Continuing Education Program
Center for Computing and Information Technology
Fakultas Teknik Universitas Indonesia

Information Search and Analysis Skill

(ISAS)

Implementation of Security Concept on Cloud Security

Group

Name : Muladi Aprianto Manalu

Christian Frans Mukuan

Class : 4 SC 3

CEP CCIT

FAKULTAS TEKNIK UNIVERSITAS INDONESIA

2021

PREFACE

First of all, we want to thanks to Almighty God because of his bless and grace, the entitled “Implementation of Security Concept on Cloud Security” can be finished on time as ISAS requirements 2021.

The paper is a requirement to fulfill the assignment from Mr. Tirta Akdi Toma Mesoya Hulu as our faculty. And we also thank him for all the guidance to complete it.

We hope this paper can be usefully to all people and increase knowledge for all of us. We realize that this paper is still far from perfect in the arrangement or in the content of paper. We hope that the suggestion from all of you can be a support to make us better in the next ISAS.

Finally, we expect that it can be a medium for the reader to deepen the knowledge about the “Implementation of Security Concept on Cloud Security”.

Depok, May 17th 2021

Authors

TABLE OF CONTENTS

TABLE OF FIGURES

CHAPTER I

INTRODUCTION

1.1 Background

Cloud Security has evolved through a number of implementations which include application service provision (ASP), grid and utility computing, and Software as a Service (SaaS). But the overarching concept of delivering computing resources through a global network is rooted in the sixties. The idea of an "intergalactic computer network" was introduced in the sixties by J.C.R. Licklider, who was responsible for enabling the development of ARPANET (Advanced Research Projects Agency Network) in 1969.

Cloud Security is a computing style in which scalable and flexible IT functionalities are delivered as a service to external customers using Internet technologies. Cloud Security is not a revolutionary idea; Instead, it is an evolutionary concept that integrates various existing technologies to offer a useful new IT provisioning tool.

Cloud applications extend their accessibility through the Internet by using large data center and powerful servers that host web applications and services. Anyone with a suitable Internet connection and a standard Internet browser can access a cloud application. Rapid evolution of Cloud Security technologies can easily blur its definition perceived by the public. Yet, there are five key attributes to distinguish cloud computing from its conventional counterpart:

1. Service-based
2. Scalable and elastic
3. Shared
4. Metered by usage
5. Uses Internet technologies

Cloud Security encompasses many aspects of computing (from hardware to software) that a single solution is not able to provide all aspects.

1.2 Writing Objective

The purpose of writing this paper entitled "Implementation Security Concept on Cloud Security" is to work on tasks related to the Information Security Concept and to learn more about Cloud Security.

1.3 Problem Domain

Accordance with the title of ISAS "Implementation of Security Concept on Cloud Security" authors will discuss about:

1. To know understanding about Implementation of Security Concept on Cloud Security,
2. To know the work principle of Security Concept on Cloud Security,
3. To know the advantages and disadvantages of Cloud Security.

1.4 Writing Methodology

The writing method that we use is a method of literature review, which is the collection of materials to be used and then analyzed from trusted sources.

1.5 Writing Framework

To facilitate writing of the ISAS, this discussion was organized into systematics as follows.

Chapter I : Introducing

In this chapter we will discuss about background, writing objective, problem domain, writing methodology used, and writing framework about this ISAS.

Chapter II : Basic Theory

In this chapter we will discuss about definition of Security Concept, types of IT Security, definition of Cloud Computing, and Definition of Cloud Storage.

Chapter III : Problem Analysis

In chapter III will discuss about overview of the theory that contains the answer to the problem formulation in chapter one, Work Flow Cloud Security, Cloud Security Issues, Risks and Challenges, Cloud Security Solutions, Cloud Security Capabilities, and Advantages and Disadvantages of Cloud Security.

Chapter IV : Conclusion and Suggestion

In chapter IV contains the conclusions obtained after analyzing about Implementation Security Concept on Cloud Security and giving a suggestion to readers about Cloud Security.

CHAPTER II

BASIC THEORY

II.1 Definition of Security

The term security describes techniques that secure information processing systems in the protection goals of availability, confidentiality and integrity. The primary aim is to protect against attack scenarios, to avoid economic damage and to minimize risks. Encryption of transmission paths and data storage, firewalls, protection against viruses and Trojans, ensuring availability (or protection against system failures) all these things are considered to be part of IT security.

Hacker attacks on IT systems threaten both from the outside and the inside. The primary aim is to gain access to data in an unlawful way in order to gain economic advantages. Whereas in earlier times viruses only destroyed hard drive contents, identity theft is now at the top of the list of cybercrime. This particularly affects private individuals whose e-mail accounts or accounts of online shops have been hijacked. The field of industrial espionage also belongs in this area. Here it is important to prevent intruders into company networks by means of suitable firewall technologies.

Often underestimated is the threat from within through weaknesses in the system. Time and again software errors are exploited by hackers to gain access to IT systems. Manufacturers of user programs and operating systems are constantly striving to provide updates to close these security gaps. But even the personnel of your own company can pose a threat to information security. Former employees who still have access to business-critical data can cause damage, as can the misuse of Internet access within the company, where the distribution of copyrighted material by means of file sharing can result in warnings.

Hackers can also easily gain access to data and IT infrastructures using social engineering methods. Here, every single employee of a company represents a danger through unconscious actions. A phone call from an alleged employee of the IT department is often enough to ask for passwords. Here it is important to sensitize every single user of the company network to scenarios of this kind.

II.2 Types of Security

Security prevents malicious threats and potential security breaches that can have a huge impact on your organization. When you enter your internal company network, IT security helps ensure only authorized users can access and make changes to sensitive information that resides there. IT security works to ensure the confidentiality of your organization's data, and here there are several types of IT Security.

II.2.1 Network security

Network security is used to prevent unauthorized or malicious users from getting inside your network. This ensures that usability, reliability, and integrity are uncompromised. This type of security is necessary to prevent a hacker from accessing data inside the network. It also prevents them from negatively affecting your users' ability to access or use the network.

Network security has become increasingly challenging as businesses increase the number of endpoints and migrate services to public cloud.

II.2.2 Internet security

Internet security involves the protection of information that is sent and received in browsers, as well as network security involving web-based applications. These protections are designed to monitor incoming internet traffic for malware as well as unwanted traffic. This protection may come in the form of firewalls, antimalware, and antispyware.

II.2.3 Endpoint security

Endpoint security provides protection at the device level. Devices that may be secured by endpoint security include cell phones, tablets, laptops, and desktop computers. Endpoint security will prevent your devices from accessing malicious networks that may be a threat to your organization. Advance malware protection and device management software are examples of endpoint security.

II.2.4 Cloud security

Applications, data, and identities are moving to the cloud, meaning users are connecting directly to the Internet and are not protected by the traditional security stack. Cloud security can help secure the usage of software-as-a-service (SaaS) applications and the public cloud. A cloud-access security broker (CASB), secure Internet gateway (SIG), and cloud-based unified threat management (UTM) can be used for cloud security.

II.3 Definition of Cloud Security

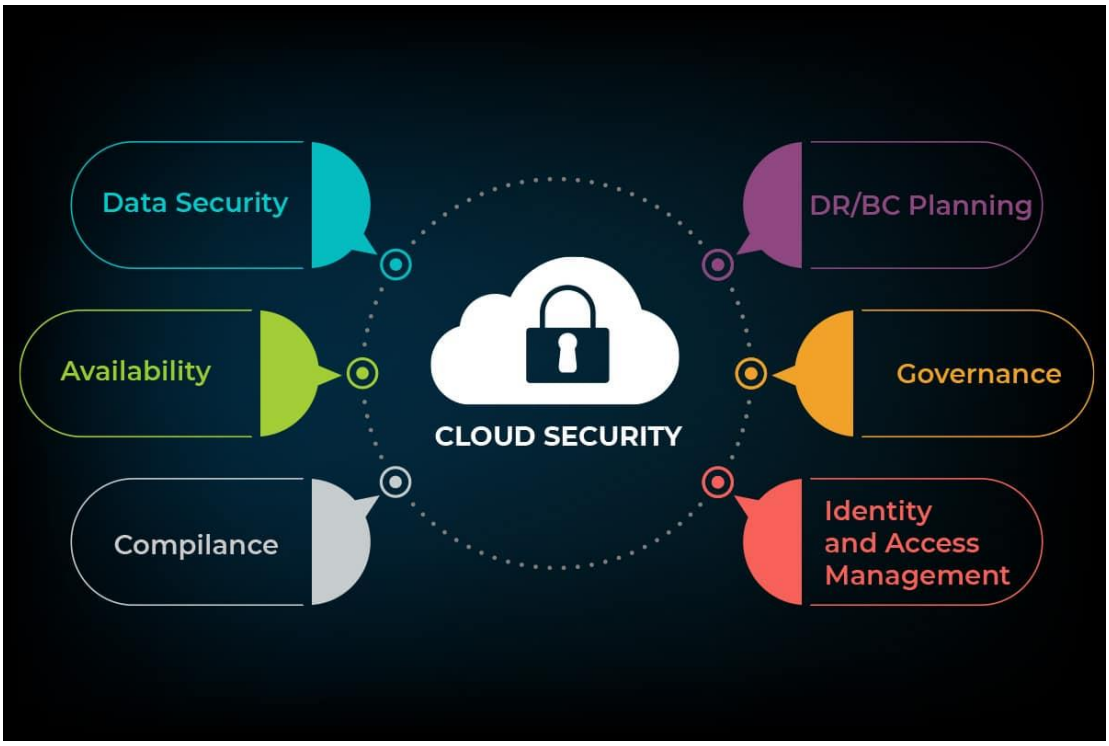

Figure 1 : Cloud Security

Cloud security is a discipline of cyber security dedicated to securing cloud computing systems. This includes keeping data private and safe across online-based infrastructure, applications, and platforms. Securing these systems involves the efforts of cloud providers and the clients that use them, whether an individual, small to medium business, or enterprise uses.

Cloud providers host services on their servers through always-on internet connections. Since their business relies on customer trust, cloud security methods are used to keep client data private and safely stored. However, cloud security also partially rests in the client's hands as well. Understanding both facets is pivotal to a healthy cloud security solution.

At its core, cloud security is composed of the following categories:

1. Data security
2. Identity and access management (IAM)
3. Governance (policies on threat prevention, detection, and mitigation)
4. Data retention (DR) and business continuity (BC) planning
5. Legal compliance

Cloud security may appear like legacy IT security, but this framework actually demands a different approach. Before diving deeper, let's first look at what cloud security is.

Cloud security is the whole bundle of technology, protocols, and best practices that protect cloud computing environments, applications running in the cloud, and data held in the cloud. Securing cloud services begins with understanding what exactly is being secured, as well as, the system aspects that must be managed.

CHAPTER III

PROBLEM ANALYSIS

III.1 Work Flow Cloud Security

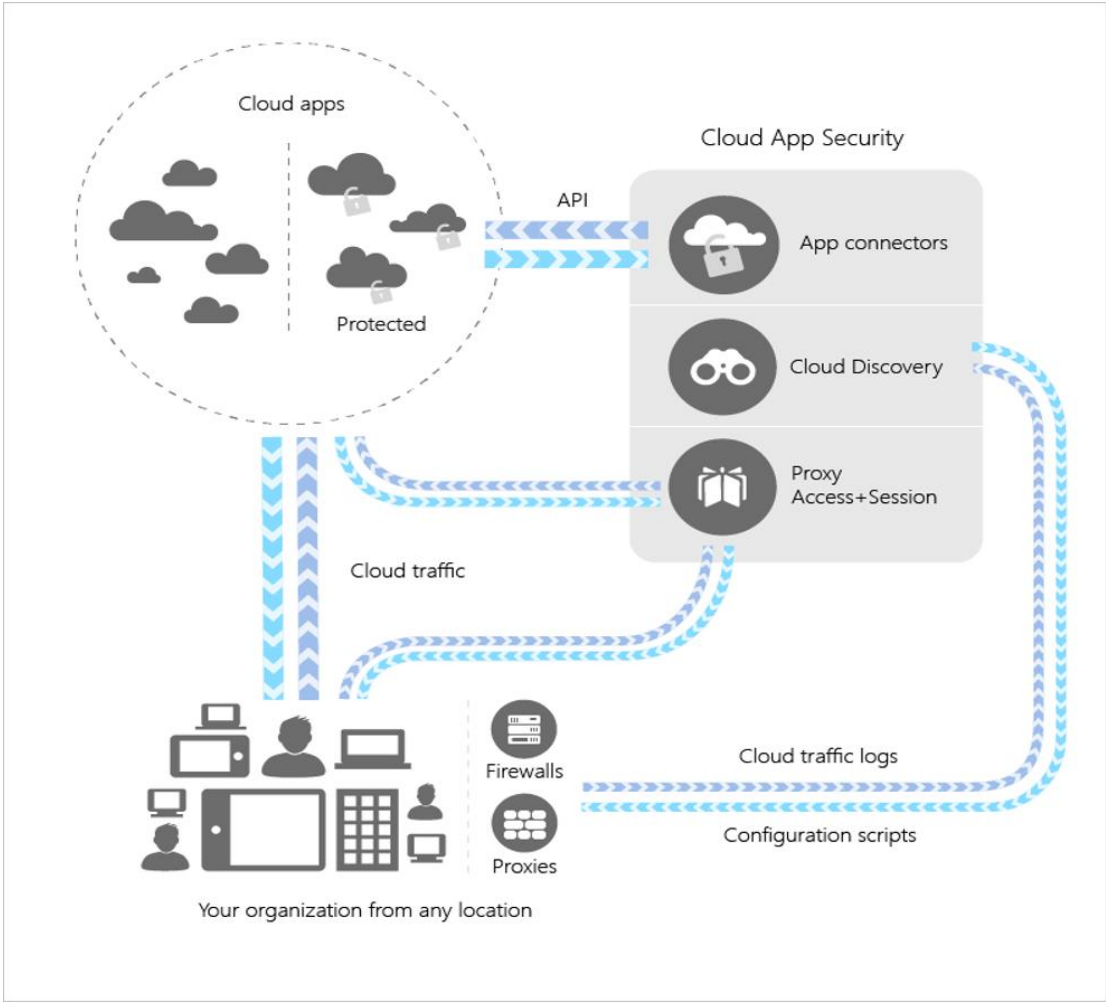

Figure 2 : Workflow Cloud Security

Cloud security refers to a wide range of strategies and policies formulated to provide controls to protect data applications and the cloud system apps. Most organizations have shifted their business information to cloud service from the traditional in premises access of data.

Cloud App Security integrates visibility with your cloud by:

- Using Cloud Discovery to map and identify your cloud environment and the cloud apps your organization is using.
- Sanctioning and unsanctioning apps in your cloud.
- Using easy-to-deploy app connectors that take advantage of provider APIs, for visibility and governance of apps that you connect to.
- Using Conditional Access App Control protection to get real-time visibility and control over access and activities within your cloud apps.
- Helping you have continuous control by setting, and then continually fine-tuning, policies.

III.2 Cloud Security Issues, Risks and Challenges

The rapid growth of cloud computing in recent times has transformed the global. However, it has also brought forth numerous security challenges and threats. The increasing utilization of the public cloud, involving humongous data, is leading to growing cloud security issues and risks.

Figure 3 : Cloud Security Risk and Issues

1. Data Breaches

A data breach involves the release of protected or confidential information to unauthorized individuals or groups. These can result from targeted attacks or even poor security practices, application vulnerabilities, or human error.

The vast amount of data hosted by Cloud Service Providers (CSPs) makes them susceptible to the risk of data breaches. While cloud providers take responsibility for their services, the customers or businesses are also responsible for protecting their own data.

Multifactor authentication and encryption are two of the security measures that ensure protection against data breaches.

2. Inadequate Identity and Access Management

Attacks and security breaches can also result from non-usage of multifactor authentication, lack of ongoing automated rotation of cryptographic keys and certificates, as well as weak password usage.

Lack of scalable identity and access management systems also contributes to unauthorized data access. Multifactor authentication systems such as a smartcard, OTP and phone authentication can go a long way in addressing this issue.

The authentication system should support the enforcement of policies for strong password usage and organization-defined rotation period, in case of legacy systems that involve the usage of passwords alone.

3. Insecure APIs

As Application Programming Interfaces (APIs) enable the provisioning, management and monitoring of cloud services, their security is of prime importance. The interfaces must be designed to prevent any malicious efforts pertaining to authentication, access control, encryption and activity monitoring.

4. System Vulnerabilities

Attackers can infiltrate and take control of the systems in addition to disrupting the service operations, utilizing the system vulnerabilities or exploitable bugs.

To reduce the security gaps and mitigate the damage caused by system vulnerabilities, installation of security patches or upgrades, regular vulnerability scanning and following up on reported system threats are mandatory.

5. Account or Service Hijacking

Service hijacking includes attack methods such as phishing, fraud and exploitation of software vulnerabilities that enable attackers to misuse the account access, steal data, impact cloud services and systems, and damage the overall reputation.

Wherever possible, organizations should prohibit the sharing of account credentials among users and leverage strong two-factor authentication techniques.

6. Malicious Insider Threats

The threat caused by insiders with malicious intent, who might be system administrators having access to critical systems and sensitive information, can have a tremendous impact on a company's security.

To control this, the CSP needs to ensure effective policies, segregation of duties and proper logging, auditing and monitoring of administrators' activities.

7. Advanced Persistent Threats (APTs)

Advanced Persistent Threats (APTs) steal data and Intellectual Property (IP) by infiltrating the IT systems of target companies. The common points of entry for APTs are spear-phishing, direct hacking systems and use of unsecured or third-party networks.

Though APTs are difficult to detect and eliminate, they can be restricted with proactive security measures.

8. Malware Injection

Malware injection attacks are becoming a major security concern in cloud computing. These are malicious scripts or code that enable attackers to eavesdrop, steal data and compromise the integrity of sensitive information.

9. Data Loss

Data loss can occur because of multiple reasons such as a catastrophe like fire or earthquake, or even accidental deletion by the CSP. To avert this, both the providers and the users need to ensure proper data backup measures and follow the best practices pertaining to disaster recovery and business continuity.

10. Insufficient Due Diligence

Organizations need to perform the necessary due diligence and develop a proper roadmap before adopting cloud technologies and selecting the cloud providers, failing which they might be exposed to several security risks.

11. Poor IP Protection

Safeguarding IP demands the highest encryption and security protocols. In addition to identification and classification of IP for determining potential security risks, vulnerability assessment and appropriate encryption must be carried out.

12. Abuse of Cloud Services

Malicious attacks can also result from issues such as unsecured cloud service deployments, fraudulent account sign-ups and free cloud service trials. Large-scale automated click fraud, hosting of malicious or pirated content, launching distributed DoS attacks, phishing campaigns and email spam are some of the examples of cloud-based resource misuse.

13. DoS Attacks

Denial-of-Service (DoS) attacks cause the consumption of disproportionately large amounts of system resources including memory, disk space, network bandwidth and processor power by the targeted cloud services, thereby preventing the users from accessing their data and applications.

14. Vulnerabilities Caused by Shared Technology

CSPs deliver scalable services by sharing infrastructure, applications and platforms without substantial alterations to the off-the-shelf hardware and software.

If the underlying components such as CPU caches and GPUs do not offer strong isolation properties for a multitenant architecture (IaaS), multi-customer applications (SaaS) or re-deployable platforms (PaaS), it could lead to shared technology vulnerabilities.

15. Communication with CSPs

Customers need to define the exact security requirements in the Service Level Agreements (SLAs) with CSPs. They can use the CSA Security, Trust and Assurance Registry (CSA STAR) as a reference for understanding the security controls offered by CSPs.

CSPs also need to provide details on how they protect multi-tenant boundaries and ensure PCI and Federal Information Security Management Act (FISMA) compliance.

III.3 Cloud Security Solutions

Data protection solutions for cloud storage security provide complete visibility and policy-based control over how data can be moved to and from the cloud, ensuring that only authorized data leaves the company's environment and that data access is limited to authorized parties. Encryption is one of the best ways to secure your cloud computing systems. There are several different ways of using encryption, and they may be offered by a cloud provider or by a separate cloud security solutions provider:

- Communications encryption with the cloud in their entirety.
- Particularly sensitive data encryption, such as account credentials.
- End-to-end encryption of all data that is uploaded to the cloud.

Within the cloud, data is more at risk of being intercepted when it is on the move. When it's moving between one storage location and another, or being transmitted to your on-site application, it's vulnerable. Therefore, end-to-end encryption is the best cloud security solution for critical data. With end-to-end encryption, at no point is your communication made available to outsiders without your encryption key.

You can either encrypt your data yourself before storing it on the cloud, or you can use a cloud provider that will encrypt your data as part of the service. However, if you are only using the cloud to store non-sensitive data such as corporate graphics or videos, end-to-end encryption might be overkill. On the other hand, for financial, confidential, or commercially sensitive information, it is vital.

If you are using encryption, remember that the safe and secure management of your encryption keys is crucial. Keep a key backup and ideally don't keep it in the cloud. You might also want to change your encryption keys regularly so that if someone gains access to them, they will be locked out of the system when you make the changeover.

Configuration is another powerful practice in cloud security. Many cloud data breaches come from basic vulnerabilities such as misconfiguration errors. By

preventing them, you are vastly decreasing your cloud security risk. If you don't feel confident doing this alone, you may want to consider using a separate cloud security solutions provider.

Here are a few principles we can follow:

1. Never leave the default settings unchanged. Using the default settings gives a hacker front-door access. Avoid doing this to complicate a hacker's path into your system.
2. Never leave a cloud storage bucket open. An open bucket could allow hackers to see the content just by opening the storage bucket's URL.
3. If the cloud vendor gives you security controls that you can switch on, use them. Not selecting the right security options can put you at risk.

Basic cyber security tips should also be built into any cloud implementation. Even if you are using the cloud, standard cyber security practices shouldn't be ignored. So, it is worth considering the following if you want to be as secure as possible online:

- Use strong passwords. Including a mix of letters, numbers and special characters will make your password more difficult to crack. Try to avoid obvious choices, like replacing an S with a $ symbol. The more random your strings are, the better.
- Use a password manager. You will be able to give each application, database, and service you use separate passwords, without having to remember them all. However, you must make sure you protect your password manager with a strong primary password.
- Protect all the devices you use to access your cloud data, including smartphones and tablets. If your data is synchronized across numerous devices, any one of them could be a weak link putting your entire digital footprint at risk.
- Back up your data regularly so that in the event of a cloud outage or data loss at your cloud provider, you can restore your data fully. That backup could be on your home PC, on an external hard drive, or even cloud-to-cloud, as long as you are certain the two cloud providers don't share infrastructure.

- Modify permissions to prevent any individual or device from having access to all your data unless it is necessary. For instance, businesses will do this through database permission settings. If you have a home network, use guest networks for your children, for IoT devices, and for your TV. Save your 'access all areas' pass for your own usage.
- Protect yourself with anti-virus and anti-malware software. Hackers can access your account easily if malware makes its way into your system.
- Avoid accessing your data on public Wi-Fi, particularly if it doesn't use strong authentication. However, use a virtual private network (VPN) to protect your gateway to the cloud.

Figure 4 : Cloud Storage Security Solutions

III.4 Advantages and Disadvantages of Cloud Security

Cloud Storage is like a server or place where you can store all your files and data into it safely. You can store all your files such as videos, photos, Docs, PDFs and etc. It can be managed by either individual or joint venture, both parties can manage the files in a joint project. And this is the advantages and disadvantages of Cloud Security.

The advantages of Cloud Security include:

1. **Protecting your business from threats** – protect data by allowing you to set access lists for different assets. For instance, you might allow specific employees application access, while restricting others. A general rule is to provide employees' access to only the tools they need to do their job. By maintaining strict access control, you can keep critical documents from malicious insiders or hackers with stolen credentials.
2. **Guarding against internal threats** – encrypts identifiable information, such as names. This maintains data integrity by keeping important information private.
3. **Preventing data loss** – Disaster recovery is key to security since it helps you recover data that are lost or stolen.

The disadvantages of Cloud Security include:

1. **Dependency on Internet Speed** – If the Internet connection is slow or unstable, we might have problems accessing or sharing the files.
2. **Dependency on a Third Party** – A third party service provider (company) is responsible for the data stored and hence it becomes an important pre-requisite in selecting a vendor and to examine the security standards prior investing.
3. **High Cost for Huge Data** – Require a large amount of storage may also find costs increase significantly even after the first few gigabytes of data stored.

CHAPTER IV

CONCLUSION AND SUGGESTION

4.1 Conclusion

The role of cloud based security solutions is to ensure that customer's information is safe at all time. A cloud service filters information and restricts unwarranted access. It offers back up for the client's information and offers data recovery in case of any data loss. It provides the security of data through encryption and has applications to manage a private cloud in case a client has sensitive information that needs maximum protection.

4.2 Suggestion

While there are issues of non-uniformity across cloud vendors there is a requirement to provide uniform user interfaces and seamless integration with the mainstream desktop and server computing. Moreover, since a cloud infrastructure is a distributed system, storage facilities may be designed like the distributed file system.

.

BIBLIOGRAPHY

[1] Jake Frankenfield. *Cloud Security.* Retrieved 17 May 2021. <https://www.investopedia.com/terms/c/cloud-security.asp>

[2] Margareth Rouse. *Cloud Security Solution.* Retrieved 17 May 2021. <https://searchstorage.techtarget.com/definition/cloud-security>

[3] Kapersky. *Cloud Security,* Retrieved 17 May 2021. <https://www.kaspersky.com/resource-center/definitions/what-is-cloud-security>

[4] Veritis. *Cloud Security Risks and Issues.* Retrieved 17 May 2021. <https://www.veritis.com/blog/top-15-cloud-security-threats-risks-concerns-solutions/>

[5] Veritis. *Cloud Security Advantages and Disadvantages.* Retrieved 17 May 2021. <https://phoenixnap.com/blog/what-is-cloud-security>