iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.60595

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Governance for Azure and AWS Cloud Services

Ahmed Abdelghany[1], Mohamed Gamal[2], Dr. Tarek Aly[3], Prof. Dr. Mervat Gheith[4]
[1, 3, 4]*Software Engineering Department Faculty of Graduate Studies For statistical research, Cairo University Cairo, Egypt*
[2]*Information System Department Faculty of Computers and Artificial Intelligence, Cairo University Cairo, Egypt*

Abstract: ***These days, cloud computing services are utilized in all business, academic, and governmental domains to build IT infrastructure. Cloud computing services are one IT solution that is becoming more and more popular among different types of enterprises. Cloud computing services face many challenges, like how to protect and raise user knowledge. These problems and difficulties also pertain to cloud computing services, which could result in a number of important risk areas. One of the problems is not being aware of the hazards associated with cloud computing services and the controls that are required to reduce these risks. Because governance is difficult to execute in the cloud computing environment and has the responsibility of assessing performance and adherence to predetermined goals and objectives, it hinders the adoption of cloud computing services. This study aims to develop a model that ensures that the required controls are applied in cloud services offered by Microsoft Azure and Amazon Web Services (AWS) and assesses the risk if the controls are not applied.***
Keywords: Security, Cloud computing services, Governance, Audit, AWS, Azure, CIS, Controls, Compliance check

I. INTRODUCTION

Numerous cloud computing models have different definitions. A shared pool of different computer resources that can be quickly supplied and issued with little administration work or service provider interaction is made possible by the cloud computing concept [1]. One of the numerous advantages that consumers get from cloud computing services is scalability, which allows the client to grow horizontally by simply adding or deleting new stations. If a user uses a cloud service, they may access their data and services from any location [2]. Because cloud computing offers more flexibility in work routines, it helps employees to be more adaptive in their work habits. One of the most important advantages of cloud computing is business continuity since most service providers have a disaster recovery strategy. Data security is strengthened by the measures cloud service providers implement in their data centers.

The transition to using cloud computing services comes with many difficulties, including cyberattacks, performance expectations, data security, and data breaches. The service model will determine how the controls are shared between the cloud service provider and the cloud client. This means that the cloud client will have problems with regulatory compliance. These factors contribute to the worries that many organizations have when it comes to moving their data and operations to the cloud.

The authors of this study want to offer a model that will assist the auditor in evaluating the cloud service provider side controls. The auditor can use this model to get the necessary missing controls that he needs to implement on Microsoft Azure or Amazon Web Services (AWS).

II. BACKGROUND

First, Cloud computing provides an on-demand service where users can contribute computer resources (network, storage, and server time) as required. Broad network access is an additional feature that enables regular protocols to access all network resources. Using a multi-tenant approach, the cloud service provider pools its computer resources to support multiple cloud clients. Continually allocated and reallocated physical and virtual resources are contingent upon customer demand [3].

The deployment models for cloud computing have been split into four categories [4]:

Private: It is seen to be the safest deployment approach when the company controls the cloud data center.

Public: Apps, storage, and a range of other cloud services are made available to cloud clients by cloud service providers in public clouds. All organizations will be able to benefit from unlimited memory storage and expanded data exchange via the Internet with this cloud model.

Community: To reduce IT operational expenses, its infrastructure is utilized and monitored by a variety of organizations that share projects, core enterprises, or common specifications, including hardware and software.

Hybrid: includes both private and public models. Because the costs are divided among the firms, it helps to lower the cost of paying benefits for its establishment.

©IJRASET: All Rights are Reserved

Benchmarks are the only best-practice security configuration guidelines that are accepted and established by academics, businesses, governments, and industry. Prescriptive guidance on security option selection for a portion of AWS is provided by the Centre for Internet Security (CIS), with an emphasis on fundamental, testable, and architectural settings. A novel consensus-based approach is used to produce the CIS [17] Benchmarks, including subject matter experts and cyber-security specialists from all around the world [5].

60% of company data was kept on cloud servers in 2022. It is anticipated that this number will rise as cloud usage picks up steam. Only thirty percent of company data was kept on cloud servers in 2015. The fact that the amount of data stored on the cloud has doubled in just 7 years is evidence of the significant influence that this game-changing technology has had on business [6].

As of the most recent data, both AWS (Amazon Web Services) and Microsoft Azure are among the leading cloud service providers globally, with millions of users utilizing their platforms for various computing needs. According to recent reports, AWS continues to maintain a significant market share in the cloud computing industry, serving millions of customers worldwide, including startups, enterprises, and government agencies [7]. Figure 1 illustrates the main services of AWS. Similarly, Microsoft Azure has also experienced substantial growth in its user base, with millions of organizations leveraging its services for cloud computing, storage, and other solutions [8]. Figure2 illustrates the main services of Microsoft Azure.

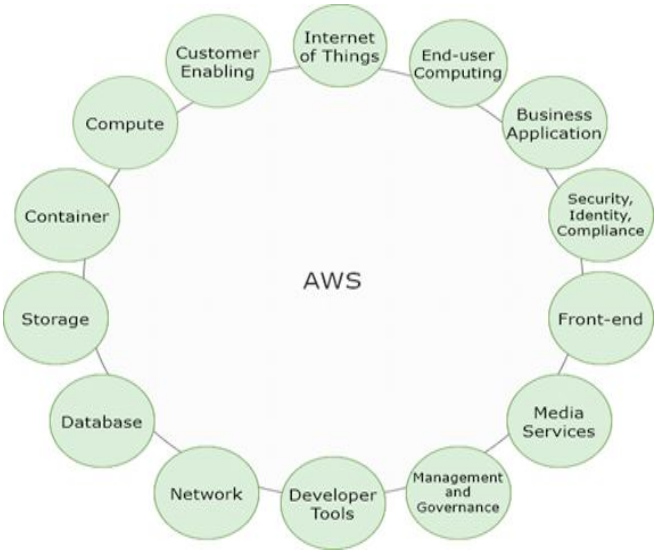


Fig. 1. AWS main services

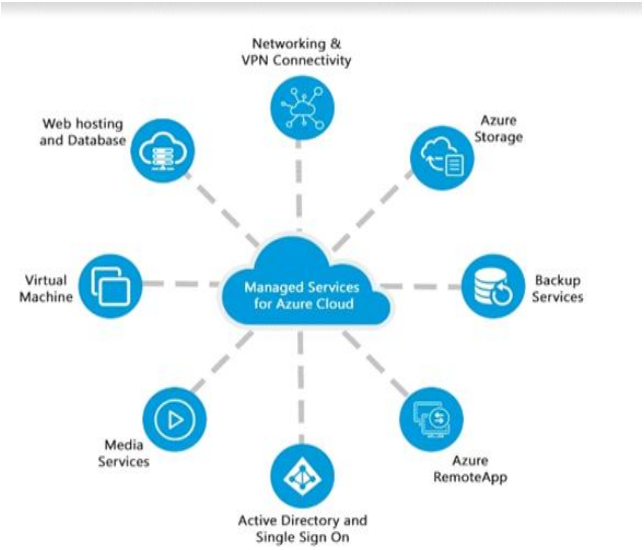


Fig. 2. Microsoft Azure main services

III. RELATED WORKS

A. Characteristics of cloud computing services

One feature of cloud computing services is on-demand self-service: cloud resources like storage, network access, server time, and web apps may all be allocated automatically by clients as needed. 2) Cost-effectiveness: The services offered by cloud service providers are comparatively cheap, if not free. Because the payment model is consumption-based, there is no need to purchase infrastructure, which also reduces maintenance expenses. 3) Wide Network Access (mobility): Using a range of devices, users may access cloud resources over the Internet at any time and from any location. 4) Resource Pooling: In the cloud, virtual and physical computer resources are merged. Since the user has no control over their position or awareness of it, these resources are not location-dependent. 5) Fast Elasticity: In response to user demand, computing resources may be allocated and released in a flexible and timely manner. Customers think these resources are endless and can be purchased anytime, in any quantity. 6) Measured Services: To monitor, manage, and optimize cloud resources and services, cloud service providers deploy a pay-per-use business model. 7) Multitenancy: A cloud is a system that offers network, host, and application services to many users simultaneously. Users share cloud resources, but each user is separated within a personalized virtual application instance [9,10].

B. Cloud Services Challenges

1) Customers using cloud computing are particularly concerned about security. There might be a security risk when using cloud computing services when databases and application software move to a big data center [11,12].
2) Compliance: Using cloud computing may result in a violation of CC legislation and the loss of part or all of the controls.
3) Cost model: Using cloud computing services raises the price of the license that each CC user will need to use as well as the cost of data transmission [13].
4) Migration: To maintain the core function independently, the majority of organizations are concerned about moving all of their data and operations to the cloud [13].
5) Charge model: Extra expenses for designing and rebuilding while transferring to the cloud, particularly in cases where the client chooses the SaaS model
6) Charge model: Extra expenses for designing and rebuilding during the cloud migration, particularly in cases when the client chooses the SaaS model.
7) Downtime: Any calamity or loss of the cloud service provider and cloud client connection might result in downtime, which can harm a company's brand or result in financial loss.
8) Service Level Agreement (SLA): Because most businesses are wary of transferring their data and entire functions to the cloud, they keep the core function in-house, which creates a migration problem [14].

C. Cloud Services Issues

Whichever paradigm is employed, there are several risks to the cloud client. One of the biggest risks when some or all controls are transferred from the cloud client to the cloud service provider is control loss. Due to resource sharing among several cloud clients, multi-tenancy poses a significant risk of denial-of-service attacks and reputational damage if one of the other cloud clients engages in improper behavior. Additionally, cloud client anticipates 100% availability, but things could not go as planned. If SLA does not meet all conditions, then it will be a weak area for cloud client [15]. Because I/O operations vary in duration based on memory type and virtual machine scheduling, cloud computing performance is unpredictable. Rapid scaling may become problematic as it might lead to a rise in expenses. Scaling down lowers costs as well. CC might not be aware of these price differences. Furthermore, the location of the data is crucial as, in some organizations and nations, exporting data will be against the law [13].

Although there are several issues, most of the controls in the IaaS model are still connected to cloud clients. IaaS considers all online risks, including DNS poisoning, ARP spoofing, and IP spoofing, to be a problem. Protecting the physical layer from unwanted access is also very important [13,14].

If PaaS is not secure, it might lead to an attack. Another risk is vendor lock-in because the cloud service provider employs certain software and tools for frameworks, databases, and storage systems. Thus, the cloud client needs to utilize comparable or equivalent tools. Vulnerabilities in browsers and APIs used by cloud service providers might impact the entire business process. Users of cloud client will require software licenses, which can be expensive because they must pay for them themselves [16].

Table 1. Services Categories

IaaS	PaaS	SaaS	General
Internet Protocol	Security threats	Access Control	Authentication And Authorization
Infrastructure failure	Lack of secure software development process	File storage way and its encryption level	Multitenancy
Physical security	Tools and Services access to User Files	Availability	Integrity
Virtual Machine Escape	Bugs in large distributed systems	Data Security	Availability of Services
Insecure VM migration	Using suspicious Software	Data Confidentiality	Performance Unpredictability
TCP/Session Hijacking	Account or service hijacking	Port Scanning	Scaling Quickly
Shared technology vulnerabilities	Insecure APIs	Data destroying way after finishing service	Changes of Business Model

IV. PROPOSED MODEL

The suggested model, which verifies the controls implemented by the provider, is based on the CIS benchmark for AWS and Azure. Based on the resources consumed, it verifies the controls. The model provides a list of adequately implemented controls, high-risk non-controlled resources, and medium-risk non-controlled resources to the cloud client auditor. This model will be helpful in pointing out any Azure or AWS controls that are lacking and might increase risk when the service is released. It will also offer recommendations for all areas of risk. As a result, it will help the auditor maximize service utilization and apply any missing controls.

A. Model Components

The model consists of a parser that runs the model engine and displays exceptions and errors upon successful authentication. The main responsibilities of the engine are to access all resources and check if the controls related to each resource are activated. The engine also powers the report generator, which encodes the results of the engine's validated controls and generates the report files.
This model will help detect any controls that are lacking that might increase risk when the service is released on the part of the cloud service providers (Azure, AWS), and it will also offer recommendations for all areas of risk. As a result, it will help the auditor maximize service utilization and apply any missing controls. By taking the advice, the auditor will be able to achieve governance. In order to attain governance, we must implement pertinent controls, which necessitate the identification of the resources and the risk areas that require control. Consequently, we will deconstruct our model into three steps: (1) List the AWS or Azure resources that are being utilized; (2) identify any potential risk areas that require management; and (3) examine the controls on the resources that are being used.

B. AWS Main Resources

1) Compute Resources

Lambda: is a serverless computing service that runs your code in response to events while autonomously managing the underlying compute resources.

Elastic Compute Cloud (EC2): is used to manage storage, handle networking and security, and build as many or as few virtual servers as needed.

Elastic Load Balancing (ELB): is employed to split up incoming application traffic across many targets automatically.

Load balancer (Elbv2): is used to distribute inbound traffic across destinations. [7]

2) Management Resources

CloudFormation is a service that simplifies the design and provisioning of a collection of linked AWS and third-party resources for developers and enterprises. (b) CloudTrail is used to gather logs, monitor, and record account activity associated with its AWS infrastructure. (c) CloudWatch is an AWS, hybrid, on-premises, and infrastructure resources monitoring and management solution. [19]

CloudFormation: offers developers and organizations a straightforward method for assembling a collection of connected AWS and external resources.

CloudTrail: may manage the governance, compliance, operational auditing, and risk auditing of your AWS account using this service.

CloudWatch: a system for managing and monitoring infrastructure resources that provides data and insightful analysis for hybrid, on-premises, AWS applications.

3) Database Resources

Relational Database Service (RDS): a web application that makes relational database maintenance, scaling, and setup easier on the AWS Cloud. [18]

Redshift: is a rapid, fully managed, petabyte-scale data warehouse solution that makes it simple and economical to utilize the cloud client's existing business intelligence tools to analyze all data efficiently. [7]

4) Network Resources

Route 53: is in charge of responding to DNS queries for TCP and UDP traffic; the word "Route" may refer to either routing or the widely accepted highway naming standard.

Virtual Private Cloud (VPC): gives the cloud client the ability to begin using AWS services inside a specified virtual network. With the advantages of utilizing the scalable infrastructure of AWS. [7]

5) Storage Resources

Simple Storage Service (S3): is an object storage service that delivers performance, security, and scalability that dominates the market. [7]

C. Microsoft Azure Main Resources

1) Compute Resources

Azure Functions: Serverless compute service for running event-triggered code without managing infrastructure.

Virtual Machines (VMs): On-demand computing resources for deploying and managing virtual servers.

Azure Kubernetes Service (AKS): Managed Kubernetes service for deploying, managing, and scaling containerized applications. [8]

2) Management Resources

Azure Resource Manager (ARM): Provides a consistent management layer for deploying, managing, and organizing Azure resources.

Azure Policy: Service for implementing and enforcing organizational standards and compliance controls across Azure environments.

Azure Monitor: Comprehensive solution for collecting, analyzing, and acting on telemetry data from Azure and on-premises environments. [8]

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

3) Database Resources

Azure SQL Database: Fully managed relational database service for building, deploying, and scaling applications.
Cosmos DB: Globally distributed NoSQL database service for building highly responsive and scalable applications.
Azure Database for MySQL/PostgreSQL: Fully managed database services for MySQL and PostgreSQL applications.[8]

4) Network Resources:

Azure Virtual Network (VNet): Provides a private network within Azure for deploying Azure resources.
Azure Load Balancer: Balances inbound and outbound connections to applications or service endpoints.
Azure DNS: Hosting service for managing and resolving domain names using Azure's global network of DNS servers. [8]
Azure Virtual Network (VNet): Provides a private network within Azure for deploying Azure resources.
Azure Load Balancer: Balances inbound and outbound connections to applications or service endpoints in Azure.
Azure DNS: Hosting service for managing and resolving domain names using Azure's global network of DNS servers.

5) Storage Resources:

Azure Blob Storage: Object storage service for storing large amounts of unstructured data.
Azure Files: Fully managed file shares in the cloud accessible via the industry standard Server Message Block (SMB) protocol.
Azure Disk Storage: Managed disks for virtual machines and other Azure services, providing scalable and durable block storage. [8]
Azure Blob Storage: Object storage service for storing large amounts of unstructured data.
Azure Files: Fully managed file shares in the cloud accessible via the industry standard Server Message Block (SMB) protocol.
Azure Disk Storage: Managed disks for virtual machines and other Azure services, providing scalable and durable block storage.

D. AWS Main Risks

1) Compute Risks

There are several danger areas with computer resources. The AMI, for instance, ought not to be made public. Verifying if the ports are open poses another risk, since it might lead to widespread attacks on the resources. The use of default security groups, which may suggest that the concept of least privilege is not being consistently implemented, is one of the major hazards. Customized security groups are necessary to provide proper power and access management.
Whitelists for security groups Setting up non-Elastic IP addresses is against corporate policy. The EBS volume has to be encrypted as well. Addresses in AWS IP ranges can be allocated to EC2 instances in any AWS account. Furthermore, there are services that enable connection to any AWS account, which might activate these IP ranges and expose your AWS account to external activity. ELB Access Logs are crucial since they provide details that may be utilized to look at traffic patterns and security concerns, such the time the request was made, the client's IP address, latency, request routes, and server answers.
A secure protocol (HTTPS or SSL) that adheres to recommended standards for encrypted communication should be used by the load balancer. If a load balancer uses an encrypted protocol without a listener, then man-in-the-middle and eavesdropping attacks are possible. Using an outdated version of the SSL/TLS policy is another problem, as updating to the latest version will fix any issues found in earlier versions. [7]

2) Database Risks

For the redshift One of the most important controls for the database is encrypting all data. Clusters that are publicly accessible pose a significant risk since they allow other AWS users to view your cluster and the data it contains.
For the relational database cloud client needs to do an automatic minor version upgrading as a convenience control. As soon as a new minor database engine version is released, cloud Client's database gets updated. [7]

3) Management Risks

Since IAM users with privileges inside the CloudFormation scope inherit the stack's role's permissions by default, passing a role to CloudFormation stacks may result in privilege escalation for management. Global service logging duplication is problematic as well since an excessive number of log entries complicates the analysis of possible issues.
If the trail is not connected to CloudWatch, it will be a big problem since it will be hard to monitor both historical and real-time data, as well as create alerts and notifications for strange account behavior.

If the data events recording is configured to occur "Without a connection to CloudWatch," you may monitor both historical and real-time data, as well as create alerts and notifications for unusual account behavior. [7]

4) Network Risks

There are several threats associated to the network. For example, there are no flow logs available to examine occurrences of illegal network traffic, such as data exfiltration or site pivoting by an attacker. Peering routing tables are essential because they stop the peered VPC from accessing resources outside of these routes, reducing the effect of a breach.

The domain has to be locked in order to stop someone from transferring it to another registrar without the owner's consent. Additionally, if the top-level domain transfer is not supported, it may lead to an unapproved registrar. Losing control over the client's domain names will result from activating the domain renewal automatically. [7]

5) Security Risks

All security certificates must be current in order for the cloud service provider to retain security. Deactivating the transparency logging feature of the ACM certificate is another problem since it might make browsers refuse to accept your certificate because of the logging.

Users ought to be restricted to accepting only those tasks for which they are competent. Using secure passwords is another crucial factor to take into account. Especially for the root account, users should be required to provide their AWS MFA device's authentication code in addition to their password when utilizing multi-factor authentication (MFA). [7]

6) Storage Risks

Versioning the buckets prevents cloud Client from recovering from application errors and unintentional user behavior. Because detailed records of bucket requests would be lost, disable bucket access logging is concerned. Additionally, the client may use these server access logs to help with security and access audits as well as comprehending the Amazon S3 charge. If HTTPS is not enforced on the bucket policy, clients and S3 buckets can interact via unencrypted HTTP. Sensitive information may therefore be transmitted in plain text across the network or Internet. [7]

Azure Main Risks

Compute Risks:

Making virtual machine images (VMIs) public can expose sensitive configurations and data, posing security risks.

Failure to verify and manage open ports can leave virtual machines vulnerable to widespread attacks.

Reliance on default security configurations may indicate inadequate implementation of least privilege principles, increasing the risk of unauthorized access [8].

Customized security groups are essential for proper access management and control, ensuring that resources have appropriate levels of power and access.

Failure to whitelist security groups can lead to unauthorized access, compromising the security of Azure resources.

Violating corporate policy by setting up non-Elastic IP addresses can result in compliance issues and security vulnerabilities.

Encrypting Azure Disk Storage volumes is crucial to protect data from unauthorized access and potential breaches.

Allowing allocation of Azure IP ranges to resources in any Azure account can expose sensitive data and resources to unauthorized access.

Database Risks:

Encrypting all data stored in Azure databases is critical to protect against unauthorized access and data breaches.

Publicly accessible database clusters pose significant security risks by allowing unauthorized users to view and potentially exploit sensitive data.

Enabling automatic minor version upgrading for Azure relational databases helps ensure that databases are up-to-date with security patches and fixes [8].

Management Risks:

Passing roles to Azure resources like Azure Resource Manager (ARM) templates may lead to privilege escalation, granting excessive permissions to users.

Duplication of global service logs complicates the analysis of issues and may hinder effective management and troubleshooting.

Failure to connect Azure Trail to Azure Monitor (formerly CloudWatch) makes it difficult to monitor historical and real-time data, potentially leading to missed security incidents and issues. [8]

Network Risks:
Lack of flow logs in Azure Network Watcher makes it challenging to detect and analyze illegal network traffic, such as data exfiltration or unauthorized access.
Properly configured peering routing tables are essential to prevent unauthorized access between peered virtual networks, reducing the impact of potential breaches.
Failure to lock domain registrations can result in unauthorized transfers to other registrars, compromising domain ownership and security. [8]

7) Security Risks:
Maintaining up-to-date security certificates is crucial for Azure service providers to ensure continued security and trust.
Disabling transparency logging for Azure certificates may result in browser rejection, undermining trust and security.
Restricting user permissions to tasks they are qualified for helps mitigate the risk of unauthorized access and potential security breaches.
Enforcing secure password policies, especially for root accounts, and implementing multi-factor authentication (MFA) enhances security by requiring additional authentication factors. [8]

8) Storage Risks:
Enabling versioning for Azure Storage accounts helps mitigate the risk of data loss due to application errors or unintentional user actions.
Disabling access logging for Azure Storage accounts may hinder security audits and access monitoring, reducing visibility into access patterns and potential security threats.
Enforcing HTTPS on Azure Storage accounts helps protect sensitive data from interception and unauthorized access during transit over the network or Internet. [8]

E. Azure Main Risks
1) Compute Risks:
Making virtual machine images (VMIs) public can expose sensitive configurations and data, posing security risks. Failure to verify and manage open ports can leave virtual machines vulnerable to widespread attacks. Reliance on default security configurations may indicate inadequate implementation of least privilege principles, increasing the risk of unauthorized access [8]. Customized security groups are essential for proper access management and control, ensuring that resources have appropriate levels of power and access. Failure to whitelist security groups can lead to unauthorized access, compromising the security of Azure resources. Violating corporate policy by setting up non-Elastic IP addresses can result in compliance issues and security vulnerabilities. Encrypting Azure Disk Storage volumes is crucial to protect data from unauthorized access and potential breaches. Allowing allocation of Azure IP ranges to resources in any Azure account can expose sensitive data and resources to unauthorized access.

2) Database Risks:
Encrypting all data stored in Azure databases is critical to protect against unauthorized access and data breaches. Publicly accessible database clusters pose significant security risks by allowing unauthorized users to view and potentially exploit sensitive data. Enabling automatic minor version upgrading for Azure relational databases helps ensure that databases are up-to-date with security patches and fixes [8].

3) Management Risks:
Passing roles to Azure resources like Azure Resource Manager (ARM) templates may lead to privilege escalation, granting excessive permissions to users. Duplication of global service logs complicates the analysis of issues and may hinder effective management and troubleshooting. Failure to connect Azure Trail to Azure Monitor (formerly CloudWatch) makes it difficult to monitor historical and real-time data, potentially leading to missed security incidents and issues. [8]

4) Network Risks:
Lack of flow logs in Azure Network Watcher makes it challenging to detect and analyze illegal network traffic, such as data exfiltration or unauthorized access.

Properly configured peering routing tables are essential to prevent unauthorized access between peered virtual networks, reducing the impact of potential breaches. Failure to lock domain registrations can result in unauthorized transfers to other registrars, compromising domain ownership and security. [8]

5) Security Risks:

Maintaining up-to-date security certificates is crucial for Azure service providers to ensure continued security and trust. Disabling transparency logging for Azure certificates may result in browser rejection, undermining trust and security. Restricting user permissions to tasks they are qualified for helps mitigate the risk of unauthorized access and potential security breaches. ISD2024 GDAŃSK, POLAND Enforcing secure password policies, especially for root accounts, and implementing multifactor authentication (MFA) enhances security by requiring additional authentication factors. [8]

6) Storage Risks:

Enabling versioning for Azure Storage accounts helps mitigate the risk of data loss due to application errors or unintentional user actions. Disabling access logging for Azure Storage accounts may hinder security audits and access monitoring, reducing visibility into access patterns and potential security threats. Enforcing HTTPS on Azure Storage accounts helps protect sensitive data from interception and unauthorized access during transit over the network or Internet. [8]

Model Components

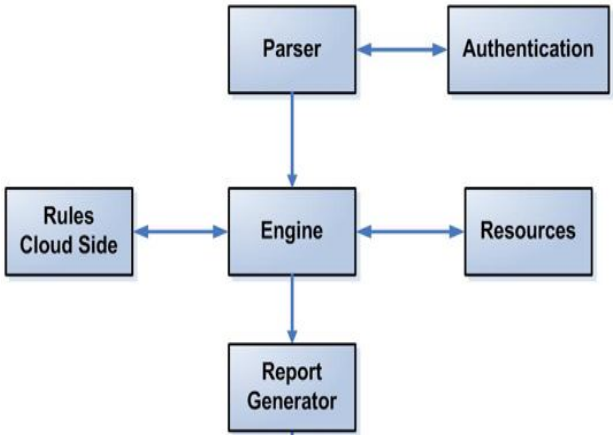


Fig. 3. Model components

Search Engine

The Test Engine oversees creating the compliance tests that are kept in resources for review and managing the report generation. The file, which executes the rules for each resource, recursively tests criteria for a path to verify the resources. It must consider every potential "id" in order to do this.

Rules

There are two sections to it. Each rule is associated with a particular resource, and the first section contains all of the rules that will be recorded as a result of the resources being tested in the final phase. The basic file, which makes up the second section, requires the rules to be checked to remove any unnecessary rules. One example of a rule is to verify if the elastic block storage (EBS) is encrypted. The report's header (EBS volume not encrypted) is represented by the description. The justification will demonstrate why there is a danger associated with this missing capability (data is encrypted both in transit and at rest when encryption is enabled on EBS discs).

Report Generator

The report generator is in charge of reading data from the result file and creating an online interface that lists all the resources in this account along with their respective levels of risk. Based on the CIS benchmark, this report will help the auditor assess each resource's risk level and offer suggestions for lowering it. The first section is the outcome of the testing of cloud-based resources. Figure 4 shows an example of the results of verifying the AWS account’s utilized resources and table 2 shows the sample of controls related to the AWS resources and its risk level. Figure 5 illustrates a sample of Microsoft azure results. Table 3 illustrates the sample of controls related to the Azure resources and its risk level.

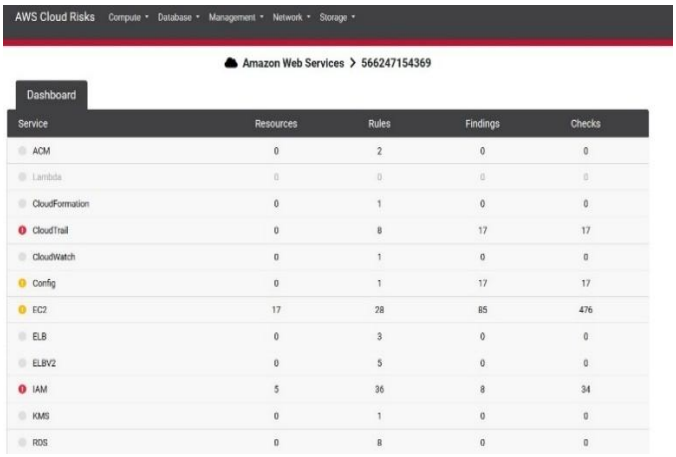


Fig. 4. AWS result sample

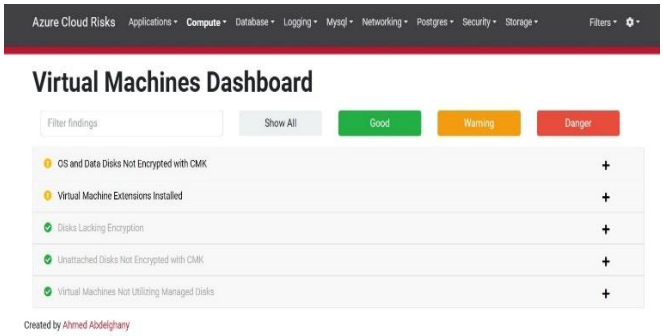


Fig. 5. Azure result sample

Table 2: Aws controls sample

Risk	Risk level	Group	Resource category
Potential secret in instance user data	Critical	EC2	Application
Default security groups in use	Medium	EC2	Application
Security group allows ICMP traffic to all	Controlled	EC2	Application
Lack of deletion protection	Medium	ELBV2	Application
Load balancer allowing (HTTP) communication	Critical	ELBV2	Application
RDS instance has a deprecated certificate authority assigned to it.	Controlled	RDS	Database

Security group allows all IP addresses	Not Used	RDS	Database
Cluster database encryption disabled	Critical	Redshift	Database
Role passed to stack.	Controlled	CloudFormation	Management
CloudTrail service not configured	Critical	CloudTrail	Management
Data events logging not configured.	Not Used	CloudTrail	Management
Alarm without action	Controlled	CloudWatch	Management
Domain transfer lock not supported by TLD.	Not used	Route53	Network
Network ACLs allow all egress traffic.	Medium	VPC	Network
Subnet with A¨ llow All" egress NACLs.	Medium	VPC	Network
Subnet without a flow log.	Medium	VPC	Network
ACM certificate expiring in less than 7 days.	Not used	ACM	Security
ACM certificate with transparency logging set to disabled.	Not Used	IAM	Security
Managed policy allows ¨IAM:PassRole" for all resources.	Critical	IAM	Security
Bucket allowing clear text (HTTP) communication.	Medium	S3	Storage
Bucket without MFA delete.	Medium	S3	Storage
All actions	Controlled	S3	Storage

authorized to all principals.			
Bucket's permissions world-readable.	Controlled	S3	Storage

Table 3: Azure controls sample Change

Risk	Risk level	Group	Resource category
HTTP Traffic Allowed	Critical	Main	Application
Client Certificates Disabled	Medium	Main	Application
App Service Authentication Disabled	Controlled	Main	Application
Disks Lacking Encryption	Medium	Main	Virtual machines
"Send Threat Detection Alerts" Disabled for SQL Databases	Critical	SQL	Database
Auditing Disabled for SQL Servers	Controlled	SQL	Database
Secure Transfer (HTTPS) Not Enforced	Controlled	Main	Storage
Trusted Microsoft Services Enabled	Controlled	Main	Storage

V. CONCLUSION AND FUTURE WORKS

The widespread adoption of cloud computing services by businesses underscores their numerous benefits. However, given the diverse range of distribution and deployment options available with other tools, our model must be adaptable to incorporate additional controls to effectively evaluate these varied choices. Transitioning to cloud computing introduces new risks as previously established controls may no longer be applicable, with the cloud service provider assuming responsibility for enforcing limitations. The abstract highlights the challenges associated with cloud computing, emphasizing the need for increased user awareness and robust safeguards against potential risks. Our study aims to address these challenges by proposing a comprehensive model that evaluates risk factors and ensures the implementation of necessary controls in cloud services offered by major providers like Amazon Web Services (AWS) and Microsoft Azure.

Moving forward, it is imperative to develop a model that can be universally applied across all cloud service providers. This will enable cloud clients to thoroughly assess each provider's environment and select the most suitable option for their requirements. Additionally, expanding the scope of rules tested will further enhance control over cloud services, thereby strengthening overall security and risk management protocols.

VI. ACKNOWLEDGMENTS

We would like to express our gratitude to Mohamed Gamal for his invaluable support throughout the duration of this study. His dedication and assistance have been instrumental in shaping our research endeavors.

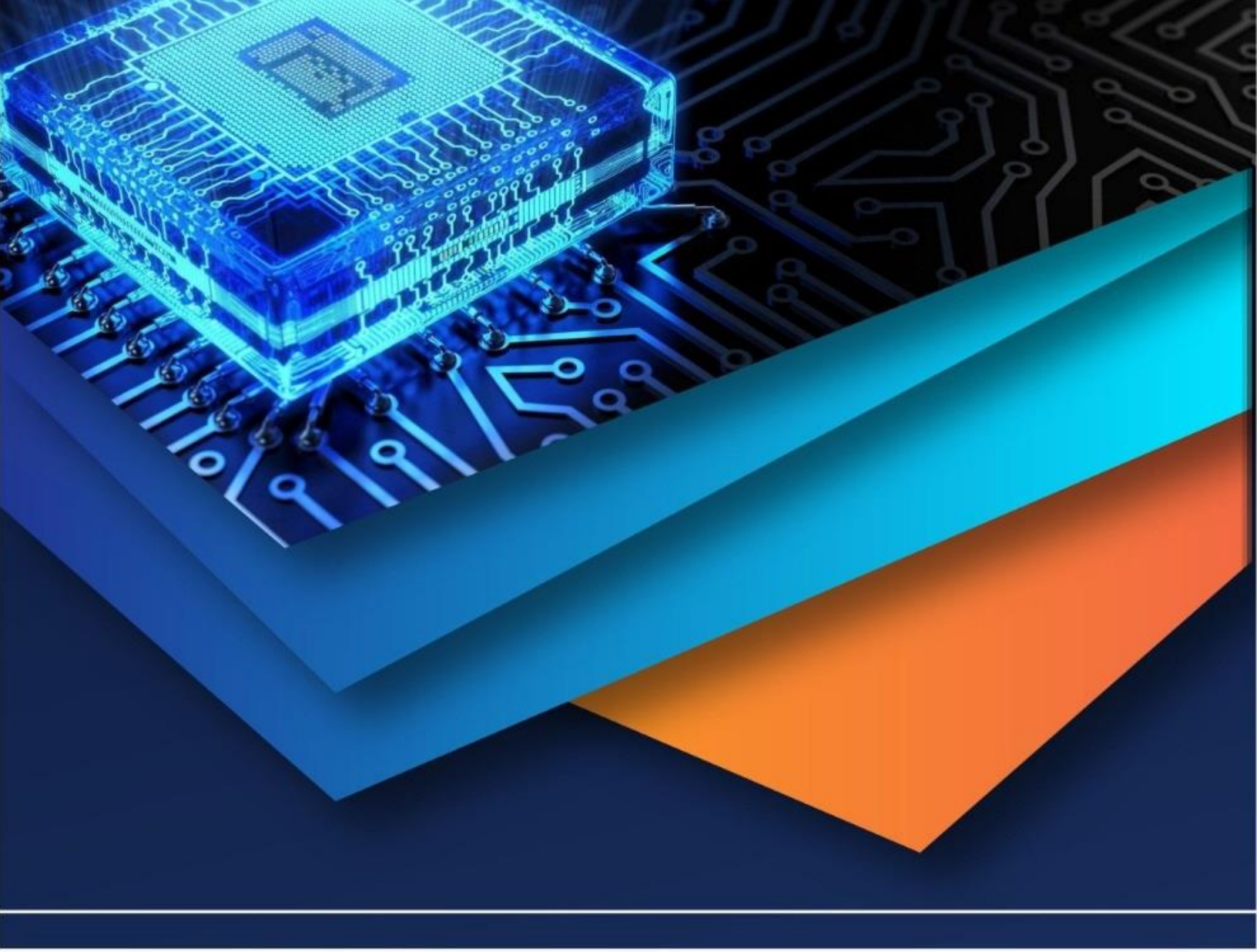
Additionally, we extend our sincere appreciation to Dr. Tarek Ali and Prof. Dr. Mervat Gheith for their insightful guidance and expertise. Their contributions have significantly enriched our understanding of the subject matter and provided invaluable perspectives.

We are also thankful to all those who have contributed to this work in various ways, directly or indirectly, and whose support has been indispensable in bringing this project to fruition.

REFERENCES

[1] Birje, M. N., Challagidad, P. S., Goudar, R. H., & Tapale, M. T. (2017). Cloud computing review: concepts, technology, challenges and security. International Journal of Cloud Computing, 6(1), 32-57.
[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A view of cloud computing,” Commun. ACM, vol. 53, no. 4, pp. 50−58, Apr. 2010
[3] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.
[4] Ara, R., Rahim, M. A., Roy, S., & Prodhan, U. K. (2020). Cloud computing: Architecture, services, deployment models, storage, benefits and challenges. International Journal of Trend in Scientific Research and Development (IJTSRD), 4(4), 837-842.
[5] CIS, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq, 15-1-2022
[6] https://aag-it.com/the-latest-cloud-computing-statistics/#:~:text=The%20Most%20Popular%20Cloud%20Services%20in%202023&text=After%20Q1%202023%2C%20AWS's%20market,second%2Dlargest%20cloud%20service%20globally.
[7] Free Cloud Computing Services - AWS Free Tier (amazon.com)
[8] Cloud Services - Deploy Cloud Apps & APIs | Microsoft Azure
[9] Kaur, H. (2020). Characteristics of cloud computing. IJRAR-International Journal of Research and Analytical Reviews (IJRAR), 7(1), 916-924.
[10] Rashid, A., & Chaturvedi, A. (2019). Cloud computing characteristics and services: a brief review. International Journal of Computer Sciences and Engineering, 7(2), 421-426.
[11] Al-Dhuraibi, Y. (2018). Flexible framework for elasticity in cloud computing (Doctoral dissertation, Université lille1).
[12] Bhatia, S., & Malhotra, J. (2018). CSPCR: Cloud Security, Privacy and Compliance Readiness-A Trustworthy Framework. International Journal of Electrical & Computer Engineering (2088-8708), 8(5).
[13] Sharma, P. K., Kaushik, P. S., Agarwal, P., Jain, P., Agarwal, S., & Dixit, K. (2017, October). Issues and challenges of data security in a cloud computing environment. In 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON) (pp. 560-566). IEEE.
[14] Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A comprehensive survey on security in cloud computing. Procedia Computer Science, 110, 465-472.
[15] Alhamad, M., Dillon, T., & Chang, E. (2010, April). Conceptual SLA framework for cloud computing. In 4th IEEE international conference on digital ecosystems and technologies (pp. 606-610). IEEE.
[16] Höfer, C. N., & Karagiannis, G. (2011). Cloud computing services: taxonomy and comparison. Journal of Internet Services and Applications, 2, 81-94.
[17] CIS Benchmarks (cisecurity.org)
[18] https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html
[19] https://link.springer.com/chapter/10.1007/978-981-99-4764-5_8

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)