ASSIGNMENT Component 1

TECHNOLOGY PARK MALAYSIA

032024-CT105-3-M-CIS

CLOUD INFRASTRUCTURE SERVICES

HAND OUT DATE: **4th April 2024**

HAND IN DATE : **24th May 2024**

STUDENT NAME : **Muhammad Arif Bin Jamaluddin**

TP NO : **TP067696**

WEIGHTAGE: 50%

INSTRUCTIONS TO CANDIDATES:

1 Submit your assignment Online via Moodle

2 Students are advised to underpin their answers with the use of references (cited using the APA System of Referencing)

3 Late submission will be awarded zero (0) unless Extenuating Circumstances (EC) are upheld

4 Cases of plagiarism will be penalized

CLOUD INFRASTRUCTURE SERVICES IN ENVIRONMENTAL MANAGEMENT SYSTEM FOR URBAN FLOODING

A report submitted in fulfilment of the
requirements for the module
CLOUD INFRASTRUCTURE SERVICES

ASIA PACIFIC UNIVERSITY OF TECHNOLOGY & INNOVATION (APU)
SCHOOL OF COMPUTING AND TECHNOLOGY

…..2024

Abstract

Cloud computing recently has drastically improved many industries and domains all over the world where many organizations and business entity started to adopt cloud computing to improve their business operations and organizations. Cloud computing able to help environmental management where it can help with energy efficiency and provide support with renewable energy where companies such as Google, Amazon and Microsoft design their respective cloud services to be green energy friendly and the hardware services of cloud computing is designed to be environmentally friendly. It provides good and sustainable resource allocation where multitenancy allows many users to share same resources and thus this provides efficient use of hardware and energy compared to traditional IT. In this case for water environmental cloud computing can help with real time monitoring using cloud services and also can implemented cloud-based solutions with automated control systems.

Key Words: Cloud computing, allocation, multitenancy, efficiency, environmental management

Table of Contents

Abstract 3

1.0 Introduction 5

2.0 Objectives & aim of study. 8

3.0 Problem of Statement 8

4.0 Body & Outcome of the assignment 9

4.1.1 Conceptual Or Theoretical Framework of the cloud adoption in environmental management including introduction into cloud computing. 10

4.1.2 Introduction to cloud infrastructure services in the domain of environmental management. 23

4.1.3 Cloud computing roles in the domain of environmental management particularly in flood management. 26

4.1.4 The suitability of various cloud services and deployments model for the flood management system. 30

4.1.5 How the various cloud services features such as scalability, automation, efficiency, and availability influenced Natural disaster management or flood management system. 33

4.1.6 Critical review of the features available of the Amazon Web Services to enhance and facilitate the performance, innovation, and transformation in flood management system. 38

4.1.7 The potential challenges that might occurs utilizing cloud services in the flood management system in terms of security and privacy concerns and other management related issues. 44

5.0 Conclusion 50

6.0 References 51

7.0 List of Figures 55

8.0 List of Tables 56

1.0 Introduction

Cloud infrastructure services or also known as cloud computing has been significantly rising and being adopted by many organizations where many big tech companies provide cloud services to this company and organizations to enhance their business operations to make it more seamless and improve efficiency. In the domain of environmental management cloud computing can be a powerful tool to address environmental challenges that very persistent recently as the world currently experience climate changes where severe drought happening that causes water dam to be dried due to unpredictable weather that happen in the last 4 years. Other than that, due to excessive raining or natural disasters major flood can happen and with unproper drainage system it makes the situation much worse, and the main topic chosen for this assignment is to study the adoption of cloud technology in mitigate the risk of urban flood.

Hence, imagine with the adoption of cloud-based platforms technology where it utilizes cloud technology to collect data from sensors and devices. This can be seen for example cloud-based technology used in SCADA technology where stands for Supervisory Control and Data Acquisition that used in industrial plants such as dam water to monitor levels of water in the dam. Hence integration can be done by integrating SCADA devices with cloud services such as it ensures to transmit data and receive in a format where both party or software able to understand and communicate with one another. Other applications of cloud services in environmental management are sensors can be used to monitor air quality, water pollution and deforestation and hence it can be shown that cloud-based solutions able to support renewable energy initiatives, waste management programs and disaster response efforts.

Urban flooding has been an ongoing issue that causes disasters and casualties all over the world and many statistics has been recorded where from Emergency Events Database, natural disasters has caused around 3 trillion dollars of economic destruction and around 1.3 million casualties with 4.4 billion people injured between the year of 1998 and 2017. (C. Center for Research on Epidemiology of Disasters, Economic losses, 2018).

Urban flooding happened due to the city landscapes unable to absorb excess water after having such a long time of intense and prolonged rainfall, river overtopping or storm surge happening. For example, in other country like India flood is one of the major disasters where it huge effected major essential sites such as agriculture, infrastructure and property and it is known that the main cause of urban flooding is due to unplanned development, deforestation and fast urban growth. This happened in North Bihar and due to overflow of water that comes from

Nepal, and this causes major flood that ravages these regions. (Freer, J., Beven, K., Neal, J., Schumann, G., Hall, J. and Bates, P., 2013) (Kumar, H., Karwariya, S. K. and Kumar, R, 2022)

Other than that, there is also a few case studies done in several state in Malaysia that experience flooding where historically in Malaysia the worst flood happened in 1926 where it causes major damage to infrastructure and agriculture. The consequence of this major flood causes major losses to people surrounding the Klang Valley River around 12000 Straits Dollars. In other parts of Malaysia, in the state of Pahang, major destruction occurs on a private railway that linking the plantation to mines at Sungei Lembing that was washed away and later trains has to be retrieved from the muds. (Williamson F, 2016).

Based on the statistic recorded by Malaysian government from the department of irrigation and drainage, flooding has become a normal event that happen in Malaysia every year since 1963 where it causes damage to more than 4.82 million people and damages cost around RM915 million (Department of Irrigation and Drainage (DID) 2009,). Other than that, there is also case study done on the particular town in the state of Johor, Malaysia called Segamat where it suffered flood in the year of 2006, 2011 and 2017. It is known that in December 2006 and January 2007, flood cause property damages over RM 1.5 billion in Segamat Johor which deemed as the worst flood disasters in 100 years. (Tengku Asmara, T.A and Muhamad Ludin, A.N. 2014) (Reza, M.I.H., Choy, E. & Pereira, J.J. 2017)

Hence it can be deduced that flood is one of the major disasters that causes major damages and hence cloud companies can play role and mitigating and lessen the risk of flooding especially in the urban areas by adopting cloud technology. This can be seen recently where trends like mobility, big data and social media drive the adoption of cloud technology to most companies.

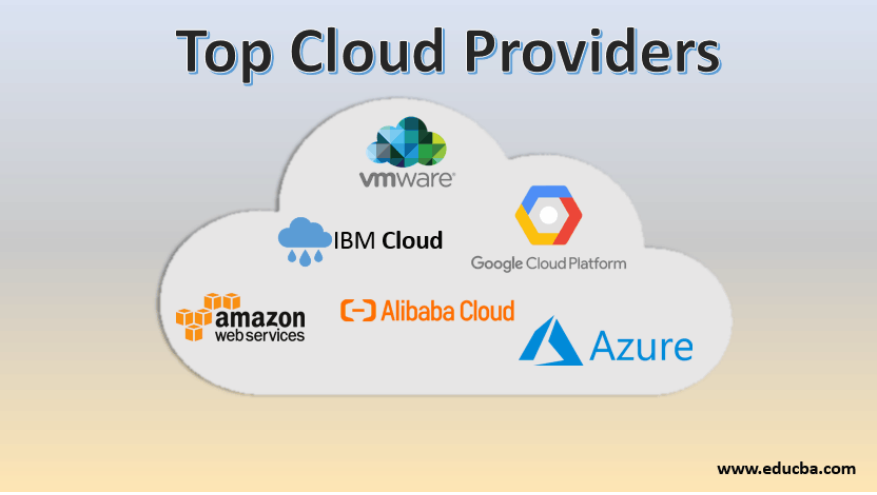


Figure 1

Figure above shows several top cloud services providers such as the most popular one Amazon Web Services, IBM Cloud, Microsoft Azure, Google Cloud Platform and Alibaba Cloud which being used by many organizations and companies. In this module, the cloud providers used for learning purpose and assignment is Amazon Web Services although other cloud providers can be used to do this assignment but there are few reasons why Amazon Web Services is popular due to AWS is the first of its kind to establish cloud computing as a service model and hence it allows to lock more people earlier in their services.

Table 1

AWS advantages	Explanation
Easy to work	AWS provide skills and training or tutorial online for junior cloud developer using platform such as AWS academy that teaches fundamental of AWS cloud services
Very flexible	It is very flexible as it can be used on run on any platform such as macos, windows, linux and indicates that AWS is very customizable
Reliable	AWS has 80 availability zones and 25 geographic regions covered as the way it works is if there are availability issues, another available zone from other region able to replace it.
Scalable	It is very scalable as it can be easily tweaked and customize the settings.
Strict data security	The core infrastructure of AWS is that its complies and adheres to 90 security standards and certifications

Based on these key points in the table above it is denoted that these are the reasons why most organizations such Netflix, Twitch, Facebook, Linkedin used AWS. Amazon Web Services is one of the largest infrastructures as a Services (IaaS) and platform as a Service (PaaS) as for now. This can be seen from Statisa, where the quarterly revenue of AWS in 2014 goes from $1.05 billion to $9 billion in 2019 and it's expected to increase more now based on report around $24.2 billion in 2023.

2.0 Objectives & aim of study.

The objectives and aim of the study of this assignment is to conduct the research on how cloud computing providers such as Amazon Web Services able to mitigate the risk of urban flooding in environmental sectors. The learning outcomes of this assignment is to debates and do detail discussions on how digital transformation, Industrial Revolution 4.0or digital twins able to drive the adoption of cloud computing. Other than that, is analysing the cloud computing infrastructure and models where the concern is mainly on the security issues, privacies and management issues in an organization or company.

3.0 Problem of Statement

The problem statement of this assignment is that recently many companies and organizations experienced a huge and drastic change in their IT landscape as the ICT industry has been growing tremendously and hence cloud infrastructure services is a must adoption in their IT business. This can be seen that cloud computing able to impact and influence many domains such as agriculture, construction, tourism industry, cybersecurity, Artificial Intelligence and Machine Learning, Urban development, scientific research, creative industries, social impact sector and many more.

This is due to cloud computing able to offers flexible scalability, business agility, high availability and also provide cost reduction. Its widespread adoption recently in diverse industries and sectors shows that it has the potential to revolutionize and change many operations and also enhance efficiency. This also allowed company to utilize cloud technology to empower organizations and to leverage cutting edge infrastructure while paying only for the resources that they only need to utilize.

Flooding has been major issues that ravages lot of country, industry, and infrastructure that cause billions of lost every year. It has been ongoing issues lately where major cities in the world suffer from draining due to excessive raining and improper drainage system that worsens the problem that happens. The definition of urban flooding is that it happened due to inundation of land structures because of these problems which are excessive rainfall and improper drainage system. There is a difference between urban flooding compared to rural areas that in village or small town, the overflowing of water can be easily absorbed by soil and flow of the water can

be channelled into natural water bodies. This is very different in the city landscape where most of the surfaces are impervious such as concrete where it unable to absorb water effectively.

Figure 2

Hence this assignment requires to investigate the impact of cloud computing in environmental management sector especially mitigating the risk of urban flooding.

4.0 Body & Outcome of the assignment

In this section it consists of several topic where it is one of the major components of this report where the main topic is structured by headings and subheadings. It is known that the domain chooses for this assignment is environmental management as the main topic or title for this assignment is “Cloud Infrastructure Services In Urban Flood Management System”.

These issues happen or occurs when company tried to adapt cloud infrastructure services to ensure their business or organization run smoothly without any interruption on daily basis. Another learning outcomes is that to conduct assessments and study on how multiple aspects of cloud such as applications, services and orchestrations and modern infrastructure. This includes the physical, virtual and software defined infrastructure. The body of this assignment consists of the conceptual framework of the cloud adoption in the domain of environmental management as shown in subheadings below.

4.1.1 Conceptual Or Theoretical Framework of the cloud adoption in environmental management including introduction into cloud computing.

This section consists of six major key components or the assignment requirements that are used in the cloud technology for environmental management such as

1. Introduction to cloud infrastructure services in the domain of environmental management.
2. Cloud computing roles in the domain of environmental management particularly in flood management.
3. The suitability of various cloud services and deployments model for the flood management system.
4. How the various cloud services features such as scalability, automation, efficiency, and availability influenced the flood management system.
5. Critical review of the features available of the Amazon Web Services to enhance and facilitate the performance, innovation, and transformation in flood management system.
6. The potential of challenges that might occurs utilizing cloud services in the flood management system in terms of security and privacy concerns and other management related issues.

Figure below shows in general how the conceptual framework of cloud computing in environmental management.

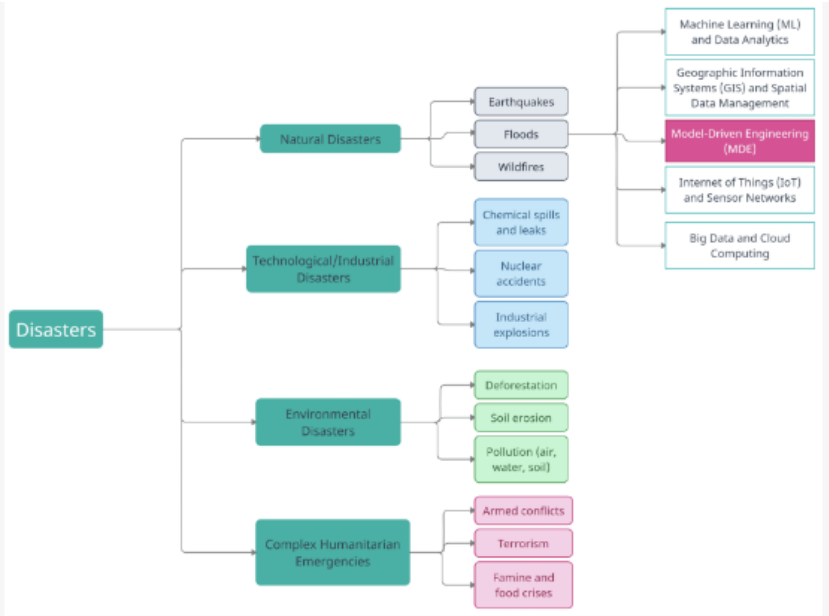


Figure 3

Cloud computing

The definition of cloud computing is it's a model that enable convenient and on-demand network access to a shared environment of configurable computing resources for example such as servers, networks, services, applications, and storages. (P. mell and T. Grance,2011) This model can be provisioned easily with little management or the need to interact with service providers. It can be said that cloud computing adopts the technology of internet based where it offers processing powers storage capacity, business applications and more to clients (Haynie, M, 2009). This is a game changing technology where the consumers and users can use it everywhere whereby the software and hardware are easily accessible where on demand access across network is feasible without use of device or location (Marston, S, Li, Z, Bandyopadhyay, S, Zhang, J. and Ghalsasi, 2011)

Table below shows the differences between traditional IT vs modern cloud computing.

Table 2

Traditional IT	**Cloud computing**
It is very expensive	Less expensive
IT resources are owned and managed	Rented as a service
Underutilized resources where unused services are being charged	Provide utilization and hence allow business agility
It is designed for peak usage	Resources consumptions are metered
Required loading time to load the resources	Provide on demand access everywhere anywhere
Usually does lack support business that require agility	Self service provisioning of resources

Based on the information from table above it can be concluded that characteristics of cloud computing are it provides on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured device. Some of these features provide shows that cloud technology offers a portal for example in AWS catalogue where users can specify their request on cloud services, and this shows that cloud computing offers flexibility. Other than it offers broad access network where the cloud services can be accessed everywhere over a network. Resource pooling on the other hand, is a situation where cloud suppliers provide a temporary expendable service to multiple tenants, customers, and clients (Www.naukri.com, 2024).

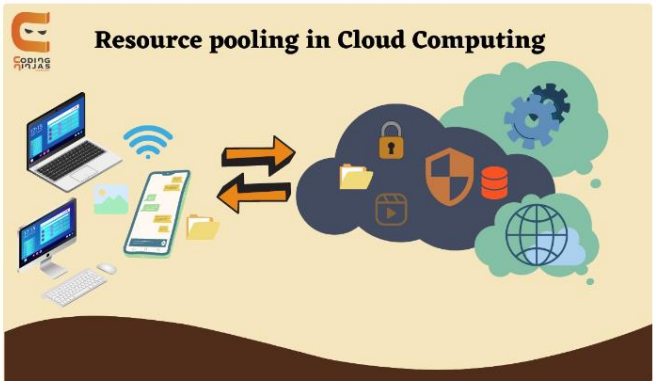


Figure 4

Figure above shows resource pooling where service providers use multi-tenant model with different physical and virtual resources assigned and reassigned based on customer demand. Multiple tenancy indicates that same hardware is shared between multiple users as these resources is high. This can be seen in AWS where it has its own regions, availability zones and data center from all over the world and each availability zones are designed 100km away from each other where if one is impacted the other can still be operated as it acts as a backup plan and recovery. It also connected with low latency and high-speed fibre that allow fast transmission that enhance connectivity. Some of the resources in cloud environments are primary resources such as compute, storage, and network. Compute includes processing power, RAM, storage on the other hand such Dropbox, Google Drive and network is bandwidth.it

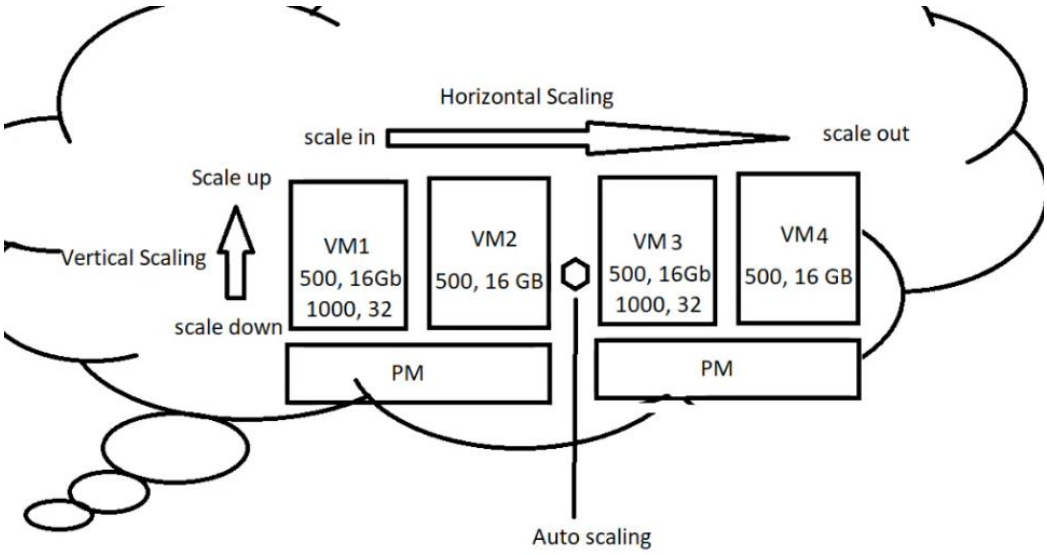


Figure 5

Figure above shows in resource pooling where there is two option which are vertical scaling and horizontal scaling. Vertical scaling refers to increase or decrease size and capacity of current resources such as virtual machines and databases. Horizontal scaling on the other hand

refers to adding or removing pooling resources such as instances and containers. Hence, all of these services are called auto scaling.

Rapid elasticity on other hand indicates how fast the application can be scaled up or down based on the demand or in other words indicates speed of scalability. Hence, organizations that want to use cloud services able to adapt variations in workload where for example an airline company has a website where for example it has 15000 daily users' traffic where it needed only 3 applications servers but during promotion day it has 1000000 where it needed 200 applications servers.

This create 197 application servers remain idle for whole year except the 3 days and hence cloud migration/cloud scaling and cloud bursting is the solution to solve these idle issues and cloud provide business agility. This shows that if an organization have more users it has to pay more and vice versa. The last one is measured services where the billing of the services used in cloud computing can be easily monitored and this allow transparency between provider and consumer and can be seen in AWS billing and monitoring.

Figure below shows some of the AWS Resources services where is it one of the key components in AWS. Amazon Web Services is one of the largest cloud computing platforms in the world offering more than 200+ resources from infrastructure to machine learning. (allcode,2023).

Figure 6 (BB Agency, info@bb. agency, & Slingerland, C. 2024)

Figure above shows the some of the AWS platforms in the AWS cloud services offered where the clients/users able to monitor the services. Some of the services are amazon compute EC2 where it is one of the first cloud computing services created in 2008. EC2 is a cloud platform that offers a secure and resizable compute capacity where the main objective is to allow easy access for web scale cloud computing.

Other services such as Amazon RDS (Relational Database Services) allow databases to be configured, managed, and scaled easily in the cloud. It is available in database instances where it is designed to be optimized for memory and performance and it provides databases such as Oracle, MySQL, SQL Server and more. This allows database migration from current database to Amazon RDS easily.

Other than that, is Amazon S3 where it is known as simple storage service and the type of storage it used is object-based storage. It is also known as object storage where the method used to manage data is by manipulating the data storage as distinct units called object (netapp, 2024). It also manages unstructured data in format named as objects and as most companies nowadays analyse and process huge amounts of unstructured data for example audio files, photos, email, sensor data and more (AWS, 2024a). Table below shows the difference between object storage, file storage and block storage.

Table 3

Object storage	File storage	Block storage
- Each piece of data is treated as its own object. - The data is stored separately with its own metadata	- The data is stored as individual pieces with folders. - It's called hierarchical storage	- It breaks down files into much smaller blocks of data. - It stores each block separately. - Each block was given unique addresses

Amazon S3 provides data availability, scalability, performance, and security as it is suitable to be used for business to protect their business property such websites, storage backups and applications. Amazon Lambda is one of the serverless computing service where it allows organizations to run code without ever to own or manage server. Amazon VPC is also known

for as Virtual Private Cloud where it allows AWS resources at a scale in a virtual environment. This allows the organization to choose own IP addresses, create own route tables and network access point.

Hence figure below shows the figure of object-based storage system, file-based storage system and block-based storage system. It is known that some of the most common cloud storage systems is AWS s3 and for example each storage has features available on AWS where for File it uses Amazon Elastic File System (EFS) that able to operate on cloud and local storage. It provides Standard Storage class where the EFS throughput is more than 10GBps.

For block storage it used Elastic Block Store where (EBS) where it complements well with Amazon Elastic Compute (EC2) and for object base storage it uses Amazon S3 (Simple Storage Service) where it said to have 99.99% annual durability or 11 nines availability.

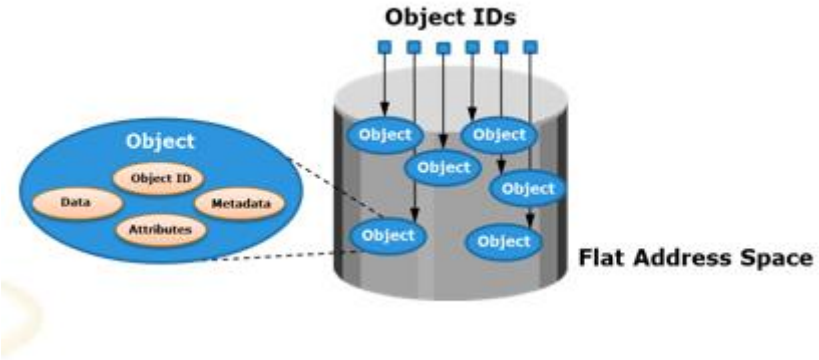


Figure 7 : Object based storage system.

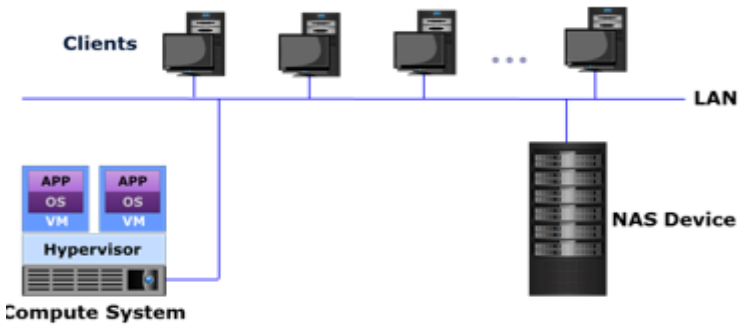


Figure 8 : File based storage system.

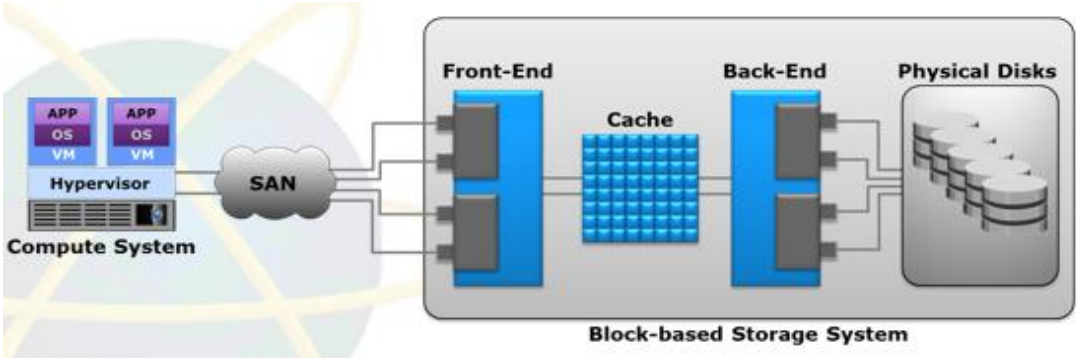


Figure 9 : Block based storage system.

Table below shows the other options of using cloud storage besides AWS such as Microsoft Azure and Google Cloud Platform.

Table 4

	Microsoft azure	Google cloud platform
File	Azure Files: It uses SMB and support concurrent file sharing. The maximum storage capacity is 4PB, ungress 25Gbps and egress 50Gbps.	Cloud Filestore : Google Compute Enginer and Kubernetes offer NAS Standard : 1TB to 10TB and provides a read throughput of 180MBps and 1000 IOPS Premium 3.5Tb and provides a read throughput of 1,2GBps and 60,000 IOPS
Block	Azure Disk: Provides managed disks for Azure virtual machines. It provides 59 availabilities. The Ultra disk has maximum disk size of 65,536 GB. The standard disk from 160, 000 to 32, 76Gb	Persistent disk block: It runs up to 64TB and offers - Persistent disks - Persistent SSDs - Local SSDs - Nvme Storage

Object	Azure Blob : It offers petabyte scale storage with 16 nines availability	Google object: The main storage tiers - Standard - Nearline - Coldline - Archive

Object storage: It is used for applications that stored huge amounts of data where this system is the basis of services such as Dropbox, Facebook file system.

Block storage: It is related to the growth in cloud-based virtual machines where some of the examples are Azure Disk that works with Azure VMs, Google Persistent Disk that works with Google Cloud VMs and Amazon Elastic Block (EBS) works with Amazon EC2.

File storage: File based storage able to gives flexibility on where the data is located and for example Amazon EFS is orchestrated to combine cloud and on-premises volumes but also brings flexibility of the cloud.

Amazon web Services

Some of the features in AWS is IAM it allows the user to have access to AWS account where the main role of Identity and Access Management (IAM) is for authentication, and it is known as root account that hold administrative rights to all of the accounts. AWS IAM categorized into identity based and resources based where for identity based its managed user, group, policy, and roles meanwhile for resourced based it manages access to service to amazon s3 storage for example.

IAM allows users to have IAM programmatic access where it allows the cloud subscribers to interact with the resources such as AWS tool kits, AWS CLI, SDKs, and command line in which the users can do automated tasks and manage resources. AWS CLI is a command line interface in which the AWS resources can be managed using scripts and its suitable to handle large scale deployments. AWS CLI allow to support services such as S3, EC2 and Lambda. Other than that, is AWS management console allow the control of IAM users access where all of the resources can control, monitored, and allow which users can have access to the resources such as EC2 instances, Amazon S3 bucket and more.

The AWS management governance consists of IAM authorization where it uses the principle of least privilege. Least principles are one of practices done in AWS where it is a principle of

only granting certain access to a feature to complete a task. For example, user 1 only can have read only access to s3 support meanwhile user 2 only has read only access to EC2 support and user 3 able to view, start and stop EC2 admin.

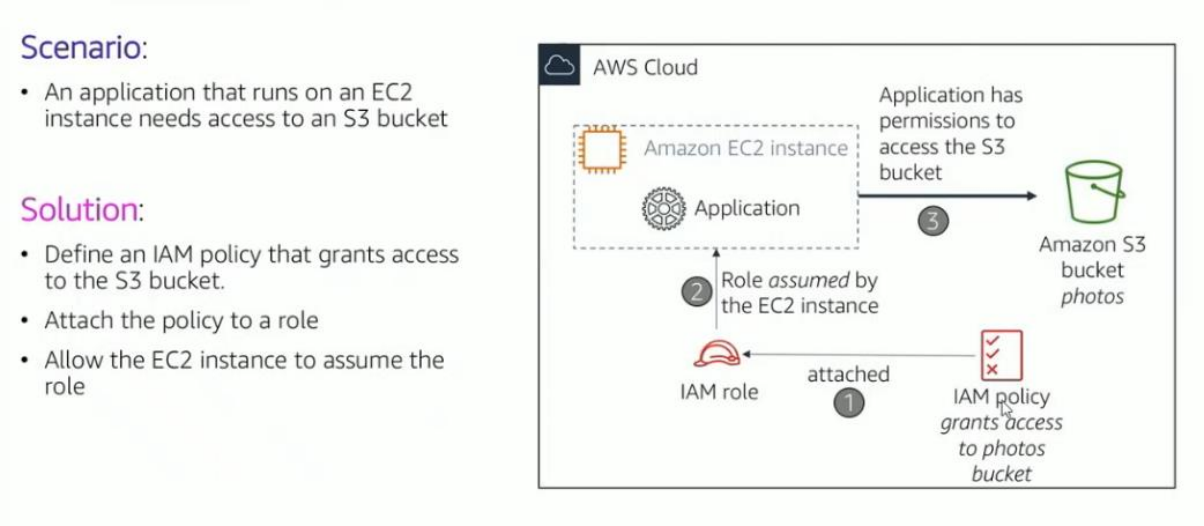


Figure 10

Figure above shows the demonstration of least privilege where IAM policy grouped into IAM entities such as user, group, and roles. Other than that, is IAM access account where for IAM user it represents people who uses this service to interact with AWS. The IAM user account can be accessed by following.

1) Stop using account root user: Not recommended and for single AWS account user with administrator access is preferred.
2) Enable multi-factor authentication (MFA): to provide more security to the user account.
3) AWS cloud trail: It allows to do risk auditing, compliance, and governance of AWS account where it allows event recording using console login which recorded through log message and File Login through saving log messages.
4) Billing report: To monitor cost and usage of AWS services such as EC2 instance compute.

To secure and manage multiple AWS accounts, AWS organizations can use OUs organizational units where it can greatly manage the accounts. It uses service control policies where it can manage various accounts where it is quite similar to IAM in which it has centralized controls and some of the features using AWS KMS, AWS cognito and AWS shield. Below shows the table of some of aws features.

Table 5

AWS KMS	Key Management services is that allow easy control to protect user data using keys and it can easily integrated AWS Cloudtrail
Amazon cognito	It's a platform provides access to mobile and web apps
AWS shield	It provides protection from DDOS attack and able to minimize application downtime and latency.

Other than that, is AWS compliance programs where it provides information about the policies where it able to help organizations to understand better about how AWS able to maintain security and compliance in the cloud. The IT standards can be categorized into

1) Certifications & attestations
2) Laws, Regulations & privacy
3) Alignments & frameworks

AWS config allow the access to AWS account where it is a service that allow to assess, audit, and evaluate configurations of AWS resources. Some of these resources are EC2, EBS, VPC and more. Detail explanation on VPC (Virtual Private Cloud) will be explained further. On the other hand, AWS artifact is a service where it provides on-demand downloads of AWS security and compliance documents and hence its act as a resource for compliance related information.

VPC

VPC stands Virtual Private Cloud where it allows to create an isolated section of the cloud where resources such as virtual machines (EC2 instances), databases, web application server and more. Amazon VPC can be used where it acts as traditional virtual network where the main essentials of VPC is that it can go across multiple availability zones (AZs) but VPC cannot go beyond regions. For example, 1 VPC cannot have 2 regions, but it can have only 1 region and multiple AZs.

Subnet is a range of IP addresses in the VPC where the subnet can be connected to internet, route traffic and routes tables where each subnet is for one AZ and on the other hand, CIDR range represent the VPC IP range where it is also an allocation method that significantly improves data routing efficiency. Each subnet takes a subset of VPC range called subnet range and public subnet usually has direct route to internet gateway (public internet) meanwhile private subnet do not have access to internet gateway. Below shows the VPC and subnets

explanation and when VPS was created the IPV4 CIDR block must be specified where large block size has /16 netmask meanwhile /28 for smaller block size.

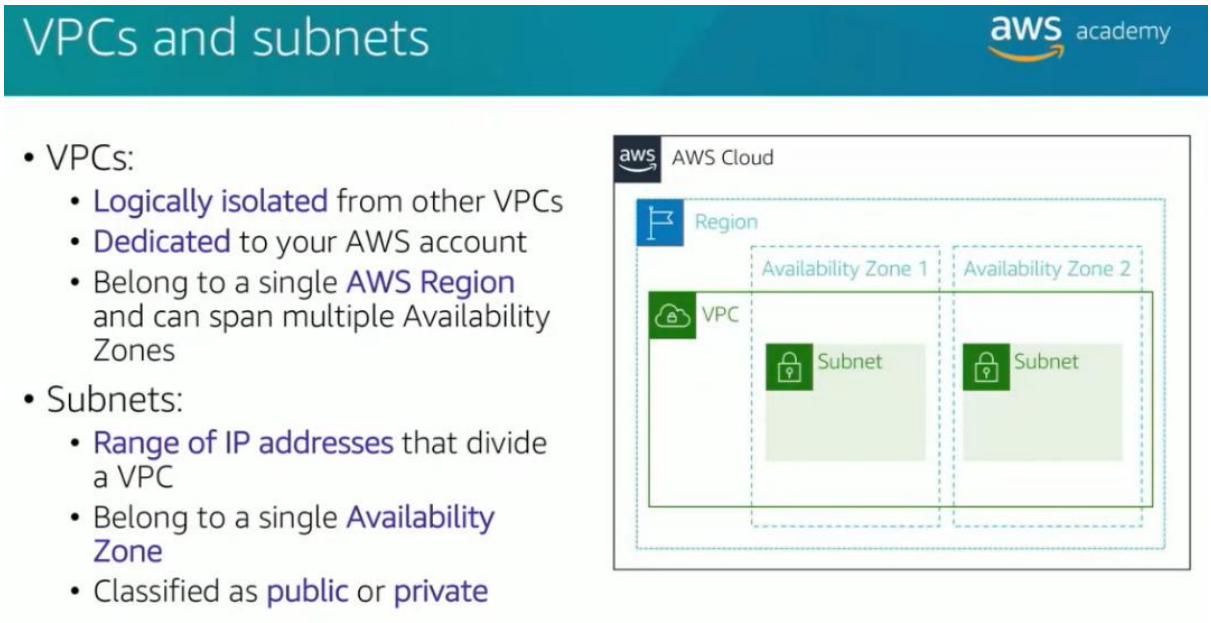


Figure 11

Public subnets are connected to route table which connected to internet gateway where route table comprised of routes that able to determine the network traffic from subnet or gateway directed. Internet gateways allow communication between VPC and the internet.

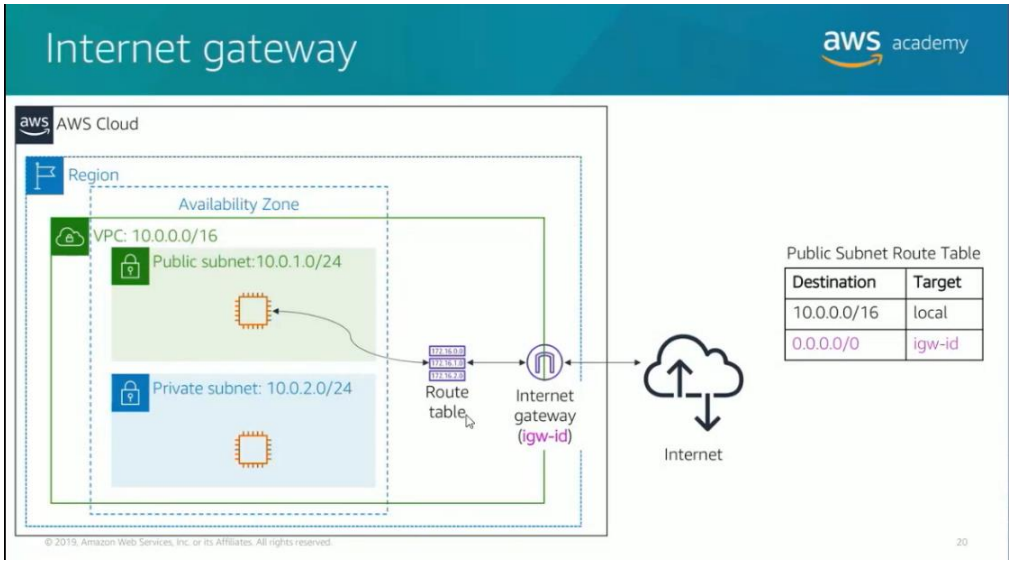


Figure 12

Figure above shows the connection of public subnet to route table and eventually internet gateway and figure below shows the connection of private subnet to private NAT gateway. Both of the private and public NAT gateways map the source private IPv4 address of the

instances to the private IPv4 address of the NAT gateway. In a nutshell, the internet gateway routes traffic from private subnets through the public NAT gateway, using its associated Elastic IP address to represent the traffic on the internet.

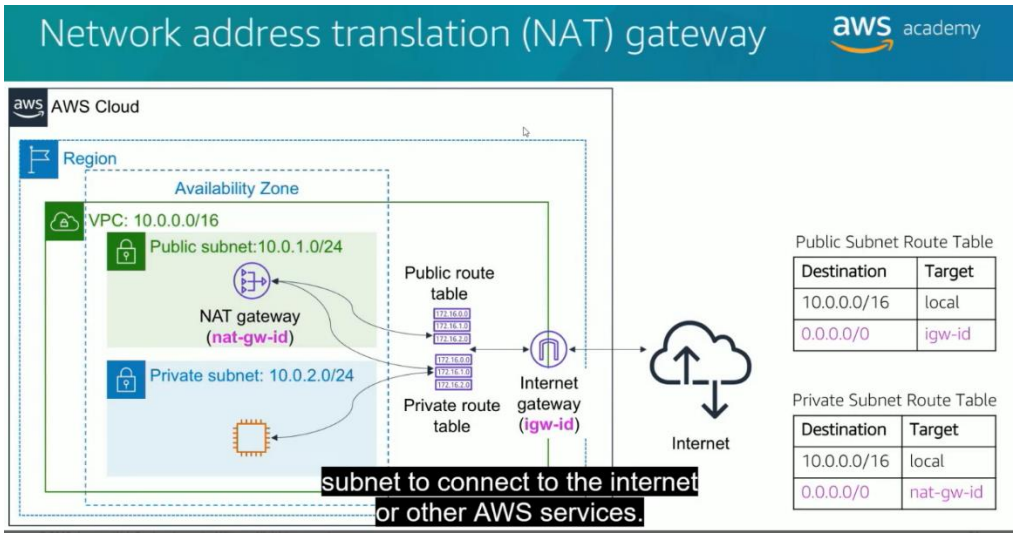


Figure 13

Figure below shows the private subnet and public subnet where for private subnet it is connected to EC2 instance and RDS instance and for public subnet it is connected to NAT gateway, EC2 instance and Amazon Redshift. The basic of NAT gateway is that it is a Network Address Translation (NAT) that allow instance in the subnet to connect with services outside of the VPC network.

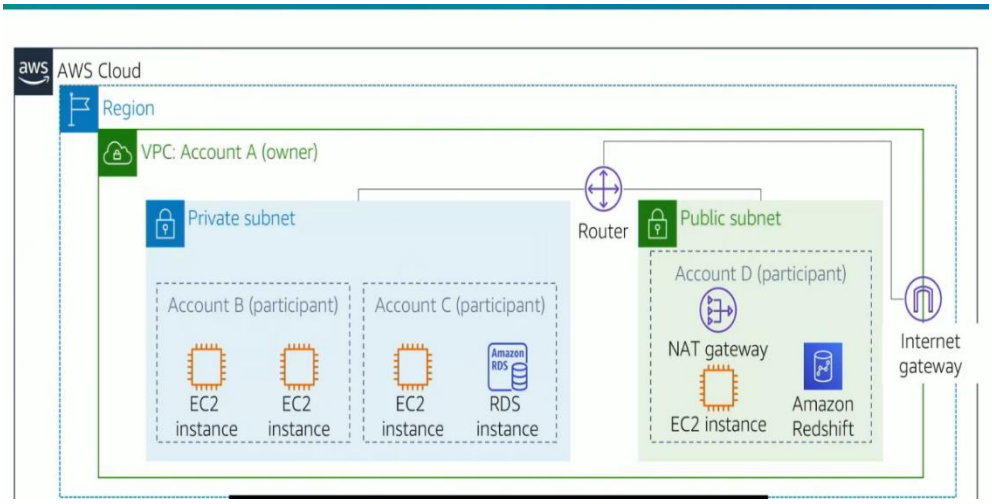


Figure 14

Figure below shows the VPC peering where it is a peering connection links two VPCs, allowing traffic to flow between them using private IPv4 or IPv6 addresses. This enables seamless communication between instances in both VPCs, as if they were part of the same network.

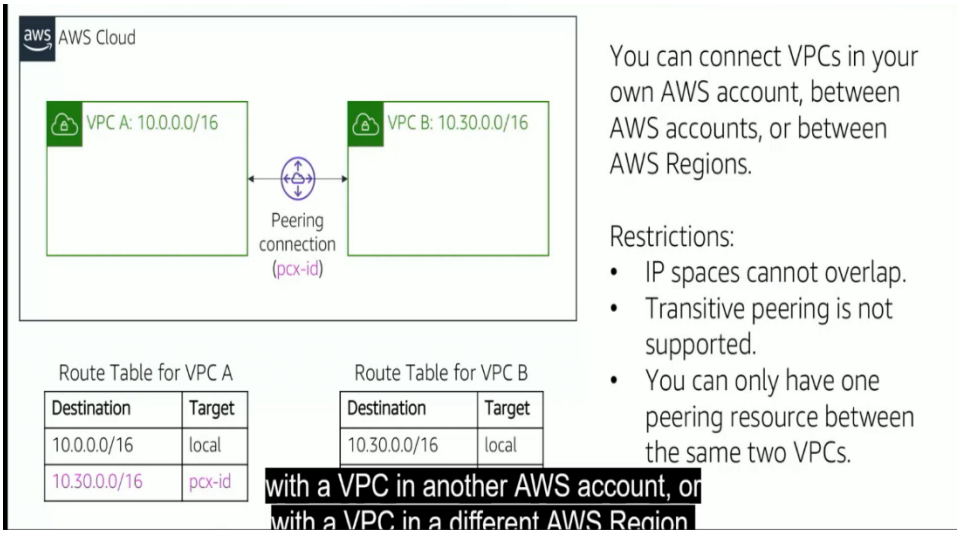


Figure 15

VPC endpoints on the other hand allow organizations or users to securely connect to AWS services and VPC endpoint services powered by AWS PrivateLink.

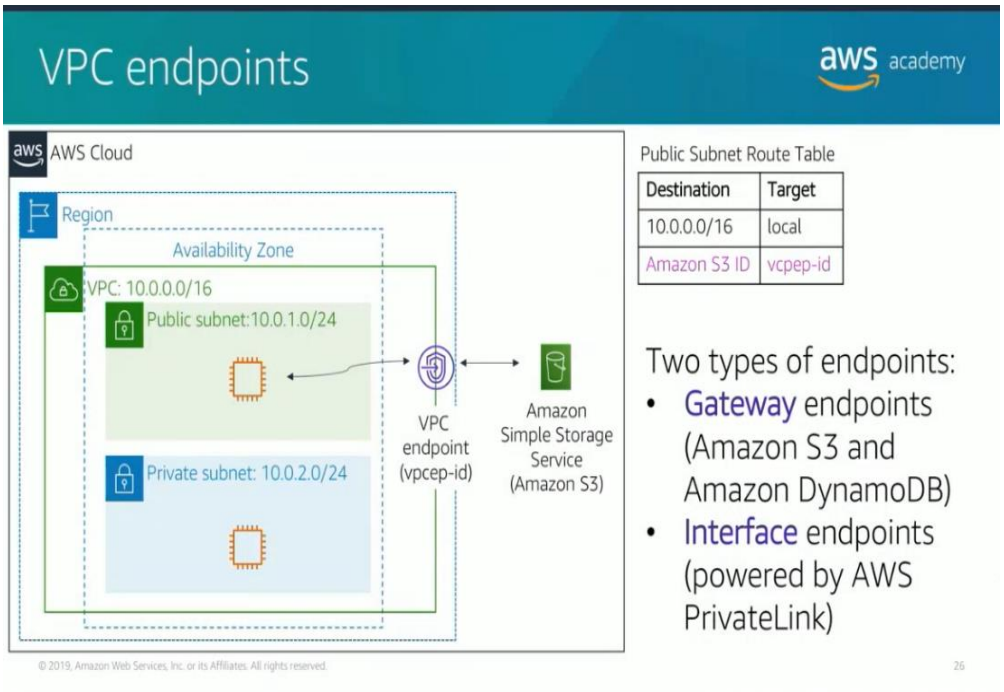


Figure 16

Figure below shows the complicated networks of VPC where later it can be simplified using AWS transit Gateway where it can connect to on-premises VPC networks where it can simplify connectivity and reduced the complexity of peering relationship.

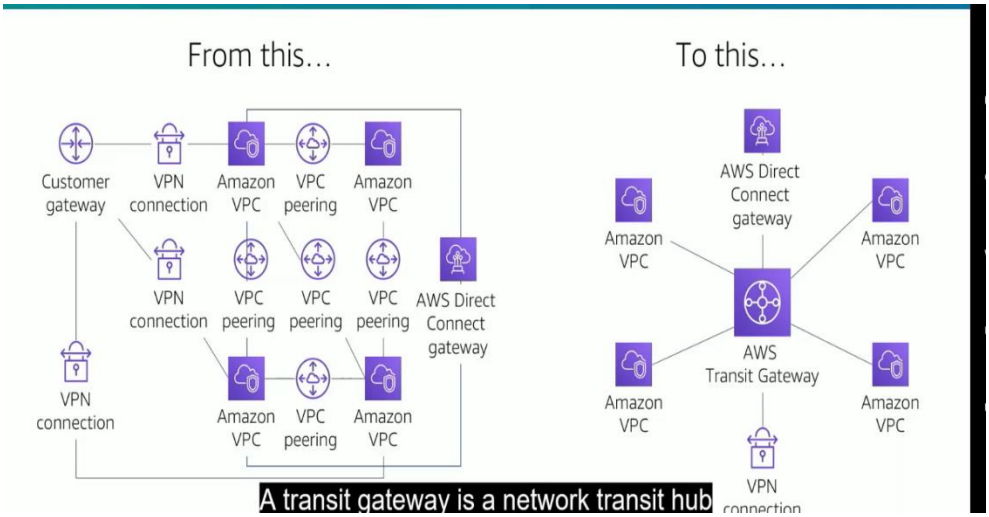


Figure 17

4.1.2 Introduction to cloud infrastructure services in the domain of environmental management.

There are so many domains where cloud infrastructure can be implemented where in this case the topic selected is environmental management. The introduction part discusses the brief overview of environmental management, its key components and challenges it is facing. The risk of urban flooding can be categorized under environmental management but this part here is to discuss environmental management in general.

Environmental disaster is a very important topic needed to be addressed and that's the reason a lot of effort initiated by companies, governments agency and organizations to combat these issues. In the domain of environmental management, Geospatial data are widely used to mapped the terrain or the city landscape identify the geographical image of certain areas, and which is able to identify the sources of water overflowing or clogged drainage. A lot of research models had been carried out to integrate the use of technology such as ICT in Geospatial data for disaster management where figure below shows the 6 main components of ICT. The 6 main components of ICT are cloud computing, software, internet access, hardware, transactions, communications technology, and data.

Figure 18

Many challenges in Natural Disaster Management (NDM) where lot of models has been created to predict the risk of natural hazard disasters such as wildfire spread model (Prometheus, 2018), a flood spread model (R. Cohen, J. Hilton, S. Hasan Khan, Y. Wang, M. Prakash,2015) and another one is a landslide prediction model or Landslide Hazard Assessment for Situational Awareness (LHASA) model (G. Schumann, D. Kirschbaum, E. Anderson, K. Rashid, 2016). There are some challenges in geospatial science such as network, storage, and computation and hence cloud computing able to solves this problem as geospatial data over the years has become very data intensive as in need to servers that able to collect, stores, process, analyze and simulate data 24 hours a day across various regions.

This resorts into cloud computing as combination between natural hazard model with geospatial become more complies as traditional IT services can't keep up with more complex algorithms created in NDM. Cloud computing provide some of the features such as resources pooling and its also doing software integration between physically distributed computing with recent computing technologies (Q. Huang, J. Li, Z. Li, 2017) Based on previous discussions regarding the essential characteristics of cloud computing, this adheres to the demand of geospatial and NDM as it able to provide on demand and elastic access to various resources. These resources include storage, computational storage, network, and application servers and hence indicates it provides availability, broad network access, scalability and more. Below shows the core pillars of geospatial technology where cloud computing can be utilized and where in this sector it used sensors, advanced information collecting techniques, Iot devices and more.

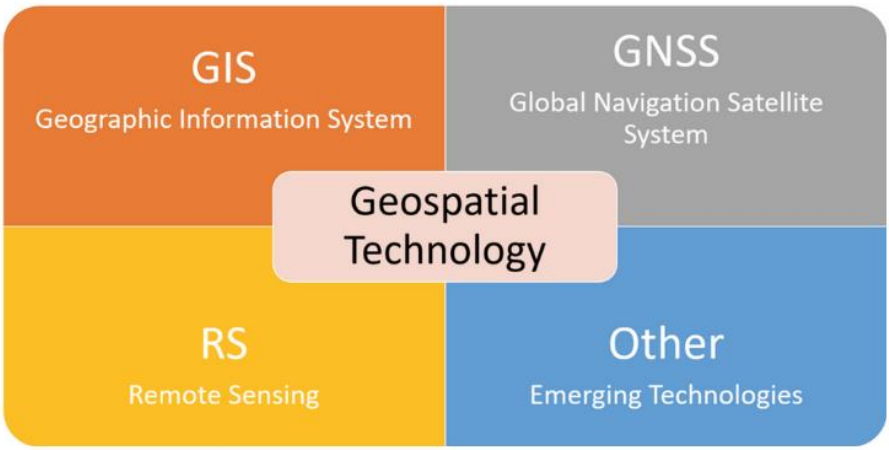


Figure 19(Connect, C.-C. E.2021)

Natural disaster management is an ongoing issue faced by many countries and hence authority's figures are trying to implement techniques to mitigate the risk and reduce the dangers of natural disasters such as flood, wildfire and more. There is an approach developed to mitigate natural disaster management which is called PPRR framework where it stands for prevention, preparedness, response, and recovery. Figure below shows the approach to mitigate natural disaster management.

Figure 20

Prevention refers to early mitigation solutions to prevent any possibilities of natural disasters that might happened to a certain area. For example, in environmental management, water overflowing from a dam happened due to unpredictable weather and cloud computing able to

help create a digital twin's ecosystem where multiple SCADA system control in dam connected with cloud platforms able to communicate directly and provide live streaming to the control room and hence able to create trigger warning. This eventually will create an environment where it can mitigate the risk of overflowing of water of dam where it can create dangerous situations to surround area and worst-case scenario cause urban flooding in city Centre.

Hence digitalization needed to be applied in water management system where digital twins' technology able to be apply in water dam to ensure much more efficient water management system using data driven solutions along with cloud computing. This can be seen in some research where it uses Google Earth Engine Cloud Platform to study the changes of water surface area in certain geographic regions. (Huang, S.; Chen, X.; Ma, X.; Fang, H.; Liu, T.; Kurban, A.; Van de Voorde, T, 2023).

Other than that, is Web GIS platform can be deployed to do monitoring of water resources where it allows exchange of information using internet access in which adhere to the characteristics of ICT. (Hasan, M.A.; Abed, F.H, 2023). In other domain for example, in agriculture it uses blockchain technology and IoT to help achieve smart and efficient water management resources (Zeng, H.; Dhiman, G.; Sharma, A.; Sharma, A.; Tselykh, A, 2023)

Other than that, is preparedness where if the natural disasters can't be contained or controlled, it resorts to getting information from the disasters to reduce the impact that will happen. For example, in the case of earthquakes getting an open space as a temporary place as shelter is one of effective method. Response on the other hand, happen during natural disaster happen where authorities' figures gather data from live streaming where later on it is examined to carry out much more effective response. The last part is recovery where it happens in post disaster where records of damaged happened must be documented where assessment needs to be done and evaluate for cost of repair and damaged.

4.1.3 Cloud computing roles in the domain of environmental management particularly in flood management.

This part here is to discuss how to effectively deploy cloud solutions to address challenges faced in adopting cloud solutions to solve environmental management issues. Various countries all over the world faced flooding issues where some of the root causes of this are climate

changes that result into natural disasters such as ad urban flooding, landslides, drought, and wildfires (Dhar O, Nandargi S, 2003).

Urban flooding or flooding in general has been an ongoing issue where a lot of issues related to hydro dam power plant suffer from overflowing of water increased lately in Asia and South-East Asia. Hence many developing countries suffers from this climate change issues where several countries such as China, India, Pakistan, and Bangladesh hugely affected by the flooding. (James E ,2008)

Urban flooding usually happens in crowded or densely populated area such in the city where these floods are caused by flash floods, river floods, coastal floods, and improper drainage design. It is one of major global issues that contribute to greenhouse gas emissions where towards the end causes global warming. There are other factors that contribute to urban flooding, where overdevelopment in the city area such as building more high-rise apartments, offices, and residential housing with more migration from town to urban area leads to this issue.

In Malaysia where, the country that located near the equator received massive amount of rainfall every year where it is on the third place on the world ranking receiving 3387mm of rainwater just behind the Palau and Micronesia. It is also known that any country that is located near the equatorial climate receives on average every year around 250 cm rainfall (Department of Irrigation and Drainage (DID), 2007) and hence this also contributed to urban flooding issues.

Cloud computing in general is a model that allows users to access computing services virtually without needing to manage the infrastructure physically where these services include storage, network where it is rented as a service. Usually in software services the cloud providers the software application to the users, organizations, or consumers over the internet. (Chandramohan, J & Ramasamy, U, 2023). Cloud computing requires over the internet access as usual by agreeing to use any vendor of cloud services provider the company data are stored in offsite data centers which the application can be used online.

It also allows scalability where the organization can scale computer resources as it meets any business that demands cost effective solutions for their organization (Ram, M., Selvabaskar, S., Guhan, R., & Rajarathi, K. , 2023). Another benefit of cloud computing is it offers efficiency as it allows organizations to shared resources and services which can reduce waste and better resources utilization (Ghasemi, M., Rajabi, M & Aghakhani, S., 2023). The table below shows many more benefits of cloud computing simplified in table format.

Table 6

Advantages	Explanation
Provide business agility	- It allows faster and quicker resource provisioning. - Accelerate innovation.
High availability	- Provide on demand resource availability based on consumers' needs. - Allow fault tolerance
Increased collaboration	- It allows easy collaboration which allow faster exchange of information
Simplified infrastructure management	- Organizations only used resources that are required to access cloud services
Business continuity	- Reduces the impact of downtime
Flexible scaling	- It allows scaling resources to meet demand such as unilateral and automatic resources scaling.

Cloud computing can be used in ICT for NDM where for example for a flood response a prototype of architecture of flooding response model can be created using Amazon AWS cloud where it can massively improve Geospatial service response to a flooding system. This method used mobile agent and cloud technology to response to any potential flood where the proposed method is able to avoid transfer huge amounts of geospatial or big spatial data. This results in more efficiency and optimization as by combining cloud computing and mobile agent the geospatial chain will significantly improve (X. Tan, L. Di, M. Deng, 2015).

Mobile agent is a software program that is autonomous and able to move through diverse networks where it allows execution from one machine to another machine. In layman terms, the role of an agent is that if the execution is suspended in one platform, it can be resume in another platform by continuing where its lefts. It is known that cloud computing is SOA play key role in integrating existing application into cloud services and between cloud where SOA stands for Serviced Oriented Architecture. The recent advancement of cloud services facilitates deployment of web services because cloud computing is known for its scalability, and

consistency of improving services and data which eventually improves mobile applications (Lomotey RK, Deters R, 2013).

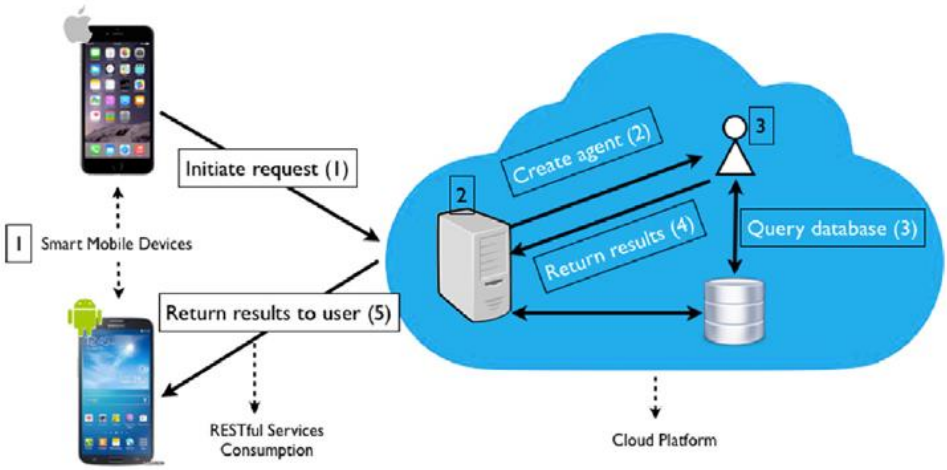


Figure 21 (A. S. Abdelfattah, T. Abdelkader and E. S. M. EI-Horbaty, 2020)

Figure above shows the mobile agent architecture where it shows the communication process between its components where figure above used middleware approach. It is known that middleware method introduces a gateway between mobile client and web service where it reduces all of the burden of heavy communication within the service. A fast binary protocol will be ignored as mobile client requires to sustain a simple client-server communication and a very lightweight one (He Yejun, Salih Omar S, Wang Cheng-Xiang, Yuan Dongfeng, 2015)

Hence, based on the previous information regards to mobile agent it shows that mobile agent can be integrated with cloud services as shown in figure below that denotes the architecture of flooding response model using cloud system. This method further optimizes the flooding response model where it used Yangtze River Basin in China to study the suitability of using cloud computing in flood response model. The hardware part is the upper tier of cloud computing architecture where it consists of CPU, GPU and network and storage is used to transfer huge amounts of data into the cloud which in this case is AWS.

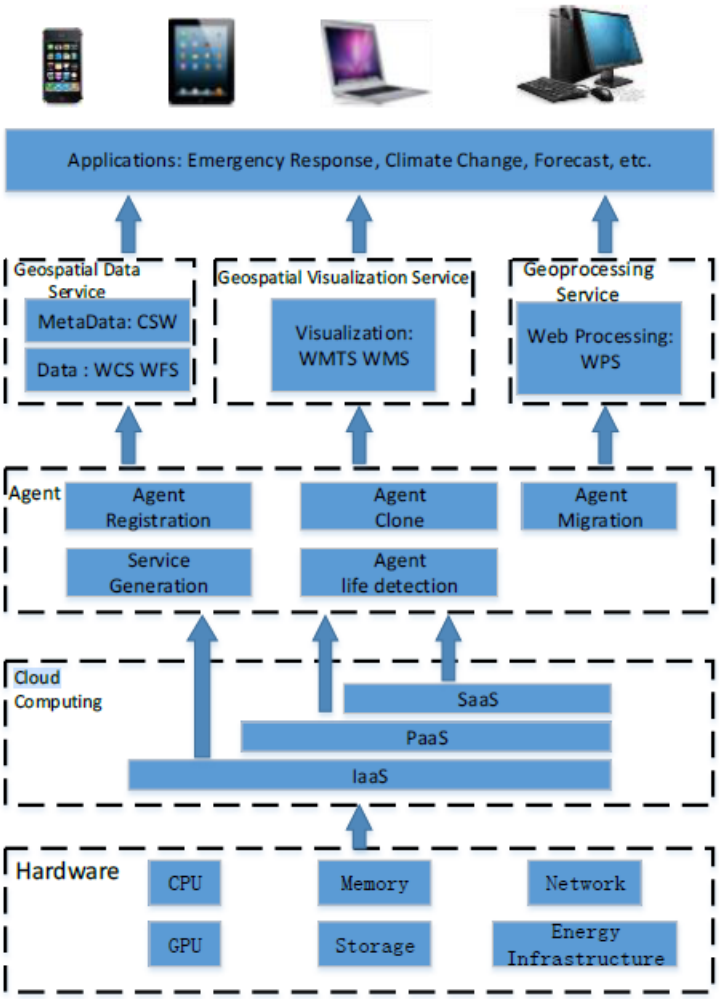


Figure 22 (Xicheng Tan, et al, 2015)

Further explanation on the agent and cloud geospatial service architecture for the flood response model will be further discussed in chapter 4.1.4 as it related to cloud services and deployment model.

4.1.4 The suitability of various cloud services and deployments model for the flood management system.

Before going into further detail of suitability of multiple cloud services it is required to understand the type of service models where in cloud infrastructure it can be categorized into three primary one which are Infrastructure as a service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

IaaS sits on the lowermost layer of cloud services where it provides cloud service ecosystem with virtualized and pre-configured hardware services. Amazon Elastic Compute Cloud (EC2) is one of IaaS where it provides networking services, virtualization, servers, and storage. Other software such as Apache Cloudstack is another example of IaaS.

PaaS on the other hand, it handles all the hardware-related tasks, including installing and updating the operating system, maintaining security patches, and offers a flexible platform for developers to create, test, and launch applications with various features. Some of PaaS solutions are Google Cloud platform and Microsoft Azure.

SaaS on the other hand, uses web-based services using the internet where the users have least amount of freedom in terms of flexibility of the hardware and the environment on which the services are running on. The providers of the services will provide maintenance, backup, and update where some of popular software existed are Gmail, Netflix and more. The table below shows the service models and their functions.

Table 7

Service Models	Functions
IaaS	Network, Compute, and storage
PaaS	App, development, integration, dashboards
SaaS	Events, task, services

It is known that there are many various cloud services providers and hence each different cloud provider would have a different approach to deployment model. For this assignment, the cloud services used are Amazon web services where in cloud computing the deployment model can be categorized into private, public, community and hybrid cloud model. Public cloud offers subscriptions-based model where any general public or organizations can has easy access to cloud services provider. The reason why most companies selected public cloud services is it has many advantages such as it is very cost effective, allows quick resource provision, provides ease of scaling and has better global reach.

This is in contrast to private cloud where its only entity is only dedicated to one organization where it does not shared with other organizations where there are 2 types of variants which are on-premises and externally hosted. On-premises clouds are usually deployed by an organization on its data center whereby externally hosted clouds outsourced its cloud to external providers. The payment method is using fee-per unit time, and the top reasons organizations choose private cloud is it provide more security and less risk than public cloud.

Community cloud is tailored for a business community that use cloud computing from cloud providers where businesses share the cloud infrastructure, but they have their own private cloud space to ensure common privacy, security, and compliance requirements are met within the

community. Hybrid cloud on the other hand, is where the cloud deployment falls between public and private, with sensitive and critical data stored in private clouds for maximum security, while other operations are conducted in public clouds. Hybrid clouds can assist businesses in cost reduction by offering choices to run services over the public clouds without needing to compromise sensitive and confidential data. There are certain examples of use cases of hybrid cloud where it can be used in cloud bursting, web applications hosting, application development and testing, and migrating packaged applications. Thus, it is very important to know the suitability of choosing what type of cloud services are used especially for flood response systems. The table below shows the deployment model and each of their functions.

Table 8

Deployment models	Function
Private	- Own or outsource. - Separate data center - Lease or buy
Public	- Very scalable - Available for all organization
Community	- Several stakeholders - Cloud for set of users with certain needs
Hybrid	- Combining public and private clouds. - Private cloud is more suitable with much more sensitive data.

In NDM, Natural Disaster Management, it is very crucial to understand what type of deployments model needs to be chosen, for example whether it is private or public cloud as each of it has their own advantages and disadvantages. For NDM, there is mixed usage of private and public cloud where the deployment of cloud services used in wildfire it used public clouds and for disasters and impact it used private clouds.

Hence based on figure 10 previously it shows the agent and cloud geospatial system for flood response model where cloud computing provides resources as a service across distributed networks. Within Infrastructure as a Service (IaaS), hardware resources like CPU, GPU, memory, storage, and network can be virtualized into virtual machines (VMs) or clusters, while disks can be transformed into network storage services.

Additionally, virtual network services such as Virtual Private Networks (VPNs) can be offered to support geospatial services. Platform as a Service (PaaS) delivers operating systems and basic cloud development environments to users. Through PaaS services, automatic adjustments to the number of VMs or the scale of virtual clusters are achievable and can be deployed immediately. Some of the SaaS software used on the cloud such as Geoserver, 52 north using cloud services where later on after the cloud computing, at the agent tier it provides components such as registration, clone, migration, generation, and life detection where each of these agents communicate with one another.

Later it communicates with geospatial tier where it includes geospatial data service, geospatial visualization service and geoprocessing services where it is all converted into the agent tier. These services are designed based on the OGC specifications which is one of the standards for Data encoding, Data access, Data processing, Data visualization, and Metadata and Catalogue services. (Standards, 2024) This causes the geospatial services to have good interoperability and can be combined in a standard form. Eventually, it reaches to the application tier platform where it used the combination of geospatial services whereby some of the applications are emergency response, climate change and forecast which indicates the endpoint user of cloud computing in geospatial services.

4.1.5 How the various cloud services features such as scalability, automation, efficiency, and availability influenced Natural disaster management or flood management system.

This part here is to discuss on how the cloud infrastructure features such as scalability, availability, automation are able to help improved flood management system. It is known in geospatial services that cloud computing features such as scalability, availability and more able to addressed the complex data, storage, and processing for energy information management (D. Liu, Y. Wang, L. G. Liu, 2013).

Another characteristic of cloud computing is that it provides automation where for natural disaster management, it requires real-time live monitoring solution to solve data dependent problems and provide on-demand services to fluctuating number of ends users (Q.-q. Li, T. Zhang, Y. Yu, 2011). In terms of availability cloud computing able to help predict the availability of water and the spread of natural risks (B. Behzad, A. Padmanabhan, Y. Liu, Y. Liu, S. Wang, 2011). There are several challenges to implement NDM such as it is very compute intensive, data intensive and concurrent access intensive where cloud computing able to address these challenges.

Computational power is one of the crucial factors in natural disaster management especially to simulate or forecast flooding and thus cloud computing able to provide much accurate predictions without need to invest in expensive hardware devices. It is also known that in geospatial data it deals with huge amounts of datasets especially in natural disaster management such as water management system, urban flooding, earthquake disasters, wildfire and more. (D. Cui, Y. Wu, Q. Zhang, 2010)

There is a real-life application of using AWS in real time inundation of flood mapping where a company called FloodMapp utilizes cloud computing to forecast flooding happened in Houston, Texas, USA. The help of cloud computing which in this AWS is able to solve the problem in which the traditional technology cannot be due as the mapping unable to be scale and run in real time. There are few reasons and challenges occur in flood forecasting where the first reason is in order to predict the rainfall and weather, a meteorological solution needs to be executed. Another reason is the model need to be simulated with hydrology model with other inputs such as height, elevation, catchment areas and the last one is to produce forecast map of the flood from the previous stages.

This shows that flood forecasting is very complex process and in general natural disaster management requires especially in the domain of environmental management such water management system or urban flooding requires huge computational power and sources to simulate. For example, traditional computing requires 600 hours to simulate of $500km^2$ of catchment area model. This company uses AWS to create a massive scale of data pipeline where AWS able to launch billions of data where it able to host large scale data pipeline using solutions such as AWS Batch and ECS services (FloodMapp Leverages AWS for Real-Time Inundation Flood Mapping to Save Lives and Assets | AWS Startups Blog, 2020). Figure below shows the case study of simulation terrain used to simulate using AWS cloud infrastructure services.

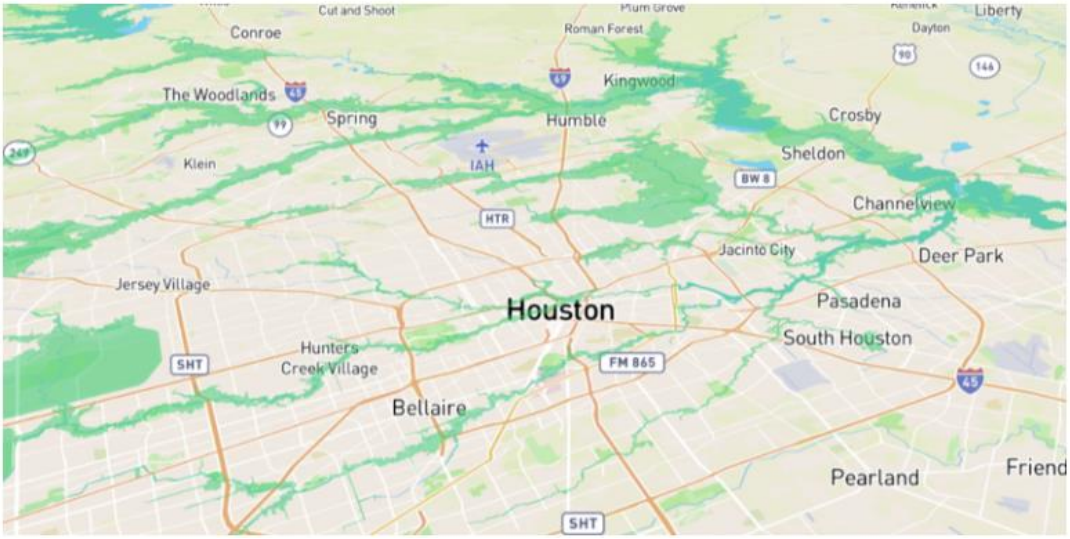


Figure 23

Below shows how the desired solution of cloud bases solution comprised of how the various cloud features such automation, scalability, optimization and more able to help with natural disaster management. The desired solution can be divided into 3 categories which are user interface, control mechanism, and cloud infrastructure where each of it comprised of features of cloud computing that needed in natural disaster management.

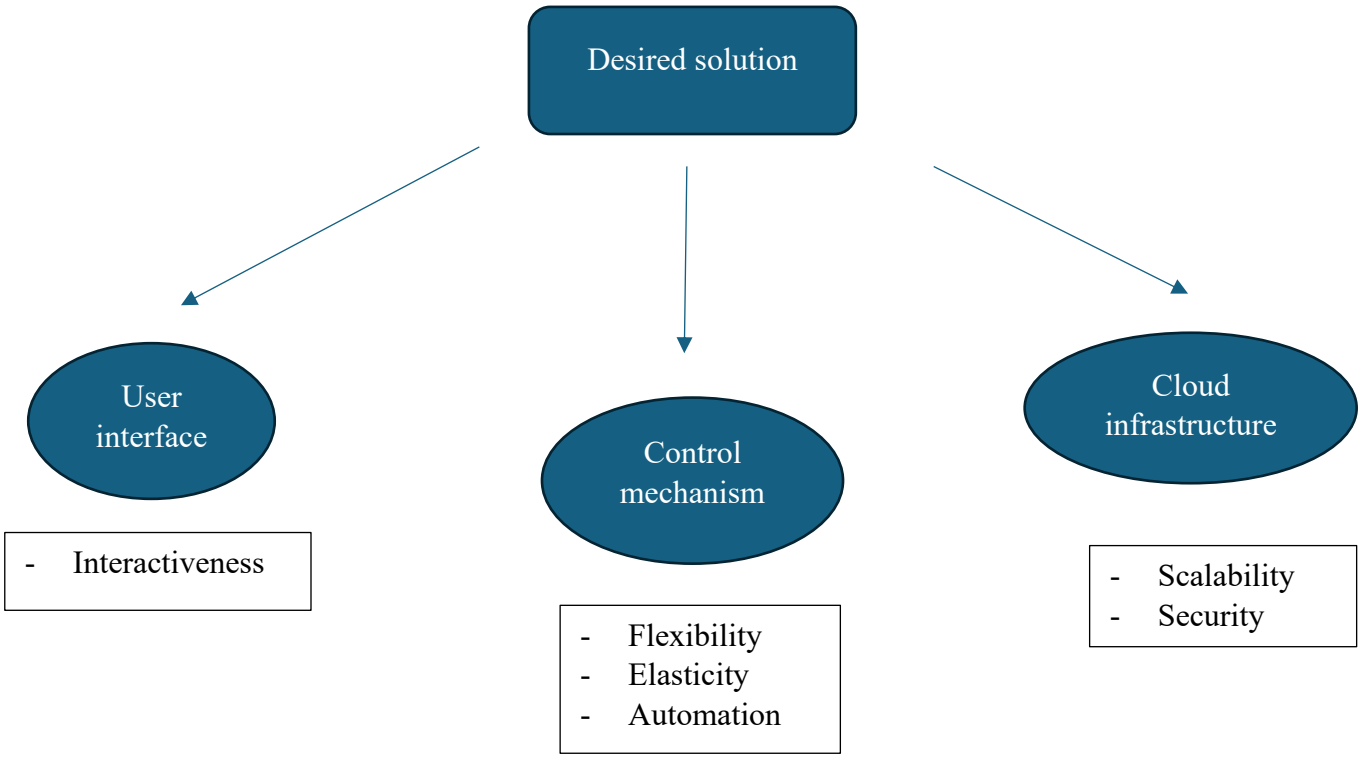


Figure 24

For example, user interface is one of the primary or the first conceptual block in the proposed cloud solution for natural disaster management where this is the front end of cloud computing where users or organizations access to it. This approach uses application program interfaces (APIs) and web services where user interface act as bridge of interaction between users and system. One of the characteristics of user interface proposed is interactiveness as for natural disaster management and this can be seen with cloud computing such as AWS provide interactive user interface.

Next is control mechanisms where a good control mechanism for natural disaster management is needed to efficiently and effectively to distribute the model into the cloud. There are several features of cloud computing under control mechanisms which are flexibility, elasticity, and automation. Hence for flexibility in natural disaster management is crucial as it is the key factor on how to run the control mechanism. The appropriate output is altered by the control mechanism where it depends on the availability of recourses in the system.

For elasticity the disaster management can be done with various functions where for instance, demand for bushfire-related services tends to surge during fire season but declines during other times. Similarly, access to flood-related services peaks during rainy periods and decreases during drier times. Thus, an effective mechanism is needed to manage these fluctuations in usage and access, ensuring optimal resource utilization. During periods of high user access, the mechanism should scale up resources to maintain system performance, while during low usage, it should scale down to minimize resource wastage. Hence, cloud computing able to meet real time demands of these rapid changes of events that happen.

On the other hand, for automation it is much needed to use cloud services as frequent interaction between these processes can significantly slow down the entire system due to the large-scale data exchange. Additionally, in Disaster Management systems, where operations are highly distributed, minimizing data exchange between computing nodes is crucial.

The third part is cloud infrastructure where it has two key features which are scalability and security where it can massively help organizations or companies to improve their business. In natural disaster management, cloud infrastructure able to scale out the number of processing nodes following various limit set by the control mechanism. For security, it is known that it is one of the crucial features of cloud computing where it can provide a secure simulation to run a disaster model to the users. Cloud infrastructure able to provide security of the user data during the operation phase.

Regarding the availability features of AWS, it has AWS region where it is a geographical area in which the AWS Global infrastructure able to deliver flexible, reliable, scalable, and very much secured cloud environment with world class global network performance. Hence if there is any event of disasters happened to Singapore region for example there is an earthquake the organisation can reroute the services with the nearest AWS region which is in Indonesia and thus able to continue with the business as usual.

This is useful for flood management or monitoring system as having no access to cloud services to monitor any potential of flood happening will cause major catastrophic. This aligned with the selecting region in AWS where proximity to the customers (Latency) and services available within the region needs to be considered.

Figure 25

Figure above shows the AWS region where the availability zones use replication of data to provide resiliency. The AWS data centers are built for security where it used points of presence in which edge locations are used. Amazon CloudFront is used for example a data is saved in one region for example Bahrain region, but the application needs to be run and operated in another region for example Oregon. Edge locations can be used with CloudFront to delivers applications or services with a reduced latency where it provides small scale or replica of the main application in Bahrain to customers in Oregon.

Figure below shows why for urban flood monitoring or environmental management AWS infrastructure is implemented because it provides elasticity, fault tolerance and high availability.

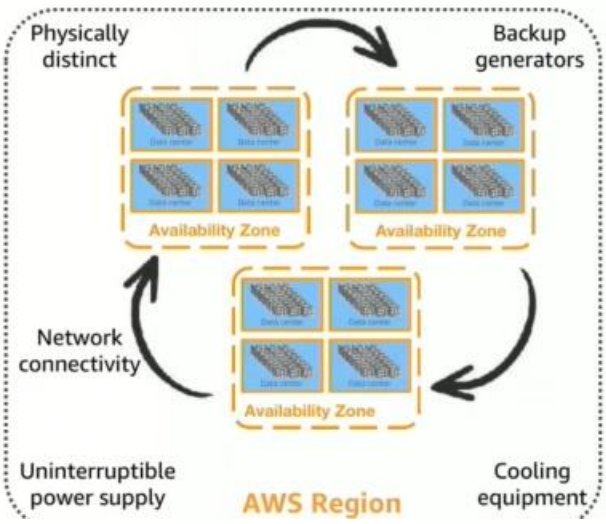


Figure 26

4.1.6 Critical review of the features available of the Amazon Web Services to enhance and facilitate the performance, innovation, and transformation in flood management system.

This part requires to choose the best cloud services providers in which how the features of the chosen cloud services providers which in this case able to help, facilitate and improve natural disaster management which in this case how amazon web services able to improve the domain choose for this assignment. The domain chosen for this assignment is natural disaster management where the particular focus is on flood management system or related case studies similar to water management system.

There are a lot of use cases of amazon web services features such as Amazon EC2, AWS Batch, AWS Elastic Beanstalk, AWS Lambda, AWS Outposts which falls under compute services and for containers such as Amazon Elastic Container Registry and more. There are also services provided by Amazon for storage such Amazon Elastic Block Store, Amazon S3 Glacier and more.

For example, some of the available features in AWS is that in geospatial hazards model it needs to have ensemble simulations where it is a type of simulations that run various simulations with various input parameters. This is very common with natural disaster modelling or simulations such as weather forecasting, flood predictions or earthquake predictions and hence cloud computing is very suitable. This can be seen in how cloud infrastructure able to run a complex dust forecasting model in ensemble mode is demonstrated by deploying the dust model in parallel on the Amazon EC2 foundation.

This approach offers cost savings compared to utilizing local resources. (Q. Huang, C. Yang, K. Benedict, S. Chen, A. Rezgui, J. Xie, 2013).Other than Amazon SQS can be used to manage the queue of users in a dependable and scalable manner while user request is being transmitted between computer under control mechanism for natural disaster management (Q. Huang, C. Yang, D. Nebert, K. Liu, H. Wu, 2010)

Figure below shows the system architecture of how cloud computing services such as Amazon Web Services are able to create a cloud-based flood monitoring and alerting system by combining with Internet of Things (IoT) sensors where the operation technology parts (OT) consisted of IoT sensors and and LoraWan Network.

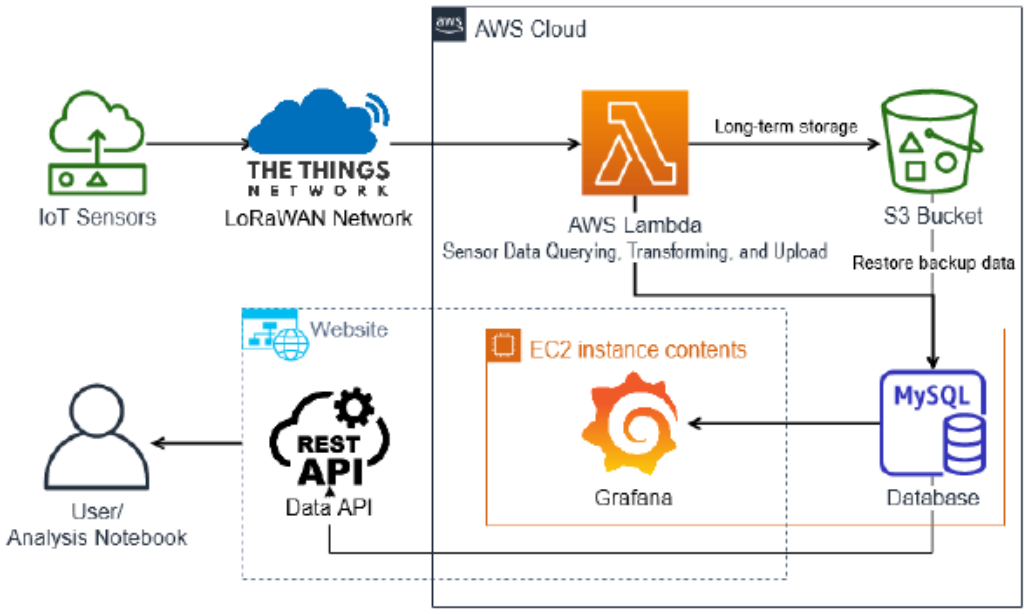


Figure 27 (Asmare, L.; Mahmood, A.; Mitchell, G.; Tenkorang, K.; Todd, C.; Goodall, J. L, 2021)

The system architecture starts with IoT sensors and LoRawan which then connected to AWS cloud that provide services such as AWS Lambda, EC2 instances, Amazon S3 bucket and more. Hence by using AWS Lambda, the measurements are queried, processed, and sent to various components of the flood monitoring and alert system via cloud-based services. The initial sensor data is stored in an AWS S3 bucket for archival and backup purposes, while the processed data is stored in a MySQL database for efficient querying. The database is then connected to a visualization tool called Grafana which will then be connected to Rest API and eventually the monitoring system reaches the users.

Because of the characteristic of Amazon Web services that are scalable and very low maintenance, the data is stored, processed, and hosted by provisioning services such as Amazon Web Services. In flood-affected areas, ensuring the computing backend is highly available is crucial for promptly analyzing incoming weather and environmental data. AWS provides high availability, incorporating regional failovers in case of data center outages. Automation of resource deployment and redeployment on AWS is facilitated by AWS CloudFormation, a tool designed to provision specified resources like Lambda, EC2, and RDS with speed and efficiency.

AWS is able to help innovate flood monitoring systems where AWS Lambda serverless computing platform manages the underlying infrastructure. Clients only need to select the runtime environment for deploying code. Lambda queries sensors for data payloads, parses and transforms the data, uploads the original payload to S3 for storage, and the transformed data to a MySQL database.

After uploading, Lambda automatically shuts off, saving costs by charging only for computing time and memory used. Lambda was chosen for scalability, monitoring, high availability, and resource efficiency. It can quickly adapt to new devices and handle multiple data reporting instances concurrently, with up to 1,000 parallel executions if needed.

On the other hand, AWS S3 can be used for long term data storage to store information about the water depth, location and etc where the data from measurement sensors is stored individually in S3 for long-term use. If the database fails or needs to be moved, these readings can be refilled using a project-specific library. This library also enables users to download readings from S3 to their local machines. All S3 readings are stored using the AWS Standard tier for regular project access.

Later Amazon EC2 instance hosts MySQL 5.7 and Grafana for the project. EC2 provides continuous cloud computing access to the database and Grafana. The project uses a t3.micro instance for cost-effectiveness and reliable performance. For scalability, larger instances can be used for more devices or quicker response times. In this project, MySQL and Grafana are hosted together on one EC2 instance for simplicity. However, for a production setup, separate EC2 instances or AWS RDS may be considered for better scalability and maintenance, despite higher costs.

Hence from the figure previously that explained the integration of IoT sensors with cloud computing solutions such as AWS indicates that cloud computing can be transformed into cloud infrastructure, virtualization and eventually into cloud orchestration. There are 2 types of cloud infrastructure deployment options which are Greenfield option and Brownfield option as shown in figure below.

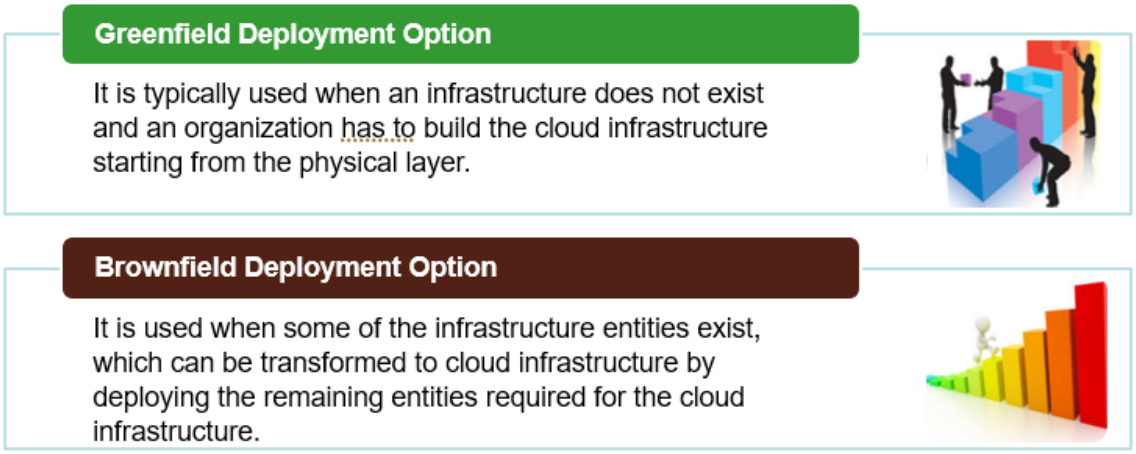


Figure 28

Greenfield option falls under cloud ready converged infrastructure solutions where it is a pre - defined cloud service the packages are already pre-configured and hence able to reduce the time taken for deployment. But the drawbacks are that it is more expensive and has vendor locked in issues which discourage to use infrastructure from other vendors.

Brownfield option on the other hand falls under Best-of-breed cloud infrastructure where it is designed to integrate various vendor infrastructure components. The advantage of best-of-breed infrastructure is that it has no vendor lock in issues, and it is less expensive, and it allows organizations to select and change vendors easily.

Table 9

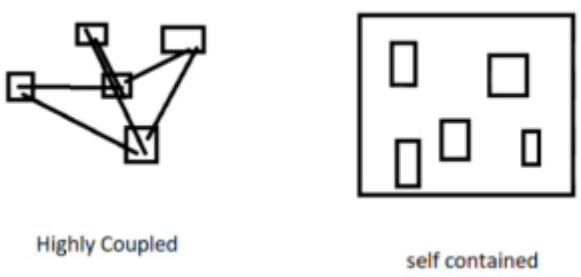
Factors that need to be considered when building cloud infrastructure	
Governance	Avoid vendor lock in
Organization	Software licensing concern
Finance	Service model considerations
Tools	Migration

Service-level agreement and service contract (SLAs)	Testing

The table above shows the list of factors that need to be considered to build cloud infrastructure and below shows the detailed explanation of each factor starting from governance until testing.

Table 10

Governance	It refers to how active distribution of decision making in an organization where IT governance ensures IT resources according to policies and provide values to the organization or companies. The governance model split into centralized, distributed, and federated model.
Organization	It creates new roles and job in cloud industry such as - Service manager. - Account manager. - Cloud architect - Service operations manager
Finance	It's geared towards how profitable cloud services are in terms of recovery of cost, profit, and return of investment . Other than that, is to segregate CAPEX and OPEX services where to determine the charge back models. Below shows the charge back models. - Pay as you go. - Subscription by time - Subscription by peak - Fixed cost - Used based
Tools	Tools such as cloud integration, API, specialized connection.
Service-level agreement and service contract (SLAs)	It's a contract negotiated between cloud providers and consumers that includes metrices such as cost,

	maintenance schedules, service availability, data privacy, data ownership and security
Avoid vendor lock in	Happened due to high migration cost, requires re-engineering and some organization used multi cloud services to avoid vendor lock in. Vendor lock in can be avoided using APIs and open standard tools
Software licensing concern	Cloud providers must understand software license rights before releasing cloud services as different OS models have different approaches to licensing rights.
Service model considerations	SaaS - Make sure the cloud applications are scalable and able process large workloads. PaaS - Support various OS, application, and deployment tools. IaaS - Ensure secure environment
Migration	Forklift - Entire application migrated at once. Hybrid - Application moved parts by parts. Migrating data to cloud uses replication technology and considers factors such as network bandwidth and data security.  *Figure 29*

	Highly coupled related to forklift approach while self-contained related to hybrid approach.
Testing	Define, Identify, Design and Test about data migration to cloud.

4.1.7 The potential challenges that might occurs utilizing cloud services in the flood management system in terms of security and privacy concerns and other management related issues.

There are some challenges that can happened if using cloud services where there will be a potential cybersecurity attack where security is a main concern. Hence, by getting locked in with only one vendor will causes security issues and concern as it is very difficult to switched between vendors as it will lead to loss of data moving between applications. (Sahoo, S. K., & Goswami, S. S, 2024).

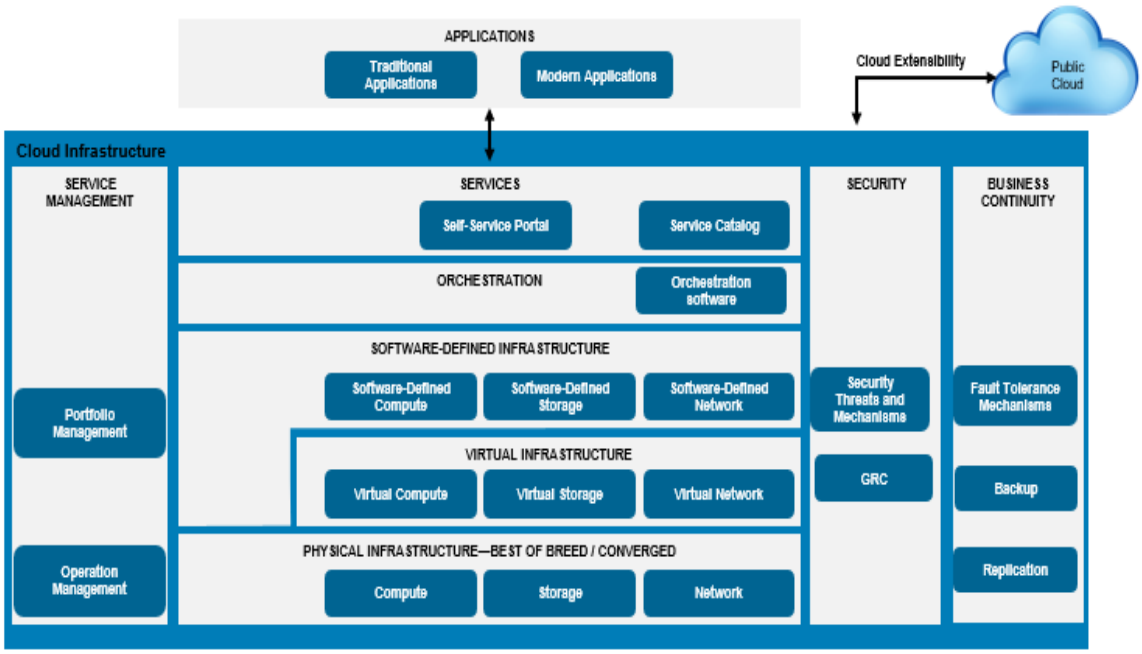


Figure 30

Figure above shows the cloud reference architecture where it consists of applications such as traditional and modern applications, cloud services, orchestration, software-defined infrastructure, virtual infrastructure, physical infrastructure, security, business continuity and

service management. The main focus is on security in which it is important to flood management system such as below;

- Cloud infrastructure is able to transform business and at same time it has created some security challenges and requirements.
- Cloud security is able to secure and protect the applications, data and the infrastructure associated with the cloud.
- Unique features of cloud able to lead to multiple security threats and one of the issues occurs is trust as trust relies on the degree of control and visibility available to customers data in the cloud environment.
- The power of cloud security can be fully maximized with Governance, Risk, and compliance.

It is known that cloud computing uses infrastructure as software instead of treating it as physical hardware, but software is sometimes faced with challenges with security threats and privacy issues. Many small enterprises benefited from cloud infrastructure such as reliability, scalability and more but there are also other issues such as targeted malware or viruses' attacks, confusing data storage regulations and insider threats ((Top Security Risks of Cloud Computing | Built In, 2024). Some of the risks of cloud computing are compliance issues, malware attacks, limited visibility into network operations, data loss and breach, account hijacking and insider threats. Figure below shows the simplified cloud security risks.

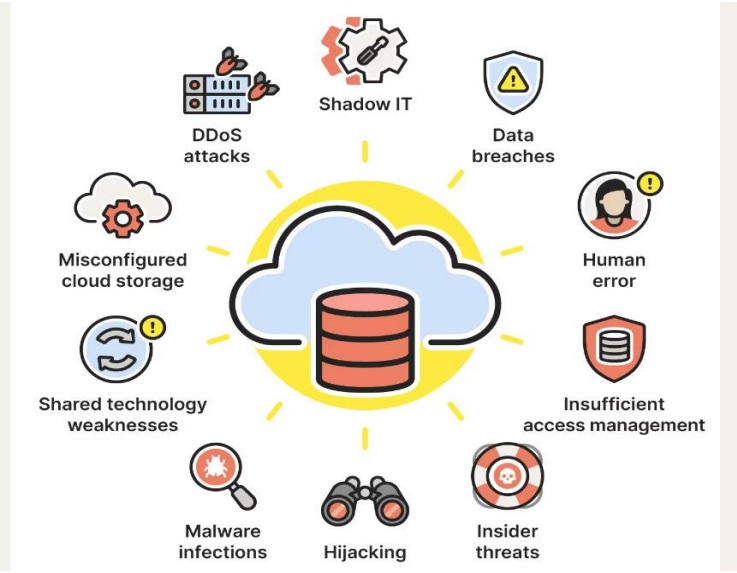


Figure 31 ((Stouffer, 2023)

There are several related works about security and privacy in cloud computing where there are five criteria for security and privacy which are accountability, availability, integrity, privacy protection and confidentiality (Xiao, Zhifeng, Xiao, Yang, 2013). There is other method where it used secret communication for example fuzzy technology, bypass, and secret channel but this technique unusual approach and the application is very limited (Johanna, Ullrich, Tanja, Zseby,2017). There is other method where it uses encryption where it studied the electronic health record (EHR), the requirements of health data in cloud environment, EHR cloud architecture and various EHR encryption and non-encryption (Shekha, Chenthara, Khandakar, Ahmed, 2019).

Hence how Amazon Web Services features able to overcome the challenges of security and privacy in flood management system is that for deployment, clients will need to establish an AWS organization with trusted users to manage AWS Identity and Access Management (IAM) roles and policies. In the current setup, students used separate AWS accounts to manage Lambda, S3, and the database, based on their specific areas of responsibility. This has led to the Lambda function relying on the sshtunnel Python library and an EC2 instance key from another AWS account to communicate with the database. By consolidating everything under a single AWS organization, the need for sshtunnel and EC2 instance keys can be removed.

Properly configuring IAM roles and policies will allow the various components to interact directly without requiring SSH protocols, enhancing overall system security and potentially improving Lambda and API performance by eliminating the overhead of establishing SSH connections for database interactions. Additionally, appropriate security groups must be configured to control user access via AWS Virtual Private Cloud (VPC).

Moreover, a website was needed to allow users to download sensor data. Initially, the API for downloading data was built using AWS Lambda and API Gateway, leveraging AWS's serverless architecture. While functional, this approach had limitations: API Gateway imposes a 30-second timeout on requests, and Lambda restricts payload size to 6 MB. These constraints posed problems for large datasets that require more time or exceed the payload limit. Transitioning to a website with an API endpoint built using the FastAPI framework circumvents these issues, as the new API does not depend on Lambda or API Gateway, thus avoiding their limitations.

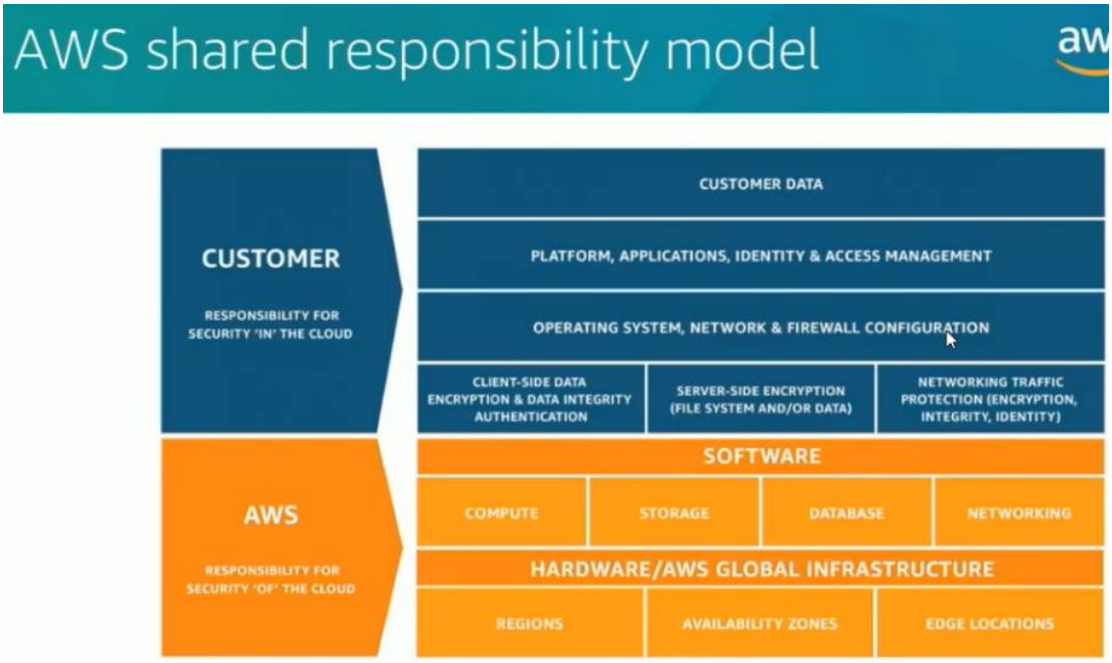


Figure 32

Hence security is a shared responsibility between the organization that used Amazon Services and with Amazon Web Services itself. Figure above shows the shared responsibility model where Amazon responsible for protecting the security of physical data centers, hardware and software infrastructure, network infrastructure and virtualization infrastructure.

Hence, it can be deduced from the shared responsibility model security and compliance is a two-way cooperation between the cloud providers and the organizations which build upon the foundation of trust. The customers take part in updating the services and software including security updates and understand the responsibilities using AWS services. This can be seen for example where the organisation responsible manage their data using IAM tools where Amazon Iam is called Identity and Access Management where it helps control resources and authenticate which resources and users can access to the services provided. (AWS, 2024).

Hence for example organizations that deals with flood management issues need to remind that buy trusting their assets for example information or databases about their dam, SCADA system, monitoring plant which has been integrated with Amazon Web Services. This aligned with five main principles of cloud security which are trust, threats, information, GRC and mechanism.

There are several cases happened in real world where physical assets and infrastructure being attacked because of lack of proper implementation of cloud security. This can be seen in USA where hackers attacked a gas and operator company called Colonial Pipeline being hacked and

need to pay $4.4m in ransom money as the hacker able to the pipeline system. (Associated Press, 2021) The money needs to be pay immediately as the community surrounds the area such school, factories, power plant rely on the pipeline services.

Figure 33

This shows that by having a secured cloud infrastructure services any security breach can be avoided in which AWS able to solve this problem with its top-notch security and firewall features. Cloud security requirements needs to have network security, rapid elasticity and resources pooling where for network security firewalls are not good enough to protect the data security without extra method such as VPNs and more. For rapid elasticity the, the security features, tools and applications must be able to identify newly provisioned resources and integrate it with existing resources. Resource pooling need to have secured multi-tenancy where features such as logical isolation of tenants needed.

Cloud security requires confidentiality where it can make the information remain secure and for integrity, the cloud provider where for this example Amazon Web Services must ensure that no authorized changes happened to the information. The last one is availability where cloud providers must make sure that resources are available only to authorized users who has account. Other than that, cloud security requires authentications where it is about the cloud username and password, authorizations are more about the privileges the users have and auditing is more about monitoring the performance of the cloud security. Velocity of attack on the other hand is about how the existing security threat in cloud could spread faster and have large impact where if the homogeneity increase, the efficient increase but at same time the security of the cloud

decreases. Information assurance is about how the cloud consumers need to understand the roles and policies using cloud services and cloud services providers need to ensure security of consumers data. Data privacy is about protecting security of data through encryption and backup while data ownership is about copyright, contract and type of data created.

Another one is Trusted Computing Based for virtualization where for TCB with Hosted hypervisor provided more security than TCB with Bare metal Hypervisor as it has Host OS while the others do not have it. Additionally, by adding more component it provides more security to the cloud environment. Table below shows the list of cloud security threats with more detailed explanation.

Table 11

Cloud Security Threats	Explanation
Data Breaches	Happened due to unauthorized entity able to gain access to cloud consumers data
Weak Identity, Credentials, and Access Management	Cyberattack can be happened where hackers able to access account of corporate employees
Insecure API	Security of cloud depend on security of API where the vulnerability of the API can be exploit. Some of the mechanism to control API threat is using authentication, security overview and only allow authorized users.
System and application vulnerabilities	Bugs in the code can be exploited and there could be errors in the program features. It could be fixed with regular security updates
Account hijacking	Use keystroke logging malware attack and man in the middle attack
Malicious insiders	This could prevent by having cloud account suspended to prevent former employee give precious information to competitors
Advanced Persistent Threats	Highly sophisticated and targeted cyber-attacks that typically aim to gain prolonged and stealthy access to a network to exfiltrate data or cause damage.
Data loss	Happened due to malicious attacks, natural disasters

Insufficient Due Diligence	Cloud provider should pay due diligence on offering the cloud services and on behalf of cloud consumers, they should understand the cloud service provider environment
Exploitation of Cloud Services	Misuse of cloud services, low cost
DoS & DDoS	Denial of services and distributed denial of service
Shared Technology Issues	Happened due to failure of multitenancy, compromising a hypervisor

5.0 Conclusion

It can be demonstrated that cloud infrastructure is very crucial to many domains and industries where organizations can utilize cloud features their business operations and solve problem happened in their industries. Cloud infrastructure able to provide scalability and flexibility using automatic scaling and resource flexibility. Automatic scaling allow organization to scale resources easily and this is suitable for organizations that deal with fluctuate data in the environmental management industry where the datasets obtain is about water level, elevation height and more.

Other than that, is cost efficiency where cloud infrastructure services provide subscriptions-based pricing where payment only made based on the services uses where this shows that this model able to reduce operating costs and capital expenditure. This eventually will reduce IT cost overhead where for organization that deal with water level management or environmental management where it needed to have huge resources of data centres to monitor water level and more.

Cloud infrastructure provides data redundancy and business continuity where it able to provide data backup services and data replication where the data stored, and access can be replicated in various regions to protect data from failure in case is there any event of hardware failure from natural disasters. Cloud providers also provide high availability to ensure business continuity where nowadays lot of domains of industry are data driven and thus this is crucial for any business and organisation.

6.0 References

C. Center for Research on Epidemiology of Disasters, Economic losses, 1668 https://www.cred.be/sites/default/_les/CRED Economic Losses 10oct.pdf, 1669 2018.

Freer, J., Beven, K., Neal, J., Schumann, G., Hall, J. and Bates, P., Flood risk and uncertainty. In Risk and Uncertainty Assessment for Natural Hazards (eds Rougier, J., Sparks, S. and Hill, L.), Cambridge University Press, Cambridge, 2013, pp. 190–233; https://doi.org/ 10.1017/CBO9781139047562.008.

Kumar, H., Karwariya, S. K. and Kumar, R., Google earth engine-based identification of flood extent and flood-affected paddy rice fields using Sentinel-2 MSI and sentinel-1 SAR data in Bihar state, India. J. Indian Soc. Remote Sensing, 2022; https://doi.org/10.1007/ s12524-021-01487-3

Williamson F (2016) The "Great Flood" of 1926: environmental change and post-disaster management in British Malaya. Ecosyst Health Sustain 2(11):1–9. https ://doi.org/10.1002/ehs2.1248

Department of Irrigation and Drainage (DID) 2009, Flood Management Manual 2009, vol.1, viewed 20 June 2018, http://smanre.mygeoportal.gov.my/smanre/aduan/Volume1Flood%20Management.pdf

Tengku Asmara, T.A and Muhamad Ludin, A.N. 2014, 'Mapping Perception of Community Preparedness towards Flood in Muar River, Johor Malaysia', IOP Conference Series: Earth and Environmental Science, vol.8, pp.1-6, http://iopscience.iop.org/article/10.1088/1755-1315/18/1/012126/pdf

Reza, M.I.H., Choy, E. & Pereira, J.J. 2017, 'Vulnerabilities of local people and migrants due to flooding in Malaysia: Identifying gaps for better management' in C. Middleton, E. Elmhirst and S. Chantavanich (eds.), Living with floods in a mobile Southeast Asia: A political ecology of vulnerability, migration and environmental change, Routledge, London, pp.167-187.

P. mell and T. Grance, "The NIST Definition of cloud computing Recommendations of standards and Technology" Nat.l Stand. Technol.lab, Vol. 145, p.7, 2011.

Haynie, M. "Enterprise Cloud Services: Deriving business value from cloud computing. Microfocus, Tech. Report, 2009.

Marston, S, Li, Z, Bandyopadhyay, S, Zhang, J. and Ghalsasi, A, “Cloud computing—The business perspective”, Decision support systems, 51(1), pp.176-189, 2011.

allcode. (2023). *Top aws services list 2023*. AllCode. https://allcode.com/top-aws-services/

BB Agency, info@bb. agency, & Slingerland, C. (2024, March 26). 25 AWS Monitoring Tools & Best Practices (updated 2024). CloudZero. https://www.cloudzero.com/blog/aws-monitoring/

What is object storage? - object vs. File Vs. block | netapp. (2024). https://www.netapp.com/data-storage/storagegrid/what-is-object-storage/

What is object storage? - cloud object storage explained - AWS. (2024a). https://aws.amazon.com/what-is/object-storage/

Www.naukri.com. (2024). Code 360 by coding ninjas. https://www.naukri.com/code360/library/resource-pooling-in-cloud-computing

Scion, Prometheus, https://www.scionresearch.com/rural- re1681 research/tools/prometheus, 2018. Accessed: 2018-07-12.

R. Cohen, J. Hilton, S. Hasan Khan, Y. Wang, M. Prakash, Swift: A 1683 gpu based coupled hydrodynamic/hydraulic framework for urban ood 1684 prediction. (2015)

G. Schumann, D. Kirschbaum, E. Anderson, K. Rashid, Role of earth1693 observation data in disaster response and recovery: From science to1694 capacity building, in: Earth Science Satellite Applications, Springer, 1695 2016, pp. 119{146.

Q. Huang, J. Li, Z. Li, A geospatial hybrid cloud platform based on 1723 multi-sourced computing and model resources for geosciences, Interna1724 tional Journal of Digital Earth (2017) 1{21.

Connect, C.-C. E. (2021, July 3). Geospatial Technologies. LinkedIn. https://www.linkedin.com/pulse/geospatial-technologies-cmtionline/

Huang, S.; Chen, X.; Ma, X.; Fang, H.; Liu, T.; Kurban, A.; Van de Voorde, T. Monitoring surface water area changes in the Aral Sea basin ssing the Google Earth engine cloud platform. Water 2023, 15, 1729.

Hasan, M.A.; Abed, F.H.Web-based GIS software and database tools for water resources management. Eurasian J. Eng. Technol. 2023, 14, 22–28.

Zeng, H.; Dhiman, G.; Sharma, A.; Sharma, A.; Tselykh, A. An IoT and Blockchain-based approach for the smart water management system in agriculture. Expert Syst. 2023, 40, e12892.

Dhar O, Nandargi S (2003) Hydro meteorological aspects of flood in India. Nat Hazard 28:1–33

James E (2008) Getting ahead of the next disaster: recent preparedness efforts in Indonesia. Dev Pract 18(3):424–429

Department of Irrigation and Drainage (DID) (2007) Fenomena Banjir Malaysia. Retrieved from http:// Www.Water .Gov.My/Image s/Pdf/Fenom enaba njir_Msia.Pdf

Chandramohan, J & Ramasamy, U. (2023). A sustainable inventory model for growing items considering carbon emissions, product expiry, and profit-sharing policy.Journal of Future Sustainability, 3(4), 201-222.

Ram, M., Selvabaskar, S., Guhan, R., & Rajarathi, K. (2023). The effect of digital communication technologies in retail supply chain management: Evidence from Indian small retailers.Journal of Future Sustainability, 3(3), 125-132.

Ghasemi, M., Rajabi, M & Aghakhani, S. (2023). Towards sustainability: The effect of industries on CO2 emissions.Journal of Future Sustainability, 3(2), 107-118.

X. Tan, L. Di, M. Deng, etc., "Cloud-and Agent-Based Geospatial Service Chain: A Case Study of Submerged Crops Analysis During Flooding of the Yangtze River Basin" IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, Vol.8, no.3, pp. 1359–1370, 2015.

Lomotey RK, Deters R. Reliable consumption of web services in a mobile-cloud ecosystem using REST. In: Proc. - 2013 IEEE 7th Int. Symp. Serv. Syst. Eng. SOSE. p. 13–24.

A. S. Abdelfattah, T. Abdelkader and E. S. M. EI-Horbaty, RAMWS: Reliable approach using middleware and WebSockets in mobile cloud computing, Ain Shams Engineering Journal, https://doi.org/10.1016/j.asej.2020.04.002

He Yejun, Salih Omar S, Wang Cheng-Xiang, Yuan Dongfeng. Deterministic process-based generative models for characterizing packet-level bursty error sequences: Deterministic process-based generative models. Wirel Commun Mob Comput 2015;15(3):421–30. , http://doi.wiley.com/10.1002/wcm.v15.3. , http://doi.wiley.com/10.1002/wcm.2356. doi: https://doi.org/10.1002/wcm. v15.310.1002/wcm.2356

Xicheng Tan, Liping Dib,, Meixia Deng, Aijun Chen, Ziheng Sun, Chen Huang, Yuanzheng Shao, Xinyue Ye, ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume II-4/W2, 2015 International Workshop on Spatiotemporal Computing, 13–15 July 2015, Fairfax, Virginia, USA

Standards. (2024). Open Geospatial Consortium. https://www.ogc.org/standards/#:~:text=OGC

D. Liu, Y. Wang, L. G. Liu, (2013) Discussion on power grid magnetic storm disaster monitoring system based on cloud computing, in: Advanced Materials Research, volume 341, Trans Tech Publ, pp. 641{645.

Q.-q. Li, T. Zhang, Y. Yu, Using cloud computing to process intensive floating car data for urban trac surveillance, International Journal of Geographical Information Science 25 (2011) 1303{1322.

B. Behzad, A. Padmanabhan, Y. Liu, Y. Liu, S. Wang, (2011) Integrating cybergis gateway with windows azure: a case study on modflow ground- water simulation, in: Proceedings of the ACM SIGSPATIAL Second International Workshop on High Performance and Distributed Geographic Information Systems, ACM, pp. 26{29.

D. Cui, Y. Wu, Q. Zhang, Massive spatial data processing model based on cloud computing model, in: Computational Science and Optimization (CSO), 2010 Third International Joint Conference on, volume 2, IEEE, pp. 347{350.

FloodMapp Leverages AWS for Real-Time Inundation Flood Mapping to Save Lives and Assets | AWS Startups Blog (2020) aws.amazon.com. Available at: https://aws.amazon.com/blogs/startups/how-floodmapp-leverages-aws-for-real-time-inundation/.

Q. Huang, C. Yang, K. Benedict, S. Chen, A. Rezgui, J. Xie, Utilize cloud computing to support dust storm forecasting, International Journal of Digital Earth 6 (2013) 338{355.

Q. Huang, C. Yang, D. Nebert, K. Liu, H. Wu, (2010) Cloud computing for geosciences: deployment of geoss clearinghouse on amazon's ec2, in: Proceedings of the ACM SIGSPATIAL international workshop on high performance and distributed geographic information systems, ACM, pp. 35{38.

Asmare, L.; Mahmood, A.; Mitchell, G.; Tenkorang, K.; Todd, C.; Goodall, J. L. Title. Smart Cities 2021, 4, Firstpage–Lastpage. https://doi.org/10.3390/xxxxx

Sahoo, S. K., & Goswami, S. S. (2024). Theoretical framework for assessing the economic and environmental impact of water pollution: A detailed study on sustainable development of India. Journal of Future Sustainability, 4(1), 23-34.

Top Security Risks of Cloud Computing | Built In. (2024). Builtin.com. https://builtin.com/articles/risks-of-cloud-computing

Stouffer, C. (2023, July 11). 20 cloud security risks + cloud cybersecurity best practices for 2022 | Norton. Us.norton.com. https://us.norton.com/blog/privacy/cloud-security-risks

Xiao, Zhifeng, Xiao, Yang, 2013. Security and privacy in cloud computing. IEEE Commun. Surv. Tutor. 15 (2). SECOND QUARTER.

Johanna, Ullrich, Tanja, Zseby, Second Quarter 2017. Network-based secret communication in clouds: a survey. IEEE Commun. Surv. Tutor. 19 (2)

Shekha, Chenthara, Khandakar, Ahmed, 2019. Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE Access 7.

AWS. (2024). Shared Responsibility Model - Amazon Web Services (AWS). Amazon Web Services, Inc. https://aws.amazon.com/compliance/shared-responsibility-model/

Associated Press. (2021, May 20). Colonial Pipeline confirms it paid $4.4m ransom to hacker gang after attack. The Guardian. https://www.theguardian.com/technology/2021/may/19/colonial-pipeline-cyber-attack-ransom

7.0 List of Figures

Figure 1 6
Figure 2 9
Figure 3 10
Figure 4 12
Figure 5 12
Figure 6 (BB Agency, info@bb. agency, & Slingerland, C. 2024) 13
Figure 7 : Object based storage system. 15
Figure 8 : File based storage system. 15
Figure 9 : Block based storage system. 16
Figure 10 18

Figure 11 20
Figure 12 20
Figure 13 21
Figure 14 21
Figure 15 22
Figure 16 22
Figure 17 23
Figure 18 24
Figure 19(Connect, C.-C. E.2021) 25
Figure 20 25
Figure 21 (A. S. Abdelfattah, T. Abdelkader and E. S. M. EI-Horbaty, 2020) 29
Figure 22 (Xicheng Tan, et al, 2015) 30
Figure 23 35
Figure 24 35
Figure 25 37
Figure 26 38
Figure 27 (Asmare, L.; Mahmood, A.; Mitchell, G.; Tenkorang, K.; Todd, C.; Goodall, J. L, 2021) 39
Figure 28 41
Figure 29 43
Figure 30 44
Figure 31 ((Stouffer, 2023) 45
Figure 32 47
Figure 33 48

8.0 List of Tables

Table 1 7
Table 2 11
Table 3 14
Table 4 16
Table 5 19
Table 6 28
Table 7 31
Table 8 32
Table 9 41
Table 10 42
Table 11 49