UNIVERSITY OF TURKU

Risk management and architecture design in securing cloud platforms: Case study of cloud models

Master's thesis

Master's Degree Programme in Information and Communication Technology (M.Sc. Tech)

Author(s):

Samuli Nevalainen

Supervisor(s):

Jouni Isoaho

Antti Hakkala

14.6.2022

Turku

UNIVERSITY OF TURKU

Master's thesis

Subject: Master's thesis
Author(s): Samuli Nevalainen
Title: Risk management and architecture design in securing cloud platforms: Case study of cloud models
Supervisor(s): Jouni Isoaho, Antti Hakkala
Number of pages: 78 pages + 8 appendix pages
Date: 14.6.2022

Utilization of cloud environment has become more relevant for different companies and industries and should be considered when building new projects and migrating service from different service providers. As companies are trying to utilize cloud environments the knowledge about these might be lacking and thus increasing knowledge and introducing possible solutions is essential. This means that increasing knowledge about different approaches possible in cloud also different issues can be identified. Based on this kind of knowledge can the discussion about the possibility for utilizing cloud environments be improved.

The use case for this study is the risk management and architecture design comparing of different cloud types and models based on a case study. Also, based on these different kinds of cloud types and models the security issues and countermeasures are discussed in a way that these measures could help to control or mitigate issues from happening. For finding feasible architecture designs these measures are to be considered alongside the responsibilities for different cloud models with the help of risk management. Risk management itself introduces risks and issues that are identified from cases and discussed as of how to control them within different cases.

This thesis studies the possible issues and risks through a literature review that are associated with different cloud types and models. Also, introducing case study of three different cases that utilize these approaches and introduces such issues and risks associated with those cases. For identified issues and risks also relevant security methods and measures are studied through literature review and introduced to be utilized in risk management and architecture design. Based on these reviews a risk management is conducted to introduced cases where issues and risks are introduced with identification of real-world use case. Also, architecture design is introduced in a way that utilizes identified risks, control, and mitigation measures for protecting resources. What different possibilities and components to consider depending on different cases are also discussed as not all the risks can be mitigated with certain measures and would need more thought on as of what cloud type and model to utilize. Thesis also discusses about the three identified topics of risks, security measures and architecture and identifies relevant information from them for consideration.

Thesis discusses about three different cases that were studied in a way as of how they differentiate from each other in the common field of risks, security measures and architecture design as they utilize the cloud in a different way. Discussion introduces the results and more detailed discussion that were identified from these three main topics. Detailed discussion itself contains similarities and differences identified from different cases and introduces more discussions based on those topics.

Key words: Risk management, Architecture, Cloud security, Case study, IaaS, PaaS, SaaS

Table of contents

1 Introduction 1

1.1 Context 1

1.2 Goal of the thesis 2

1.3 Methods 2

1.4 Use cases 3

1.5 Research question and structure 4

1.6 Limitations 5

2 Security 6

2.1 Security methods 6

2.2 Security measures 8

3 Cloud architectures 14

3.1 Different cloud types 14

3.1.1 Public Cloud 14

3.1.2 Private Cloud 15

3.1.3 Hybrid Cloud 15

3.2 Different cloud models 16

3.2.1 Infrastructure as a Service (IaaS) 17

3.2.2 Platform as a Service (PaaS) 17

3.2.3 Software as a Service (SaaS) 18

3.3 Cloud issues and challenges 18

3.3.1 Infrastructure as a Service 18

3.3.2 Platform as a Service 21

3.3.3 Software as a Service 23

3.4 Cyberattacks to cloud environments 25

3.4.1 Different attacks 25

3.5 Recovery methods 28

4 Case study: Risk management and architecture design 30

4.1 Overview of cases 30

4.1.1 Case 1: Cloud migration 30

4.1.2 Case 2: Platform to run custom code 32

4.1.3 Case 3: IAM solution as a service 33

4.2 Risk management 34
4.2.1 Risk management types 34
4.2.2 Risk management process 35
4.2.3 Case 1: Cloud migration risk management 37
4.2.4 Case 2: Platform for Docker risk management 42
4.2.5 Case 3: IAM solution risk management 44
4.3 Architecture 47
4.3.1 Case 1: Cloud migration architecture 47
4.3.2 Case 2: Platform for Docker architecture 50
4.3.3 Case 3: IAM solution architecture 52
5 Discussion 54
5.1 Risk management 54
5.2 Security methods and measures 57
5.3 Architecture design 61
5.4 General discussion 64
6 Conclusion 66
References 73
Appendices 79
Appendix 1: Case 1 Risk Management 80
Appendix 2: Case 2 Risk Management 83
Appendix 3: Case 3 Risk Management 85

Abbreviations and Acronyms

VPC	Virtual Private Cloud
IaaS	Infrastructure as a service
PaaS	Platform as a service
SaaS	Software as a service
SG	Security Group
DMZ	Demilitarized Zone
WAF	Web Application Firewall
LB	Load Balancer
IAM	Identity and Access Management
PAM	Privileged Access Management
API	Application Programming Interface
MitM	Man in the Middle
DoS	Denial of Service
DNS	Domain Name Service
SQL	Structured Query Language
XSS	Cross Site Scripting
SLA	Service Level Agreement
VM	Virtual Machine
CSP	Cloud Service Provider
DC	Data Centre
SSO	Single Sign-On
NACL	Network Access Control List
TTL	Time to Live
APT	Advanced Persistent Threat
IDP	Identity Provider
STS	Security Token Service

ERM Enterprise Risk Management

CRM Collaborative Risk Management

1 Introduction

Usage of cloud platforms and services are increasing steadily but so are the security issues and attacks associated with these [1]. Use of cloud platforms allow companies and users to have underlying service layers utilized without owning those platforms and services but instead utilizing them from centralized providers [2]. Because of this also the services utilized can vary and multiple different kinds of solutions and services can be created and are needed. This is also why security of cloud services varies a lot depending on what type and model is chosen and how different services and components are utilized [1][3]. Because of this variation it is important to note that different kinds of security measures and architectural designs must also be thought out and identify responsibilities of different services to build secure and flexible architectures on cloud platforms [1]. This master's thesis aims to find thoughts and solutions for consideration when establishing different kinds of cloud architectures by utilizing three different cases as a study to comprehend the differences of the types, models, and security issues through risk management process.

1.1 Context

Companies are utilizing cloud platforms more depending on their needs and considering this as an approach for new projects [1]. They could utilize it fully or just certain parts or even integrate cloud solutions to work with their on-premises Data Centres (DCs). These kinds of variations create complexity in the architecture design and can pose security risks if architecture design has not been thought out properly and tested to work with such solutions [3].

More traditional way of working has been the utilization of on-premises data centres where the company does all the implementations and takes care of responsibilities itself or utilizes subcontractor that manages the needed things on the data centre [1][5]. This way it has been easier to think of the architecture and components that can be placed within the specific DC and no outsiders are allowed to access it while also identifying responsibilities between the parties.

Things change radically when considering the usage of on-premises and cloud platforms working together creating a so-called hybrid model [3][4]. This way to effectively utilize both the architecture design needs to be thought out to cover both sides effectively and in a secure manner. Also, responsibilities of both parties must be thought out and utilizing both could

create gaps between these two that could pose risks if not mitigated and thought out properly [4]. These kinds of approaches also vary a lot depending on the usage type of cloud platforms and are those infrastructure, platform, or software type models. As different kinds of architecture designs apply to all these models, they are also prone to different kinds of risks and threats from security perspective.

As cloud platforms contain different responsibilities based on the models, they will be utilized differently depending on the case [3]. This also indicates that risks, costs, and benefits for such solutions are different based on the cases, types, models, and architecture design [3]. There are also different matters that indicate if the solutions can even be utilized from cloud platforms such as regulations that mandate what needs to be placed on where and what solutions can be utilized.

1.2 Goal of the thesis

Goal of the thesis is to identify risks and think of ways of controlling those and mitigate them with security measures for three different cases studied while also identifying how different cloud types and models affect risks. By identifying risks and managing them also architectural designs per three different cases will be introduced. Cloud platforms work very much the same as regular data centres but pose more security and architectural thoughts than regular ones as per different responsibilities [1][3]. As there are different sets of services that can be utilized from cloud platforms, and it is even possible to combine both cloud and on-premises data centres to function together the architecture of these different solutions must also be secure enough to mitigate issues, attacks, and security breaches [3]. There are also different kinds of utilization aspect for the cloud platforms, and this also imposes multiple different architectural decisions for design and creates different sets of security issues that could affect the solutions.

1.3 Methods

Research is based on literature review and case study methods. First security methods and measures utilized are researched from existing research and documentations that are compared to find most feasible measures for different cases discussed in this document. After finding out security measures the different cloud types and models are discussed as of what they are. Based on the utilization type and model of the cloud different security issues, challenges and attacks are introduced that are relevant in this research.

Following literature review of security and issues is the actual case study that identifies risks and ways of controlling and mitigating them based on three different cases through a risk management process. Based on the risk management outcome different architecture designs are introduced per case. These architectural decisions are discussed and introduced in more detail even though architecture is done in general and on high level.

Based on these literature review and case study the results are discussed as of what risks are identified as common and what are different per model and type. More detailed discussion is based on the risks itself as for identifying these similar points and differences and relevant information is identified from those for consideration. Similar discussion is also done for security measures utilized and architecture design. These discussion topics also include detailed discussion and identifying relevant information.

1.4 Use cases

Master's thesis is researching about risk management and architecture design in different cases based on the cloud environments type and model. Thesis is also researching how the utilization of the different cloud models affects the risk management and architecture design based on the cases studied. Risk management was chosen for the ability to research cloud type and model issues in a larger scale. For risk management process security methods and measures are researched that are relevant in cloud environments. These security methods and measures were chosen for the possibility to identify relevant ways of securing cloud environments and the risks. These methods and measures are utilized for identifying ways of controlling and mitigating risks based on the architecture design for different cloud types and models. Architecture design was chosen for the possibility to identify actual usage of the security methods and measures and identify concrete ways of utilizing these to control risks identified. Cloud platforms were chosen because of different ways of utilization based on the needs and because security aspect of cloud environments is different for different kinds of use cases [1][3].

Researched risks, security measures and measures, and architectures should be considered as a guide and give thoughts on what to consider while utilizing cloud platforms. Discussed ways of protecting cloud environments are based on the cases studied and literature and give insight of possibilities.

1.5 Research question and structure

Academic work is often related to specific issues occurring or examining cloud platforms to be utilized more effectively instead of providing risks and architectural design to mitigate security issues and attacks within the platform. Thesis provides different security methods and measures to tackle different issues identified in cloud types and models based on literature research. As per these types and models there are different issues, challenges and attacks that are discovered through research. This thesis compares different kinds of cases that can be utilized from cloud platforms through case study. By studying literature about security methods and measures research question (RQ) 1 is answered. More literature-based research is done to also answer research question 2 to identify different issues and attacks targeted towards cloud environments. Research question 3 is answered by utilizing case study method of identifying and comparing three different cases that utilize cloud environment in different ways. Research question 4 can be answered by the answers to questions 1, 2 and 3 and comparing the results based on the cases.

RQ1: *What different security methods and measures are applicable in building secure cloud environment?*

After identifying different security methods and measures that are feasible for the cases studied, these are then considered as part of risk management and if these can be utilized to control and mitigate identified risks. As cloud environments have their default security measures in place, these still are not enough to protect resources in different kinds of cases utilizing cloud types and models.

RQ2: *What different kinds of issues and attacks are associated with different cloud types and models?*

Identifying different issues and attacks targeting cloud environment from literature it is possible to identify these from the cases in case study chapter. What different issues and attacks are applicable in these cases are then identified per case and control and mitigation methods are considered. Based on these the different methods are being utilized in answering research question 3.

RQ3: *What to consider when designing cloud architecture?*

This research question is answered based on the case study and identifying answers from questions 1 and 2. By identifying case and needed information that is relevant to that case it is possible to identify methods, issues and attacks targeted towards that specific case. Based on these identifications different architectures are designed for each case introduced in this thesis to control identified risks.

RQ4: *How the utilization of different cloud types and models affect risk, security measures and architecture design?*

This research question is discussed based on the case study and risk management and comparing results of other research questions in the discussion part. By identifying similar risks, measures, and architecture per case, it is possible to compare and identify as how different models and responsibilities affect control or mitigation of the risks or will the risks be accepted.

1.6 Limitations

As perfect security does not exist, and no solution and architecture are the same it is impossible to mitigate all the security issues and problems [4]. Different architectures identified in this thesis will not protect all the resources within the cloud platforms. Building secure ways of working and architectures are ever evolving solutions to control and mitigate risks. Architectural points in cloud can cover very high-level architectures and very detailed ones that differentiate between both kinds of architectures. As there are attackers trying to find vulnerabilities and issues within different parts of the architectures it is critical to update architectures also in time to match these threats and risks. Not all the architectural point of views and mitigation issues can be considered as the solutions and utilization of the platforms vary and complexity of the different solutions vary a lot when utilizing cloud platforms and different tools [1].

As there can be a lot of different technical issues involved when configuring setups mentioned in this thesis, these are not addressed in this thesis. Technical issues vary a lot depending on the environment, components and tools utilized and regarding the compatibility of these is the utilizers responsibility [1][4].

This thesis does not consider as of how the different components and tools mentioned are to be configured. As these configurations are different per cases and needed configurations are prone to change these are limited out of the scope of this thesis [4].

2 Security

This chapter identifies different security methods that are used to protect assets within the cloud environments. These methods include various ways to prevent and identify threats that are needed to be included in different parts of cloud environments and per different cases studied. Chapter also introduces different security measures that can be utilized to prevent different kinds of issues from happening or mitigate the risk and likelihood of different risks and attacks.

2.1 Security methods

There are multiple different security methods that need to be identified within cloud environments to address security issues and challenges [1][3]. All these security methods are in one way, or another involved within protecting the environment and needs to be thought out accordingly to create safer environments. Following is an introduction of what these methods are and why these are needed.

Authentication is one of the security methods that is heavily utilized for protecting different parts of the systems. With this method the access to different services and servers are allowed or not based on the identity provided [3][19][34][39]. Authentication is a mean to verify an entity and pose it as a legitimate user [3][34][39]. As cloud enables the services to be available from everywhere authentication needs to be addressed properly [19]. By authenticating into the services, it is possible to log about who and what has been done [39].

Authorization gives permissions to do certain tasks or have certain level of admin rights on the servers or solutions [3][19][34]. Authorization provides the permissions for users that are authenticated [3]. Authorization is an important factor to address as for only authorizing correct identities with correct permissions [19]. Authorization can be implemented in multiple ways such as groups or roles [34]. Authorization itself can prevent issues that could be caused by too vague permissions or no permissions.

Anonymization is utilized to hide data and trails leading into it and can be utilized to increase privacy of the data [3]. Anonymization can prevent different attacks where data is involved and tracking of the user based on the data is utilized.

Audit gives different views and can find possible weak points of the whole architecture or given components when being audited [19][34]. Auditing helps to avoid same incidents from

occurring multiple times [2]. This enables different protective measures to be taken to use if issues are identified. Audit gives information as of who, when and what has been done and this information can be used for preventing issues [34]. Audit also increases knowledge of the components and their integrations to provide better security for future consideration.

Assurance can be an important part of the security as it introduces the identification and levels of the methods and measures that are utilized [19][45]. With assurance in place, it would enable transparency over what and how things are done while indicating possible problems points [19]. Assurance must take into consideration authentication and authorization, change management and backups [45].

Availability means that the services would be running most of the time without downtime [5][31][39][44]. Availability can be achieved with virtualization and geographic redundancy [1]. Availability needs to be analysed with more details to forecast usage and scale resources with that data [5]. Availability can be increased with different technologies such as clustering or load balancing [5]. Availability can also mean that data should be available alongside the services to work [31]. Availability is one of the requirements as to what cloud type or model to choose from and can be identified within Service Level Agreement (SLA) [39]. With availability in mind the services are constructed to withstand attacks targeting it and protective methods utilized with different parts of the system for countering attacks.

Administration can be also identified as a security method as it enables the users, roles, and groups to be administered to mitigate access and authorization issues while having someone overlooking the systems [12].

Encryption is a method which ensures that data traveling between different connection points or stored is encrypted appropriately and not visible as plain text [12][24]. This ensures that data is secured and hard to crack into a visible form if attacked on network level [12]. Same approach can be utilized to encrypt data on the database [12]. There are different standards and ways such as tokenisation to ensure data is protected accordingly [24].

Compliance is important to be identified as also security method as it provides rules and sets of points to be identified and considered in the solutions [12][19][24][28][33][39]. Solutions must meet compliance of the regulations that give a framework as of how the solutions should work and what needs to be considered [12][28]. Compliance is a way to show that standards and regulations have been considered [19][39]. There can be management platform provided

to ensure compliance in cloud [33]. For compliance the business requirements, compliance aspects and data requirements need to be understood to find feasible solutions [24]. These requirements should be understood and considered in the shared responsibility model and coordinated between the parties [28]

Governance is a security method that governs over the set of rules and policies [19][23][28][33][49]. This indicates that governing over these is a way to create an environment that has framework to work under and improves security, better operations, and risk management [19][33]. With governing over these sets of rules, the planning, implementation and managing solutions becomes easier and can be better maintained [28]. Utilizing cloud itself increases the needs for more governance over it as per the responsibilities model [28].

Privacy and confidentiality are a way to ensure that data is stored and secured in a way that privacy and confidentiality can be ensured [33] [31]. There are different methods for utilizing alongside such as encryption and data location to ensure that it is legislative within regulations. Encryption is the proposed security method to ensure privacy but also Single Sign-On (SSO) and authentication and authorization should be added [31]. As there are different laws in different countries the privacy must be matched in the operated country [33].

Integrity means that the information passed down alongside the solution and between components can be ensured to be unchanged [35] [37] [39]. There should be considerations for atomicity, consistency, isolation, and durability to ensure that integrity is matched [39]. Hardware level integrity should also be considered alongside data [37]. With this kind of method in place the data can be ensured to be the same that has been provided or fetched and can be managed in a way that is secure and protected accordingly [35].

2.2 Security measures

There are multiple different security measures that can be utilized within cloud environments to address security issues and challenges [1][3]. All these different security measures are in one way, or another involved within protecting the environment and needs to be considered when applicable to create safer environments and architectures in cloud. Security measures are to be utilized together as they are specified for certain purposes and one measure itself does not provide enough protection in all different cases.

Risk Management is an important security measure as it identifies the risks associated with the different systems involved [11][19][33]. With this risk management it is possible to identify, control and mitigate certain risks and identify compliance issues [19]. This kind of approach helps identify components and risks associated with it and what other components it is connected into, increasing knowledge, and raising awareness [28]. With risk management it is also possible to calculate risk levels based on severity and likelihood of that risk and based on this it is possible to identify most critical risks and create a plan for those risks to be controlled and mitigated with or utilize a framework containing needed information [33]. Risk management should be a constant program that adapts into the landscape and evolves over time to respond new issues and threats that are identified [28]. As monitoring the environment, it is possible to identify the security level of the systems and support risk management processes [28].

Key management is a security measure that enables signing, encryption, and key rotation for different parts of the systems where keys are utilized [9][12][33]. Keys should be managed securely and all the access and access rights for them should be logged and checked [9]. Key management services are provided by Cloud Service Provider (CSP) and third-party services and should be considered to enable key management services across utilized cloud [12]. With this security measure it is possible to control and mitigate risks related to data security, communication, and other parts of the system where keys could be utilized [33].

Identity and Access Management (IAM) is one of the most utilized security measures as this includes access rights and identities that has authorization to do different things [12][33][58][49]. With IAM it is possible to mitigate access to different resources and only authorize identified people to access those [12][49][58]. With this measure it is also possible to allocate certain access rights with limited authorization to people or associate groups, so people can only do what they are needed to or even enable the utilization of automation with technical user rights [33].

Private cloud type can be considered as a security measure as it increases security as based on the needs the whole cloud services provided is only to be utilized by this specific organization [12].

Virtual Private Cloud (VPC) is a security method that allocates a private zone from the public cloud provider to establish private zone only to be utilized by this specific organization [33][51][42]. This measure increases security in network and application level as it becomes

possible to mitigate access more properly as the zone is dedicated [33]. VPC offers certain advantages comparing to a private cloud that are better scalability, hybrid cloud deployment possibility and performance [42][51].

Web Application Firewall (WAF) is also one of the utilized security measures to check incoming requests to identify those that are malicious or not allowed to be performed [9][26][37][41]. Firewall protection and WAF should be considered to block unauthorized access with analysing requests [9][37]. With this measure it is possible to mitigate certain attacks and increase security of the architecture design [27][41].

Network Access Control Lists (NACLs) are a security measure that restricts access in and out of the network. With these it is possible to restrict access to and from certain IPs and/or zones [27][37]. NACLs are rules that indicate as of what kind of network traffics are allowed and what are denied [37]. This measure allows for more detailed solution in network level and works similarly as firewall.

Security Groups (SGs) are groups containing rules for the network and could be considered as a firewall adding extra security within VPC alongside NACLs [27][41]. SGs control the traffic coming in and out of that specified instance that contains the needed resources [19]. SGs work in similar way as WAF and create one point to block access with virtual perimeters [27]. With these it is possible to secure networks adding an extra layer of security and even associate different SGs for different components within VPC.

Identification of all the different resources such as users, assets, environment, components, policies, vulnerabilities, threats, and risk management are considered as a security measure [11][12][19][33][43]. Knowing and identifying different parts of the system is essential to build security on top of those identified resources [12][33]. Identifying the assets, it is possible to specify ownership and responsibilities of that resource [19][43]. There are different kinds of audits, scans, and tools to help with identifying resources and with this kind of approach it is possible to control and mitigate issues as the knowledge of the identified resources is increasing.

Security Controls must be in place to define and control different parameters, policies, data, users, and infrastructure [9][12][21][58][59][41]. As having different levels of security control services, privileges and responsibilities can be managed with different cloud models [9]. Security controls should ensure that there is visibility and fidelity to provide security [12].

These controls provide a way for access control, policies, and key management to target different threats [21][41]. With these controls it is possible to mitigate unnecessary access and control of who and what components has access to do and what they can do [58]. With these in mind the responsible people can be identified and based on those different kinds of controls addressed for different needs [59].

Security by Design means that different aspects must be designed into to the solutions such as responsibilities, configurations and what should be automated to increase security in design phase [11][19][58][49][43]. Security architecture is a combination of different methods such as security layers, design, and best practices among others [11][43]. Security should be considered per responsibilities of different resources and per different regulative actions to be taken [19]. By designing security into the solution, it becomes easier to identify, control and mitigate different risks and build solutions that enable security methods and measures. This also increases the knowledge about risks and ways of identifying and controlling them in the design phase.

Asset Protection is a measure which protects identified assets [12][23][49]. These assets should be protected against tampering, loss, or damage [23]. This could be through encryption hiding the assets from plain view or hiding the assets in the network so that no other people are able to access and have visibility on those [9]. Asset protection should be automated and managed across all environments [12]. With this kind of measure in place the identified assets are identified and protected against identified risks.

Perimeter Security is the different communications done between components and how they are secured [6][43]. Perimeters can be operated as SGs that are protected with different rules [6]. By utilizing this measure, it becomes possible to limit access from only certain components and protect the traffic while it stays in the environment. This measure itself decreases the possible attack surface for the component's as only authorized traffic can proceed.

Segmentation or isolation means that different components are segmented and isolated from the rest of the components into own segment [19][27][33][59][41]. As for isolating components it can be done with a hardware or software types, and these can separate different resources [1][59]. As isolating different resources, the resource type, itself such as data should be considered and based on that the different solutions would be considered [19][27]. Isolation enables the services to be deployed more securely and better protect them on the

public internet [33]. This way it becomes possible to secure different components, limit access and manage those components within own segments and fix issues within them.

Data confidentiality and integrity is a measure to ensure that data can be processed, transferred, and stored safely [5] [12][44]. This can be achieved with dependable hardware [1]. Also, to determine the data integrity it is possible to use tools with confidence level [5]. With such a measure the data is safe from different kinds of attacks. This measure would try to prevent sensitive data from leaking and being exposed to public [44].

Automation enables that configurations and different security measures can be provisioned with minimum human interaction [11][12][59][43]. Utilizing automation, the infrastructure can be scaled per needs and issues can be fixed faster [11]. Utilizing this measure, it is possible to build different parts of the system or environments to function through code-based approach or to respond to threats, risks, and service disturbances with identified solution [12][59].

Logging and Monitoring is an essential security measure to be taken into use [6][12][32][59][41]. This measure is to be done within different parts of the system such as the applications and Virtual Machines (VMs) [6]. With this it is possible to identify unwanted behaviours and identify different issues occurring within the environment [12][32][41]. Utilizing this measure solutions are compliant, gain more visibility what is happening and increase awareness of what different issues and threats are happening within the environment [12]. By monitoring the environment also, the possible limitations and bottlenecks of the components can be identified to improve the environment [59].

Visibility means that all the different tools and processes are visible in a way that they can be identified to be relevant [12][19][28]. With this utilizing different tools or automation these components would be visible to be utilized in the whole environment rather than on one place and decrease the possible issues such as shadow IT [19]. This measure would also impose that knowing about certain components there would be no duplicates and unknown applications or assets [12]. Having continuous ways of collecting the data about the environment and monitoring it ensures that it is possible to manage security risks and issues [28].

Flexible Design means that architecture design itself can be modified to enable new services or develop existing ones to ensure that security is not sacrificed [11][12][43]. For building flexibility also specific designs such as thresholds and servers or services must be thought out

[11]. Flexible design allows the solutions to adapt into different cases [12]. With this kind of approach different components and segments could be properly managed, improved or completely new ones could be added [43]. Flexible design could also consider utilizing microservices and different APIs to be implemented. Flexible design would also allow utilization of different cloud types and models to be possible for implementation.

Different kinds of tools such as intrusion detection tools and other security enhancing tools are considered as a measure to increase security in the cloud environment [32][35][58][57][33][41]. Utilization of Intrusion Detection System it becomes possible to identify problems and mitigate different attacks [32][41]. As by utilizing different tools the possible vulnerabilities, threats, intrusions, and other security issues could be identified and controlled [33][35]. Tools can also apply to migration phase and could provide an ability to import data in a secure format [58]. This kind of measure works specifically for that specific case the tools are designed to and different tools should be considered to target different kinds of issues as per identified risks and their types [57].

3 Cloud architectures

This chapter is about studying different cloud types and models that are utilized for different purposes and their security issues and challenges. Relevant cyberattacks and ways of recovering from issues are also introduced for better understanding. Knowing about the different issues and attacks allows further knowledge about the usage of security methods and measures to control issues. Understanding these differences in the types and models is important to find ways of utilization for cloud environments and tackle issues identified in them.

3.1 Different cloud types

For different kinds of utilization and needs there are also different kinds of cloud types [2][3]. These are public cloud, private cloud, and hybrid cloud types [2][3]. These different cloud types work with different needs, and each has their own use cases. Choosing one over other is based on use cases and their individual needs and needs to be thought thoroughly. Certain cloud types are more preferred per different industries and organizations than others and knowing about the cases is essential as of what type should be chosen.

3.1.1 Public Cloud

Public cloud is cloud type that shares the servers, hardware, and software with others from a third-party provider [6][9][22][48]. With public cloud the Cloud Service Providers (CSPs) create different resources available for customers and companies with easy access over the internet [4][9][48]. Public cloud can be more easily configured and deployed in comparison to other types [22]. The provider will take care of the maintenance and infrastructure allowing more time to focus on actual tasks. There are certain aspects to make this appealing approach such as the on-demand resources make solution more scalable and reliable. This kind of approach can be useful for cases where predictability or resources are needed on-demand. Approach also reduces complexity as the CSP takes care of most of the computing resources.

This type also comes with a downside and can be utilized when data compliance is not an issue, controlling the hardware is not needed and tight security measures are not needed. [9][47][46]. With public cloud, the customers have limited visibility and control over the infrastructure that could cause compliance issues [4][47]. Public cloud can be easy to maintain and cost effective, but they lack in security and security processes [4]. As same

infrastructure is shared between multiple parties' issues such as data leaks can occur because of multi-tenant architecture [9]. As public cloud model is provided by a third-party provider the security is also lacking in a way that CSP is responsible of many resources and services that they provide and there is no knowledge about these how these resources are secured and patched [46]. There is also the issue with not knowing about the underlying hardware and issues associated in that.

3.1.2 Private Cloud

Private cloud is a cloud type that is owned and operated by a single organization [22]. This means that the servers and infrastructure are in a safe environment and dedicated for that single organization [6][9][22][48]. Private cloud is utilized when needing better security level and control over the applications within a reliable environment [4][9]. By utilizing private cloud, it is possible to meet certain compliance and regulations identified relating to data and enhance security. This approach is useful when talking about regulated industries that contain also sensitive data as it is possible to have control over it as of where the data is stored. This type of cloud can also accept more custom solutions for enhanced security and can be utilized to meet the needs of the utilizer be it scalability, flexibility, or performance.

This type of approach also comes with a downside as it needs a lot more maintaining, troubleshooting and increases costs [4][9][47][46]. As the services and resources need to be bought, built, and managed for this private cloud customer it becomes with more costs [4][9]. There can also be issues with virtualization techniques and because of this the risks towards hypervisor should be analysed properly [9]. There are also issues with unpredictable scalability as the resources are built and limited in a way that the on-premises resources would be and needs to be added in co-operation with provider [47].

3.1.3 Hybrid Cloud

Hybrid cloud type approach is utilizing both public and private cloud types or multiple Cloud Service Providers (CSPs) [4][6][9][22][48]. This type of approach allows data and applications to be moved within both types and different CSPs and has benefits such as meeting regulations, data requirements, low latency, and a lot more [13][48]. Utilizing this kind of approach, it is possible to meet the demand when needed to and build the needed resources based on that. This type of approach could utilize private or public cloud solutions

per case as if it has been identified to contain data that is not sensitive or add reliability based on the designed approach [9][22].

There are also downsides for this approach as to how the data is managed and what sensitive data is sent and can be seen by others utilizing the public cloud part of the system [4][9][47][46]. As these services can utilize multiple CSPs or cloud types also the differences in security platforms, maintain and demonstrate compliance and problems with Service Level Agreements (SLAs) can be considered as a challenge [4]. There are still lacks mechanisms and tools for security and control over the data within these kinds of environments [9]. This kind of solution also increases complexity as a way that all the different clouds included must be maintained and be operational as these are needed [47].

3.2 Different cloud models

Cloud platforms are usually identified to be utilized by three different methods that are Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a Service (SaaS) [2][3]. All these different cloud models have also their different architectures and security issues associated with them [2][3]. As different components depending on the model are responsibility of the providers and others are the company's responsibilities to take care of. Having such a gap between those can and will pose security risks and issues if the whole solution is not thought out properly filling the gaps and identifying the points of problems. Different responsibilities can be identified from table 1 that showcases high-level responsibilities of different cloud models. These responsibilities may also vary based on the cloud type utilized.

IaaS	PaaS	SaaS	On-Premises
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Physical servers	Physical servers	Physical servers	Physical servers
Physical hosts	Physical hosts	Physical hosts	Physical hosts
Physical network	Physical network	Physical network	Physical network

CSPs or Vendors responsibility
Customers responsibility

Table 1: Overview of responsibilities

3.2.1 Infrastructure as a Service (IaaS)

IaaS is utilized when companies require underlying servers and network to be utilized but they do not actually want to own the servers [6][9][12][16][22]. IaaS can be considered as a foundation layer of the three cloud models [6]. IaaS can also be seen as most comprehensive and flexible type as it enables provisioning and management over the internet [22][55]. Companies utilize these via virtualization technologies provided by cloud providers [3][14]. This also means that as the companies are responsible for these virtualized servers, they must maintain the software running on the server's even though they do not utilize the hardware associated [33]. As this kind of approach can benefit companies in multiple cases such as standardization of the environment and automation procedures the security issues associated needs to be thought out and build in a secure manner [16]. So, more responsibilities are issued to company to manage these and make sure that architecture design supports this.

This kind of model is utilized when wanting to have more control over the infrastructure and more flexibility is needed [55][54][53][48]. Automation and management of this kind of model are also better as the resources can be retained as per need [54]. IaaS is useful when control over the infrastructure is preferred and building flexible environment in the cloud based on the needs is identified to be an important factor [53].

3.2.2 Platform as a Service (PaaS)

PaaS is utilized when companies require a platform to run their applications and software's [6][9][12][16][22]. PaaS can be seen to be built on top of the IaaS and inheriting the relation between these layers and capabilities [6]. This way also the other responsibilities are included into PaaS model such as OS, middleware, and runtime tools [22]. These applications can be customized and scaled more easily with this kind of solution and outsourcing different responsibilities to meet the needs to manage just the applications [14][28][33]. PaaS has different things built-in such as tools, security, and interfaces [16][54]. This kind of approach also imposes its own risks and issues that requires a lot of consideration as of when to utilize this and who is responsible for different parts of the utilized cloud platforms.

As the resources in this model are based on the need this approach also allows the possibility for multiple users to be incorporated to utilize resources provided by this model [55][54][53][48]. This model allows just the needed resources to be running that the people

can then utilize or build on top of allowing more focus on the automation and on to the actual solution rather than underlying resources [48][53].

3.2.3 Software as a Service (SaaS)

SaaS is utilized when companies require to run just software without thinking of underlying hardware's, applications, and other parts of the infrastructure [6][9][12][14][16][22]. This way the underlying application where the software is run is maintained by other parties [14][33]. SaaS can be seen to be built on top of the PaaS and inheriting risks and capabilities of the underlying resources [6]. This eases up the possible utilization in a way that the solution can be reached from multiple places and the management of it is done by the vendor [16][55]. As the SaaS is a developed solution and managed by that party it allows for more proficient business services to be delivered [22]. There are different security issues associated with this approach and when to utilize it depends on various factors. These different issues are provided with more details in next chapter.

As this model is incorporated with the vendor providing service it means that vendor itself is responsible for maintaining, securing, and enabling compatibility of the service allowing only the utilization of the service in different cases [55][54][53][48]. SaaS also can eliminate applications to be installed locally and instead utilize them over the internet [48][53].

3.3 Cloud issues and challenges

As all these methods to utilize cloud platforms differentiate in few ways also the issues and challenges related to them are a little bit different [2][3]. There are different types of security issues associated in all of them that will be identified in this chapter. As these different models also utilize service providers in different ways also different kinds of challenges arises from that and these challenges will be introduced alongside issues [2][3]. Specific model and issues associated with cloud models are introduced but same issues can also be incorporated with other models.

3.3.1 Infrastructure as a Service

Infrastructure as a service (IaaS) model has multiple different issues and challenges that are associated with it as the responsibilities of this model is greater than in other models [9]. These include different cases from technical perspective to people involved with it. As within this kind of approach there are more responsibilities for organization to take care of, there are

different kinds of risks associated within the responsibilities. Following is an introduction of common issues that are associated with IaaS approach.

Misconfiguration is a common issue with IaaS approach as there are multiple different kinds of services involved [52][50][49][43]. This issue can occur in multiple parts, but one main concern is misconfiguring authentication and authorization methods [43]. As the visibility and control over infrastructure might be lacking, they could also need to rely on Cloud Service Provider (CSP) provided controls [52]. This way unauthorized access is possible within different resources and could go even further down the infrastructure causing issues [50].

Data leaks are one major issue with this kind of approach of utilizing IaaS [25][35][31][52]. This issue is one of the biggest concerns for organizations [25][52], Data can be leaked with two different ways that are static and dynamic leakage [2]. Static data leakage affects the data stored within the environment and dynamic leakage refers to data that is transformed within the environment [2]. As there are large number of users and large amount of data authorizing mechanisms can become a complex task [3]. Data storages might also be prone to changes that could cause issues with data leakages [35]. There could be regulations and compliance issues that need to be managed and data should be protected accordingly in these cases. Data leaks can be a problem in different parts of the system and all variations can be hard to identify [31].

Data security is one major concern for IaaS approach [3][24][58]. This issue is relevant when talking about multitenancy of the environment that shares the resources underneath [3]. As for data security it might be challenging to implement feasible solutions architecturally and other data protection features would be needed [24]. Data should be encrypted for security purposes as if it is not; data is exposed to unauthorized access and theft [3]. Data security itself can also mean that data transferred to other components are vulnerable or data stored is not having enough protection.

Cyberattacks are relevant issues as they are highly targeted towards cloud environments due to the high amount of data and services within [3][58][43]. There are different types of attacks and each pose different kinds of risks and target different parts of the environment [43]. There are also common ones and new ones being developed to be more sophisticated [58].

Vulnerabilities of the applications and services are one of the issues associated with IaaS [12][30][58]. As there are different kinds of environments within cloud, the vulnerabilities

can cause issues with the environment the applications are run [5][58]. There should be procedures and tools in place for managing and identifying vulnerabilities [12]. As there can be layers built on top of the framework it increases complexity and could allow more vulnerabilities within the environment [5]. Vulnerabilities can be on the application, Virtual Machine (VM) or in different parts of the infrastructure configurations [3][30].

Lack of awareness and knowledge can also be considered as one of the issues with cloud environments as this increases the chances for other issues [8][33][57][53]. By not having awareness or knowledge it can lead to other issues such as vulnerabilities and inadequate risk management thus security management is lacking [8][53]. As utilizing new environment such as cloud from different kinds of Cloud Service Providers (CSPs) it is critical to have people that know what to do [33]. As for this kind issue the people that do not have enough knowledge could cause other issues to happen such as misconfigurations, vulnerabilities, data issues, operational problems, and architecture design failures [33][57].

Service Level Agreement (SLA) issues can also pose security risks as if the provider is not responsible to take care of the issues on time [18]. As SLA is an agreement between parties the context should provide enough details to know the responsibilities of the parties [18]. This could cause security issues or downtime of services which in turn causes harm to the organizations.

Insider threats pose security issues as these people have access to the servers and data that resides within the provider [20][51][50]. As there is a lack of transparency and other issues with services the users can gain higher level of access and have access to different parts of the system or data [3][50]. As there is not enough transparency over the insiders and recruitment it is possible to cause issues from the provider side or the organization side [20]. These people could do a lot of harm to the environment or services or have access to sensitive data which is a security risk and privacy issues arise [51].

Complexity can also be identified as an issue as utilizing cloud can differentiate from more traditional approach [28]. Cloud environments themselves have different responsibilities and even services and components are built differently, and this might cause difficulties of overseeing the environment [28]. Adding into this are the different security measures, maintaining and upgrading them and all the other infrastructure related tasks.

Availability of the services can be an issue as the services needs to be available to be utilized in a way they are designed to [14][20][24]. As the availability of the services or infrastructure is needed for organizations the problem of how to ensure it can be seen to be as an issue without proper SLA in place [20]. As if the utilized data is not available it might cause other issues for services [24]. If the availability of the services is not proficient then this will cause issues later and could even be a compliance issue and leading to other issues such as attacks and even data leakage.

Privacy can also be an issue as of possibility of violating regulations and compromising sensitive data [14][15]. One of the biggest concerns is the privacy and handing it over to different provider as it can be compromised [14]. As users' data can be stored within the cloud it is targeted by attackers as to gain benefits based on the sensitivity of the data [15]. As privacy itself needs different issues to occur it is hard to identify as an issue as it is also involved within data leak and needs security measures for compliance.

Compliance itself can be seen as an issue with this model as the responsibilities are in the utilizers care [3][52][49]. As SLA is important document within the cloud it contains the agreement of both sides to ensure that compliance is matched at different fields agreed within the document [3]. This means that the solution needs to be compliant based on the regulations and if unknown factors are included it can be hard to grasp such issue [52]. For compliance issues there should be identifications done as of what different data and resources are regulated.

3.3.2 Platform as a Service

Platform as a Service (PaaS) model approach has its own issues and challenges compared to others. There are also certain technical aspects that need to be considered more and identify the parts of the system that are not the responsibility of the company utilizing this model [9]. PaaS issues will be introduced to identify what different kinds of issues are associated with it.

Data security is also one of the major issues with PaaS approach [3][58]. This becomes more relevant when multitenancy is included as same resources are shared but tried to be isolated to certain users [3]. As if the data is not encrypted and protected, they are prone to unauthorized access and even theft. Data security can be an issue in transferring or storing the data.

Data leaks are also issues with PaaS as the data must be managed and transferred properly within the solutions [3][35][31][52]. As the data or platforms can be used multiple times or

changing there can be improper sanitation done to data that could cause data leakage [3][35]. Data leaks can be an issue in multiple parts as also the network, storage and applications involved could leak the data [3]. Confidential information might be leaking or lost as when this issue occurs and could cause negative impact on business of both parties [31].

Unauthorized access or access control to different parts of the systems can be major issue with PaaS [7][10]. Network communications and access should be controlled with the usage of authentication, authorization, and traceability to enable proficient access control [7]. Enabling different ways of protection such as two-factor authentication could protect also certain resources [10]. This kind of issue can provide too much access within network or certain servers and there should be Identity and Access Management (IAM), or Privileged Access Management (PAM) solution that provides authentication, authorization, and traceability to mitigate this [12]. By lacking access control there can be issues with too vague access rights and shadow accounts.

Underlying infrastructure security is one issue of PaaS approach. This means that these parts of the system are provider's responsibility, and it is up to them to implement security fixes and mitigation methods for these parts of the system [58][57][56]. As for not knowing about the underlying infrastructure, there can be unknown vulnerabilities involved with different platform configurations [57].

Integrations between different services is also an issue with PaaS as there can be challenges integrating these to work properly together [27][53]. As the usage of these integrations can be different and the configurations for different integrations can also vary thus causing issues and challenges [27][53].

Runtime issues are one issue that is also related to PaaS approach as it indicates that solutions might not be optimized to be utilized by wanted means and services [59][53]. If the PaaS service is designed to be utilized in certain way, it might not be functional with other needs and causes issues [53]. In case of runtime failure there could be other issues such as isolation failures [59].

Operational limitation can also be identified to be an issue with PaaS solutions as it may limit how solution is managed, provisioned, and operated [58][53]. As the PaaS solution is Cloud Service Providers (CSPs) responsibility the limitations might become a hindrance for better utilization of the solution [53].

Complexity of the platforms can be considered as an issue [28][56]. With different kinds of platform utilization, identifying and adding the correct components to work together could prove to be difficult [28]. Adding into this is the possible customization that might be done and integrating these into the platform which could increase complexity and need further inquiries.

Customization of the PaaS solution is also identified issue as if designing this solution to work only with certain tasks can neglect the future needs of the solutions and upgrades [17][53]. As for not having enough possibility for customization was introduced to be one of the biggest concerns [17]. But building solution to work with different needs could also increase the complexity and maintenance while adding vulnerabilities into the platform itself [53].

3.3.3 Software as a Service

Software as a Service (SaaS) model has many similar issues that has been identified already but there are also different issues and challenges. This model is tied up more towards the utilization possibilities and standards of the service being provided with outsourcing certain responsibilities and functionalities to the vendor [9][29]. Following is the identifications of SaaS issues and description of what is meant by each.

Application security is one concern regarding SaaS approach as it indicates that the application itself should be secure enough to meet requirements and future issues [27][57]. As applications are used from the vendor, vulnerabilities might not be known [57].

Data security is also concern within this approach [35][58][57]. As the SaaS could be utilized more in a multitenancy mode it is also an issue towards data security [3][57]. As the data could be residing or transferred within untrusted channels the security can be seen as an issue [35]. This is because organizations must rely on the providers to meet the security measures regarding the data, and these might be lacking [57].

Interoperability is an issue for SaaS approach as it means that if the service is not following standards the integration may not function properly [29]. This could lead to designing own solutions or reduce dependencies with the service utilized.

Lack of support can also be seen as issue with SaaS as there might be a lot of support needed to enable functionalities to work properly and in secure manner [28][53]. There could be

various resources causing issues and lacking in support this could cause larger issues if not managed properly [28]. This could also increase the complexity of the solutions if not possible or taking a long time and custom solutions are added [53].

Customization is also an issue as the service is built for multipurpose and this limits the usage and could also pose security risks [53]. As there are no customization possibilities this could increase complexity as different components and solutions would be needed to mitigate issues [53].

Performance and downtime can be seen as an issue with SaaS as the vendor controls that part of the solution and manages the underlying services [19][53]. As for this kind of issue the contract and Service Level Agreement (SLA) should be appropriately covered [19][53]. This poses threats and security issues towards the vendor and decreases the possibilities to mitigate certain risks from happening [53].

Lack of control over the utilized SaaS solution is an issue identified [19][24][28][56]. As for lack of control the understanding of provider's controls and patching and releases needs to be known [19][56]. Solution might still need modifications, and this would also need time for before proper usage of the solution [24]. As there can be multiple assets within the cloud there can also be mismanagement of those assets that causes issues [28]. This would indicate that if something has issues over the utilized software then the control methods cannot be utilized and certain tasks and methods needs to be raised towards the supplier.

Limitations of the software are also one identified issue of the SaaS model as it indicates that software has certain limitations in which it must be utilized [24][58][43]. This indicates that if wanting to utilize software in certain way it might not be possible and only certain flow of work can be done [43]. As the solution might still need other modifications because of limitations this would hinder the usage of such solution [24].

Security in underlying parts can also be raised as an issue as it is impossible to know what happens inside the software and infrastructure without asking from the vendor [28][58]. Even though there can be simplifications on the interfaces it might inherit other issues such as complexity, privacy, and security issues [28]. If there are security issues within the software or infrastructure, then these must be raised towards the vendor and wait for new releases.

Security in utilization of the SaaS can also be identified to be an issue [27][56][45]. As the solution is provided as SaaS the utilization of the solution might also pose issues [45][56].

Organizations might need to consider additional security measures to tackle this issue [27]. As if utilized in wrong way it might not provide the needed information or give too vague knowledge if utilized in wrong way.

3.4 Cyberattacks to cloud environments

Following is introduction about attacks that might occur on cloud services. There are multiple different kinds of attacks, and therefore it is also relevant to consider such attacks to be mitigated with good architecture design, security measures and decisions to enable the integrity of the systems [1][3].

3.4.1 Different attacks

Cloud environments are also targeted to be attacked by different kinds of attackers and attacks [1]. This chapter will discuss these different kinds of attacks and identify what they are and how can these pose issues within the cloud environment.

Denial of Service (DoS) attack is an attack that tries to render the servers or services unavailable with flooding a lot of traffic and calls to the servers [1][3][25][26][32][37]. This is one common attack towards cloud environments as it can cause issues with multiple parties depending on the approach of the cloud type and model utilized and servers targeted [1][3][32]. DoS attacks can be categorized into two different types that are network level and application level [1]. As DoS is one of the most threating attacks towards cloud environments it becomes with problems that services are unavailable and could increases workload that is matched with more computational power that could lead into bigger problems [1][37]. DoS attack could cause economic value issues and availability issues as the resources are exhausted [26].

Side channel attack is an attack that targets virtual machines and their services running on the same host server to gain access or information from targeted machines [3][30][32][35][37]. As the resources are shared there can be attacks targeted towards Virtual Machine (VM) or even cache [30]. This attack can cause issues within the VMs of the cloud and be considered as a critical one but is not easy to perform [3]. This attack utilizes the surface of one host and multiple VMs running on top of that host and sharing equipment can be dangerous [32][37]. This attack can cause all the data or sensitive data to be compromised for the attacker [30][32].

Malware injection attacks are an attack type that tries to take control of user's information [25][26][37]. These can include malicious code insertion or even malicious VMs to be inserted into the solutions [3]. These could also affect the cloud services by modifying the functionalities [5]. Attackers try to add their own services or VM instances for this purpose and try to get users to be redirected to these malicious implementations [37]. Common forms of this kind of attacks are Cross-site Scripting (XSS) and Structured Query Language (SQL) injection attacks [26][38].

Man-in-the-Middle attacks are an attack where attacker tries to get in between user and the server to intercept the messages between these entities [3] [25][32]. This attack utilizes network packets, filters, and transmission protocols to gain access to intercept the traffic and gain the information and later utilize that for malicious activity. This kind of attack is possible if the communication channel is not secured properly [3]. Attack could even be done to access data communication between data centres [5].

Domain Name System (DNS) attack is an exploit where vulnerabilities of the DNS system are targeted [38]. As DNS is heavily utilized by different services the attacks can vary a lot depending on the targeted system. DNS security is used for protecting the DNS system from the attacks [25]. As per this kind of attack the DNS data and origin might be compromised to cause issues with data integrity [25].

Zombie attack is an attack that slows down the network and throughput of the network and is mainly utilized as a part of the DoS attack [5][21][35]. This attack can utilize different hosts within network to send requests and these are called zombies [5]. This attack floods the services and can cause issues for availability by exhausting all the resources with DoS or Distributed Denial of Service (DDoS) [5][21].

VM Escape is an exploit that tries to bypass isolation of the host and Virtual Machine (VM) to gain access to the hypervisor [1][3][21][30]. VM escape is not easy to deal with and could even need new design on hypervisor to control this attack [30]. Even one breach in the VM can cause huge impact towards the whole virtualization environment and can be achieved with malicious code placed in VMs [1]. With this attack the attacker can monitor and gain access and even root privileges to the environment and even shutdown the VM [3]. With VM escape attacker can gain access to the operating system and other VMs running on that physical machine [21].

Backdoor channel attack is an attack type that utilizes the applications and their vulnerabilities and debug functionalities [3][5]. This attack could breach the privacy and confidentiality of the data [3]. This attack could also enable the affected resources to be controlled or utilized in a zombie attack [5]. This way attacker can gain access to underlying application or server to run their code or find other ways of attacking [38]. One example of such is Log4J attack that has had a big impact in cloud environments.

Metadata spoofing is an attack that targets systems based on the data utilized for communicating with web service or with services metadata file [3][5]. This data can be modified by attacker and if this is successful then they get access or other relevant information from the service without actual proper metadata [3].

There are also different **virtualization issues** such as specific attacks for insiders and external and co-residential or side-channel attacks [30][35]. Virtualization can be seen to affect different parts such as application, hardware, network, and storage and each one of them can have different issues [30]. For insider attack the knowledge about the utilized VM can lead to vulnerabilities and attacks [30]. External attacks include a way to utilize the VM in a malicious way as there might not be proper authentication and authorization in place [35]. Services and VMs could be compromised with these issues, and this could cause privacy issues for data and availability issues in network, application, and hardware level [30].

Rootkit in hypervisor can also be seen as an attack targeting cloud environments as it tries to compromise hypervisor and gain access on to the VM [21][35][40]. Rootkit itself tries to hide itself from being identified and this way gain access into the underlying system and VMs [40]. This attack makes it possible to control of any of the VMs that are running on the host and activities to be modified on the system [21][35]. This attack can also be used for creating backdoors into the systems [40].

Advanced Persistent Threats (APTs) are also attack types that try to continuously attack the environment in a way that attack is designed [58]. These attacks target data for example and can adapt to different measures giving more accesses along the way of the attack as per needed to [58]. With these attacks the attackers can gain access to the systems and networks and use that to steal the data or use it for other malicious activity [58].

3.5 Recovery methods

This chapter introduces ways for recovery after issues have occurred or attacks have been performed. These different methods have been identified to be ways of controlling and mitigate aftermaths of issues or attacks.

Scaling of the services and adding more servers when needed is one way to recover when issues start occurring that relate to resources and utilization spikes of the solutions [39][43]. As the services can be scaled based on the demand certain cloud types might be more preferred [39][61]. This method enables more robust implementations for the servers and can enable servers and services to be measured per usage enabling only the needed resources to be run at a time.

Different Cloud Service Providers (CSPs) offer own **tools** for recovering from issues and controlling or mitigating them [58][57][33]. Tools are usually independent for that cloud provider [33]. As one of the tools to utilize is also Web Application Firewall (WAF) that could identify specific threats and trigger an event based on that data [57]. There can also be tools for backups that are taken and ensured to be available in case of disaster [58]. Utilization of these tools depends on the case and the need for the services and these tools can give ease of usage as a third party is taking care of the identified issues.

Automation of the deployments and building infrastructure in a way that enables the environment to be implemented from code is also one way to recover from issues [59][43]. This kind of methods helps keep track of the changes and ensuring that the environment is configured with needed properties and decreasing hand made errors throughout the environment and systems [59]. Automation should contain as much of the needed resources and infrastructures as possible as a relevant way to recover [59].

Backup and restore is one of the common recovery methods to be utilized [14][36]. Backups are helpful to keep crucial data at hand and utilizing cloud solutions could help keep the data available in case of disaster [14]. This recovery method is one of the easiest, cheapest, and fastest [36]. This method takes backups of the servers, applications, and data. When disaster strikes, these backups can then be restored to different servers or taken into use elsewhere for a fully functional system. Depending on the backup periods there might be some loss for data or other relevant configurations.

Replicas of the data or services utilized are one way to recover from data loss or even mitigate issues regarding it [61][44]. This method can ensure that there are certain services or sets of data always available to be utilized. With these replicas it is also possible to ensure that only certain methods are allowed such as read only of data to mitigate issues of data manipulation.

Controlling traffic amount automatically can also be a recovery method to ensure that only certain amount of traffic gets through to services mitigating issues with Denial of Service (DoS) types of attacks [44]. This ensures that at least some amount of traffic is always getting through while trying to find other mitigation methods for utilization in case of an issue.

Pilot light is a recovery method that utilizes only the bare minimum of the core services and components to be replicated [36][60]. When disaster strikes this approach ensures that there are still core services running and enables to start recovering on top of these services saving time.

Warm standby is a recovery method that has smaller scale of the working environment up and running on different location than where the main servers are running [36][60]. This way it is possible to start utilizing these servers with little to no time wasted when the main location is out of service.

Multisite deployment model is an approach which enables the services to be operational on multiple different regions or Data Centres (DCs) at the same time [36][60]. This solution can be utilized to be fully working all the time or certain regions being on a standby like in few other methods.

4 Case study: Risk management and architecture design

This chapter discusses about different cases that utilize different cloud models. This chapter includes an overview of the cases and what is needed in those. There will also be discussion and risk management done for all the introduced cases to identify the issues and risks associated. Based on the risk management also control and mitigation methods are introduced. This chapter introduces also architectural design as of what kind of setups would be feasible with each case and why. As per these architectural designs security measures are introduced in the architecture as a way of controlling and mitigating risks if applicable. From these it is also possible to identify the differences of the cloud models and how they differentiate.

4.1 Overview of cases

This chapter will discuss about three different cases with different kinds of utilization of cloud models. Cases include a large-scale cloud migration, platform to run custom components and Identity and Access Management (IAM) solution as a service. Cases are introduced as of what they are and general information about them will also be introduced. Components involved and recovery methods are introduced in a way of why these are relevant specified case.

4.1.1 Case 1: Cloud migration

Case 1 is about a large-scale cloud migration from on-premises data centre to cloud provider. This case introduces many aspects of what different services and security measures are needed to be included when thinking of migrating services from one provider to another one. As before things were done with another service provider the lack of information and what was happening in the systems proved to be causing issues. By moving to other service provider on cloud it was identified that they would have more information about the underlying infrastructure, and therefore specific cloud type and model was applied into this case. As this is a cloud migration of the already built infrastructure and services there are already multiple different components that needs to be in place in the design.

As in this case the data and services utilized needs to be **compliant** with regulations private cloud type was chosen for this. This ensures that cloud servers and needed resources are in specified location and defined to be utilized only for this case. Based on the regulations the corresponding resources that can be utilized must be in specified location and this is also why only certain Cloud Service Providers (CSPs), and solutions can be utilized. Mainly because of

such regulations the usage for private cloud type is identified to be a correct approach for utilization of cloud environment.

This approach includes multiple different **components or services** to be included within as the whole infrastructure was migrated while allowing different components to have the needed systems and updates that are needed for those to work properly. There are components related to network, cache, security, and data that need to be operating to create a large-scale solution such as in this case.

Because of such a large-scale implementation the utilization of **network related components** such as Domain Name System (DNS), Load Balancer (LB), Web Application Firewall (WAF) and firewalls are required to be operational. Different kinds of LBs are needed as per the usage and possibility to mitigate issues. WAF is identified to be needed for adding a security layer for mitigating risks. Different kinds of firewalls or equivalent are also needed to ensure that traffic can be limited to only allowed resources.

Reverse Proxy server is identified to be added into this architecture to control the traffic, add rules and policies to increase the security further down. Addition to this there are other services utilized for creating tokens and build federations between different services. This was utilized from own service as it can be configured without causing downtime for other services included and thus mitigate certain issues from happening.

Cache servers were identified to be needed as sessions were enabled to be managed by such. This way externalizing cache layer the utilization and storing of such could be utilized in a way to have centralized session store that replicates the data for failover

Data itself must be residing with own segment and managed with authorized access to be compliant with regulations. As this data is residing with own section it must be also available in case issues occur. This also means that certain security measures must be added on to this layer as of mitigating issues.

As ways of **recovering** from certain issues in this case the utilization of scaling, automation, backups, replicas, and multi-site deployment is considered. Scaling itself increases the resilience towards issues with resources being exhausted. Automation should be utilized for deployment and ways of establishing environment from scratch. Backups should be taken as a possible way of restoring data and environments. Replicas were also identified to be a recovery method as it enables the utilization of services even if other service would have

issues and thus enabling availability. Other utilization of the recovery methods is the multisite deployment model to have high availability of the services as these can be run from different places thus mitigating issues.

4.1.2 Case 2: Platform to run custom code

Case 2 is about creating a custom platform where custom Docker image and custom codes are to be run. This kind of approach was needed to ensure that certain underlying components per custom needs were in place for the specific tasks. This approach was also needed to ensure a place where custom automation needs were to be run and platform that could be isolated from the rest of the components while enabling access to only those required components.

As this case has an approach for updating different configurations when needed, the case could be implemented within the private or public cloud, but **hybrid cloud** approach was chosen for this case considering future needs and the need for communicating between both public and private clouds. This platform is only needed at the time when updates are to be defined and implemented so the possibility to run this platform when needed can also be considered. Application itself utilizes public cloud and can access to parts of the private cloud that are considered relevant. As the data of the platform resides in a repository the platform has only the needed Docker image that can be updated per needs.

By adding a **platform with custom Docker image** to be in place for this solution the required packages and components can be more feasibly managed by the utilizer while still minimizing the updates and server-side changes. This way it is possible to focus on the applications and data it utilizes. Also, access to this platform can be restricted more feasibly and different kinds of access rights needs to be in place.

This kind of case of Platform as a Service (PaaS) solution needs certain **components** to be in place that are an Identity and Access Management (IAM) solution, platform for the custom needs, repository for configurations and the servers for updating. Solution also needs components related to security and to match network issues certain security measures must be ensured to be taken into use. This solution itself does not take part as of how the servers are protected outside of this solution but ensures that access to those servers comes from specific Virtual Private Cloud (VPC) containing this platform. So, for this Network Access Control Lists (NACLs) and Security Groups (SGs) are to be considered for network security alongside VPC. With similar measures also the access to other resources that are not needed can be

blocked. Also, IAM or Privileged Access Management (PAM) solution should be in place as to mitigate the access towards the platform. Repository access and related protection are to be considered alongside.

Recovery methods for this case include automation and backups. As this platform itself is utilized for automation also the provision for it should be automated for future usage. On the other hand, the backups of the platform and residing data such as Docker image should be implemented. This backup would allow the future usage or even another platform to be utilized.

4.1.3 Case 3: IAM solution as a service

Case 3 describes a case where resources are protected with the utilization of Identity and Access Management (IAM) as a Software as a Service (SaaS) solution. This enables the people to focus on the services they are responsible while externalizing identities to Identity Providers (IDPs) and access rights to the solution. This approach was needed to ensure the utilization of trusted IDPs to provide identities to access the services developed and running.

This case could utilize all the different cloud models, but **public cloud** model was utilized for this case. Case itself does not need to be in private cloud as it does not contain specifically regulated data that would need it to be run in private environment but if the services or the application would require that it could be considered as an option.

This kind of case has fewer **components** in place and really needs the service that is IAM solution to function properly, Load Balancer (LB) to control traffic and backend servers to run the applications. There are also certain network layer components and security measures that need to be in place to mitigate certain issues. Services are still considered to be utilized from Virtual Private Cloud (VPC) and controlled by Network Access Control Lists (NACLs) and Security Groups (SGs). These would be feasible solutions to controlling the traffic and what type of traffic and where traffic is allowed.

Case itself has different kinds of issues being **compliant** and having security in place for the solution. In the risk management chapter these security issues are introduced in more detail and ways of mitigating these.

Extracting **IAM layer** out of the architecture the whole architecture becomes more simplified, and solution can trust what is provided by the IAM service. This way it is possible to

centralize IAM solutions and have the user and access data be provisioned from another place rather than from this one. Solutions can then manage the data they receive and add the values they need but still having a general place to get the identity information and if that user has access to their service or not.

Recovery methods for this case include scaling of the services, automation, backups, and tools such as the utilization of the IAM. There is also the possibility of utilizing pilot light, warm standby and multisite deployment for this case to recover from issues. But in this case the utilization of warm standby was most relevant. As case itself tries to have services up and running most of the time the utilization of warm standby was identified to be most useful. Utilizing scaling enables this solution to ensure that services are available to the users. Automation should be considered as of the possibility for recovering and establishing the environment. Backups are needed to ensure that services can be restored till certain point in time if something were to happen. Certain tools such as the IAM service in this case is ensuring that identities and accesses are easily accessible also in case of issues with other parts of the system.

4.2 Risk management

This chapter consists of identifying risk management types and process as well as introducing risk management of the three cases that were introduced earlier. Different risks are identified per case and their control methods and mitigation methods introduced. Risk management allows for better understanding of security issues and ways of mitigating these within different kinds of cases and approaches [28]. Risk management itself should start with a set of risks and later contain a lifecycle as it must be updated to manage also new risks that are identified and monitored constantly [28].

4.2.1 Risk management types

There are various kinds of types and frameworks built around the concept of risk management and these types and frameworks might tackle different industry needs or propose additional points to be considered at different stages of risk management process [62][63]. As with such differences in the types or the frameworks provided organizations should find the feasible solution that fits their needs of risk management or create a custom approach for it. These frameworks might also be used just for specific parts that are involved with risk management and could also differentiate depending on the risks type.

There are certain different types of approaches such as traditional risk management, Enterprise Risk Management (ERM) and Collaborative Risk Management (CRM) that can be seen to propose different frameworks for risk management [62][63][64]. As for the traditional risk management type it can be considered as to be utilized to identify issues or risks for further consideration and mostly considers impact of the risks [62][64]. For ERM approach it adds layers on top of the traditional risk management and considers about the severity and likelihood of the risk and other aspects related [62]. ERM also tries to add a possibility for preventing the risks from happening and increases the possibility to match these risks that are identified [62]. CRM is another type of approach for risk management that tries to enhance the collaborative field with own procedures and standards to be utilized while also sharing relevant information and establishing a way for joint decision making [63].

As there are different types of the approaches for risk management there are also different frameworks such as with ERM approach. For ERM there are COSO, ISO, COBIT and NIST frameworks among others such as custom solutions [65]. These frameworks each contain their own phases to work with and the number of phases may wary, and each phase contains a set of procedures to be applied into the process [65].

The risk management approach for this case study was to go with ERM and utilizing the severity and likelihood attributes of the ERM type. This will enable the utilization of the risk management tools while indicating procedures and processes to be followed of this approach. Utilizing this approach also helps to add a layer of the approach containing the attributes and ways of identifying controls and mitigation methods for identified risks.

4.2.2 Risk management process

Risk management process itself could contain different steps regarding of the approach or the framework taken but it mainly consists of steps such as identification, assessment, actions, and monitoring [66][67][68]. Risk management process can also be seen from figure 1 which contains these four main steps. These steps could also include additional steps or split the bigger steps such as assessment into analysing risk and calculate risk level [68]. Actions step could be split into identifying relevant measures to be taken for controlling the risk and introduce those into use [66].

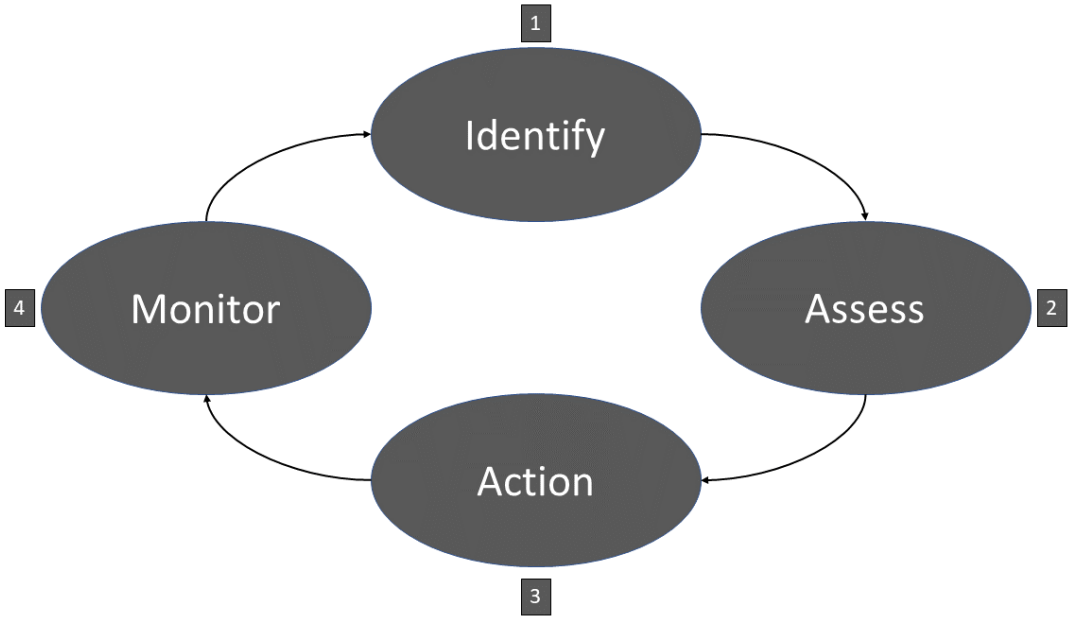

Figure 1: Risk management process overview

Identifying phase is an important step of the risk management process as in this step risks and issues are introduced for further consideration [66][67][68]. Risks can be identified at different stages of the projects and with adding these into risk management the next steps targeting that specific risk can be discussed [67]. It is important to identify common risks and issues for further discussion and identifying the relevant ones for that specific task at hand. Also, the different factors associated for those risks should be introduced as these are very common cause for issues [66]. As these risks might vary a lot depending are they internal or external risks or what types of risks such as regulatory or environmental risks etc. they are [66]. It becomes essential to identify risks as to target them on the correct place of the risk management process [66].

Assessment phase of the risk management process contains the parts of the process where analysing the risks is important to have good knowledge about the risk [66]. From this analysis and how it affects the project it is then possible to determine likelihood of the specified risks alongside the severity of the risks [68]. With these identified resources it becomes possible to rate the risk and treat it accordingly [66]. One way to rate the risk is the utilization of the risk scoring matrix where the likelihood and severity plays an important part to identify is the risk considered to be rated high or low [67][68]. Based on these outcomes it becomes possible to have actual discussion is the risk relevant to be controlled or mitigated and how much resources should it take for control and mitigation [66].

Actions phase for the risk management process is the part where the identified control and mitigation methods are used when considering should the risk be mitigated or not [66][67][68]. There could be multiple different ways for controlling the risks in risk management process [67]. For controlling the risks for this case study there are different control methods introduced that are avoidance, prevention, reduction, separation, duplication, and diversification. Avoidance means that issues or risks are avoided from happening but still monitored [67]. Prevention means that issues or risks are tried to be prevented from happening [66][67]. Reduction means that attack surface and possibility is reduced to minimal [66][67]. Separation means that different components are separated from one another. Duplication means that resources or components are duplicated to withstand issues or risks. Diversification means that risks and issues are diversified into multiple different parts thus reducing the possible risk or issue from happening [67]. Within the action phase these control methods are identified for specific risk and based on the methods following mitigation measures can be considered and taken into use.

Monitoring phase of the risks is an important part of the risk management process as it indicates that identified risks have been assessed and control and mitigation methods taken for those [66][68]. Risks need to be monitored and managed in a way that the process is completed, and actual methods taken into use [67]. Based on the monitoring also new risks and issues can rise and the risk management process should start to add these new risks into the risk management lifecycle [66][67]. By utilizing risk management in this way, it becomes possible to proactively raise risks and issues but also increase security as if the process itself allows the process to be robust enough to manage these newly found risks and their mitigation [67]. By monitoring also, the risks it becomes possible to also add possibility to control risks that might have not been dealt with at the first phase as it was not rated high enough [67].

4.2.3 Case 1: Cloud migration risk management

Case 1 has multiple different kinds of risks associated with it from cyberattacks to internal threats and different misconfigurations. List of identified risks can be seen from appendix 1 with control methods and mitigation methods while also evaluating the likelihood and level of the risk. These identified risks are discussed and how they should be managed or mitigated with security methods and measures.

As the approach for this case is the utilization of the cloud and taking responsibilities of the infrastructure while outsourcing the other parts of the environment to Cloud Service Provider

(CSP). This approach means that the different **responsibilities** must be understood by the organization and applicable people and knowledge must be gained. As for the responsibilities there must also be Service Level Agreements (SLAs) identified towards those and ensured that CSP meets them when there are risks or issues identified that targets them or is identified to be on a so-called grey area which is between responsibilities.

There can be different **insider threats** identified that in some cases mean that the CSP people that are responsible for the servers can be malicious or then the people deploying and developing applications and services. These are to be considered as two different risks as one is more subjective to how and who can access the actual servers running and how the CSP manages these people. As in this kind of case strict SLAs and contracts must be made to mitigate such issues from happening but it still does not remove the possibility of this kind of breach from happening but instead compensates it. Other approach of the insider threats are developers and deploying solutions that can be mitigated with multiple different solutions such as automation and testing. This indicates that applications and servers are two different entities and must be managed differently.

What can be seen as an issue with insider threats is an **unauthorized access** to servers. This kind of issue can cause huge impacts to business and give different issues to the whole infrastructure and services causing issues to both CSP and organization responsible of the applications. Unauthorized access to servers can be controlled with different options but one of the most useful solutions is the utilization of Identity and Access Management (IAM) solution. Even Privileged Access Management (PAM) could be utilized when accessible for this to further increase the security and access rights to servers. By utilizing IAM it is possible to only give access to those that need it alongside correct rights to do the needed. As taking IAM into use in the whole infrastructure it is possible to limit the access to all the different servers and services to certain groups and people that need it and even allocate these per server needs. IAM solution limits and controls the accesses to servers while also having monitoring for the irregularities occurring to seize unwanted behaviours and accesses.

As moving to new environment, the **responsibilities and knowledge of the new environment** can be lacking for multiple people. This kind of issue can be considered as a risk as it increases the possibilities of other risks such as misconfiguration or unauthorized access. People should be considered to trained for this kind of work in new environment and indicate different security issues to be considered alongside to mitigate and control this risk.

As people's knowledge is not good enough utilization of the IAM solution can also be utilized to mitigate accesses and what they can do. Also, utilization of the automated solutions such as pipelines can mitigate parts of the identified risk depending on the servers and environments. For application part of the knowledge there must also be identifications to be done as those risks are different from access rights.

As in this case there can be multiple different kinds of attacks done to this environment and each of these are a risk to be identified and control and mitigation methods needs to be implemented. As **Denial of Service (DoS) attacks** are easy and quite common to implement it can be a big issue rendering services unavailable that should be up and running most of the time. This kind of attack can be mitigated with utilization of different kinds of tools such as Web Application Firewall (WAF) or if CSP has their own tools for this kind of attack mitigation. By configuring WAF properly it can identify malicious requests and monitor the traffic that is going through it and block those requests from reaching resources and services. Other way to mitigate and control this solution is to consider scaling of the servers and what capacity is enough to withstand such an attack. This comes with its own benefits and issues as it can be costly if no limitations and descaling's are done.

Man-in-the-Middle (MitM) is an attack that must also be included as a risk in this case as there are different parts of the system handling different kinds of data that can be valuable for attackers. As for controlling this risk there must be security methods in place that ensure data integrity and protect that data. As for the protecting the data it should stay in an encrypted state when transitioning over the different servers and services when needed to. This ensures that even if the data is tampered with it is not feasible anymore as it takes more time to change it and validate it. One other way is to also utilize a model where the calls never end up to the user and calls are done between servers. This way the mitigation and controls are done to ensure that the backend calls and data cannot be seen and accessed to.

Domain Name System (DNS) attack would impose that the domain name of the service is either hijacked and targeted to another resource than the specified one or DNS is like the original and phishing can be done with that domain. For controlling this kind of risk, it is possible to configure DNS on a controlled environment and controlling the access into that service. For phishing attacks the information about those and raising awareness should be considered.

Side Channel attack can also be considered as a risk when starting the project and considering what type of cloud to utilize. As this attack can be controlled and even mitigated with the utilization of private cloud type using it would be a feasible solution.

Malware Injection is in terms like MitM attack that it tries to move user to another Virtual Machine (VM) or domain altogether with certain injections done to services. This kind of attack can be controlled in certain ways such as protecting the resources from unauthorized access and then on the other hand extracting ways of injecting malicious code out of the solutions. For controlling and mitigating such a risk private cloud can be used but it only controls the risk till certain point and other methods are needed to mitigate this risk such as scanning tools.

VM escape can also be considered as a risk at least in the point when thinking about attacks that are possible. As this attack requires more of the shared host it can be controlled and mitigated with the utilization of the private cloud model.

Backdoor channel attack is a risk that was also identified to be a part of this case. As this attack consists of methods such as debug functionality to be enabled it can pose security risks for allowing code or other methods to be exposed. This kind of attack can be controlled by having procedures to ensure that no such methods are being utilized in environments that do not require it. Also considering that these kinds of attacks can be targeted for the areas that are CSPs responsibility it must be ensured that there are SLAs to manage such cases. Other ways for controlling this is to control access and traffic flow to stop the malicious or suspicious calls from getting that far by utilizing WAF or similar tool and limit access to enable such options from services and applications.

Misconfiguration is a big risk in this case as depending on the configuration item it can have large issues coming out of it. Traffic could be routed to wrong place or services rendered unavailable. Too many rights and authorizations could be done enabling unauthorized access or even the applications could be vulnerable because of this. So, depending on the case it can have huge issues involved and there should be different control and mitigation methods thought out for this. As for the control methods the changes should always go through different pipelines depending on the case for ensuring that they are working as intended and human interventions should be minimized to take out the human factor from this risk. So, building automated solutions and pipelines it is possible to mitigate issues till certain point.

As there are multiple different servers for different purposes, these can be **visible to public network**. This visibility is also an identified risk as it can allow attackers visibility of the servers in the environment and create more attack surface. For controlling these servers, the visibility must be thought out and identified as to what should be placed in private visible state and what in public. By creating this kind of plan different solutions can be utilized such as private cloud type and virtual private cloud areas for different cases. Also, straight visibility to servers should be minimized and load balancing should be used that renders the Load Balancer (LB) to be visible instead of the actual servers.

As **data** is particularly important in this case the handling and storing of the data must be considered as a risk. Data must be managed in a compliant matter and for this kind of case private cloud must be considered and identified if data can or cannot be moved outside of the location. For controlling this, the laws and regulations must be inspected, and Cloud Service Provider (CSP) consulted that their Data Centres (DCs) are in correct locations while ensuring that the data is not replicated outside of these. Data must also be controlled as of what is transferred from one place to another and what is visible in the transmitting of the data. For controlling this encryption should be considered and utilized to prevent data leakage and enhance security. Also, servers containing the data should be protected accordingly as these host the data and it might be visible on the servers. So, access to these servers should be minimized to only authorized people and the data should also be encrypted when resting on the servers. When utilizing the data there could also be replicas utilized for protecting the data and even increase the capacity of the servers to fetch the data, they need instead of writing onto it. Creating LB solution will also increase the usage rate of the data and minimize the accesses to the data as per this approach it is possible to limit the access only from the LB to the replica and block other access tries to ensure more secure environments.

This case also includes **session** affinity and that the session identifiers must be present for different services to work. So, handling and storing of the session can be a risk as it could be lost or hijacked. This session hosts valuable data to represent the user's session to be matched with what services they utilize and when. If session would be lost it would cause issues as different parts of the system would then not be working as intended. This kind of approach could be controlled and mitigated with session cache and utilizing replication to backup session data. Even if session or connection would be lost the identifier could still be found from cache and resumed as needed to. Correct session affinities and services managing sessions must also be identified to ensure correctives of the session. For this case session

should be managed by own service and replicated. Hijacking the session should also be identified as a risk as this way other people's sessions could end up in wrong hands. Sessions should be managed properly and utilizing session service instead of cookie-based solution would control and mitigate this till certain point. Also, utilization of token based, and zero trust architecture could mitigate and control this as this way there would be more verification done for ensuring integrity.

4.2.4 Case 2: Platform for Docker risk management

Case 2 has similar risks like in other cases, but it also imposes new set of risks to be identified as the approach, case and utilized methods are different. For a list of the risks identified and control and mitigation methods refer to appendix 2. As of this case also the responsibility model is different that imposes changes to risks and ways that they are managed or mitigated.

Insider threats are a risk for this case as they can access the underlying resources so this kind of risk can be controlled and mitigated by outsourcing the responsibilities to Cloud Service Provider (CSP) when approach taken is company people. Other way of thinking is the CSPs insider threats that can only be controlled through Service Level Agreements (SLAs) but cannot be mitigated. Although it is also possible to limit the access and possibilities for configuration that are in the scope of this case it does only control a portion of it. This risk also needs proper Identity and Access Management (IAM) or Privileged Access Management (PAM) solution for functioning depending on the approach if the platform would be based on the private or public cloud model. That way the control of the accesses can be configured properly, and unauthorized access mitigated till certain degree. Also, one way to control this risk the utilization of automation as it removes the human factor from the platform controlling access to be technical instead of human based.

As it was identified **misconfiguration** is a risk in this case and controlling this there should be automated deployments or pipelines added into use for controlling and mitigating risk till certain level. If human interventions are involved utilization of the IAM or PAM should be implemented to mitigate access and ensure who can run configurations. Misconfiguration itself can also pose issues at different parts of the system and certain validation tools should be considered for controlling risk.

Man-in-the-Middle (MitM) is an identified risk as it would pose that attacker could get in between the data sent or in between what is fetched. This kind of case they could get some

general information out of it or even try and modify the data. This risk would be controlled and mitigated with protecting data assets and enabling network hardenings. This would impose that data sent is encrypted and network structure itself is protected from outsiders. Different measures could be considered here such as Virtual Private Clouds (VPCs), Security Groups (SGs), Network Access Control Lists (NACLs) and encryption tools.

Thinking also certain risks that could occur on **Virtual Machine (VM)** level such as VM escape, and side channel attack can be identified to be a risk for this case. These both could pose issues if attacker gains access to the underlying host and via that into this specific VM. This kind of issue can be controlled in a way that VPC is utilized but also so that the data itself is not contained within the platform but fetched when utilized and removed after. Also access rights as of who can do and what they can do is a way of controlling this risk, but it will not mitigate it if attacker gains root access.

Unauthorized access to the servers is an identified risk that can be controlled with IAM or PAM solution. As there are different kinds of servers involved with this case also certain measures such as SGs, NACLs and VPCs must be thought out to block access from certain areas and allow it from specific areas. This way it is possible to control the access points that communications are done only between authorized services.

Visibility of the servers can also be identified as a risk as it can pose too much information to outside world. This risk is an issue with only a portion of the solution as only certain parts need to be hidden from public network. For controlling and mitigating this issue VPCs, SGs and NACLs should be utilized.

Security of utilization and network are also identified as a risk. As the utilization of the platform is to run certain configurations from GIT repository configurations the utilization environment must be addressed to only work with identified resources and nothing else. This would also pose risk towards the network structure if not done with the least privilege method as different parties could just send their configurations or other information into the resources or fetch the configurations. For utilization of the solution automation and pipelines should be considered and appropriate network security such as VPC, SG and NACLs configured to prevent unauthorized utilization and false repositories being accessed.

As this platform is utilized to run certain Docker image and configuration files the **access** to fetch those files must also be imposed as a risk. This access must be set for certain time or

utilization of one-time tokens from IAM solutions and Security Token Service (STS) could be utilized to provide technical access to certain repository point. This kind of solution would control and mitigate issues as the token could be restricted to be used for this one solution only with restricted access to only fetch certain files.

Utilization of the platform and the solution could also be a risk as if people do not actually know what to do and how it can be utilized it could cause issues. As this platform is needed only when certain updates are needed it should not be accessible all the time but instead run when needed and with correct information in place. This kind of risk can be mitigated with automating processes and building certain pipelines for achieving full use of the platform and its core needs. This way it is possible to mitigate issues with platform being hung out waiting and people getting access onto it.

As this platform is in the centre of different services it could easily have too **vague access** to different services and servers that is an identified risk. This kind of risk must be thought out as to where it should have access and communication possibilities to and how those are managed, and all other accesses should be blocked. So, for controlling this kind of risk utilizing NACLs and SGs to allow only the certain communication types and methods to go through would be a feasible solution.

4.2.5 Case 3: IAM solution risk management

Case 3 introduces a model where most of the responsibilities are outsourced leaving more room for the actual tasks. List of the risks identified, and control and mitigation methods can be found from appendix 3. Even in this case there are still certain security requirements and risks that are identified and different measures for controlling and mitigating these risks will be identified. This case introduces different kinds of risks to be identified as trust to the software and services that is the Identity and Access Management (IAM) solution must be built in a way that it is trusted by the backend components. By utilizing this kind of solution, the usage of the provider’s data must be ensured to be correct, and that solution cannot be bypassed by outsiders. As the identities and access management is controlled by one solution it is possible to simplify the solution design but this itself gives more possibilities for errors, risks, and responsibility issues.

This case has externalized Identities and Access rights to Software as a Service (SaaS) service, that itself imposes issues with **data**. These risks that were identified to be relevant

were data security, data integrity and data segregation. This risk would impose that the data could be accessed and modified in some way in the SaaS provider's platform or with the Identity Providers (IDPs) end and based on this incorrect access or data would be imposed to the users. As data is particularly important in this case it is also possible to build control methods into this such as verifying data based on identifier. Most controls are still done by the vendor and the service itself.

As most of the network layer is outsourced into the IAM solution the remaining **network security** is identified to be a risk. Remaining servers and services must still be protected accordingly. So correct communication points, Network Access Control Lists (NACLs) and Security Groups (SGs) with Virtual Private Cloud (VPC) must be implemented to control the remaining network that is in this cases responsibility. Also, issuing a Load Balancer (LB) in front of the backend negates the attack surface to be minimized and the controlling of the traffic and access.

Man-in-the-Middle (MitM) can be included as a risk in this case as it would impose the possibility to hijack the traffic between the IAM solution and backend. Controlling such a risk would need actions done for encrypting traffic between these components and ensuring that this data sent has certain Time to Live (TTL) period for being valid.

Denial of Service (DoS) attacks are also a risk as it would impose possibility for having service breaks and exposing data from products if there would be vulnerabilities involved. For controlling and mitigating this there should be identifications done if the IAM solution has applicable tools for this or are other components needed to protect the solution such as Web Application Firewall (WAF).

For this case also **Side Channel attack** can be considered as a risk as of the possibility to infiltrate the part of the system utilized from public cloud. This can be controlled in a way with the utilization of VPC to limit the access zone.

This case also introduces the possible risk of **metadata spoofing** that could be utilized in communicating between IAM SaaS and the identity provider itself or communicating to backend. This could be utilized in a way to get unauthorized access to the services running. This kind of attack should be controlled and mitigated with the possible encryption and validating the metadata based on identifiers.

Backdoor channel attack can also be identified as a risk in this case. As with this case there are different things to consider such as the Cloud Service Providers (CSPs) provided services and servers and their backdoors. Alongside this there is also the vendor provided SaaS solution that could contain such possibility for this kind of attack. These are the reasons that this attack contains enough to be identified to be a risk. For control methods the CSPs Service Level Agreements (SLAs) should be discussed as of possibility to fix issues if occurred. Vendor should also be consulted about the possibility for updating and fixing these issues if they occur. For own components that are not responsibility of others the solutions should be audited, assured and vulnerabilities identified. Controlling these there should be automated pipelines for deploying and testing solutions.

As this case introduces a trust relationship with the SaaS provider the possible **misconfigurations** are a risk at it could possible mean that service is unprotected, unavailable or wrong identity provider utilized. This risk can be controlled by utilizing properly the service and enabling automated configurations. For mitigating such issue in this case, the configurations should go through review process and be tested properly.

Security in utilization of the SaaS can also be identified to be a risk in this case. As this SaaS solution needs to be incorporated in a way that all traffic goes through it to verify the access rights and identity from the provider. This would pose problems if the SaaS solution would be bypassed, or any unauthorized access done via the SaaS solution. Solution should be incorporated to work like it is designed and certain amount of knowledge should be incorporated to know what to do.

Unauthorized access to servers can be considered as a risk also in this case. These needs to be protected with own access rights and network security for preventing access. Risk can be controlled with the internal usage of IAM and with network measures such as Virtual Private Cloud (VPC), Network Access Control Lists (NACLs) and Security Groups (SGs).

Bypassing the Identity and Access Management (IAM) solution is an identified risk as it would enable attackers to access services and thus cause issues. For controlling this risk there should be certain identifiers identified for ensuring that the information is provided by correct solution. Other possibility for this is the control of traffic flow and what components can communicate with each other. This bypassing relates to different parts of the whole system as one point would be between the Identity Provider (IDP) and the IAM SaaS and another one while accessing from SaaS to actual service.

Visibility of the backend servers can be identified as a risk as this provides attack surface to be identified from public view. This would enable attackers to find unnecessary information about the machines and try different kinds of network attacks and attacks targeting Virtual Machine (VM) against the servers. This risk can be controlled by utilizing VPC and limiting the visible components to be only the relevant ones.

Lack of support can also be included to be a risk as it imposes possibilities for misconfigurations and establishing trust-based communication can be seen difficult. As if the support is lacking then the utilization of the solution could be misleading and wrong kinds of access or identities could be identified. For controlling such risk, the service provider should be consulted, and details about support should be discussed.

Vendor lock can also be considered as a risk in this case if the IAM solution and the data it provides is heavily customized or utilized in a way that it is specified for this solution. This kind of risk can be controlled with identifying the vendors utilized methods and are standards used. By utilizing standards, it is possible to control the utilization of the service and create possibilities for future usage of different products and different vendors.

4.3 Architecture

This chapter introduces architecture designs that control or mitigate identified risks per identified cases studied. Chapter includes discussion of why such solutions are relevant and what kind of components would be needed to be included for the solution to work. There is also discussion about general architecture of each of the cases and based on the cases relevant architecture design topics are raised for later discussion.

4.3.1 Case 1: Cloud migration architecture

As this case involves a large-scale cloud migration and large number of servers with different usages and integrations it needs certain types of security measures to establish secure architecture solutions. Almost all the components involved can be scaled to meet the demand and figure 2 shows what the architecture design looks like. Case itself introduces the dilemma about how well can the already built infrastructure be moved on to the cloud. As in this case the architecture had to be changed to function well enough on cloud environment to meet scalability and flexibility issues.

Architecture is built around the concept of least privileges as the components are accessible only from the desired components and only authorized people have access to servers. As most of the components involved are in this cases responsibility the different components and their places should be considered in a way that they work together.

This architecture involves different **load balancers** to balance the load to multiple different sources. There is a load balancer for data usage to match read operations and prevent direct unauthorized accesses to servers. Backend components also have load balancing for different reasons as the solution must be highly available and even microservices can be introduced. This would assume that there are different layers of the backend servers and between them load balancers to even the load.

Web Application Firewall (WAF) is being utilized in this architecture to mitigate and control certain risks and attacks from happening. WAF itself does not work properly if not configured into correct place in the architecture to monitor for malicious traffic.

Reverse proxy server is also included with this architecture as it prevents certain unauthorized access from happening by building custom access management configurations in place to ensure only allowed URLs can be called from resources with enough access rights. This solution also checks requests that they contain valid information and based on these calls from another appliance creates appropriate token for further usage. This server would be allocated in a Demilitarized Zone (DMZ) that is a subnet of its own for isolation within the cloud environment.

Cache can also be identified to be needed as a part of the architecture as to ensure a place to store relevant data that is needed if disaster were to happen, and servers would be unavailable. By adding cache there are possibilities to store certain session information onto it and utilize this for failovers and keeping a track of the sessions. Enabling clustering for the session store the possible failover situation becomes also faster as the data can be replicated within the cluster and utilized from all the sources within the cluster.

As the architecture itself is already in **private cloud** the utilization of Virtual Private Cloud (VPC) is not needed in this case. But instead, there still needs to be Security Groups (SGs) and Network Access Control Lists (NACLs) in place to control the traffic flow within the cloud environment. With these groups it is possible to segmentate the different components into own zones containing their identified configurations and allow traffic to go through from

only certain places. Then with addition to these NACLs are needed to control the traffic and the types of which are allowed to go through. With the utilization of these methods security of the architecture is increasing as is the flexibility. As this would impose that it is easier to work within certain segment rather than the whole architecture itself.

Backends (BEs) could be different in multiple ways, and they would need their own zones within the architecture. As some of the BEs could be built around microservice methodology and some might just be plain websites provided, it becomes easier to control these within their own zones. This way the changes done to one of them would not cause issues with others and security itself would be increased as, if possible, attack would land on one of the backends it would not have access outside of that zone.

Database (DB) layer itself is also needed to be thought out as it needs own segment inside the architecture. This way it can be protected against unauthorized access and adding Load Balancer (LB) in front of it the security is increased even more as it could be possible to only allow access from the LB and not from other components. With this kind of approach also other utilizations done from BE could also be allowed if needed to.

As identifying several different components that needs to be involved within this architecture, this provides the possibility to build **flexible design** as different functionalities are segmented. While segmenting these different bases it also enables the future to be considered and is there solutions that could fit better into the architecture and replace older components. This also imposes that certain security risks are mitigated with such approach to prevent multiple different types of usages in one segment.

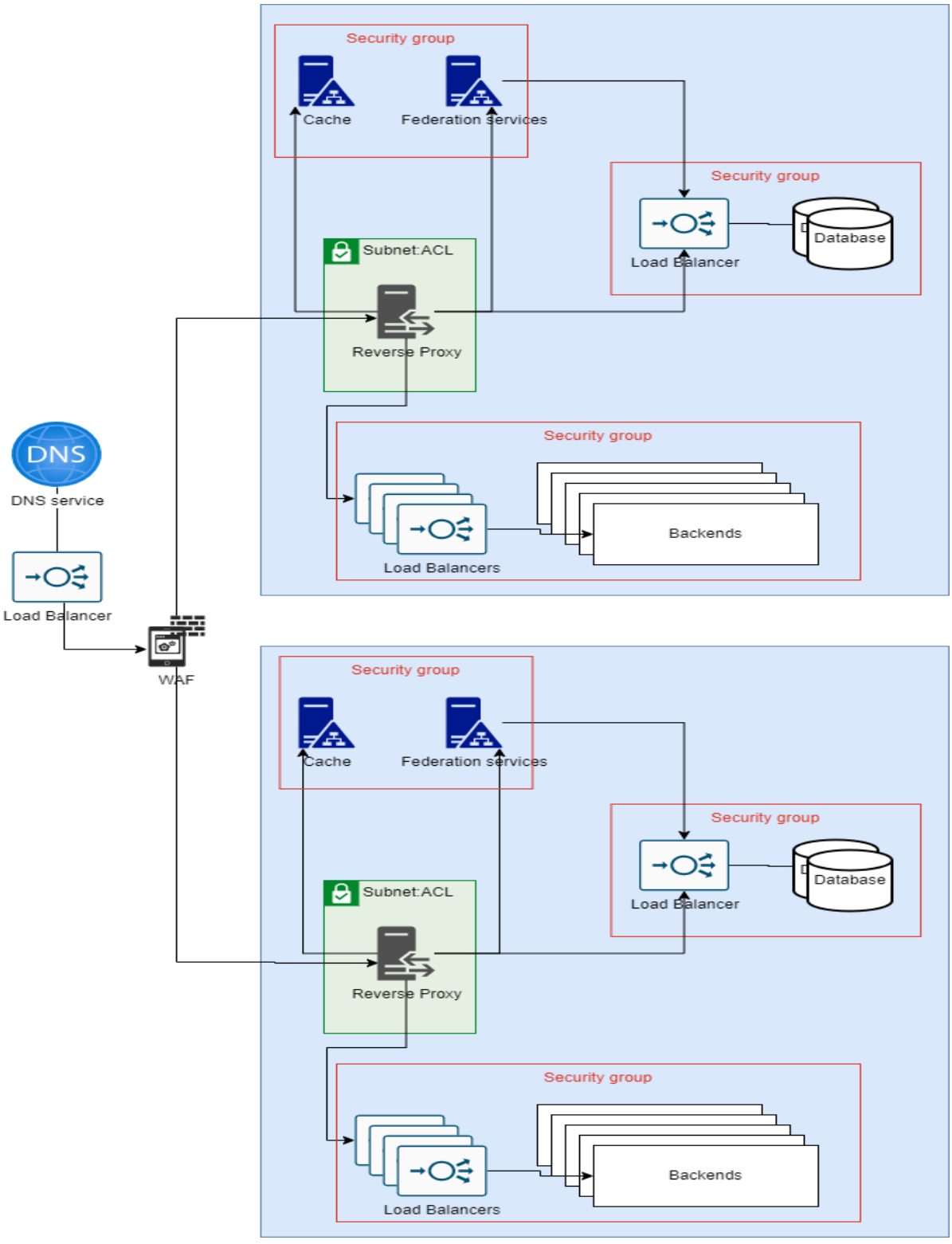

Figure 2: Case 1 architecture

4.3.2 Case 2: Platform for Docker architecture

This case introduces a platform to be utilized in a middle of the architecture. Overall picture of the architecture can be seen from figure 3 that contains high-level architecture design. This

platform is needed to run custom Docker image as needed to and fetch configurations from GIT repository and run these on to the servers identified. As this case the platform is only needed to be run when needed to it is possible to commission and decommission as needed.

Architecture itself utilizes least privileges as this platform needs to be only able to be run by certain people and no one else outside of that group needs to have access to this. Connections to the servers and GIT can only come from this platform and therefore certain security measures such as Security Groups (SGs) and Network Access Control Lists (NACLs) are utilized.

Components that are included in this architecture are Identity and Access Management (IAM) or even Privileged Access Management (PAM) could be considered as a solution to meet the access requirements in this case and ensure that only these people or group of people can access the server. Architecture also includes own Virtual Private Cloud (VPC) zone containing servers and another for the automation platform. Also, included is the GIT repository for the configurations. For this Platform as a Service (PaaS) solutions VPC there needs to be SGs identified for this to be protected from unauthorized access. Also, similar SGs and NACLs must be included in the other parties that are GIT repository and the servers to be accessing from PaaS. As per the servers there can be multiple different ones which the automation solution should be able to connect into. These servers must be seen to either belong in one SG or in multiple ones depending on the needed number of servers.

As this is a platform that is needed to be utilized in the automation flow the utilization should be restricted into only the needed tasks and only **authorized persons should be able to access** the platform. The GIT repository connection is needed to ensure that certain configurations and utilized libraries and documentations are fetched from the correct place to be utilized. This way the certain repositories are given access to be fetched by this solution. For the connections and security for the servers to have configuration updates, there are network layer security that must be addressed and VPC be able to be integrated into use to build more security into the system and disallow other parties the possibility for a breach and risks.

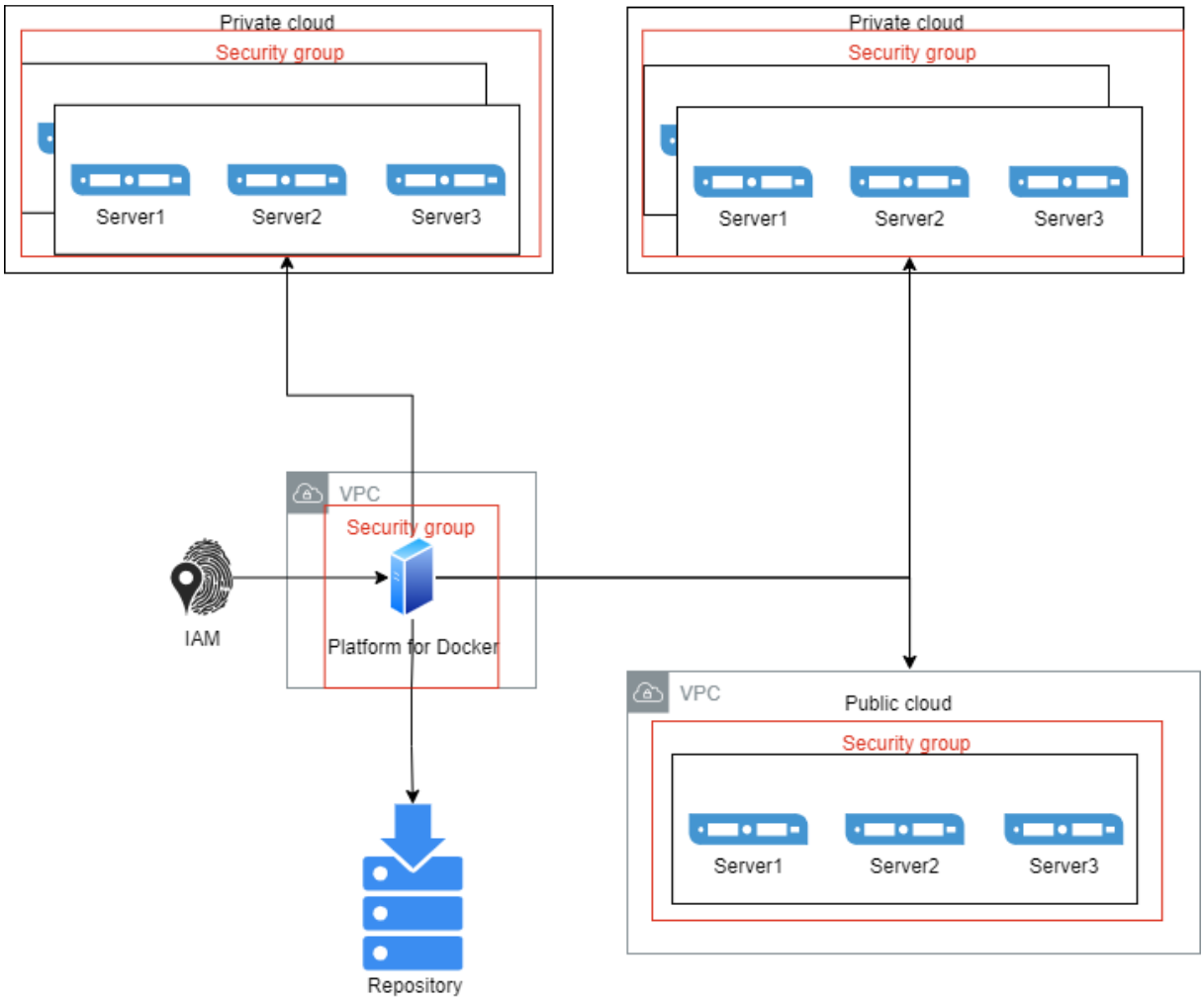

Figure 3: Case 2 architecture

4.3.3 Case 3: IAM solution architecture

Architecture in this case follows up the least privilege model as others but in this case all the Identity and Access Management (IAM) solutions for users are extracted to own software. This kind of solutions simplifies the architecture a lot as certain parts of the integrations are out of the scope and outsourced to others for taking responsibility. Figure 4 shows the high-level architecture of the solution for case 3.

As this case introduces **IAM solution** to be utilized as a service there are a lot of different components involved with that and these can be removed from architecture design as it is responsibility of others. The IAM solution itself is an important component in this case and all authentication calls should go through it to ensure that there is needed information present for the solution running on backend.

Load balancing is also needed for this case as the solution running needs to be scalable to meet the demand when needed to. Load Balancer (LB) also hides the backend from being found in plain sight and creates a point of contact in front of the resources.

As within this case there is quite simplified solution to be added as most tasks are done already by the Software as a Service (SaaS) software. This case needs the LB to meet the scaling issues and providing one point of contact to reach backend. **Networking** itself must be protected accordingly as Virtual Private Cloud (VPC) is in place to ensure that within the network there are no middleman involved. This case needs Security Groups (SGs) for the utilization and Network Access Control Lists (NACLs) to prevent further communication methods as only certain methods should be allowed between the components. Web Application Firewall (WAF) could also be utilized in this case to protect resources if issues with Denial of Service (DoS) attacks were to occur.

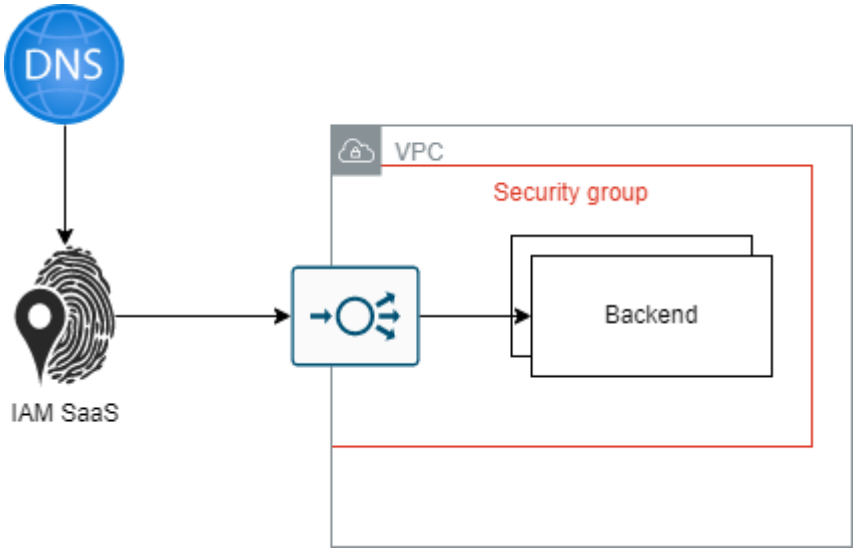

Figure 4: Case 3 architecture

5 Discussion

Discussion about the three different cases and how they differentiate from risks and architecture is discussed within this chapter. Also, differences in security measures taken will be discussed and possible solutions based on those identified as to what increases security. Chapter also involves comparison discussion as of how the different responsibilities also affect risks and measures taken while designing architecture.

5.1 Risk management

As it was identified there are different responsibilities for different cases and these responsibilities itself affect also as of how and whom to consider to be responsible for controlling different risks and mitigate them. These responsibilities affect a lot as of what kind of measures and approaches can be chosen but they also depend on the case itself. As responsibilities vary a lot depending on the case it brings forth the issues with who can control the risk or is it a risk that is just needed to be accepted as Cloud Service Providers (CSPs) are responsible for those risks. The responsibilities are also an important factor to consider as if the cloud itself is feasible solution or on-premises Data Centre (DC) is better suited for that usage and these certainly is dependent on multiple different factors such as industry, data utilized, use case or solution itself, among others. As taking more responsibilities it also affects the workload by increasing it and based on this the most feasible solution and risks should be compared if those are compliant and have benefits if provided from CSP.

What was also identified that the number of risks and issues involved is quite related to what kind of approach is taken and if there is the need for support internal and external users. As the amount is quite increasing based on the cloud model and type also the case itself poses differences as of the possible data type and utilization and security related to that. Also, the approach taken, and the responsibilities of that model was identified to have an impact as of what level the risk is identified to be as same risk with different approach and model could pose larger impact and needs to be protected more thoroughly depending on case. By giving responsibility to others the possible underlying hardware can ease up on the control of the risks, but it can also widen the gap as of how and when the possible risks can be controlled and mitigated as the CSPs, and vendors might take a long time to address these identified risks.

Attacks itself can be quite same in all the cases as they are targeting cloud environments in general. But the responsibilities and measures for controlling and mitigating the attacks are quite different in each case. Regarding the attacks also the different cloud types and models affect a lot as of how the risks are or can be managed. As these cases show the differences in the cloud models and types that are ways of utilizing cloud in such a way that risks are controlled and mitigated enough. To consider the solution to be secured from most relevant of the attacks that do pose most threats the case must be identified with enough details. This indicates that not all the attacks can be protected against as it might require a lot of other information depending on the cloud type and model utilized. By identifying details and the risks of those attacks pose to the service then these attacks can be controlled or avoided with designing the services or adding security measures. This identification itself imposes the possibility for adding measures but could provide a lot of further issues if those measures would increase complexity or cause gaps between responsibilities as of who can control and mitigate the risk or is the need for different cloud type and model to be considered more feasible.

Access rights to all the cases can be challenging issue as there needs to be different kinds of accesses allowed per case. For case 1 there needs to be external user's access implemented alongside internal users. Even the internal user's access is different as there are different components running and different people who are responsible of those specific components are to be given access. External users should have own credentials to access the services and utilizing them in a way they need and are allowed to. As in case 2 only internal access is needed and considered to be relevant as this is about building custom automation solution. In case 3 the external user's access is externalized to SaaS provider and only internal access rights need to be managed. So based on this the approaches of risk management for access rights can be quite complicated and based on the cases themselves more as of how the user's data and access is managed by and whom. As the different kinds of access rights are involved there is also the issue with different types of data to be managed per access type. For controlling access rights, the data utilized needs to be correct also to base the access on trusted source. This also indicates that building certain kind of trust relationship between provider and the solution can be a feasible method for controlling access. What can be identified from these cases is that having internal and external users increases the number of risks and causes different kinds of solutions to be thought for implementing security measures based on the approach taken for managing them.

Configurations itself can be seen as an issue in each of the cases. Depending on the case discussed the need for different configurations and different actions that needs to be taken wary a lot. All the different components that are involved with case 1 increases complexity of the environment and thus increases the risks of misconfigurations and issues rising from those. For the other cases as the responsibilities are different and the number of components is smaller the complexity issue is not getting that hard to control. But still as the utilization in case 2 is based on a GIT repository located configurations those itself could contain possibilities for raising issues based on mismatches. Case 3 itself includes the smallest number of configurations needed to apprehend as the load balancer and backend is needed to be configured properly while allocating most of the other components to the responsibility of the SaaS utilized. So really based on the cases, cloud types, models, and the configurations the amount of time, risks and responsibilities that needs to be managed is increasing and finding feasible security measures for all the cases becomes more difficult. The risk level of the configuration issues also varies as per what kind of environment and component is utilized. As the differences in cases also indicate that even if in more complex environment would have a misconfiguration happening it might not be that big of an issue as there are multiple different measures in place. This might be very different in other cases as the whole solution could be rendered unavailable for certain time if it were to happen. So, utilizing multiple different security measures could also control risk of misconfiguration depending on the case and the type of configuration.

Vulnerabilities of the different systems and services involved are mostly dependant of the number of components that are the responsibility of the utilizers. As even if identifying multiple different vulnerabilities within cases 2 and 3 the responsibility of the specified components may wary, and it might even take a long time to get those identified and fixed in that end. If considering case 1 it is more straightforward in a way that multiple different things are in the scope of case 1 and can be managed accordingly. So having different kinds of setups depending on the model and type of the cloud also poses issues as for the possible breaches, attacks and other vulnerabilities decreasing response time and security of the system. This could also pose issues increasing complexity if relevant components should be added into the environment to mitigate such vulnerabilities. As there can be different kinds of vulnerabilities included but having more responsibilities can also ease up the managing of those risks. As for knowing about the environment and having the tools for identifying such

risks, the risks and vulnerabilities can be managed more easily as more security measures can be added or vulnerabilities can be fixed if identified to be a high-level risk.

Data related risks are also relevant in all the cases as there are different kinds of data involved. Data itself poses a lot of risks as per type and usage of it in a way that there can be different compliance issues based on that. When the data is considered to target sensitive information, it also needs more protection and measures as it poses a higher rating of being targeted and thus considered as a higher risk. As in the case 2 the data utilized is not that sensitive as it is mainly configuration items. So based on this the data type itself is an important factor to consider and identify issues with it in different parts of the systems. As the same data can be utilized in different parts of the system only the relevant information should be stored and secured to ensure that it is compliant. This is more related to cases 1 and 3 as discussing about sensitive data but if thinking of configuration data then it is relevant to all the cases as the data type itself that is utilized renders certain type of information to be visible. Depending on this data itself could pose issues as this is based on the usage in the case and what information the data holds. What can be identified from this is that the sensitivity of the data and what parts of it are used affects risk ratings. Also, the responsibility of such data can be identified to increase risks and risk rating as the data must be protected by the one responsible and storing it.

5.2 Security methods and measures

It was identified from the literature review and case study that there are several different kinds of security measures involved that provides measures to tackle different issues or attacks. There are a lot of different security methods and measures involved in the cases but identifying the relevant ones can be a case-by-case solution based on the approach taken. As these security methods and measures and number of them are quite relevant of the case details of the solution and having different kinds of usage, it can increase or decrease the number of measures to be taken into use. Also, the possible security measures that can be taken is changing in a way that who has the responsibility of the named component and would the increase of measures and components really control or mitigate the possible issues and risks. By utilizing certain security measure is only proficient in protecting against certain types of issues, threats, or risks and what different measures work together is to be considered when thinking of the bigger picture. Knowledge about the different security measures and what

issues these measures control is identified to be useful as to identify relevant security measures for the different cases with the help of risk management.

There are many security methods to be considered in each of the cases and by identifying the relevant ones, ways of protecting the environment or resource can be seen to be improving per method if relevant. As the methods might not be that visible and these might be implemented through different security measures the methods are the fundamental point that must be identified to be in place for that specific service, asset, or resource. As the fundamental work is seen to be an important factor when considering the relevant measures to be taken or can these be implemented and as of what ways there are for utilization of these measures. By ensuring that these methods are approached with correct knowledge it becomes possible to identify concerns relating the cases. As there can be multiple different issues identified from these cases that can be seen in the risk management section, certain cases must be compliant with the regulations and because of this only certain methods and measures can be taken or certain cloud type utilized. This also affects the information about how and what to have governance over as to identify the responsibilities of the utilizer and Cloud Service Provider (CSP). Different security measures themselves needs to have security methods identified and in place such as identifying assets and resources, having authentication and authorization and handling privacy and integrity or is there need for anonymization of the data. As for identifying these methods the correct security measures can be taken to ensure the fundamental part of the method and why some measures are or can be utilized.

Cloud types itself and security measures such as the utilization of Virtual Private Cloud (VPC) can be seen to protect the resources depending on the usage and case. As the utilization of VPC is done within two of the three cases the approach itself reserves the certain part of the cloud to the utilizers. As with the case 1 the VPC approach was not enough and whole private cloud model needed to be done to ensure that the case is compliant with regulations. The differences in the cases and the issues with these are to be a point as if certain models and types can be utilized and to what extent. Private cloud and VPC itself are similar in a way that both allocate certain resources only to the utilizer, but they operate on the different cloud types. The utilization theme which one to choose from comes from what can be considered as a compliant manner for that specific case. This private model approach increases security and privacy of the solution but needs more security measures alongside. By increasing the privacy aspect with VPC or private cloud type companies can address different issues regarding the location of the solutions or identifying components within. As there are a lot of differences

based on the industry and data utilized it comes from regulations as of what different measures can be utilized or can the cloud even be relevant solution.

For increasing security in a more fine-grained manner the Security Groups (SGs) and Network Access Control Lists (NACLs) were identified to be relevant security measures. As these methods can allow or deny certain types or specific IPs from reaching the resources it can provide more detailed security aspect. This approach works on a network level and really needs to be thought when it is relevant and from where the traffic should be allowed. So, this approach needs good identification of components and traffic that goes through them to function properly. By utilizing these methods security can be increased but there is also the maintainability aspect to be taken as if environment is changing the maintaining could prove to be difficult to maintain. From maintenance aspect as there can be multiple SGs and NACLs involved per solution it must be identified as for what purposes they are and that they work for that specific component or segment. By having multiple different SGs and NACLs the maintenance can be an issue and there should be considerations for utilizing automation or other approach for identifying configured methods and resources these are used for.

Segmentation of the components were identified to be a strategic point of a security measure as it involves different components to be grouped together. With this approach it is easier to utilize, maintain and update the components without affecting rest of the pack. This is similar in each of the cases but the number of groups wary based on the cloud model utilized as to comprehend the responsibilities and the components in different cases. With segmentation in mind the security can be increased to match the specific usage of the segment and different kinds of measures can be added also within the segment if needed. Considering all the cases the segments must still be managed and this could pose issues later if misconfigured. By segmenting components, it also increases the maintainability and time it takes for configurations but adds security and flexibility.

Web Application Firewall (WAF) can be considered to an interesting method to be utilized as for it is added on to the case 1 but could be added to case 3 also but was identified that it was not needed. For case 2 it was not implemented at all. As what makes these cases different in a way is that the usage and the purpose of the cases are different and what differentiates them is the utilization of the cloud types, models and the data utilized. This security measure itself provides only certain type of protection and could be utilized when risk level increases. WAF can be useful tool when identified to be needed and configured properly and needs

maintaining to work according to the rules provided into it. It increases security in this aspect but can also be useless if not configured or placed in wrong place in architecture design.

Load Balancers (LBs) itself are relevant in all the cases but for case 2 it was excluded as it was not actually needed. Utilization of the LB can be seen to help with multiple issues and enable useful utilizations to make architecture more flexible and secure. With LBs the scalability and availability issues can also be targeted and building solutions that can scale automatically is enabled. This measure itself also creates possibilities for other risk management such as hiding backends and creating one point where the communication is done through. LBs are useful when more components are involved to redirect traffic into but do not really add value if there are single components involved. LBs itself does not provide that much protection from threats but is needed for different methods to be utilized.

Identity and Access Management (IAM) from internal and external access to the solutions in all the cases vary in a way that case 2 introduces only the need for internal access. But IAM is one of the most utilized measures as it restricts the access in all the cases. This itself simplifies the solution and providing access rights to the identified resources from centralized and managed solution helps with managing. When having the external users involved it requires a lot more security measures to be considered, issues identified and increases the number of risks involved. As for having external users, there needs to be a relevant solution for handling those users that increases number of components for maintaining them. This itself imposes a negative aspect as two different kinds of IAM solutions needs to be managed and increases workload and maintainability. By utilizing IAM the security of the accesses and identities becomes more manageable, and it enables other means for adding more layers of security into the systems. This also allows the restrictions and increases the knowledge while reducing shadow IT and accounts as if the IAM is incorporated into the procedures also. IAM itself is useful solution for increasing security but needs procedures and automation to function well in a changing environment.

Recovery methods that could be utilized also vary a lot depending on the cases. As case 1 introduces multiple components and building multiple ways of recoveries as different parts of the systems might need the recovery method to be accessible as the multisite deployment. This is a hefty recovery method, but it ensures services to be available almost all the time. Cases 2 and 3 are not that complicated and relating recovery methods there are a lot less than in case 1. As what is enough for case 2 is not enough for other cases. Case 2 utilizes the least

amount of recovery methods, and it does not need backup solutions such as multisite or pilot light methods as the usage is quite different from the others. For case 3 the recovery methods utilized could have been almost any of the introduced methods, but it was chosen as a warm standby to reduce the time services are unavailable. A common theme here is the different responsibilities and what kind of solutions has been outsourced seems to affect what recovery methods are feasible. From security perspective the different methods utilized tackle certain problems and usually for preventing multiple issues from occurring also multiple recovery methods are to be utilized. For considering more about the usage of recovery methods it is per details of case and the risks involved as to what to choose from and what kind of issues are acceptable.

5.3 Architecture design

As it can be identified by all the different cases the utilization of different components and different cloud types and models comes with own architecture decisions as of how to protect resources and by who is responsible for building such measures. This indicates that architecture of the systems involved vary as of who is responsible of which part of the system. The need for building flexible and robust architecture can be also identified from this as the responsibilities are changing per case. Each of the cases also introduce the possibility to scale and segment different parts of the system to match the needs of that specific case. By utilizing such a flexible architecture, the solutions can be better utilized to match future needs and changes. Flexible architecture itself can also be important aspect to consider as it enables different security measures to be taken and certain types of risks to be controlled. This kind of architecture also profounds the longevity of architecture as it is easier to consider different factors as the architecture can change with new components or segments or services rather than just forcing architecture to be locked up and not being able to change or add new services with ease. But also building solutions that are flexible and matching future needs the maintenance can become an issue as several different components or segments must be maintained within the architecture. This itself also increases the complexity of the architecture design as it increases segments and components within to be managed and secured.

As the network architecture in all the cases are a little bit different from one another, it can be seen to match the differences in components and responsibilities. As case 1 includes multiple different segments and components the networking architecture must be on par with needs and secured in multiple parts. From cases 2 and 3 the networking setup is more simplified as

there are not that many components involved. And utilizing SaaS as in case 3 this decreases the network layer work even further as the outsourcing of the responsibilities and components included in SaaS are taken care by others. From network architecture similar solutions are utilized for enabling scaling and availability as these can be found useful in providing solutions for issues. What needs to be considered more is the usage of the cases and cloud types and models utilized when discussing about network architecture. As having more responsibilities, it also affects the network architecture in having multiple different parts of the system to be considered on its own and where to allow accesses from and to. So, increasing responsibilities also increases the maintenance and design in architecture as to protect the resources on network layer.

What can be seen also from these cases is that certain network layer security measures are utilized in each of the cases and others utilized is depending on cloud type. Virtual Private Cloud (VPC) is utilized in two of the cases but is very similar to private cloud utilized in case 1. Both are to ensure that solution is running only for that specific utilizer, and this really depends on the case, and does it contain such sensitive information that it needs to be protected in a private cloud or can the VPC solution of the public cloud be utilized. Relating to the utilization of VPC and private cloud is also the utilization of Network Access Control Lists (NACLs) that is like a firewall in terms of allowing certain types of traffic from certain place to be reachable. This is one of the measures that is utilized in all the cases to limit the possibility of intruders trying to find weak points in the environments. Another one is the utilization of Security Groups (SGs) to increase the layer of security even more. These two combined increases the security layer and can limit the access even more. So, similar components are utilized in all the cases, but the number of needed configurations varies a lot as of the approach taken. This would indicate that the solution would be simpler to maintain as fewer configurations are needed. As by utilizing VPC, SG and NACL the security can be improved on network layer, but it also means that it must be managed properly, and the possible automation implemented to check the configuration items. Using such solutions is related to what kind of usage in the case they are targeted to and what level of security is sufficient as even if implementing these the underlying security issues might still allow for further risks and issues.

By utilizing these different network security aspects, it is possible to limit or increase the security of the architecture. Utilizing the VPC or private cloud the privacy of the system is increased to match part of the compliance issues based on the needs. As the privacy is related

in all the cases in different levels the possible solutions needed, and architecture design needs to be considered. Network level architecture needs to fulfil criteria's that data is moving securely and between authorized components. Increasing systems privacy and enabling accesses to the systems, the utilization of the NACLs and SGs are to be considered in a way that one of these is to be taken into use to control access internally with addition of IAM. As for privacy consideration in the architecture the logging must be implemented in a way that all the possible violations towards privacy can be identified. Privacy aspect itself poses issues as per the data utilized and how to protect that from the privacy issues. As if the storing must be managed and if the data in transit must also be managed, this increases architecture design and measures to be taken to protect privacy of the data as it also increases the maintainability and monitoring. Multiple different security measures must be in place like in case 1 but measures could be a lot less like in case 2 and 3 as the data sensitivity was different and data was provided from another source. So, having responsibility over the data also the privacy aspect is included, and this means more measures, resources and knowledge are needed to upkeep it if data type needs it.

What can also be identified from the cases is the problem that comes with thinking of complexity or the simplicity of the system. As with more responsibilities the architecture itself involves multiple different segments, security measures and maintaining access rights in those. With the utilization of the cloud models that have less responsibilities the possibility for simple architecture can be identified. Taking care of the different parts of the architecture such as data increases one layer or segment into the architecture that can be seen from case 1 and 2. As these cases utilize the model where data is the responsibility of the utilizer that data must also be protected accordingly. Adding more layers or segments into the architecture seems to also increase number of components that could increase complexity. This is also why flexible design should be considered in architecture to control complexity even if number of components increases. In case 3 this layer is outsourced and is not visible in the architecture. This itself simplifies the architecture but poses other issues as discussed earlier. Similar kinds of complexity versus simplicity issues can be identified for the network layer as of where the access to different segments should be considered. Overall, the different approaches of the cloud types and models are considered as a way of affecting overall architecture complexity. This would also indicate that it is important to consider whole architecture rather than just a part of it and think of the bigger picture to keep maintaining the complexity of the systems and identifying bottlenecks of the architecture. As for complexity

issues the knowledge of the assets and resources involved is crucial to identify dependencies between them and what measures and risks are associated to take care of. As for knowing about the assets it becomes possible to identify and maintain the architecture in a way that it is relevant for that case and can be incorporated with future needs. Also, by having knowledge about this it becomes possible to address the complexity issue and maintain it or consider solutions that simplify it. As all these trade-offs are in between the complexity and simplicity, the correct measures and approaches taken is dependent on the knowledge of the case that enables designing the architecture in a way that it takes care of this kind of usage as also how it incorporates into the bigger picture.

As the architecture itself is quite different in all the cases it was identified that different cloud types and models affect it quite a lot as has been discussed already such as complexity and simplicity and security measures of those solutions. What also affects the architecture is the responsibilities and the possible ways of controlling and mitigating risks as not all those measures are to be implemented. Based on the type of cloud utilized there are several underlying issues that cannot be mitigated but only controlled till certain extent, but the issues would still be relevant. Even if the architecture is different in all the cases, most relevant components should be identified to be included in the architecture and consider it in a way that it is flexible to meet the future needs and updates. Architecture itself gives certain frames to work with but becomes more relevant in the way of identifying the usage of the cases and risks associated with those. This would impose that knowledge of the big picture with more detailed information about the cases is needed to consider the architecture approaches and components involved. This also indicates that knowing about the detail's possible utilization type and model for cloud can be chosen and based on that it comes out for establishing architecture design. Thus, knowing about the details, identifying risks and security measures it becomes possible to think of a flexible and design security into the architecture.

5.4 General discussion

By identifying these differences in risks, security measures and architecture design it can be said that there are various ways to utilize cloud platforms. This itself imposes several issues for consideration as of what is the approach to be taken when considering cloud platform utilization. As even if identifying all the risks associated the possible security measures to be taken varies as per the cloud type, model, and the use case itself. This enables the possibility for variation between types and models and it comes down to knowing details about the case

and the requirements in details as of what kind of legislations, compliance and other issues are associated for the case. The knowledge about the case is important factor as to consider what components are to be included. As for knowing the details the architecture design can be discussed as a lot of things varies based on the information and approaches that can be taken is also identified from the details. So, all of this indicates that knowing about the use case is essential to even consider what type, model, security measures and even architecture design can be applicable. By identifying this information and assets then the possible approaches to be taken can be identified, risks from those can be managed, security measures be thought out with risk management and architecture be designed per identified resources and measures.

6 Conclusion

What was identified and discussed within this thesis was the different security methods and measures to take for controlling security issues and risks and build a robust architecture model based on three different cases through the risk management process and literature review. These cases and literature identified different cloud types and models and how different they are in comparison of the responsibilities, risks, security methods and measures taken and architecture design. As discussed, utilizing certain cloud types and models does not fit to all the cases as there are multiple differences in needs, legislations, and usage. Architectures and risk management process introduced in this document were all targeted for the cases identified and studied, and could be different based on other cases, components and the industry utilized in. Risk management also identified differences in cloud types and models and based on these feasible security methods and measures were introduced to be utilized in architecture design.

Through risk management process it was identified that even though similar issues and risks were involved with the cases studied the risk level did change based on the cloud type and model utilized. As for identified risks amount of them was deemed to be increasing based on the cloud type and model taken as well as what kind of usage is there for the services. Having the responsibilities over the external and internal users and what type of data was included and is it considered as sensitive did increase the risk level of different issues and risks identified. As for risk management process itself it becomes more difficult to identify relevant threats and what can be done to control and mitigate them as cloud service providers are taking responsibility over different parts of the system. This means that understanding the responsibilities and identifying the gaps in between them is needed to ensure that risk management process can be incorporated properly into use as well as the service level agreement to manage these identified gaps in the responsibilities. As there are also various kinds of attacks targeted towards cloud environments identifying these based on the risk management is essential. These attacks could pose serious issues if not taken proper security measures against them. Most common types of attacks can be identified to be Denial of Service type of attacks that try to render services unavailable and is unaffected about the cloud type or model utilized. Another type of attack that is troublesome in cloud environment is targeting the Virtual Machines (VMs) and gaining access on those on the public cloud and as for controlling these attacks targeting VMs, a lot of work would be needed to mitigate them and could even need a new design on hypervisor. By utilizing proper risk management

process, it becomes easier to identify risks, threats, issues, and the possible architectural designs can be discussed as it enables solutions to tackle risks proactively and identify relevant security methods and measures to be implemented.

As for security methods and measures there were multiple different ways identified through literature for adding security as a fundamental and practical ways but utilizing only one out of many methods or measures can be seen to not pose enough security for the environment but needs multiple different methods and measures. For identifying when to utilize these methods and measures the risk management process is needed for having a way of ensuring the relevance of the method or measure considered to be utilized. As based on the different kinds of risks, also the thought of the fundamental idea of the security method is needed for identifying a point of view on the actual risk. Based on these methods also relevant practical ways such as security measures can be taken for actual protection. For finding these relevant security methods and measures the cloud type and model utilized is having an impact for the number of and what measures can be utilized. As based on this the responsibilities and risk management are needed for ensuring the relevance of the measures used and responsibility of those measures. By identifying the cloud type, model, and responsibilities the applicability and number of security measures utilized can be identified for further consideration in the architecture design.

Architecture design can be seen to implement identified security measures to control risks. As the architecture design itself can be seen to be impacted by the cloud type and model utilized, it becomes critical to see architecture as an evolving part of the organization plan. With this kind of robustness built into the design possible future issues and risks can be considered proactively to be implemented into design. Based on the cloud model utilized the design is larger and number of security measures taken is increasing based on the responsibilities of the utilized cloud model. Ideally there is not only a single measure that is implemented, and the design is affected a lot in a way of what are the relevant risks identified and what measures there are for controlling that risk. Architecture design should be implemented in a way that also components and networking design is built around the concept of least privilege and that they only communicate with identified resources and components through secured channel when applicable to control different risks identified. For controlling all or most of the identified risks in an architecture design the measures to be taken increases complexity and it can be hard to implement such measures into the design based on the cloud model utilized where cloud service provider is responsible for multiple parts of the environment. This also

means that the relevance of the measures and in what parts of the design the measure is protecting needs to be thought out to ensure if it fits into the cloud model utilized. By the differences in the architecture designs in the cases studied it was also seen to be an ever-evolving field that needs to be maintained to match the risks identified after initial risk management process. So, architecture design should consider to be built in a flexible and secure manner to also match those future needs.

Thesis introduced research questions (RQs) to be answered through cases studied. Research questions outlined in section 1.5 were following:

RQ1: What different security methods and measures are applicable in building secure cloud environment?

RQ2: What different kinds of issues and attacks are associated with different cloud types and models?

RQ3: What to consider when designing cloud architecture?

RQ4: How the utilization of different cloud types and models affect risk, security measures and architecture design?

In this thesis for RQ1 it was identified that there are numerous different security methods and measures that can be taken for securing cloud environments. Security measures identified in the thesis were risk management, key management, Identity and Access Management (IAM), private cloud, Virtual Private Cloud (VPC), Web Application Firewall, Network Access Control Lists (NACLs), Security Groups (SGs), identification of the resources, security controls, security by design, asset protection, perimeter security, segmentation, data confidentiality and integrity, automation, logging and monitoring, visibility, flexible design and different kinds of tools. As there are so many different security measures to take, for choosing the relevant ones there must be a risk management process that identifies the relevant measures for that specific cloud environment. Few of the most utilized and most applicable measures include private cloud type and VPC that increase the security of the cloud environment by adding more privacy and dedicating computational resources for the organization. Other measure that can be seen to be applicable is the utilization of IAM that improves security with adding roles, groups, and other security factors to tackle unauthorized access and allowing only relevant people or resources to have access and authorization to utilize resources. Also, relevant accesses between components are controlled with NACLs and

SGs that are applicable as these decreases the attack surface by allowing communication only from allowed components with allowed request types. Other measures are also good to consider, but they can be seen to be more targeted to match a specific type of problem and is based on cases details as of when to utilize them.

As for security methods targeted by RQ1 there was many security methods introduced that were authentication, authorization, anonymization, audit, assurance, availability, administration, encryption, compliance, governance, privacy and confidentiality, and integrity. Most relevant ones to be identified from the list that were included in each of the cases studied were availability, authentication, authorization, privacy, and confidentiality that can be ensured with mentioned security measures. These security methods can be seen to allow other security methods to be taken care of such as compliance and governance and ensure that cloud environment is more robust, and security is enhanced.

For research question (RQ) 2 this thesis identified several different issues and attacks that target different cloud types and models. There can be person related issues, technical issues and even software issues that are dependent on the cloud type and model. For different cloud types this thesis identified that there are issues with private cloud needing more maintaining, troubleshooting and being more costly that other types. For public cloud there was issues with data compliance, lacking hardware control and security level being lower. For hybrid cloud there was similar issues like other two had but also issues about data handling between environments, compliance issues, and other complexity issues.

For RQ2 and issues with cloud models this thesis identified that there are issues with Infrastructure as a Service (IaaS) that include misconfiguration, data leaks and security, cyberattacks, vulnerabilities, lack of knowledge, Service Level Agreement issues, insider threats, complexity, availability, privacy, and compliance. For Platform as a Service there were similar issues like in IaaS but also adding following issues such as access control, underlying infrastructure security, integrations, runtime issues, operational limitations, complexity, and customisation. For Software as a Service similar issues are inherited from the other models but in addition there is issues with application security, interoperability, lack of support, performance and downtime, lack of control, limitations of the software and security in utilization.

Most relevant issues found in this thesis for RQ2 were the virtualization issues, unauthorized access and data related issues that are involved in consideration of what cloud type and model

to utilize. As the virtualization technology is part of all the cloud models the number of responsibilities is changing based on the model and this responsibility change in the models also affects as of how the virtualization issues can be tackled. Data related issues itself are similar and not dependant on the cloud type and model utilized but the sensitivity of the data and utilized cloud type and model affects the risk rating of these issues. Unauthorized access is a huge issue as it is relevant in every cloud type and model utilized as it can incorporate internal users or external users and be it services or the servers that are vulnerable to unauthorized access.

For different attacks regarding RQ2 this thesis identified Denial of Service attack, side channel attack, malware injection attack, Man-in-the-Middle attack, Domain Name System attack, zombie attack, backdoor channel attacks, VM escape, metadata spoofing, rootkit in hypervisor, advanced persistent threats, and different virtualization issues. From these different attacks this thesis identified that most utilized attack type was Denial of Service type attacks that tries to render the services unavailable and based on the cloud model utilized could also affect other utilizers services. Other type of attacks that can be identified to be hard to counter and cause a big issue in cloud environments were attacks targeted to virtualization and Virtual Machines (VMs). These attacks are not easy to implement but the impact could be big as the VM could contain sensitive data or access to other components and services. This attack itself is more concerning when utilizing resources from the public cloud as the resources are shared with different utilizers.

In this thesis for research question (RQ) 3 there was identification done that for designing cloud architecture the architecture should consider the relevant risks and threats based on the case and the details when identifying approaches. Also, designing architecture in a way that it can also match future needs and implement security enhancements when needed should be considered to enable longevity of the architecture. For finding the relevant components for the architecture design, the risk management process can ease up the decision of what security methods and measures are implemented and in which part of the architecture they are relevant while also mitigating the utilization of unnecessary components. Relevant attacks towards the environment should be identified as countermeasures can be added into the architecture design for control and mitigation purposes. Not all the security methods and measures can be implemented right away but the importance of components and sensitivity of the data involved needs to be considered as to design architecture in a way that it secures overall system and especially most important parts of the system. Architecture design should also

ensure that issues identified with risk management are relevant to be secured with architecture design and the design supports the business with possibilities while ensuring that certain level of security is always designed into the architecture. Recovery methods should also be considered in the architecture design and identified if solution needs to be running within multiple data centres and what components should or is needed to be easily taken into use in case of disaster or issues. If utilizing a recovery method that requires multiple data centres or regions this must be incorporated into the architecture design in a way that it is fully functional based on the recovery method taken and its details.

For research question (RQ) 4 this thesis identified that utilizing different cloud types and models affects the risks of the solution in a way that based on the approach taken the risk level and severity changes. As for utilizing a model that contains more responsibilities the risk level and severity is higher than on a model with less responsibilities as this based on what kind of data and components are and can be utilized and how much of the responsibilities are relinquished to cloud service providers care. Utilizing different cloud types, the risks and their levels can differentiate as security can be enhanced with utilizing private type of cloud or utilizing hybrid type the number of risks can increase as all the different parties or environments involved must be included in the risk management process. Even if the risks involved can be same with all of the cloud types and models utilized the risk levels and their severity vary per the responsibilities of the cloud model utilized.

Thesis also identified for RQ4 that the utilization of the cloud model with less responsibilities is also affecting security measures as the measures to be taken might also be part of service providers responsibilities or those measures cannot be added into use without a lot of other work, and costs, and could cause a lot of complexity issues. Security measures that can be taken should be considered through the risk management process that also identifies the relevant risks that can be controlled with these measures. As there are different number of responsibilities with cloud types and models this straight up affects the security measures to be taken as the number of measures is increasing and these measures must be thought out more properly to fit into the big picture while controlling or mitigating relevant risks.

For RQ4 thesis also identified that for architecture design the utilization of the different cloud types and models can be seen to decrease the number of components and reduce complexity overall based on the number of responsibilities but at the same time outsourcing processes and components, the issues and risks associated with outsourced components is decreasing the

security aspect of the cloud environment. As for the utilized cloud type the architecture must be thought out in advance for the private and hybrid cloud types as there are possibilities for different kinds of issues with adding or modifying required services and servers into design. The design itself can be seen to be more complex based on the cloud model utilized as having more responsibilities means that more security measures must be included in the architecture and the correct placement, and allowed traffic, and components must be thought out in more detail. As for the utilization of the public cloud and Software as a Service model can ease up the architecture design it also alleviates that the security of the architecture has more hidden or unidentified gaps in it that could pose issues.

In general understanding of the risk management process and identifying risks and issues can be seen to be a good starting point for considering relevant security methods and measures for controlling these risks in cloud environment. As the cloud models are fundamentally different in comparison to each other it becomes apparent that with risk management process the responsibility risks and gaps can be identified that are dependent on the model utilized. These risks are then considered as part of understanding the responsibilities of cloud type and model to be utilized. As the cloud type and model heavily affects the security methods and measures that can be utilized, the feasible methods and measures needs to be identified properly through correct processes. Cloud type and model also has an impact on the architecture design as the feasible security methods and measures varies over the taken approach. The architecture design itself also varies a lot based on the number of responsibilities as the design could be simplified when knowing and understanding responsibility areas and complex if the responsibility areas are not understood. The whole process of risk management and architecture design should be actively monitored for reacting into new risks proactively and designing architecture to control or mitigate newly identified risks.

References

[1] Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2017). Cloud security: Emerging threats and current solutions. Computers and Electrical Engineering, 59, 126–140. https://doi.org/10.1016/j.compeleceng.2016.03.004

[2] Che, J., Duan, Y., Zhang, T., & Fan, J. (2011). Study on the security models and strategies of cloud computing. Procedia Engineering, 23, 586–593. https://doi.org/10.1016/j.proeng.2011.11.2551

[3] Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. In Journal of Network and Computer Applications (Vol. 79, pp. 88–115). Academic Press. https://doi.org/10.1016/j.jnca.2016.11.027

[4] Balasubramanian, R., & Aramudhan, M. (2012). Security Issues: Public vs Private vs Hybrid Cloud Computing General Terms. In International Journal of Computer Applications (Vol. 55, Issue 13).

[5] Munir, K., & Palaniappan, S. (2013). Secure Cloud Architecture. Advanced Computing: An International Journal, 4(1), 9–22. https://doi.org/10.5121/acij.2013.4102

[6] Rajawat, J. S., & Gaur, S. (2014). An Overview of Security Models and Threats in Cloud Computing. www.ijltemas.in

[7] T, D., & R, G. (2015). Platform-as-a-Service (PaaS): Model and Security Issues. TELKOMNIKA Indonesian Journal of Electrical Engineering, 15(1). https://doi.org/10.11591/telkomnika.v15i1.8073

[8] Cheng, Y., Deng, J., Li, J., Deloach, S., Singhal, A., & Ou, X. (2014). Metrics of Security.

[9] Poniszewska-Maranda, A. (2014). Selected aspects of security mechanisms for cloud computing - current solutions and development perspectives. In Journal of Theoretical and Applied Computer Science (Vol. 8, Issue 1). http://www.jtacs.org

[10] Reddy, P. B., & Bhupathi, V. (2017). International Journal of Computer Science and Mobile Computing Survey on Security Issues in Platform-as-a-Service Model. In International Journal of Computer Science and Mobile Computing (Vol. 6). www.ijcsmc.com

[11] Aspire Systems. (n.d.). E-BOOK 1 BUILDING A ROBUST CLOUD SECURITY ARCHITECTURE FOR IAAS.

[12] Security Agency, I. (2021). CISA Cloud Security Technical Reference Architecture.

[13] Altwaijiry, A. (2021). Article title: Cloud Computing Present Limitations and Future Trends Cloud Computing Present Limitations and Future Trends. https://doi.org/10.14293/S2199-1006.1.SOR-.PPEYYII.v1

[14] Jadeja, Y., & Modi, K. (2012). Cloud computing - Concepts, architecture and challenges. 2012 International Conference on Computing, Electronics and Electrical Technologies, ICCEET 2012, 877–880. https://doi.org/10.1109/ICCEET.2012.6203873

[15] Zhang, Y., & Zhang, Y. (2012). Cloud computing and cloud security challenges. Proceedings of 2012 International Symposium on Information Technologies in Medicine and Education, ITME 2012, 2, 1084–1088. https://doi.org/10.1109/ITiME.2012.6291488

[16] Odun-Ayo, I., Ananya, M., Agono, F., & Goddy-Worlu, R. (2018, August 17). Cloud Computing Architecture: A Critical Analysis. Proceedings of the 2018 18th International Conference on Computational Science and Its Applications, ICCSA 2018. https://doi.org/10.1109/ICCSA.2018.8439638

[17] Babaraj, E. A. (n.d.). The OWASP Foundation OWASP Cloud Security-An Overview. http://www.owasp.org

[18] Kandukuri, B. R., Ramakrishna, P. v., & Rakshit, A. (2009). Cloud security issues. SCC 2009 - 2009 IEEE International Conference on Services Computing, 517–520. https://doi.org/10.1109/SCC.2009.84

[19] Standards Customer Council, C. (2017). Security for Cloud Computing: Ten Steps to Ensure Success Version 3.0.

[20] Behl, A. (2011). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. Proceedings of the 2011 World Congress on Information and Communication Technologies, WICT 2011, 217–222. https://doi.org/10.1109/WICT.2011.6141247

[21] Munir, K., & Palaniappan, S. (2013). Framework for Secure Cloud Computing. International Journal on Cloud Computing: Services and Architecture, 3(2), 21–35. https://doi.org/10.5121/ijccsa.2013.3202

[22] B. Patel, H., & Kansara, N. (2021). Cloud Computing Deployment Models: A Comparative Study. International Journal of Innovative Research in Computer Science & Technology, 9(2), 45–50. https://doi.org/10.21276/ijircst.2021.9.2.8

[23] Gov.UK. (2014). GOV.UK Guidance Summary of Cloud Security Principles.

[24] Capgemini, & Sogeti. (2015). Security Assurance in Cloud Adoption With a cybersecurity approach that's right for their business, organisations can adopt cloud with confidence.

[25] Aljumah, A., & Ahanger, T. A. (2020). Cyber security threats, challenges and defence mechanisms in cloud computing. IET Communications, 14(7), 1185–1191. https://doi.org/10.1049/iet-com.2019.0040

[26] Saripalli, P., & Walters, B. (2010). QUIRC: A quantitative impact and risk assessment framework for cloud security. Proceedings - 2010 IEEE 3rd International Conference on Cloud Computing, CLOUD 2010, 280–288. https://doi.org/10.1109/CLOUD.2010.22

[27] Amoroso, E. G. (2014). Practical Methods for Securing the Cloud.

[28] Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. https://doi.org/10.6028/NIST.SP.800-144

[29] NIST Cloud Computing Standards Roadmap Working Group. (n.d.). NIST_SP-500-291_Version-2_2013_June18_FINAL.

[30] Ranga Dinakar, K. (2008). A Survey on Virtualization and Attacks on Virtual Machine Monitor (VMM). International Research Journal of Engineering and Technology, 6558. www.irjet.net

[31] Journal, I., Cyril, R., Cyril, B. R., Britto, D. S., & Kumar, R. (2015). IRJET-Cloud Computing Data Security Issues, Challenges, Architecture and Methods-A Survey Cloud Computing Data Security Issues, Challenges, Architecture and Methods-A Survey. www.irjet.net

[32] Achbarou, O., kiram, M. A. el, & Bouanani, S. el. (2017). Securing Cloud Computing from Different Attacks Using Intrusion Detection Systems. International Journal of Interactive Multimedia and Artificial Intelligence, 4(3), 61. https://doi.org/10.9781/ijimai.2017.439

[33] IBM Corporation. (2019). Cloud-native security practices in IBM Cloud.

[34] Moreno-Vozmediano, R., Montero, R. S., & Llorente, I. M. (2012). Iaas cloud architecture: From virtualized datacenters to federated cloud infrastructures. Computer, 45(12), 65–72. https://doi.org/10.1109/MC.2012.76

[35] Abdulsalam, Y. S., & Hedabou, M. (2022). Security and privacy in cloud computing: Technical review. In Future Internet (Vol. 14, Issue 1). MDPI. https://doi.org/10.3390/fi14010011

[36] Szymański, K. (2021, June 21). Disaster Recovery in Cloud Computing. https://www.netguru.com/blog/disaster-recovery-in-cloud-computing

[37] Kumar, P. (2016). Cloud Computing: Threats, Attacks and Solutions. International Journal of Emerging Technologies in Engineering Research (IJETER), 4(8). www.ijeter.everscience.org

[38] Baiju NT, 14 Most Common Cloud Security Attacks And Counter Measures | RoboticsBiz. (2019). Retrieved May 19, 2022, from https://roboticsbiz.com/14-most-common-critical-cloud-security-attacks-and-countermeasures/

[39] Ramgovind, S., Eloff, M. M., & Smith, E. (2010). The management of security in cloud computing. Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010. https://doi.org/10.1109/ISSA.2010.5588290

[40] Xie, X., & Wang, W. (2013). Rootkit detection on virtual machines through deep information extraction at hypervisor-level. 2013 IEEE Conference on Communications and Network Security, CNS 2013, 498–503. https://doi.org/10.1109/CNS.2013.6682767

[41] Netapp. Inc. (2020, December 1). Cloud Security Architecture for IaaS, PaaS and SaaS. https://cloud.netapp.com/blog/blg-cloud-security-architecture-for-iaas-paas-and-saas

[42] Cloudflare. Inc. (n.d.). What is a virtual private cloud (VPC)? | Cloudflare. Retrieved May 22, 2022, from https://www.cloudflare.com/learning/cloud/what-is-a-virtual-private-cloud/

[43] GuidePoint Security LLC. (n.d.). Cloud Security Architecture. Retrieved May 22, 2022, from https://www.guidepointsecurity.com/education-center/cloud-security-architecture/

[44] Intel Corporation. (n.d.). What Is Cloud Security Architecture? Retrieved May 22, 2022, from https://www.intel.co.uk/content/www/uk/en/cloud-computing/cloud-security-architecture.html

[45] Chung RE, W. S. (n.d.). Assurance in the cloud - Compact. Retrieved May 22, 2022, from https://www.compact.nl/en/articles/assurance-in-the-cloud/

[46] Tambekar, A. (2021, May 22). Public Vs Private Vs Hybrid: Which Cloud Models do Companies Prefer? https://www.mygreatlearning.com/blog/public-vs-private-vs-hybrid-which-cloud-models-do-companies-prefer/

[47] Raza, M. (2020, August 31). Public vs Private vs Hybrid: Cloud Differences Explained – BMC Software | Blogs. https://www.bmc.com/blogs/public-private-hybrid-cloud/

[48] Redhat. Inc. (2018, March 15). Types of cloud computing. https://www.redhat.com/en/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud

[49] Froechlich, A., Shea, S., & Cole, B. (2021, February). What is Cloud Security? https://www.techtarget.com/searchsecurity/definition/cloud-security

[50] Triskele Labs. (n.d.). Cloud cyber attacks: The latest cloud computing security issues. Retrieved May 22, 2022, from https://www.triskelelabs.com/blog/cloud-cyber-attacks-the-latest-cloud-computing-security-issues

[51] Singh, Jitendra. (2014). Comprehensive Solution to Mitigate the Cyber-attacks in Cloud Computing. International Journal of Cyber-Security and Digital Forensics. 3. 84-92. 10.17781/P001294.

[52] Check Point Software Technologies Ltd. (n.d.). Top Cloud Security Issues, Threats and Concerns - Check Point Software. Retrieved May 22, 2022, from https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/

[53] Watts, S., & Raza, M. (2019, June 15). SaaS vs PaaS vs IaaS: What's The Difference & How To Choose – BMC Software | Blogs. https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

[54] Elbe, D. (2021, July). PaaS vs IaaS vs SaaS — differences, pros, and cons | Artifakt Blog. https://www.artifakt.com/blog/paas/paas-vs-iaas-vs-saas-differences-pros-and-cons/

[55] Sakovich, N. (2018, April 4). IaaS vs. PaaS vs. SaaS. Advantages and Disadvantages | SaM Solutions. https://www.sam-solutions.com/blog/iaas-vs-paas-vs-saas-whats-the-difference/

[56] Future Learn. (n.d.). Saas, Laas, and Paas security concerns. Retrieved May 22, 2022, from https://www.futurelearn.com/info/courses/key-topics-in-digital-transformation/0/steps/257345

[57] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 1–13. https://doi.org/10.1186/1869-0238-4-5

[58] Katrenko, A. (2020, February 26). Cloud Computing Attacks: A New Vector for Cyber Attacks. https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks

[59] Kumaraswamy, S. (2011, December 7). Introduction to Cloud Security Architecture from a Cloud Consumer's Perspective. https://www.infoq.com/articles/cloud-security-architecture-intro/

[60] A. A. Tamimi, R. Dawood and L. Sadaqa, "Disaster Recovery Techniques in Cloud Computing," 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), 2019, pp. 845-850, doi: 10.1109/JEEIT.2019.8717450.

[61] Hamadah, S. (2019). Cloud-based disaster recovery and planning models: An overview. ICIC Express Letters, 13(7), 593–599. https://doi.org/10.24507/icicel.13.07.593

[62] Saeidi, P., Saeidi, S. P., Sofian, S., Saeidi, S. P., Nilashi, M., & Mardani, A. (2019). The impact of enterprise risk management on competitive advantage by moderating role of

information technology. Computer Standards and Interfaces, 63, 67–82. https://doi.org/10.1016/j.csi.2018.11.009

[63] Friday, D., Ryan, S., Sridharan, R., & Collins, D. (2018). Collaborative risk management: a systematic literature review. In International Journal of Physical Distribution and Logistics Management (Vol. 48, Issue 3, pp. 231–253). Emerald Group Holdings Ltd. https://doi.org/10.1108/IJPDLM-01-2017-0035

[64] Williams, C. (2019, April 1). Traditional vs. ERM – Going Beyond One-Dimensional Risk Assessment - Carol Williams. https://www.erminsightsbycarol.com/traditional-vs-erm-risk-assessment-dimensions/

[65] Marker, A. (2021, March 24). Enterprise Risk Management Frameworks | Smartsheet. https://www.smartsheet.com/content/enterprise-risk-management-framework-model

[66] Islam, S., Fenz, S., Weippl, E., & Mouratidis, H. (2017). A Risk Management Framework for Cloud Migration Decision Support. Journal of Risk and Financial Management, 10(4), 10. https://doi.org/10.3390/jrfm10020010

[67] Hallikas, J., Karvonen, I., Pulkkinen, U., Virolainen, V. M., & Tuominen, M. (2004). Risk management processes in supplier networks. International Journal of Production Economics, 90(1), 47–58. https://doi.org/10.1016/j.ijpe.2004.02.007

[68] Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010). Information security risk management framework for the cloud computing environments. Proceedings - 10th IEEE International Conference on Computer and Information Technology, CIT-2010, 7th IEEE International Conference on Embedded Software and Systems, ICESS-2010, ScalCom-2010, 1328–1334. https://doi.org/10.1109/CIT.2010.501

Appendices

General information about utilized risk management tools. Identification of levels and colors with addition to risk matrix with severity and likelihood associated. Also, control methods are introduced as of what these are and for what these are used.

Levels				
1	2	3	4	5

Risk scoring matrix						
Severity	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Likelihood				

Risk rating		Very low (1-3)	Low (4-6)	Medium (8-10)	High (12-16)	Very high (20-25)

Control methods					
Avoidance	Prevention	Reduction	Separation	Duplication	Diversification
Avoiding issues or risks from happening	Preventing Issues or risks from happening	Reducing possibility and attack surface	Separating components from others	Duplicating resources or components	Diversifying risks and issues into multiple components

Appendix 1: Case 1 Risk Management

Case1				
Risks	Likelihood	Severity	Control	Mitigation
DoS	4	3	Diversification, Prevention	Tools such as WAF, reverse proxy, NACLs
MitM	2	4	Prevention	Key management, asset protection, segmentation
DNS attack	2	2	Separation	Security controls
Side Channel Attack	2	4	Prevention	Private cloud, Security controls
Unauthorized access	3	5	Prevention	IAM, Perimeter security, Asset protection, Security by design
Misconfiguration	3	3	Prevention	Automation, Identification of resources,
Visibility of the servers	2	1	Avoidance	Private cloud, Perimeter security
Services reach limit	2	3	Prevention	Logging and monitoring, Flexible design, Automation
Session hijacking	2	2	Separation, prevention	Asset protection, Segmentation, Security by design
Secret handling	2	3	Reduction	Key management, asset protection, identification of resources, IAM
Privacy issues	2	5	Prevention	Asset protection, Security controls, Data confidentiality and integrity

Compliance issues	3	5	Prevention	Security by design, Security controls, Logging and monitoring, Asset protection, Identification of resources, Private cloud
Insider threats	2	4	Avoidance	Private cloud, Logging and monitoring, Visibility, IAM
Data leaks	1	5	Prevention	Security by design, Asset protection, Segmentation, Data confidentiality and integrity
Data security	2	3	Separation, duplication	Monitoring and giving only access to do parts needed
Vulnerabilities	4	3	Diversification	Logging and monitoring, Security by design
Lack of knowledge	4	2	Prevention	Identification of resources, Training, Risk management
Complexity	4	2	Reduction	Flexible design, Security controls, Identification of resources
Shared technology vulnerabilities	3	3	Separation	Private cloud, Perimeter security, Segmentation
Malware injection attack	2	3	Separation	Segmentation, Security by design, Security controls
Zombie attack	1	2	Avoidance	Tools such as WAF, Private cloud, Segmentation

VM Escape	2	3	Prevention	Private cloud, Perimeter security, Segmentation
Backdoor channel attack	3	4	Prevention	Security by design, Tools such as scans, Logging and monitoring, Security controls
Metadata spoofing	1	2	Reduction	Asset protection
Virtualization issues	1	2	Avoidance	Private cloud, Perimeter security
Rootkit in hypervisor	1	2	Avoidance	Private cloud, Perimeter security, Tools such as scans
APTs	2	5	Prevention	Tools such as intrusion detection systems, Logging and monitoring, Private cloud

Appendix 2: Case 2 Risk Management

Case2				
Risks	Likelihood	Severity	Control	Mitigation
Misconfiguration	4	3	Prevention	Automation, Logging, and monitoring
Unauthorized access	2	4	Prevention	PAM, security groups
Visibility to public	2	2	Avoidance	Tools such as VPC, Segmentation
Access to wrong components	3	3	Prevention	Security controls, Security by design, Perimeter security, Visibility
Poor utilization	4	2	Avoidance	Automation, Logging, and monitoring
Secret management issues	2	2	Separation	Key management, IAM
Network security issues	3	3	Reduction	Tools such as VPC, Segmentation, Perimeter security
Side channel attack	2	2	Prevention	Tools such as VPC, Segmentation
VM escape	2	2	Avoidance	Tools such as VPC, Segmentation
Compromising accounts	2	4	Prevention	IAM, Logging and monitoring
Backdoor channel attack	2	3	Prevention	Logging and monitoring, Visibility
Virtualization issues	2	2	Reduction	Tools such as VPC, Segmentation
Shared technology vulnerabilities	2	2	Avoidance	Tools such as VPC, Segmentation
Data security issues	2	3	Duplication	Segmentation, Data confidentiality and integrity, Security controls, Perimeter security

Data leaks	1	2	Separation	Segmentation, Data confidentiality and integrity, Security controls
Insider threats	3	3	Prevention	IAM, Asset protection
Complexity	2	2	Reduction	Flexible design
Rootkit in hypervisor	2	2	Avoidance	Tools such as VPC and scans, Segmentation

Appendix 3: Case 3 Risk Management

Case3				
Risks	Likelihood	Level	Control	Mitigation
Data security issues	2	2	Separation	Segmentation
Data integrity	3	2	Separation	Segmentation, Security controls, Asset protection
Data leaks	2	2	Prevention	Perimeter security, Asset protection
Network security issues	2	3	Prevention	Perimeter security, Security controls, Identification of resources, Security by design
MitM	2	3	Prevention	Perimeter security, Asset protection
DoS	4	2	Avoidance	Security by design, IAM, Perimeter security
Misconfiguration	3	3	Reduction	Automation
Unauthorized access	3	2	Prevention	IAM, Perimeter security, Security by design, Logging, and monitoring
Visibility of the servers	3	1	Reduction	Segmentation, Tools such as VPC
Lack of support	3	2	Avoidance	Identification of resources
Bypassing SaaS	2	3	Prevention	Security controls, Perimeter security, Security by design
Customization issues	3	2	Avoidance	Flexible design, Identification of resources
Interoperability	1	1	Avoidance	Flexible design, Identification of resources
Session issues	1	2	Separation	Perimeter security, Security controls

Interface and API vulnerabilities	3	2	Separation	Security controls, Asset protection, Security by design
Vendor lock	2	2	Prevention	Flexible design, Identification of resources
Compromising accounts	2	3	Prevention	IAM, Automation
Performance and downtime issues	4	2	Duplication	Security controls, Perimeter security, Automation
Security of the SaaS	2	3	Avoidance	Identification of resources, segmentation
Shared technology vulnerabilities	3	2	Reduction	Tools such as VPC, Segmentation
Side channel attack	3	2	Separation	Tools such as VPC, Segmentation
Malware injection attack	2	3	Prevention	Security by design, IAM, Perimeter security, Security controls
DNS attacks	1	2	Separation	Security controls
VM Escape	3	2	Avoidance	Tools such as VPC, Segmentation
Metadata spoofing	2	3	Diversification	
Backdoor channel attack	3	4	Prevention	Logging and monitoring, Visibility
Zombie attack	1	1	Avoidance	Security by design, IAM, Perimeter security
Virtualization issues	2	2	Avoidance	Tools such as VPC, Segmentation
Rootkit in hypervisor	1	2	Avoidance	Tools such as VPC, Segmentation
APTs	2	2	Avoidance	Tools such as intrusion detection systems, Logging, and monitoring