Journal of Science and Technology
ISSN: 2456-5660 Volume 7, Issue 05 (JULY 2022)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2022.v7.i05.pp148-159*

On Making Cloud More Secure and Trustworthy

Tanmaya Kumar Das, Sasmita Mishra, Ph.D, , Hari Narayan Pratihari, Ph.D
[1]*Ph.D Scholar, Dept. of CSE & Application, Indira Gandhi Institute of Technology, Odisha, India.*
[2]*Professor, Dept. of CSE & Application, Indira Gandhi Institute of Technology, Odisha,India.*
[3] *Professor, Dept. of Electronics & Communication Engineering, St. Martin's Engineering College, Dhulapally,Secunderabad, Telangana, India.*
[1]*research.dillip@gmail.com*
[2]*sasmita.mishra.csea@gmail.com*
[3]*drhnpratihari1@gmail.com*

To Cite this Article

Tanmaya Kumar Das, Sasmita Mishra, Ph.D, , Hari Narayan Pratihari, Ph.D, **On Making Cloud More Secure and Trustworthy"***", Journal of Science and Technology, Vol. 07, Issue 05,-July 2022, pp148-159*

Article Info

Received: 26-05-2022 Revised: 18-06-2022 Accepted: 20-07-2022 Published: 30-07-2022

Abstract: *Cloud computing has grown in popularity as a result of recent advancements in technology. Academics and businesses alike place a high value on computing because of the abundance of data and the emergence of new AI paradigms. The problems of scalability and availability were quickly solved by cloud computing. However difficult it has been, cloud service providers have managed to provide low-cost options. Although servers may delete rarely viewed files to save space, certain cloud firms protect data integrity. However, they can't control server and network difficulties, thus they can't guarantee data availability. Customer data integrity, availability and exposure are feared by customers. Amazon S3 and Amazon EC2, Gmail email deletion, and the Sidekick cloud disaster validated customers' concerns. – Amazon.com A customer's primary concern is the safety of their personal information. Trust and security are handled by cloud companies. Proof and data are difficult to obtain. This paper describes the security principles and security measures of the cloud environments and presents some of the security assessment criteria based upon the deployment aspects of the cloud based application services in the autonomous environment*.

Keywords: *Cloud Architecture, Cloud Security, Hybrid Cloud, Zero Trust Model, Cloud Security Design Principles*

Introduction

The advancement of information technology has led to the rise of cloud computing. Since there is so much data and new AI paradigms are being developed, computing has become an important focus for both academics and businesses. Cloud Computing was able to address scalability and availability challenges quickly and effectively in this setting[5].

Because of their low cost and other advantages, cloud service providers have developed solutions that many businesses have adopted [2], regardless of the precautions taken to avoid potential difficulties. Even though certain cloud service providers may provide us with data integrity, servers may lose blocks of files that are infrequently used or not accessed to preserve storage space. Others make sure that data is always available to us, but they are unable to deal with unexpected server and connectivity problems properly[5]

As a result, customers are concerned about the safety of their data due to concerns about its integrity, availability, or exposure. The failure of Amazon S3 and the suspension of Amazon EC2 services, the deletion of emails in Gmail, and the Sidekick cloud disaster are just a few examples that have validated customers' anxieties. As a result, customers are concerned about the security of their data because of issues including data integrity, exposure, or availability. These challenges of trust and security are on the minds of cloud service providers, who are working to address them. Consequently, evidence and data access have become a problem. As a result, remote data audit protocols (RDAs) have been created that can efficiently complete these validations utilising various logical ways. Taking into account the progress of decentralization notions, we'll dig further into the current solutions and try to predict the future direction of this trend in Cloud Computing[3].

Background

Gaps in Cloud Security

It is important for organizations to be aware of Cloud security best practices in order to protect their data, information processing, and technical measures in Cloud computing against unauthorised access of the data processing and travelling over the internet/network, and to prevent accidental or unlawful tempering of data or loss/theft of data. Departments must implement the necessary safeguards to prevent the unlawful access to data and information that they have. Cloud Security procedures must be developed to ensure a secure cloud deployment architecture and application security on the CSP platform for all stakeholders [4].

Cloud computing architecture: A layered model of cloud computing

As depicted in Fig. 1, the architecture of a cloud computing environment can be divided into four layers: the hard ware/datacenter, the infrastructure layer, and the platform layer, as well as application layer[4

The hardware layer: This layer is in charge of managing the cloud's physical resources, such as servers, routers, switches, and power and cooling systems. Data centres are the most common setting in which the hardware layer is put into use. Thousands of servers are often housed in racks and connected via switches, routers, or other fabrics in a data center's infrastructure. Hardware configuration, fault-tolerance, traffic management, power and cooling resource management are some of the most common difficulties at the hardware layer[6].

The infrastructure layer: Virtualization technologies like Xen, KVM and VMware are used in the infrastructure layer to establish a pool of storage and computing power by partitioning the physical resources. Cloud computing relies heavily on virtualization technologies, such as dynamic resource allocation, in order to provide many of its major features[5].

The platform layer: Operating systems and application frameworks are components of the platform layer, which sits atop the infrastructure. In order to reduce the effort of delivering apps directly into virtual machine containers, the platform layer was created in the cloud. To give one example, Google App Engine provides API support for building storage, databases, and business logic in standard web applications at the platform layer level[5].

The application layer: At the highest level of a hierarchical structure, the application layer includes cloud applications. Cloud applications, unlike traditional ones, may take advantage of the automatic-scaling capability to improve performance, availability, and cost efficiency[5].

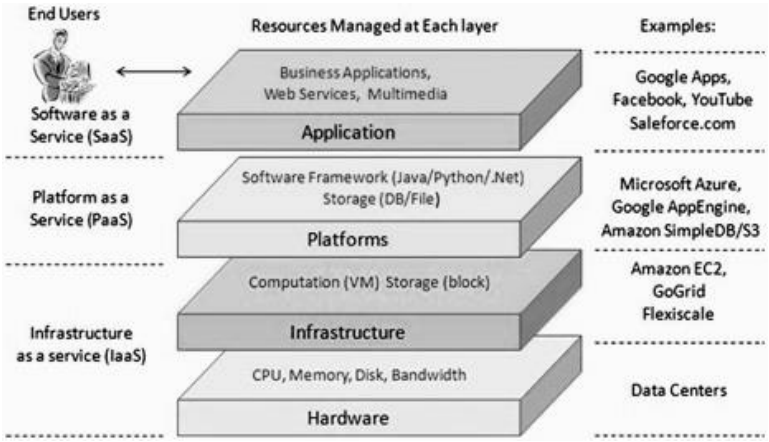

Fig.1: Cloud Computing Architecture

Cloud computing's design is more modular than those of traditional service hosting environments like dedicated server farms.. Layers are only weakly linked to one another, allowing each layer to develop independently. Similar to the OSI model for network protocols, this is a design that has been implemented. It is possible to accommodate a wide range of application needs while decreasing management and maintenance costs because to cloud computing's architectural modularity[7].

Business model

Using a service-oriented business model, cloud computing utilises the internet. This means that on-demand services are given for hardware and platform resources. As a service to the layer above, each layer of the architecture described in the preceding section can be implemented. On the other hand, every layer might be seen as a customer of the one below it. As a practical matter, cloud computing services can be divided into three broad categories, each with its own subcategory: SaaS for software, PaAS for platform, and IaAS for infrastructure (IaaS) [13].

1. **Infrastructure as a Service:** IaaS refers to on-demand provisioning of infrastructural resources, usually in terms of VMs. The cloud owner who offers IaaS is called an IaaS provider. Examples of IaaS providers include Amazon EC2, GoGrid and Flexiscale.
2. **Platform as a Service:** PaaS refers to providing platform layer resources, including operating system support and software development frameworks. Examples of PaaS providers include Google App Engine, Microsoft Windows Azure etc.
3. **Software as a Service:** SaaS refers to providing on-demand applications over the Internet. Examples of SaaS providers include Salesforce.com, Rackspace and SAP Business by Design.

Fig. 2 depicts the business model of cloud computing. It is conceivable for a PaaS provider to run its cloud on top of an IaaS provider's cloud, according to the layered architecture of cloud computing. IaaS providers are commonly part of the same company as PaaS providers, however this is not the norm (e.g., Google and Salesforce). PaaS and IaaS providers are commonly referred to as cloud service providers or infrastructure providers for this reason[13].

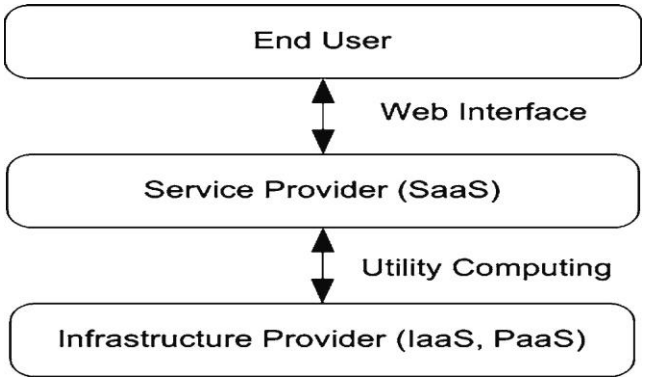

Fig. 2: Business model of cloud computing

Types of clouds

When transferring a business application to the cloud, there are a slew of considerations to keep in mind. While some service providers are primarily concerned with cutting costs, others may prioritise high levels of reliability and security. Thus, there are a variety of cloud kinds, each with its own set of advantages and disadvantages.

Public clouds: In this type of cloud, service providers make their resources available to the broader public as a service. In addition to the fact that there is no capital investment required for service providers, public clouds provide various other advantages. Many business scenarios are hindered by the lack of fine-grained control public clouds have over data, network and security settings[8].

Private clouds: This type of cloud is referred to as a private cloud since it is meant for usage only by a single company. Companies can build and maintain their own private clouds, or they can contract with third parties to do so. With a private cloud, you have complete command over the system's speed, stability, and security at all times. In contrast to traditional proprietary server farms, they have been criticised for not offering advantages such no up-front capital expenses[8].

Hybrid clouds: There are advantages and disadvantages to both the public and private cloud models, therefore a hybrid cloud combines the best of both. Part of the service infrastructure is hosted in private clouds, while the rest is hosted in public clouds in a hybrid cloud environment Both public and private clouds lack the scalability that hybrid clouds provide. By contrast with the

flexibility and scalability of public clouds, private clouds offer greater control and protection over application data. De- signing a hybrid cloud necessitates careful consideration of the appropriate balance between public and private cloud components[8].

Virtual Private Cloud: Virtual Private Cloud is an alternative solution to the limits of public and private clouds (VPC). A virtual private cloud is simply a platform that operates on top of public clouds. A VPC utilises virtual private network (VPN) technology that enables service providers to define their own network architecture and security settings, such as firewall rules. In addition to virtualizing servers and applications, VPC also virtualizes the underlying communication network. Moreover, because of the virtualized network layer, VPC enables a seamless transition from a proprietary service architecture to a cloud-based infrastructure for the majority of businesses[8].

There are numerous deployment models for the cloud that have applications. Certain firms, for example, are better suited to use public cloud services due to a variety of factors. Those who find them difficult, secret, or legally protected as intellectual property are prohibited from using them. User requirements determine the selection of the best models[8].

- Convenience: Public, community, and multi-cloud systems are the best because the ISP does the majority of the work.
- Ease of use: the public cloud and multi-cloud architectures are the most user-friendly options in this regard; however, hybrid cloud architectures can also be used effectively with the appropriate configuration settings [16].When community members work together, the data control capabilities of private, hybrid, and public clouds are elevated to a higher level of sophistication[8].
- Reliability: The reliability of a private cloud is considered to be the highest available. If it is properly tuned, a hybrid instrument can have a level that is enough for the situation[5].
- Scalability: Private and hybrid cloud environments offer the highest capabilities in this regard. Private clouds, public clouds (provided that participants conform to the company security policy), and hybrid clouds are all considered to have a higher level of security and secrecy than public and private clouds[15].
- Flexibility: When it comes to flexibility, private and hybrid clouds are your best bet because no one disturbs you to settle your resources in either of those environments.Cost: Because the cost is shared across users, public and community clouds are the most cost-effective alternatives. They also offer the lowest costs overall[17].
- Hardware needs: By definition, public clouds and community clouds do not have any requirements in this area. In spite of the numerous cloud deployment models available, users still have the option of configuring and managing their hardware in accordance with one of several fundamental service models[17].

Security in Cloud

When it comes to implementing measures and systems to protect data (such as departmental or personal data, conversational information, still images, motion pictures, or multimedia presentations, including yet-to-be-conceived ones) from unauthorised access using various forms of technology developed for generating, storing, using, and exchanging such data, Information Technology Security (IT Security) is also known as IT Security.

People, processes, and technology must all be managed to ensure the safety of data and cloud-based services. This includes a thorough examination of how a department handles its data, as well as a detailed plan for protecting it in the cloud. No modern department can afford to take a major harm to its reputation by not implementing best practises for cloud security[16].

Cloud security has evolved in much the same way that other new technologies and breakthroughs have grown in terms of security. In the unfortunate case of a data breach, having a cloud incident response plan in place is critical to reducing the effect and harm caused by suspicious behaviour. The department's response to a catastrophic occurrence can often decide the department's long-term success or failure. The cost of a data breach is often determined by the department's response strategy[16].

Cloud service companies, as well as cloud security specialists, have benefited greatly from the development of cloud computing in the Departments. Cloud security can be assured in a public cloud offering by utilising software controls, role-based permissions, storage, and hypervisor separation, but additional Cloud Deployment Models are an option if departments require even more isolation or separation of workload and data between cloud

consumers[16].

Cloud security has always been a prominent consideration when analysing the cloud, given the inherent advantages of cloud computing. Empanelment addresses the security standards that must be met by empaneled CSPs, but Departments must also follow certain procedures in order to properly roll-out their apps and services. This document highlights several cloud security practises that Departments can implement as they move toward cloud enablement[16].

If the Cloud Service Provider (CSP) does not adequately manage the responsibility of addressing IT and Cyber security parameters / controls at each layer, as it should be placed in a Cloud environment, Departments rely on CSP security and control to maintain the secure environment and mitigate potential risk. As a result, Departments must ensure that CSP adheres to the necessary security services by ensuring that the necessary Security Service Level Agreements (SLAs) are in place [16].

Need for Cloud Security

Fig.3: Cloud Security Concerns

Organizations can benefit much from cloud computing, but it is not without danger. There has been a steady stream of companies moving to the cloud service providers that have been vetted by the government. CSPs are a prime target for malicious activities since they have so much useful data in one place[16].

In order to safeguard their vital data and make sure that the essential security measures are in place, MSPs must work with CSPs, either directly or through their SIs. [16].A growing number of CSPs are concerned about the threat of insiders. Below, we've addressed some of the most common security concerns:

i) Data Breaches: Despite the fact that cloud computing services are relatively new and crucial, data breaches of all kinds have existed for decades. Many businesses are concerned about the security of their sensitive data being housed on the cloud rather than on-premises. The User Departments would benefit from increased security measures and certifications provided by the cloud service provider[11].

ii) Improper Cloud Account Management: Many organisations' adoption of the cloud has brought with it a new set of concerns about account hacking and hijacking. The department's cloud login account information can now be used by attackers to get access to critical/sensitive data housed on the platform / cloud, as well as to change and misrepresent information. This necessitates the implementation of appropriate cloud account management strategies. In some situations, a Managed Service Provider (MSP) may also have access to the Department's cloud account, which necessitates suitable controls[11].

iii) Insider Threat: An organizational intrusion may appear improbable, but the harm posed by insiders is real. Users with authorized access to the department's cloud-based services can abuse or access sensitive information such as citizen data, financial data, and other sensitive information[11].

iv) Departments must therefore design a safe plan for their cloud installation and access and ensure that an appropriate access control mechanism is in place to prevent security risks[11].

v) Regulatory Compliance: Data that is perceived to be secure in one country may not be perceived as secure in another country or region[11].

vi) Insecure APIs: It is important to customize the cloud platform through the use of Application Programming Interfaces (API). The flexibility to personalize cloud services using APIs is great, but it comes at the cost of compromising on security, authentication, and provision of access and controls[11].

vii) Increased use of APIs results in improved services, but also in increased security vulnerabilities. APIs provide programmers with the tools they need to create and integrate their own apps and systems. Application-to-application communication is what exposes APIs to attack. Additionally, they create the potential for security vulnerabilities that can be exploited[11].

viii) Denial of Service Attacks: Denial-of-service attacks are different from other types of cyber-attacks in that they don't just try to breach the security perimeter; they want to establish a foothold and collect important information over a longer period of time. Instead, they aim to prevent genuine Department users from accessing the services or systems. As a cover for criminal activity and targeted attacks, DoS can be used in some situations to take down WAFs and other security appliances (Web Application Firewalls) [11].

ix) Insufficient Due Diligence: This particular security gap is caused by a lack of clarity in a department's resource and policy allocations for the cloud, as detailed above. The departments need to keep a watch on internal controls for cloud services. To avoid operational, reputational, or compliance difficulties, a number of service settings must be carefully configured. Overlooking certain cloud configurations at the user level may provide a significant security risk due to insufficient due diligence[11].

x) Shared Responsibilities: Security in the cloud is a duty that must be shared between the cloud service provider and the cloud user. Because of this collaboration between the consumer and the provider, the consumer is responsible for taking the required steps to protect their data. Although major worldwide Cloud Service Providers do have defined protocols to secure their side of the equation, fine grain controls remain the responsibility of individual users.

xi) Data Loss: In the event of a natural disaster, the deletion of data, or a hostile attack by the service provider, data stored on a cloud platform can be lost. The loss of vital data and information can have disastrous consequences for a business that does not have a recovery strategy in place[11].

III. Related Work

Cloud Security Design Principles / considerations

For the acceptance and implementation of cloud security to secure systems, applications, and platforms, these security design principles are the most important pillars. Cloud technology deployment necessitates the consideration of the following principles[16].

1. **Security at all layers:** Make sure that multiple security measures are implemented, and that robust security is applied to all of the layers of their architecture (Physical, network, Data, Application, etc.). This will ensure that the applications and data hosted by departments on cloud platforms are protected in every possible way.
2. **Safeguard data while at rest and in transit:** Determine the criticality and sensitivity levels of the data, then identify and classify them according to those levels. Utilizing the existing security controls, such as access control, tokenization, encryption, and so on, is one way to stop this from happening.
3. **Monitoring and Auditing:** Make sure that the monitoring, auditing, and alerting systems are set up so that they can record changes made to the department's system in real time. In addition, the integration of logs and the gathering of metrics can automatically investigate, act, and respond.
4. **Access management and Controls:** It is imperative that the idea of selective privileges be put into practise, and that obligations be separated from one another with appropriate access and authority. A centralised system for managing identities and access can prevent any illegal access as well as the loss or theft of information.
5. **Readiness for security events**: It is necessary for the department or CSP to get the system ready for any

strange security occurrence. It is necessary to conduct vulnerability and security tests on a regular basis in order to identify the security issues and gaps. It is possible to carry out multiple drills in order to record the response of the Cloud systems located at various layers.

6. **Automate security best practices:** Automating software/hardware/Application based security system via AI/ML/Bots to improve the ability to secure environment which can perform regular checks and implement the controls needed to restrict the attack and enhance cloud security.

7. **Cloud Vendor Lock-in:** Departments to ensure that there is no vendor lock-in by cloud services provider while hosting the application/data, as there is no standard guidelines between different cloud providers for data migration and exports, so it becomes difficult to migrate data from one cloud provider to another or migration to on-premise Data centre.

Next Generation Model in Cloud Security – Zero Trust

An analyst working for Forrester Research Inc. came up with the idea of "zero trust" in 2010, the same year that the concept's model was initially introduced. A few years later, Google deployed zero trust security in their network, which led to an increasing interest in adoption among the technology community. [22].

The zero trust security model is a next-generation information technology security model that mandates exhaustive identity verification for every device and user attempting to access resources on a private network. This verification must take place regardless of whether the user is located inside or outside the network perimeter. Zero trust is not a specific technology; rather, it is an approach to network security that takes a more holistic and complete approach and incorporates a variety of various technologies and philosophies [22].

The concept of a castle surrounded by a moat is the foundation of the conventional approach to the security of information technology networks. When using castle-and-moat security, it is difficult to get access to the network from outside the network; yet, there is implicit trust for all users who are already inside the network[22]. The drawbacks of utilising this strategy include the fact that once an adversary has gained access to the network, they are able to exercise complete control over everything that is present on the internal networks. This limitation and vulnerability in castle-and-moat security systems is made worse by the fact that organisations and departments do not have their data centralized in just one location. In today's world, information is frequently stored with multiple cloud service providers, which makes it even more challenging to implement an unified security policy across a complete network. A security system with zero trust means that by default, no one, either from inside or outside the network, can be trusted. Verification is required for anybody who wants to use the resources on the network. The implementation of this additional safety measure was done with the goal of preventing data breaches[16].

Principles of Zero Trust Model

When Zero Trust is implemented, it is assumed that every user is dishonest. The fundamental idea that underpins a zero-trust network is the presumption that there are potential attackers on both the inside and the outside of the network. As a result, no machines or users should be trusted automatically[16].According to the findings of Forrester Research, the Zero Trust Model is based on the following principles:

1. By segmenting the network and setting Layer 7 policy, we should make sure that only valid traffic and application communication is permitted.
2. Utilize an access control technique that grants the fewest possible privileges and strictly enforce it. This indicates that users should only be granted access on a need-to-know basis, according to the needs and requirements of the system. This reduces the amount of exposure that users have to sensitive sections of the network[18].
3. Monitor and record the activity of every cloud traffic. If this is not the case, gaining access to a department's network can be regarded an easy task by a potential attacker. The idea of microsegmentation is utilised in the operation of zero-trust networks. Micro-segmentation is the process of dividing up security perimeters into smaller zones and maintaining separate access for various components of the network. As an illustration, a network that utilises microsegmentation and stores its files in a single data centre may be composed of dozens of distinct and safe zones for the files. A person or programme that has access to any one of these zones is not permitted to have access to any of the other zones unless they have received specific and individual authorisation to do so[15].

4. Multi-factor authentication, often known as MFA, is one of the fundamental components of the zero-trust approach. With multi-factor authentication (MFA), user authentication requires more than a single piece of evidence; inputting a password alone is not sufficient to gain access. In addition to password entry, cloud services customers are required to enter a code given to another device, such as a mobile phone, thereby providing a two-factor authentication. \s• Controls on who can access devices are also required for zero trust, in addition to controls on who can utilise the system[15].

Zero trust systems need to monitor the number of distinct devices that are trying to enter their network and ensure that every such device is allowed. This minimizes the attack surface of the network further. Implementing security based on zero trust through a cloud-based architecture is not only more flexible but also more cost-effective for businesses of any size or kind. IT departments can enjoy greater security without having to sacrifice simplicity of use because to the elimination of the associated maintenance costs of on-premises hardware[16].

Cloud Security in a Multi-cloud/ Hybrid Cloud environment:

It is a difficult task to secure a hybrid information technology environment that is operating from across multiple clouds. Those organisational departments that are planning to function from a combination of on-premise and Cloud systems are likely to believe that the hybrid model provides a higher level of security compared to the exclusively in-house systems. As a result, an increase in the level of security would be a significant factor that would contribute to an increase in their utilisation of hybrid or multi-cloud services. A significant number of cloud service providers (CSPs) did not have the essential controls or guarantees of compliance and security that the departments would expect until very recently; however, this configuration has undergone a dramatic transformation[17].

The term "multi-cloud" refers to the integration of several different cloud computing and data storage services into a single heterogeneous physical structure. This heterogeneous environment also refers to the distribution of cloud assets, software, applications, etc. across multiple cloud-hosting environments. This can be done in a number of ways. This multi-cloud environment aims to get rid of its reliance on a single cloud service provider by employing a multi-cloud architecture that is fairly standard and which makes use of two or more public clouds as well as multiple private clouds[17].

It is the responsibility of the department to ensure the safety of any data that is uploaded into the cloud, despite the fact that protecting the Cloud infrastructure is a requirement for the chosen CSP. As a result, in the end, it is up to the department to carry out the necessary due diligence when selecting the CSPs and MSPs in order to ensure that they satisfy the relevant regulatory and safety requirements[17].

When it comes to the responsibility of the department to protect its data, the emphasis in a multi-cloud environment shifts from securing the perimeter of the network to securing the data itself, whether it be while the data is at rest or while it is being transferred. In a setting that makes use of more than one cloud, it is essential to have a thorough understanding of how data flows and to protect it in proportion to the degree of its sensitivity [17].

When contemplating a multi-cloud deployment or environment, the following are some potential considerations that may be useful to keep in mind:

- Central strategy towards security: The internal security teams of a department or managed security providers (MSPs) would need to centralize the security control in order to maximise data visibility. This would be necessary in order to identify threats across a hybrid multiple Cloud platform and effectively integrate security strategies to address the needs of each of the Cloud platforms. In order to improve the department's ability to protect sensitive data stored in the cloud, it is necessary to coordinate the dissemination of information concerning all of the security measures and tools that have been put into place among the identified points of contact who are responsible for each cloud platform. Having a standard protocol for the enforcement of security helps to ensure a consistent approach to cloud platforms, which in turn makes it easier to have a secure integration within a multi-cloud architecture. It may be possible to scale up cloud security by employing the assistance of third-party automation services[16].
- Evolve an approach for security of a hybrid multi-cloud environment: In addition to ensuring that their applications are always up to date, organizations need to make it an absolute priority to guarantee that their

security functions are continually improved in order to keep up with the changing nature of their IT landscape and the demands placed on its security. In the modern world, those who launch cyber-attacks are constantly looking for new security flaws to exploit and developing novel methods to circumvent existing measures. Monitoring threats to a multi-cloud architecture is an ongoing process that involves security specialists to continually examine the safety of the multi-cloud via real-time data. This type of analysis must be performed in order for the process to be considered complete[16].

- Secure communications that run the application: Even though the communications between applications in a multi-cloud environment and within the applications themselves are secure, many Departments may forget to protect the communications that are designed to control how the applications function. This is because the communications are already secure. This is referred to as the control plane, and an effective security strategy for multiple clouds should take into account the requirement to encrypt communications that fall within the purview of the control plane. These communications that govern containers and virtual machines need to be encrypted, and the department's security staff need to make sure that happens. The majority of the time, these transmissions are left unencrypted and unsecured, which opens the door for potentially hostile parties to take advantage of the vulnerabilities that exist in these locations[16].
- Ensure that the departmental employee follow the security protocol: Instances in which particular end users gain access to unlawful data and services constitute one of the most serious types of security breaches that could occur. When unconnected people are granted access to unlawful or sensitive data, there is a greater chance that the data will be put at risk of exposure to security breaches or even cyber attacks[16]. In these kinds of situations, departments need to make sure that any software they obtain has been patched and is secure before distributing it to their personnel. In addition, employees need to be educated on the importance of adhering to the severe security measures that have been established in order to forestall the development of a security breach. Cloud Access Security Brokers, also known as CASBs, might also be utilised in the Department of Defense's hybrid or multi-cloud deployments in order to ensure that security controls are maintained across the entirety of those deployments[16].

The emergence of the internal use of cloud services can be accomplished by CASBs, also known as Cloud Security Gateways, through the utilisation of a number of different mechanisms. These mechanisms include monitoring the network, integrating with an already existing network gateway or monitoring tool, and even monitoring DNS queries[16]. Following the discovery of the services to which users are connected, the majority of these products then offer monitoring of user behaviour on allowed services. This monitoring is often accomplished through API connections (if they are accessible) or inline interception (man in the middle monitoring). Many enable security alerting, including data loss prevention (DLP), and also give controls to efficiently monitor the use of sensitive data in cloud services (SaaS, PaaS, and IaaS) [15].

It does not matter where the application is deployed; the security policies must still be maintained in accordance with the policy definitions. This can be accomplished through the utilisation of a solution for centralised policy administration that spans across a variety of clouds as well as data centre locations. This system needs to have the capability to manage, monitor, and enforce the policies in a standardised manner[15].

In order to support centralised security monitoring, incident management, and event analysis, infrastructure and application logs from the different CSP environments that interact to offer services should be gathered at a central location. This will offer a unified view of emerging threats across all of the data assets held by the company. This solution is going to be built on top of artificial intelligence (AI) and machine learning (ML), and it will have the ability to analyse user and entity behaviour (UEBA). This would help in minimising the amount of work and time taken to find anomalies, which in turn would minimise the amount of time it takes to resolve an event, which would result in a lower cost associated with a data breach[15].

Each individual end user ought to go via an identity access management system (IDAM solution) that is centralised. This system is able to accommodate multiple user identities and manage various user kinds, as well as facilitate a single sign-on method and integrate or have the feature to enable multi-factor authentication. Additionally, it is capable of enabling a single sign-on mechanism[15].

A centralised data backup solution guarantees that data from all of the different environments will be made available, even during a disaster, which is the time when this information is required the most[15].

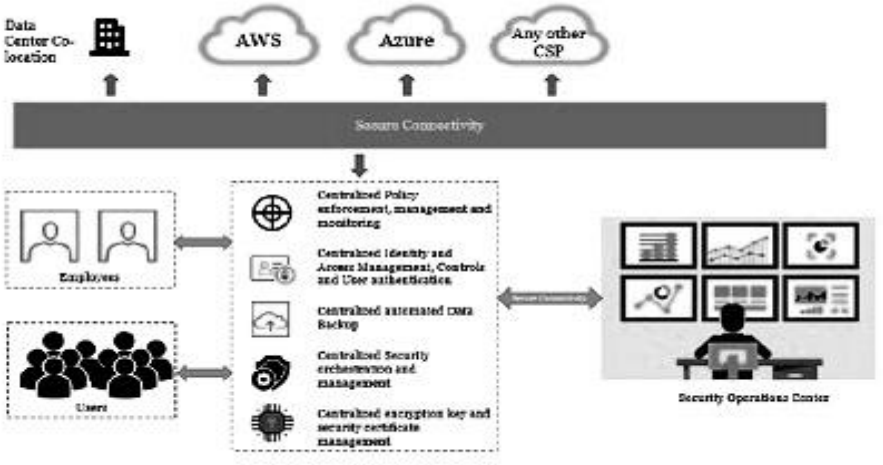

Fig. 4: Cloud Security in Multi-Cloud Environment

ICT Resilience life cycle model

In addition to determining whether or not to migrate applications into the cloud, Departments must also ensure that their activities on cloud computing are effectively incorporated into their overall information security programme. This requires an understanding of the process within the context of the ICT Resilience Lifecycle, which takes into account the preventative elements, such as risk management and information security, the reactive elements, such as incident management and continuity planning, and the overall governance process[14].

Governance: When departments make the decision to deploy applications in cloud environments, they need to ensure that they have appropriate governance policies in place for their total information technology infrastructure. This process should begin with the establishment of an overall vision of how the cloud fits not only into the necessary information security procedures, but also with the goals and objectives of those procedures and a road map for establishing them. This should be done before any other steps in the process are undertaken[17].

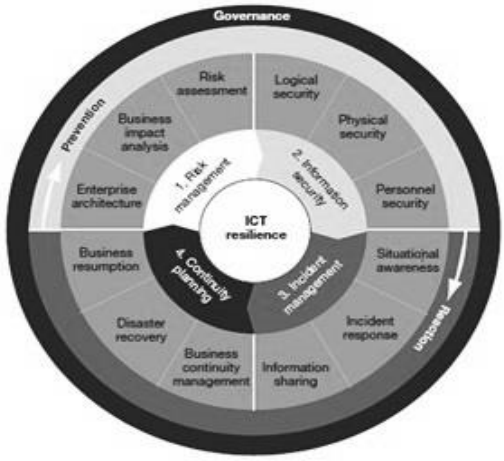

Fig. 5: ICT Resilience Life Cycle Model

- Risk management: The criteria for cloud security need to be linked with an overall understanding of risk levels at the department level as well as an internal classification of the data[16].
- Incident management: As applications are deployed in the cloud, Department's every Cloud Service Provider

must be incorporated into the Department's overall centralised incident response protocols[16].

• Continuity planning: It is imperative that business continuity plans take into account assets that have been moved into the cloud. Furthermore, these plans need to be routinely updated and tested in order to take into account new cloud architecture and provider models[16].

As a part of this effort, security practitioners are required to define the scope and boundaries of all security functions that may be relevant to cloud environments. Additionally, they must devise a strategy for improving and monitoring the performance of all of the cloud's stakeholders, which includes service providers, users, and technical staff. Finally, they should offer senior management with the tools required to obtain visibility into cloud security, such as a security-level dashboard, as well as the levers required to manage the whole cloud computing programme. This will ensure that the cloud is used safely and effectively[16].

It is necessary to make use of a centralised analytics and monitoring solution in order to manage the security architecture in all of the different environments. This instrument may also be utilised for IT infrastructure orchestration, which incorporates a wide variety of security techniques and technologies. The encryption keys and certificates can be handled from a central HSM or a key management system[16].

Last but not least, automated workflows and playbooks will make it easier to empower the Security Operation Center (SOC) by using automation technologies. For example, having a workflow that is completely automated for the approval of modification requests[16].

Conclusion

The benefits of cloud computing create a real competitive advantage for any organization. The apprehension about a lack of security shouldn't stand in the way of increased productivity and flexibility. Cloud security assessment offers organizations peace of mind that their network and assets are properly configured, adequately secured and not the subject of an ongoing attack. The ICT Resilience Lifecycle, which takes into account the prevention aspects, including risk management and information security, and the reaction elements, involving incident management and continuity planning, but also the overall governance process facilitates organisations to be ensure their effort towards moving applications into the cloud are fully integrated into their entire security program. In addition to this the adoption process of cloud technology must be passed through the cloud security design principles and certain measures which may be kept in mind while considering a multi-cloud deployment/ environment for organization to function.

References

[1] Ahmad, F., Franqueira, V.N.L., Adnane, A.: TEAM: a trust evaluation and management framework in context-enabled vehicular ad-hoc networks. IEEE Access **6**, 28643–28660 (2018).
[2] Ding, D., Han, Q., Wang, Z., Ge, X.: A survey on model-based distributed control and filtering for industrial cyber-physical systems. IEEE Trans. Ind. Inf. **15**(5), 2483–2499 (2019).
[3] Fawcett, L., Scott-Hayward, S., Broadbent, M., Wright, A., Race, N.: Tennison: a distributed SDN framework for scalable network security. IEEE J. Sel. Areas Commun. **36**(12), 2805–2818 (2018)
[4] Huang, K., Zhou, C., Tian, Y., Yang, S., Qin, Y.: Assessing the physical impact of cyberattacks on industrial cyber-physical systems. IEEE Trans. Ind. Electron. **65**(10), 8153–8162 (2018)
[5] Indu, I., Rubesh Anand, P., Bhaskar, V.: Identity and access management in cloud environment: Mechanisms and challenges. Eng. Sci. Technol. Int. J. **21**(4), 574–588 (2018)
[6] International Data Spaces association: IDS reference architecture model industrial data space (2018). https://www.fraunhofer.de/content/dam/zv/de/Forschungsfelder/industrial-data-space/IDS_Referenz_Architecture.pdf. Version 2.0
[7] Li, R., Shen, C., He, H., Gu, X., Xu, Z., Xu, C.: A lightweight secure data sharing scheme for mobile cloud computing. IEEE Trans. Cloud Comput. **6**(2), 344–357 (2018)
[8] Lin, H., Yan, Z., Chen, Y., Zhang, L.: A survey on network security-related data collection technolo- gies. IEEE Access **6**, 18345–18365 (2018)
[9] Lopez, D., Lopez, E., Dunbar, L., Strassner, J., Kumar, R.: Framework for interface to network secu- rity functions. IETF RFC 8329 (2018). https://tools.ietf.org/pdf/rfc8329
[10] Nespoli, P., Papamartzivanos, D., Marmol, F.G., Kambourakis, G.: Optimal countermeasures selec- tion against cyber attacks: a comprehensive survey on reaction frameworks. IEEE Commun. Surv. Tutor. **20**(2), 1361–1396 (2018)
[11] Network functions virtualisation (nfv); terminology for main concepts in nfv. ETSI GS NFV 003 (2018). https://www.etsi.org/deliver/etsi_gs/NFV/001_099/003/01.04.01_60/gs_nfv003v010401p. pdf. V1.4.1

[12] Open command and control (OpenC2) (2019). Language Specification Version 1.0, Committee Specification 02
[13] Open command and control (OpenC2) profile for stateless packet filtering (2019). Version 1.0, Committee Specification 01
[14] Rapuzzi, R., Repetto, M.: Building situational awareness for network threats in fog/edge computing: emerging paradigms beyond the security perimeter model. Fut. Gener. Comput. Syst. **85**, 235–249 (2018). https://doi.org/10.1016/j.future.2018.04.007
[15] Repetto, M., Carrega, A., Lamanna, G.: An architecture to manage security services for cloud appli- cations. In: 4th IEEE International Conference on Computing, Communication & Security (ICCCS- 2019), pp. 1–8 (2019)
[16] Repetto, M., Carrega, A., Rapuzzi, R.: An architecture to manage security operations for digital ser- vice chains. Fut. Gener. Comput. Syst. **115**, 251–266 (2021)
[17] Sciancalepore, S., Piro, G., Caldarola, D., Boggia, G., Bianchi, G.: On the design of a decentralized and multi-authority access control scheme in federated and cloud-assisted Cyber-Physical Systems. IEEE Internet Things J. **5**(6), 5190–5204 (2018). https://doi.org/10.1109/JIOT.2018.2864300
[18] Specification for transfer of OpenC2 messages via https (2019). Version 1.0, Committee Specifica- tion 01
[19] Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Al-Nemrat, A., Venkatraman, S.: Deep learning approach for intelligent intrusion detection system. IEEE Access **7**, 41525–41550 (2019)
[20] Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Venkatraman, S.: Robust intelligent malware detection using deep learning. IEEE Access **7**, 46717–46738 (2019)
[21] Wei, J., Liu, W., Hu, X.: Secure and efficient attribute-based access control for multiauthority cloud storage. IEEE Syst. J. **12**(2), 1731–1742 (2018)
[22] Xue, K., Chen, W., Li, W., Hong, J., Hong, P.: Combining data owner-side and cloud-side access control for encrypted cloud storage. IEEE Trans. Inf. Forensics Secur. **13**(8), 2062–2074 (2018)