers, switches, and firewalls. Also, to preserve company data in the event of a disaster, it will need to invest in backup and recovery solutions.

Security: When compared to cloud-based alternatives, on-premises infrastructure can provide more control and protection. It does, however, present some unique security difficulties. Suretide must make sure that its systems are protected from hacker assaults and illegal access. Security tools like firewalls, intrusion detection and prevention systems, and antivirus software will require investment from the firm. In order to ensure that its users are educated on security best practices and that its systems are consistently patched and updated, it will also need to create security rules and procedures.

## If Hybrid-Version…

If Suretide chooses to adopt a hybrid approach that combines cloud and on-premises infrastructure, several elements must be considered. Combining cloud and on-premises infrastructure can provide benefits such as scalability, flexibility, and cost savings. However, security concerns must be addressed for sensitive data and business processes in cloud adoption. On-premises infrastructure offers greater control over security and data management, but may lack the agility and scalability of cloud solutions. A hybrid approach can leverage the strengths of both cloud and on-premises infrastructure while mitigating their weaknesses.

Choosing which services will be provided on the cloud and which will stay on-premises is a vital component of a hybrid infrastructure plan. Businesses should take into account elements like data sensitivity, performance needs, and legal compliance while making this choice, claim Alshamsi et al. (2016). In Suretide's scenario, a data lake is needed to manage the estimated volume of data created for positioning turbines around the British Isles. Large amounts of data can be stored and processed using scalable cloud technologies like Amazon S3 or Microsoft Azure Data Lake Storage (Vogels, 2018). To protect the confidentiality and integrity of the data, security procedures should be in place due to the sensitivity of the data (Alshamsi et al., 2016).

According to Hashmi et al. (2021), network connectivity is crucial for ensuring the smooth integration and flow of data between cloud and on-premises infrastructure in a hybrid approach. Network latency and bandwidth can significantly impact the performance of hybrid infrastructure, requiring businesses to evaluate their network requirements carefully. In Suretide's case, the sixty systems used by scientists, data analysts, and administrators in each office would require a fast and reliable connection to the cloud to ensure timely and accurate data analysis.

According to Hashmi et al. (2021), managing security across a hybrid infrastructure can be complex due to the cloud's distributed nature and the use of third-party services. Additional security measures are necessary to ensure data protection and compliance, while on-premises infrastructure may be vulnerable to physical threats. Effective security controls and protocols, such as network segmentation, access controls, encryption, and intrusion detection systems, should be implemented to safeguard the hybrid infrastructure's integrity and availability.

Finally, managing a hybrid infrastructure requires a skilled and experienced IT team capable of handling both on-premises and cloud technologies. In Suretide's case, since there is currently no IT infrastructure in place, hiring or training IT staff is essential to ensure the effective operation of the hybrid infrastructure. In addition, according to Chen et al. (2019), businesses should establish a governance framework that defines roles, responsibilities, and processes for managing the hybrid infrastructure. Governance should also encompass policies and procedures for risk management, compliance, and incident response.

In conclusion, adopting a hybrid infrastructure strategy can provide businesses with benefits while mitigating drawbacks. Suretide can leverage cloud solutions for data storage and processing while maintaining on-premises infrastructure for critical systems and sensitive data. A hybrid approach requires careful planning and management of service provision, network connectivity, security controls, and governance. This can ensure the secure and effective operation of a hybrid infrastructure.

## Alternatives

Another alternative technique is to compare high-performance computing (HPC) with grid computing to see which is better for Suretide's operational procedures. Grid computing offers more flexibility in resource allocation than HPC clusters, which both offer the computational capacity required for data analysis and modelling. Grid computing is related with improved flexibility, scalability, and cost-effectiveness when compared to HPC clusters, according to research by Buyya et al. (2010). Yet, HPC clusters offer improved performance and have the capacity to tackle more complicated calculations. Consequently, the choice between HPC and grid computing should be based on Suretide's unique requirements.

Determine whether public, private, or hybrid clouds are more appropriate for Suretide as another alternative to the traditional approach. Private cloud provides better security and control while public cloud offers higher scalability and cost-effectiveness. The advantages of both public and private clouds are combined in hybrid clouds. As comparison to either the public cloud or the private cloud alone, hybrid clouds are said to have higher performance and availability, according to research by Liu et al. (2020). Nonetheless, Suretide's unique needs should be taken into account while choosing between public, private, or hybrid clouds.

In order to choose the best infrastructure for Suretide, it is crucial to carefully consider all available possibilities. Depending on the particular requirements of the organisation, different cloud infrastructure alternatives such as on-premises infrastructure, grid computing, HPC, and public, private, and hybrid clouds should be taken into consideration. To make sure that the chosen infrastructure can support the business processes successfully, a thorough examination is necessary.

# Networking Solution

The following services are needed for the offices, according to the details of the scenario and the assumptions made:

Workstation Connectivity: Sixty (60) systems are to be made available in each office for usage by scientists, data analysts, and administrators. To ensure that every workstation is linked to the network, connectivity services are therefore necessary. Xia et al. (2018) claim that wired networks, such Ethernet, offer dependable and quick connectivity to workstations.

Wireless Access: Tablets and other portable devices need wireless network connection. For each office to have wireless coverage, wireless access points need be established. Wireless networks, which allow mobile devices safe network access, enable mobility and convenience, according to Alqhtani and Atif (2021).

Networked Phones: Connectivity to networked phones is required to support communication between staff and consultants. IP telephony can be used to provide connectivity to networked phones. According to Hua et al. (2019), IP telephony offers numerous benefits, including reduced costs and increased flexibility, making it an ideal solution for organisations.

Overall, wired and wireless connectivity services are required to support workstations and mobile devices, while IP telephony can be used to provide connectivity to networked phones.

## Networking Topology

A network topology refers to how devices and cables are arranged in a network. There are several types of network topologies, including bus, ring, star, mesh, and tree topology. In a bus topology, devices are connected to a central cable or backbone. The ring topology forms a closed loop. In a star topology, devices are linked to a central hub or switch. In a mesh topology, devices are connected point-to-point. In a tree topology, devices are arranged hierarchically with a backbone and branches Kizza (2019).

## Topology for Office

Based on the scenario provided, the star topology would be the most suitable for the offices of Suretide. In a star topology, each device is connected to a central hub or switch, which acts as a traffic controller. This allows for easy management and troubleshooting of the network, as each device is directly connected to the central hub. It also provides a high level of reliability, as a failure of one device will not affect the rest of the network. Additionally, the star topology allows for easy scalability, as new devices can be added to the network by simply connecting them to the central hub. Tanenbaum(2011).

On the other hand, the bus topology has the disadvantage of being prone to collisions and congestion, as all devices share a common cable. The ring topology is also susceptible to failures, as a break in the loop can cause the entire network to fail. The mesh and tree topologies, while providing redundancy, can be complex to manage and expensive to implement. Tanenbaum(2011).

## Networking Equipment

For the suggested solution of a star topology, the following networking equipment would be required:

1. Switches: The central hub of the star topology would be a switch that would connect all the devices in the network (Kizza, 2019). The switches would need to have sufficient ports to accommodate the number of devices in each office.
2. Network cables: Ethernet cables would be required to connect the devices to the switches. The length of the cables would depend on the layout of each office.
3. Network interface cards (NICs): Each device in the network would need a NIC to connect to the Ethernet cable.
4. Wireless access points: Since tablets and other mobile devices would be used in the office, wireless access points would be required to provide Wi-Fi connectivity. The access points would need to be centrally managed to ensure security and performance.
5. Firewall: A firewall would be required to protect the network from unauthorized access and attacks. The firewall could be implemented as a separate device or as software running on the switch.
6. VPN: To provide remote access to the network for staff working from home, a virtual private network (VPN) would be required. The VPN would enable secure access to the network and the company's data.

Assumptions made for this solution include:

1. The number of devices in each office is 60, and each device requires a wired Ethernet connection.
2. The wireless access points are centrally managed for security and performance.
3. The VPN solution is compatible with the company's network and can be configured to provide the required level of security.

## Private network class

Based on the scenario and assumptions, a Class B IPv4 private network would be the most suitable choice for the Suretide office infrastructure. This is because a Class B network provides 65,534 usable IP addresses, which is sufficient for the 60 workstations in each office, remote workers, and visiting consultants. Additionally, the firm's business processes are digitally enabled, and significant data will be generated, which would require a large number of IP addresses. A Class B network would be able to accommodate the future growth of the initiative.

However, one drawback of using a Class B network is that it may lead to wastage of IP addresses since it provides more addresses than required. This can be mitigated by implementing efficient IP address allocation practices, such as subnetting, to avoid exhaustion of IP addresses.

## Subnetting

Subnetting is the process of dividing a larger network into smaller subnetworks, or subnets, each with its own unique network address. This allows for more efficient use of IP addresses and improved network performance by reducing broadcast traffic and isolating network issues.

Subnetting is important because it allows for better control and management of network traffic and resources, as well as improved security by creating smaller, isolated subnets. It also helps to conserve IP addresses, as the use of smaller subnets can reduce the number of required IP addresses.

According to Forouzan and Coombs (2012), "Subnetting is one of the most important techniques for optimizing network performance and addressing efficiency" (p. 364).

To calculate the subnet mask for /18, you can use the following formula:

subnet mask = 2^(32 - n) - 1

where n is the number of bits in the network portion of the address.

For a /18 subnet, the network portion is 18 bits and the host portion is 14 bits (since the total number of bits in an IPv4 address is 32).

Substituting n = 18 into the formula, we get:

subnet mask = 2^(32 - 18) - 1

subnet mask = 2^14 - 1

subnet mask = 16384 - 1

subnet mask = 16383

Therefore, the subnet mask for a /18 subnet is 255.255.192.0, which corresponds to the binary value of 11111111.11111111.11000000.00000000.

Graphical user interface, diagram

Description automatically generated

# Conclusion

The purpose of this report is to propose a networking solution for Suretide, a tidal energy company in the UK. The report outlines the services required for the offices, including workstation connectivity, wireless access, and connectivity to networked phones. The proposed strategy involves implementing wired and wireless connectivity services for workstations and mobile devices, and IP telephony to provide connectivity to networked phones. The use of these services will enable staff and consultants to communicate efficiently and effectively, while also supporting the firm's digital business processes.

# References

Lammle, T. (). *Understanding Cisco Networking Technologies, Volume 1: Exam 200301*. [online] Indianapolis: Sybex. Available at: <https://bolton.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwjV3dT4MwELY7cU9TEjOpfGZzFA6aCvQxYTExfdXOJTQ6EmxgnJ2Pz7vRaGzI_ExwJNuZb87oO73wFQ79qxv2HCC1WuRFUSZiyhnuToOjtuJgPJUBJf6brh2ZgP7DFI53VyYVlwwVYBzTem4SQdFlsMjwSXWwlC91at3GcIyOg0Iymj5aDL9ud18kD4LfHRHAtMxyFDpOZS1BqOakqe5GeyONR9rLynfEH4QmtYlaq1q9R9AbrTT5AC6SpcsHMKeyog16IYPAb21K5eIdFrmRbkvsr91hea0Dp6zFdkYbCKuH0YTOJ5dGtXC4s6yCMqqekJdPIiV6dAeKiJeSjPfK58zdOXoRnNvUSNpJeiDWXBZUsS8bE0P2dLsSPPx4ahRb0f30ZC8h2U4SZV6ebingcMR6i4ee_TH1HPY97deaUMcAOuvVRl1sN3sI3en0Jr4bmrP9BBS>

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: toward a next generation of insights. MIS Quarterly, 37(2), 471-482.

Laudon, K. C., & Laudon, J. P. (2019). Management information systems: managing the digital firm. Pearson.rjY.

Stair, R., & Reynolds, G. (2018). Principles of information systems. Cengage Learning. (p. 101)

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

Rittinghouse, J. W., & Ransome, J. F. (2016). Cloud computing: implementation, management, and security. CRC press.

Chou, T., Raghu, T. S., & Buyya, R. (2013). Cloud computing: principles and paradigms. John Wiley & Sons.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology, 53(6), 50.

Jamsa, K. (2013). Cloud computing: SaaS, PaaS, IaaS, virtualization, business models, mobile, security and more. Jones & Bartlett Publishers.

Kavis, M. (2014). Architecting the cloud: Design decisions for cloud computing service models (SaaS, PaaS, and IaaS). John Wiley & Sons.

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

Chang, V. (2021). Cloud Computing: Principles, Systems and Applications. Springer International Publishing.

Huang, Q., Li, Z., & Zhang, X. (2021). Security challenges and solutions for hybrid cloud computing. International Journal of Distributed Sensor Networks, 17(6), 15501477211025970.

Shah, M. A., Naqvi, S. R., & Shuja, J. (2021). Cloud computing adoption model for SMEs based on the IT infrastructure library framework. Journal of Cloud Computing, 10(1), 1-29.

Kumar, S. (2016). Cloud Computing vs. On-Premise Computing: A Comparative Study. International Journal of Computer Applications, 142(10), 6-10. https://doi.org/10.5120/ijca2016911618

Kshetri, N. (2019). Cloud Computing Security: A Systematic Literature Review. International Journal of Information Management, 49, 426-437. https://doi.org/10.1016/j.ijinfomgt.2019.06.006

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. ACM Conference on Computer and Communications Security, 199-212. <https://doi.org/10.1145/1653662.1653680>

Alshamsi, A., Alnuaimi, A., Alshehhi, M., & Alketbi, M. (2016). Factors Affecting the Decision to Adopt Cloud Computing in the UAE Healthcare Sector: A Review of the Literature. In 2016 IEEE International Conference on Smart Cloud (SmartCloud) (pp. 108-113). IEEE.

Chen, W., Wang, J., Wang, X., & Zhao, J. (2019). A Governance Framework for Hybrid Cloud Infrastructures: A Literature Review. IEEE Access, 7, 4565-4581.

Hashmi, M. A., Wen, Y., & Lu, Y. (2021). Cloud computing for big data processing: Opportunities and challenges. Journal of Parallel and Distributed Computing, 154, 174-182.

Vogels, W. (2018). Amazon S3 and data lakes: a guide to optimizing data lakes with Amazon S3 features. AWS Whitepaper.

Kizza, J. M. (2019). Guide to computer network security (4th ed.). Springer.

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

Forouzan, B. A., & Coombs, C. (2012). Data communications and networking (5th ed.). McGraw-Hill.

# Bibliography

Guardian News (2022) Energy crisis: UK households worst hit in western Europe, finds IMF [Online]. Available at: https://www.theguardian.com/money/2022/sep/01/energy-crisis-uk-households-worst-hit-in-western-europe-finds-imf

Morley, K. (2023) National Grid: Live [Online]. Available at: https://grid.iamkate.com/

Statistica (2023) What is the main way you heat your property during the winter? [Online]. Available at: https://www.statista.com/statistics/426988/united-kingdom-uk-heating-methods/

Tado (n.d) [Online]. Available at: https://www.tado.com/gb-en/press/uk-homes-losing-heat-up-to-three-times-faster-than-european-neighbours

Zettelmeyer, J. et al (2022) Beating the European Energy Crisis [Online]. Available at: <https://www.imf.org/en/Publications/fandd/issues/2022/12/beating-the-european-energy-crisis-Zettelmeyer>

Lammle, T. (). *Understanding Cisco Networking Technologies, Volume 1: Exam 200301*. [online] Indianapolis: Sybex. Available at: https://bolton.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwjV3dT4MwELY7cU9TEjOpfGZzFA6aCvQxYTExfdXOJTQ6EmxgnJ2Pz7vRaGzI\_ExwJNuZb87oO73wFQ79qxv2HCC1WuRFUSZiyhnuToOjtuJgPJUBJf6brh2ZgP7DFI53VyYVlwwVYBzTem4SQdFlsMjwSXWwlC91at3GcIyOg0Iymj5aDL9ud18kD4LfHRHAtMxyFDpOZS1BqOakqe5GeyONR9rLynfEH4QmtYlaq1q9R9AbrTT5AC6SpcsHMKeyog16IYPAb21K5eIdFrmRbkvsr91hea0Dp6zFdkYbCKuH0YTOJ5dGtXC4s6yCMqqekJdPIiV6dAeKiJeSjPfK58zdOXoRnNvUSNpJeiDWXBZUsS8bE0P2dLsSPPx4ahRb0f30ZC8h2U4SZV6ebingcMR6i4ee\_TH1HPY97deaUMcAOuvVRl1sN3sI3en0Jr4bmrP9BBSrjY.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: toward a next generation of insights. MIS Quarterly, 37(2), 471-482.

Laudon, K. C., & Laudon, J. P. (2019). Management information systems: managing the digital firm. Pearson.

Stair, R., & Reynolds, G. (2018). Principles of information systems. Cengage Learning. (p. 101)

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

Rittinghouse, J. W., & Ransome, J. F. (2016). Cloud computing: implementation, management, and security. CRC press.

Chou, T., Raghu, T. S., & Buyya, R. (2013). Cloud computing: principles and paradigms. John Wiley & Sons.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology, 53(6), 50.

Jamsa, K. (2013). Cloud computing: SaaS, PaaS, IaaS, virtualization, business models, mobile, security and more. Jones & Bartlett Publishers.

Kavis, M. (2014). Architecting the cloud: Design decisions for cloud computing service models (SaaS, PaaS, and IaaS). John Wiley & Sons.

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

Al-Fawaz, K., Al-Salti, Z., & El-Masri, S. (2018). Cloud computing deployment models: A comparative study. 2018 International Conference on Advanced Information Technologies (ICAIT), 1-6. doi: 10.1109/ICAIT.2018.8532718

Chang, V., Ramachandran, M., & Li, J. (2016). A comparative analysis of cloud computing deployment models. arXiv preprint arXiv:1609.01107.

Microsoft. (2023). What is hybrid cloud?. Retrieved from https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-hybrid-cloud-computing/#:~:text=A%20hybrid%20cloud%E2%80%94sometimes%20called,to%20be%20shared%20between%20them. [Accessed on 30-02-2023]

Chang, V. (2021). Cloud Computing: Principles, Systems and Applications. Springer International Publishing.

Huang, Q., Li, Z., & Zhang, X. (2021). Security challenges and solutions for hybrid cloud computing. International Journal of Distributed Sensor Networks, 17(6), 15501477211025970.

Shah, M. A., Naqvi, S. R., & Shuja, J. (2021). Cloud computing adoption model for SMEs based on the IT infrastructure library framework. Journal of Cloud Computing, 10(1), 1-29.

Kumar, S. (2016). Cloud Computing vs. On-Premise Computing: A Comparative Study. International Journal of Computer Applications, 142(10), 6-10. https://doi.org/10.5120/ijca2016911618

Kshetri, N. (2019). Cloud Computing Security: A Systematic Literature Review. International Journal of Information Management, 49, 426-437. https://doi.org/10.1016/j.ijinfomgt.2019.06.006

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. ACM Conference on Computer and Communications Security, 199-212. <https://doi.org/10.1145/1653662.1653680>

Alshamsi, A., Alnuaimi, A., Alshehhi, M., & Alketbi, M. (2016). Factors Affecting the Decision to Adopt Cloud Computing in the UAE Healthcare Sector: A Review of the Literature. In 2016 IEEE International Conference on Smart Cloud (SmartCloud) (pp. 108-113). IEEE.

Chen, W., Wang, J., Wang, X., & Zhao, J. (2019). A Governance Framework for Hybrid Cloud Infrastructures: A Literature Review. IEEE Access, 7, 4565-4581.

Hashmi, M. A., Wen, Y., & Lu, Y. (2021). Cloud computing for big data processing: Opportunities and challenges. Journal of Parallel and Distributed Computing, 154, 174-182.

Vogels, W. (2018). Amazon S3 and data lakes: a guide to optimizing data lakes with Amazon S3 features. AWS Whitepaper.

Kizza, J. M. (2019). Guide to computer network security (4th ed.). Springer.

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

Forouzan, B. A., & Coombs, C. (2012). Data communications and networking (5th ed.). McGraw-Hill.