Journal of Theoretical and Applied Information Technology
15th April 2023. Vol.101. No 7

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURITY MODEL FOR CLOUD SERVICES BASED ON A QUANTITATIVE GOVERNANCE MODELLING APPROACH

SWAPNA DONEPUDI[1], MADHURI A [2,]V SHARIFF[3],V KRISHNA PRATAP[4],S PHANI PRAVEEN[5], NGUYEN HA HUY CUONG[6]

[1,2,5] Assistant Professor, PVP Siddhartha Institute of Technology, Department of CSE, Vijayawada, India
[3]Assistant Professor, Sir C R Reddy Engineering College, Department of CSE Eluru, India
[4]Associate Professor, NRI Institute of Technology, Department of CSE, Guntur, India
[6]Software Development Centre ,The University of Danang, Viet Nam

E-mail: dswapna@pvpsiddhartha.ac.in[1]

ABSTRACT

The security of the cloud, in whatever form it may take, is the most important issue to consider. This necessitates the development of efficient security measurable evaluation techniques for the purpose of shielding data, services, and infrastructure from assaults that may be carried out. The cloud is now receiving a lot of attention in the market, but most businesses are not yet prepared to move their operations to the cloud for the simple reason that safety is their primary worry. No of the nature of the service being utilised by the customer, the business as well as the service provider have the responsibility for maintaining the system's security. As a direct consequence of this, a paradigm for the study of system simulation constituting governance has been provided for cloud-based systems. This article presents a cloud asset mapping and quantifiable governance security evaluation model. Components of this model include asset classification, evaluation, mapping of an appropriate security model, followed by security scanning, a security repair model, and a security quantifiable governance evaluation model. This security elevation model includes a set of assessment aspects that are relevant to a variety of areas, such as networking, maintenance, security application development, and computing, amongst others. The user G-Cloud platform is essential for the successful implementation of the quantitative governance evaluation for many cloud users. This solution walks users through the process of enhancing operation, altering configuration, and finding vulnerabilities using visual graphs to present a dynamic scanning security score. The ranking may include one or many clouds. Doing things right in order to make the cloud's resources safer. This security evaluation system protects the virtual assets of the business as well as the physical organisation by giving better security solutions.

Keywords: *Asset Mapping, Asset Classification, Cloud Asset, Cloud Security, , Quantifiable Governance Security Evaluation.*

1. INTRODUCTION

Cloud technology is employed to distribute & operate services to users. Cloud technology is probably the most popular development within the IT industry [1]. This innovation is rooted in the internet, as well as the cloud services include content and applications. Systems and other such resources may be accessible from every place depending on the demands of the client. According to the experts, grid computing is "a virtual machine that provides IT-approved solutions to clients via the internet." A cloud is a collection of virtualized servers that may be conveniently offered. Technology, equipment, and software solutions are examples of reserves. The client is not required to save information on their machine; instead, the information could be saved on an isolated virtual machine or in the web [2]. The importance of cloud technology is growing every day, and it's attracting a lot of attention from the technological and research sectors. Cloud computing may be viewed as a computing platform as well as a decentralized structure. Cloud services offer safe, easy, and speedy storage space. The basic goal of cloud computing is to perceive most computer assets as services and provide them thru the network [3]. Cloud technology is cost-effective because it is flexible, has a unified networking, which provides massive opportunity to IT solutions. Such approach facilitates flexibility, cooperation on demand, adaptability, and reliability, speeds job

creation, is able to adjust to variations, and produces an ability to cut expenses through optimal and effective computation [4]. It represents a formulation of several innovations such as web 2.0, virtualization, services - oriented design, and many others. It featured three unique deployment methods and services [5].

This internet is a cross-architecture in which data integrity is a major concern. Today, all digital computers, networking equipment, client systems, and disk drives, and so on inside a single cloud have been segregated for maintenance and security checking [6]. If cloud technology embraces additional services, data integrity might grow increasingly difficult. Another key issue for every business is keeping the uniqueness that emerges from the diversity of its client base, i.e. the organization comprises employees, consumers, collaborators, and so on. Monitoring and regulating personnel mobility inside an enterprise, typically differ based on the firm's existing market developments & responsibilities. Client identification is managed while integrating & demerging instances. This technology boosts resource utilization by using appropriate data authentication methods. In this study, a secure paradigm to cloud computing platforms is presented, along with a quantified governance assessment framework. A system backup unit, a secure quantified governance assessment model, a graphical component, a vulnerability monitoring unit, as well as other features are included in this prototype. This could assist consumers in addressing any flaws on the server.

There is a mutually beneficial relationship between security and privacy. There is widespread agreement in the academic and business communities that these two concepts are inextricably linked to the field of information and communication technologies. Digitization has had a profound effect on our daily lives. Large corporations are currently dealing with new computer paradigms that require massive computation and processing of Big Data. This information is therefore susceptible during transmission and must be safeguarded. Here we shall examine the concepts of security and privacy, together with their definitions, potential overlaps and differences, and the procedures used to protect against and counteract these risks.

Technologies related to Cloud computing are increasingly prevalent in today's networks, as is the concept of storing data remotely. The availability, reliability, and timely delivery of Cloud services and data are three of the service's most important responsibilities. Information security and privacy concerns are a major deterrent to the rapid adoption of the Cloud model, as described above. Confidentiality, data security, phishing, and multi-tenancy are just a few of the known security and privacy concerns with Cloud computing. In this section, we will investigate the several security and privacy issues that can be found in the Cloud computing system, and we will offer some recommendations for dealing with these dangers.

Users of cloud computing employ a variety of distributed cloud models to meet their unique requirements, and as a result, security and privacy risks in the cloud vary depending on the underlying cloud infrastructure. The Cloud Security Alliance (CSA) identifies information leaks, denial of service (DoS) attacks, and advanced persistent threats as the most common types of attacks against cloud infrastructure (APT).

Multilayered, tried-and-true security systems are essential for a safe Cloud infrastructure. For this reason, it's crucial to tune an existing Intrusion Detection System (IDS) to proactively track suspect threats and block attacks before they can spread across a network. In addition, it is possible to segregate the numerous observed events in order to conduct network status analysis. Threats to Cloud CIA resources and services are said to come from both internal and external actors.

Internal regulations and external regulations can both be the source of compliance needs.When it comes to the regulations that govern the workplace, they take the form of either guidelines or operational procedures.On the other side, external restrictions include things like laws, civil contracts, and regulations.This already complicated scenario gets even more entangled when you include in the possibility that special industry standards will come into play in some fields, such as banking, healthcare, insurance, or the public sector.To guarantee that risk management can be carried out in a practical manner, it is necessary to specify the requirements for compliance.

2. CLOUD COMPUTING MODELS AND ITS SECURITY POLICES

2.1 Approaches in Cloud Technology Implementation

This NIST specification defines four application scenarios.

Public-Cloud: To put it another way, public cloud services are defined by the fact that they are made available to clients through the internet by a mediator distributor of services. "Public" does not always imply open, even if it is reasonably priced or open to use, and it does not imply that the user's data is exposed to the public. In general, cloud service companies offer their clients an accessibility control method. The cloud service can enable elasticity and cost-effective service delivery [7].

Private-Cloud: Many applications available in public cloud computing, such as service-based computing and elastic computing, may be available in the private cloud. The key distinction between both the two types of cloud technology is that processing & information is kept inside the business with little or no constraints for security exposures, connectivity, or regulatory requirements while utilizing public cloud services. Furthermore, the cloud infrastructure may give the client or supplier with greater control over the reliability and safety of the virtualized environment that is because the client access and using services are defined and controlled [8].

Community-Cloud: Such associations of businesses are created by common interests such special needs for secure or generic technology, which could utilize and regulates the cloud services. All individuals may exchange data accessibility and services in the cloud network [9].

Hybrid-Cloud: A hybrid cloud is a collection of private and open clouds that can communicate with one another. On this sort of internet, clients often transfer quasi-essential information and handle it on the cloud platform while controlling the information & maintaining business critical functions [10].

2.2 Cloud Security Standards

The majority of web services prioritize protection in context. Internet services offer security standards to users by taking care of the security. Due to growing utilization of cloud computing, this becomes big market to intruders & hackers to access the information. The secure topic concentrated on several major areas for assuring reliability, privacy, integrity of information, and cloud - based services.

Information Security: Throughout the internet, all information that is to be kept is located in shared resources comprising decentralized information exchange from the separated components spatially. Controlling accessibility should be employed to safeguard information stored inside a cloud infrastructure in order to retain & secure organizational information [11]. This data comprises of profile page information and all linked to the client that exploits using data in the cloud, the participant's interaction details make the suspect's job simpler [17] [18]. Cloud services include setups, programs, framework algorithms, and customer data. For restricting access to the mentioned sections, an identity-based check is supplied [12].

Identification and Access Monitoring: The difficulty of handling credentials grows in parallel with the number of cloud services utilized by enterprises. Businesses might sometimes lose control of their service. In those cases, identity-based controls accessibility to policy guidelines is required. For the client to complete their task authorization is allowed & needed data must be supplied. Ensure that businesses' access and identification controls were constrained under secure regulatory requirements while employing online services [13].

Security Evaluation: Cloud users may proceed with the evaluation procedure. Recognizing potential dangers is indeed a critical part of cloud infrastructure security [14]. In enabling validation throughout cloud migration while without negating risk analysis & security considerations. In addition to this, there are a few other cases to offer the necessary extra security [16]. Any company with unified security policies and reliability improves risk analysis both for internet service users and for cloud platform [15].

2.3 Cloud Paradigm Challenges

Problems with data loss, privacy leakage, multi-tenancy, unauthorized access to management platforms, Internet protocol, and injection attacks are among the most common in the Cloud. Problems of this nature can open the door to assaults, provide hackers with control over permitted access, and lead to the exposure of sensitive information.

Threats to cloud computing are substantial when they involve these weaknesses, and this impacts business in a variety of ways. Identifying potential dangers and doing thorough analyses of their actions is a tried-and-true method of protecting yourself from harm. Cloud computing is discussed here, along with the various problems that can arise from using the service.

Different clients and businesses can share the same instance of software running on the SaaS provider's servers, thanks to multi-tenancy. Virtually any user firm can utilize a programme

developed for data partitioning and virtual configuration with the use of specialized software. There is a significant danger of exposure in the SaaS model since users must rely on multi-tenant apps developed by Cloud Service Providers (CSP). Since sensitive information like financial and personal data are hosted in the Cloud system, the Cloud provider is directly responsible for the maximum-security of their customers' data [19].

Although some Cloud providers use strategies like resource management and task scheduling, CSPs providers are the only ones who truly maximise hardware capability by means of virtualization. Setting up a Virtual Machine (VM) in a sandbox means isolating it from the rest of the host system. According to this philosophy, it is secure to share hardware with customers. However, security flaws in the sandboxed system can allow attackers to compromise the host. The virtualization software comes highly recommended because it can reveal modern flaws in Cloud security, such as the ability to get data by attacking a VM on another machine via a cross-Virtual Machine side channel [20].

Cloud data security places a premium on ensuring that only authorized users can view and respond to data requests. The lack of a foundational standard for data integrity highlights the necessity of developing one. Clients are expected to exhibit several values in the computer realm, one of which is trust. Trust is a challenge that many organizations face today, and it has far-reaching effects on how they handle their customer's data [21].

Giving unauthorized users access to Cloud management platforms and resources is a major security risk. Users are vulnerable because of the widespread use of similar technology in Cloud service provisioning. Access control is a reasonable mitigation strategy in such a case, as it aids in protecting the client's private data and the privacy of the client's domain. It is important to remember that Cloud service systems are vulnerable to hackers due to the usage of a single-style authentication model and weak authentication techniques[22].

There is no universal set of laws or regulations covering how an organization should go about hiring new workers or handling sensitive employee data. Some employees, however, have more seniority and are therefore granted special access to confidential information. They proposed establishing and exercising strict rules in the management of the supply chain, based on CSA, as well as implementing transparency in the general data security and management activities standard, outlining notification procedures during security failures, and using Service Level Agreement (SLA) as a demand for human resources. Working for a CSP, where everyone is presumed to be trustworthy, could make it much simpler for a malicious actor to hide their true intentions. Especially if the CSP is unable to closely monitor its employees, this person can easily become embroiled in malevolent events if they have unrestricted access to critical information[23].

Phishing attacks, in which cybercriminals pose as trustworthy individuals in order to obtain sensitive information from unsuspecting victims, can have devastating effects on individuals and businesses. The goal of identity theft is to illegally obtain private information on individuals and businesses via the Internet. An encryption key is used for all secure communications within the Cloud system, allowing for strict control over who has access to sensitive data[24].

Cybercriminals can easily acquire access to sensitive information while it is in transit from one location to another or between various systems. This happens frequently when SSL is improperly configured and therefore not sufficiently secure. Hackers can target the internal communication of Cloud systems. Limiting the damage that can be done by a man in the middle can be accomplished through proper SSL configuration and data analysis among trusted parties.

A denial-of-service (DoS) attack is one that attempts to restrict or halt the provision of a service or the provision of necessary data. This results in a situation where some or all actual users are unable to access the service. When the authorized user attempts to access the data server via Cloud services, the connection is terminated. Because the attacker's strategy involves repeatedly overwhelming the server with requests for a specific resource, the server in question becomes overwhelmed and is unable to respond to a genuine access request. This attack can be carried out in a number of methods, including through a SQL injection attack, excessive use of bandwidth, or improper management of model resources.

One popular form of cyberattack involves "phishing," in which the perpetrator poses as a trustworthy source in order to trick their targets into clicking on a malicious link. Because of the Cloud, cybercriminals may easily conceal the fact that they are hosting the accounts of many different customers who use Cloud services through phishing. Phishing can be classified as either a general or a targeted attack. Having a careless, fundamental approach that allows cybercriminals to

utilize Cloud services for even the most basic purposes, like hosting a site for a phishing attack, is a major security risk. Next, there is the issue of account hijacking using Cloud services.

3. QUANTIFIABLE GOVERNANCE EVALUAION SECURITY MODEL

Here the quantifiable governance evaluation model for security on a cross or single cloud platform as indicated in Figure. 1. The present system contains asset evaluation & mapping model, security evaluation model, security scanning module, security vulnerability database, security repairing module, establishment model module and maintenance model module.

3.1 Cloud Asset Evaluation & Mapping Model

All the domains of security should be work in efficient manner to achieve the objectives of business. How the governance, quantifiable evaluation & risk management plans to act together is represented in Figure 1. The organization basic responsibility is to control the structure of organization and implement& identify the process hence the risk management, efficient security governance, compliance should be achieved possibly. Governance means any technologies, laws and set of policies which can work within an organization and also gives directions for achieving the objectives of security. Few of organizational responsibilities are:

- Cloud provider having access risk.
- Protect sensitive information.
- Understand legal issues.
- Life cycle management of information.
- Interoperability& Portability.

To achieve effective risk management the organization should implement the framework and the risk management performance of framework is measured by metrics. For ensuring required enforce of security the organization is implemented with the service level agreement.

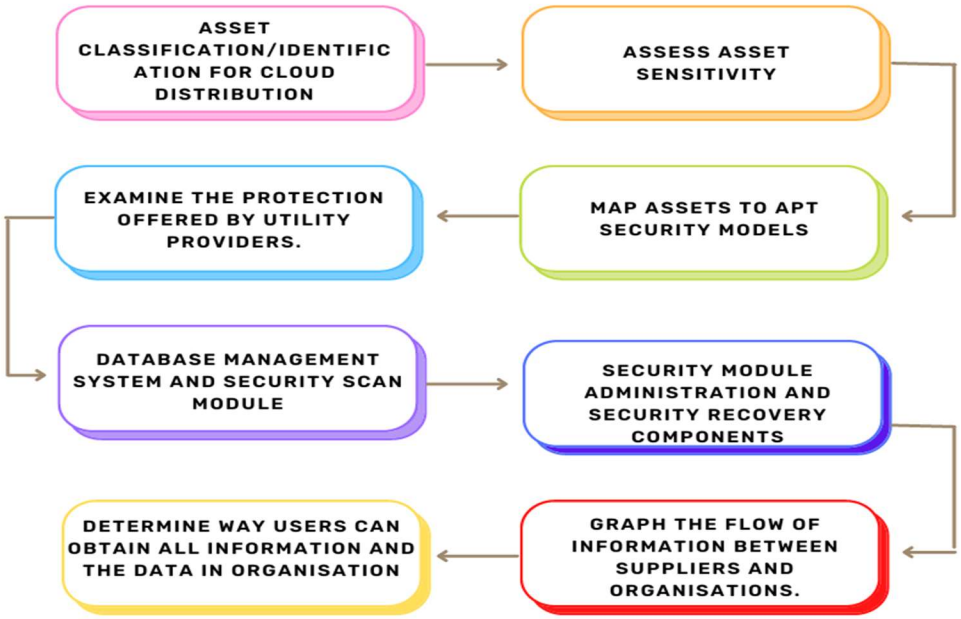

Figure. 1: Security Framework of Governance Evaluation Model

3.2 Security Scanning Module

The security scanning can be executed in parallel or serial means, and according to the definition of evaluation module it gives one out score for every resource. For one user or cloud the overall security of the result of quantifiable evaluation is score as 0 - MAX, MAX 1, 10, 100. Suppose the customer selects the vulnerabilities security repair then the repair engine is come for checking its repairs & vulnerabilities based on rules defined. The defined rules are as follows:

1. The assets of organization can only be accessed by authorized users.
2. For authorization or authentication the identity federation model is applied.
3. The log in of user depends on single sign-on capability.

4. For providing the control access the leveraging identities & managing identity services are used.

Among all, the good option is web base management identity.

3.3 Quantifiable Evaluation Security Model

The concept of quantifiable security valuation is the most important component of the current security evaluation system, according to the authors... This system denotes the repair rules &means of security evaluation. A group of security experts created this model and few times it is adopted from open source scanning or some business engine.

Security Archives and Artifacts: The security model approach is one example of such a paradigm, which is series with security fields denoted by the letters P=Ps1, Ps2, Ps3… PsN. In the field of information security, P i is one of the collections that maintains, among other things, a safety group, an application security library, an acquisition of limited access, a storage security bundle, and computing security.

One P_i of P includes variant item for checking the security P_{ij}, as VM, OS of physical server, other items of vulnerability and container systems. All items are composed as Pi as shown in equation (1)

$$P_i = \{P_{i1}, P_{i2}, P_{i3}, P_{ij} \ldots, P_{iM}\} \quad (1)$$

For every P_{ij}, security engine can check the objects current security status within the collection assets of cloud is A for one user that is given as equation (2).

$$A = \{A_1, A_2, A_3, \ldots, A_N\} \quad (2)$$

$$A_i = \{A_{i1}, A_{i2}, A_{i3}, A_{ij} \ldots, A_{iM}\} \quad (3)$$

A_i corresponds to VMs, physical machines, etc of user. $A_{ij}$is required for checking security status of one object is represented in equation (3). Suppose in checking process the scanning engine can give one triple as out$S = [S_{ij}, L_{ij}, O_{ij}]$. Here highest score is S_{ij}, vulnerable security level is Lij, one link for the fixed ways is O_{ij}.The Lij level can be very complicated, simplified means for no security risk it can be 1, for top weakness it is 0.Single $P_i$corresponding to the single S_i, this S_i, MAX is the aggregate of all totals (1 or 100) is given as equation (4) & (5).

$$S_i = \sum_{i=1}^{M} S_{ij} \quad (4)$$

$$MAX = \sum_{i=1}^{N} S_i \quad (5)$$

According to the computing security weight, network security or storage security, the Si will have one fixed score which can give one score as out. So each checking security item can give one score Si based on weight & importance. Ssi may also be a variable value, which can be altered with included checking items capacity.

Quantifiable Security Evaluation Process: The accessing of user as UP is defined in Equation (6) as the collection of resources.$UP_i$is corresponds to P_i, the checking items required for UP_i scan is defined by P_i.

$$UP = \{UP_1, UP_2, UP_3, \ldots., UP_N\} \quad (6)$$

The global resource view of one subset is the resource view of each customer. The highest privilege with the administrator view of resource is the view of global resource. In accordance with the security evaluation model the user view of resource is scanned by the security scanning engine. The items of P_{ij} are scanned with parallel or serial means and give one score out as US_{ij} as shown in equation 7.

$$US_i = \sum_{i=1}^{M} US_{ij} \quad (7)$$

The authentic security mark of all types of checking items is the view of cloud security for the view of customers cloud resource. Global security view of the administrator can be acquired with the total cloud correspondence. To improve the responsiveness of single customer towards its cloud security, this system adopts a One Veto Strategy for score reduction when cloud having important vulnerabilities.

Single Approach relates towards the customer's opinion of security; global quantifiable score is the aggregate of all values.For summarizing scores, the average or One Veto Strategy and direct summary is used here. One Veto Strategy means suppose consider single important testing element value less than cutoff, i.e L_{ij} implies 0, which makes USi as 0. Now the security view is displayed by the module of security visualization in graphical mode, i.e the security scanning scores results to cloud resources of one customer.

Repair Security Vulnerability: If the customer choose all detected gaps repair then the secure service method can trigger O_{ij}, which is equivalent of P_{ij}. Single links corresponds to repair guidelines for variant secure holes is the O_{ij}. The security holes repairing are done by repair engine either parallel or serially. For the general users or for one administrator the rapier engine is called as security system for downloading the patches, changing configures, fixing the security holes, shut the ports or services, etc. The security repair engine will close the gaps and communicate with the consumer through an interface. Then security evaluation model gives a new score as out, based

on the fixed results after the completion of repair engine work.

3.4 Mapping Data between Provider and Organization

To provide or release any service the cloud providers determined the conditions. The IDM & security services the providers should be provide various levels. To prevent the intrusions the organizations register their companies with the service providers should have good SLAs (Service Level Management). Such type of organizations should be provided with the adequate identifiable attributes which can be utilized in case of tracing the any type of Security Bridge. Therefore, end to end security is maintained. With the registry, the service providers relate well, release of any service may authorized by this unit.

3.5 Data accessing by user

Cloud Services' Registry is the one that plays major role in understanding the way in which data is accessed by the user or information on internet. In cloud computing segment, all available services are registered in the registry by the cloud services. All the services are maintained by the registers and made them available to the customers. The services are described by the service providers for releasing the customers. For determining the payment indices the register should consult the service metering unit.

4. RESULTS

Based on the customer G-Cloud platform the quantifiable governance security evaluation has been executed. Here the system environment consists of two independent clouds. Based on the G cloud OS one cloud is set upped and second one is Open Stack based. The cloud 1 had storage resource of 200 TB and 16 physical machines can be owned as computing resources (total of 512 core). The cloud 2 had it own storage resources 150TB, 10 physical machines as computing resources (total of 320 core). The two clouds shares with the 40Gb/s network bandwidth. By using the same API security the two clouds are monitored. The quantifiable evaluation means it can also evaluates the security status of single customer. The scanning module checks the security state of the client and only those resources that have been granted access are examined. Only the security view will be able to display the current security state in this case. Quantifiable methods that can provide users or administrators with a single understandable user interface for determining the security state of their systems and leading them through the process of exposing security flaws are desired. The scanning module checks the security state of the client and only those resources that have been granted access are examined. Only the security view will be able to display the current security state in this case. Quantifiable methods that can provide users or administrators with a single understandable user interface for determining the security state of their systems and leading them through the process of exposing security flaws are desired. The scanning module checks the security state of the client and only those resources that have been granted access are examined. Only the security view will be able to display the current security state in this case. Quantifiable methods that can provide users or administrators with a single understandable user interface for determining the security state of their systems and leading them through the process of exposing security flaws are desired. The scanning module checks the security state of the client and only those resources that have been granted access are examined. Only the security view will be able to display the current security state in this case. Quantifiable methods that can provide users or administrators with a single understandable user interface for determining the security state of their systems and leading them through the process of exposing security flaws are desired. To enhance the security maintenance efficiency the non-automation security tools will be replaced.

The security scanning has been done with parallel or serial mode is shown in Table 1. Suppose serial scanning model is adopted, then the module of security scanning was deployed in one server, the scanning of storage resources, network resources and computing resources (as virtual/ physical server) are done one by one. The resource scale was very large for some times. For several hours, overall sampling time remains long. By the parallel scanning model is adopted then the security module is deployed on several hosts (i.e single group contains five VM's), that divides the single host to various resources & assigns task for variant hosts for accelerating reliability of scanning & reduces span in fulfilling the customer expectation. Similarly, in the cloud resources for security scanning single host on single network or two would adjust the parallel & serial mean. Basically in 30sec one user views can be acquired, this time can be accepted within one cloud domain for their customers.

Journal of Theoretical and Applied Information Technology
15th April 2023. Vol.101. No 7

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Time Cost Of Security Scanning With Two Modes

ID	Scanning Mode	Serial Scanning Time(s)	Parallel Scanning Time(s)
1	Global Scanning for Single Cloud	3607	806
2	Global Scanning for Double Cloud	5700	1211
3	User Scanning in Single Cloud	121	30
4	User Scanning in Double Cloud	260	50

Here a case study was explained which can be applied to the present security methodology to compute risks to assets of a Cloud enterprise (CSP1). The physical hosts H1& H2 are resided in the premises of CSP. The virtual machine is the VM1 in H1 & the virtual machine in H2 is VM2. In VM1 the S1 service was deployed and in VM2 the data was stored. The Bridge Network Br0 (assets may be referred from Table 2) is shared by the hosts H1 & H2. The asset values (with dependencies) for the above mentioned assets have been listed in Table 2. Within the risk assessment scope all the assets are identified and their values required for assigning or computing. Asset Value (AV) in a Cloud scenario may be determined by employing the following metrics:

Security (SRs): It includes of confidentiality (Cs), integrity (Is) and availability (As) an asset is necessary. The following equation(8)is used to calculate security:

$$SR_s = x_s*C_s + y_s*I_s + z_s*A_s ,$$
$$\Rightarrow (x_s + y_s + z_s = 1) \quad (8)$$

x_s, y_s and z_s are the proportional weights assigned with each security criteria and can be changed by Cloud users according to their requirements and the type of assets under consideration.

Auditability (AR): Auditability is described as the requirement to gather and make accessible relevant evidence data related to the use and operation of cloud services. As a result, auditability determines asset significance as well as the entire audit environment.

Governance (GR): The governance contains 2 types and they are EG (External Governance) IG (Internal Governance). For use the cloud services there are some sort of relevant regulations or agreement, which is defined by EG. The set of policies accepted by every stockholder to assure the expected services delivery is referred by IG. The calculation of asset value is shown in equation (9),

AVs= ceil(as*SRs + bs*ARs + cs*GRs)
$\Rightarrow$ (as + bs + cs = 1) (9)

Table 2: CSP1'S Valuation

Asset IDs	SRs	ARs	GRs
HI	4.6	4	3
H2	3.6	4	3
VM1	4.6	4	3
VM2	3.6	4	3
S1	4.5	4	3
D2	3.3	4	3
Br0	4	2	2

Then the security (SR) for the each asset value of CSP1 is obtained by the following equation (10):

$$SRHI = ((5*.3) + (5*.3) + (4*.4)) = (4.6)$$
$$AVHI = ceil((4.6*.3) + (4*.3) + (3*.4)) = (4.0)$$
$$SRH2 = ((4*.3) + (3*.4) + (4*.3)) = (3.6)$$
$$AVH2 = ceil((3.6*.3) + (4*.3) + (3*.4)) = (4.0)$$
$$SRVM1 = ((5*.3) + (4*.4) + (5*.3)) = (4.6)$$
$$AVVM1 = ((4.6*.3) + (4*.3) + (3*.4)) = (4.0)$$
$$SRVM2 = ((4*.3) + (3*.4) + (4*.3)) = (3.6)$$
$$AVVM2 = ceil((3.6*.3) + (4*.3) + (3*.4)) = (4.0)$$
$$SRS1 = ((3*.5) + (5*.3) + (5*.2)) = (4.5)$$
$$AVS1 = ceil((4.5*.5) + (4*.1) + (3*.4)) = (4.0)$$
$$SRD2 = ((4*.3) + (4*.4) + (3*.3)) = (3.3)$$
$$AVD2 = ceil((3.3*.4) + (4*.2) + (3*.4)) = (4.0)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$SRBr0 = ((3 * .3) + (4 * .4) + (5 * .3)) = (4.0)$$
$$AVBr0 = ceil((4 * .4) + (2 * .3) + (2 * .3)) = (3.0) \quad (10)$$

Here the values that interpreted for the evaluation parameters described that five as "Very High", four as "High", three as "Medium", two as "Low" and one as "Very Low" on the respective parameter as shown in Table 2 and Figure 2.

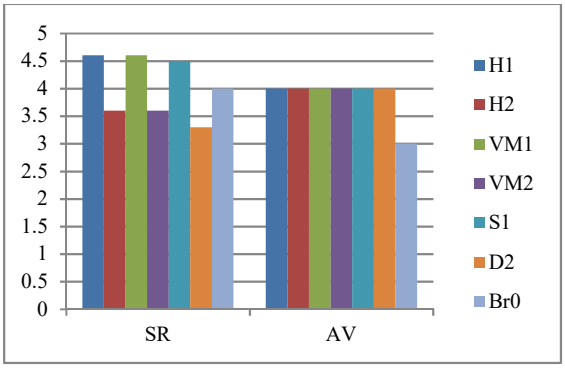

Figure2: SR and AV quantifiable evaluation results for CSP1

5. CONCLUSION

Cloud computing achieves more merits, Now a days the security is a biggest concern of its client. A framework for cloud services that includes a measurable governance modeling approach was devised in this. This model provided a cloud security models that secures organizational, physical and virtual assets. In this security model first the assets are classified and then the security scanning was carried out for the effective quantifiable governance evaluation. The quantifiable security evaluation adopted the One Vote Mechanism to count one field score and adding the sum of totals as total score. Based on G-cloud platform the quantifiable governance evaluation is applied for various cloud users. It should be noted that the asset value and security parameters are important in a specific cloud organization for specific measures (prevention/mitigation /acceptance /transfer) deciding and the security model of present paper is implemented for protecting the assets. This security model evaluated such AV and SR values then obtained high values.

The limitations as well as the threats to the framework's validity, the creation of the framework was carried out using qualitative approaches, and the threats to the framework's validity need to be assessed from this point of view. In terms of credibility the authors emphasise that the wide range of organizations that were participating in the building helped to lessen their influence over the findings.

REFERENCES:

[1] H. Wang, T. Liu, B. Kim, C.-W. Lin, S. Shiraishi, J. Xie, and Z. Han, "Architectural design alternatives based on cloud/edge/fog computing for connected vehicles," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2349–2377, 2020.

[2] B. Wang, C. Wang, W. Huang, Y. Song, and X. Qin, "A survey and taxonomy on task offloading for edge-cloud computing," IEEE Access, vol. 8, pp. 186 080–186 101, 2020

[3] C. Pahl, A. Brogi, J. Soldani, and P. Jamshidi, "Cloud container technologies: a state-of-the-art review," IEEE Transactions on Cloud Computing, vol. 7, no. 3, pp. 677–692, 2017.

[4] S. P. Praveen, K. T. Rao, and B. Janakiramaiah, "Effective allocation of resources and task scheduling in cloud environment using social group optimization," Arabian Journal for Science and Engineering, vol. 43, no. 8, pp. 4265–4272, 2018.

[5] S. F. Piraghaj, A. V. Dastjerdi, R. N. Calheiros, and R. Buyya, "A survey and taxonomy of energy efficient resource management techniques in platform as a service cloud," Handbook of Research on End-to-End Cloud Computing Architecture Design, pp. 410–454, 2017

[6] X. You, Y. Li, M. Zheng, C. Zhu, and L. Yu, "A survey and taxonomy of energy efficiency relevant surveys in cloud-related environments," IEEE Access, vol. 5, pp. 14 066–14 078, 2017.

[7] Y. Kaneko, T. Ito, M. Ito, and H. Kawazoe, "Virtual machine scaling method considering performance fluctuation of public cloud," in 2017 IEEE 10th International Conference on Cloud Computing (CLOUD). IEEE, 2017, pp. 782–785.

[8] A. Malatpure, F. Qadri, and J. Haskin, "Experience report: testing private cloud reliability using a public cloud validation saas," in 2017 IEEE international symposium on software reliability engineering workshops (ISSREW). IEEE, 2017, pp. 56–56.

[9] D. S. Linthicum, "Emerging hybrid cloud patterns," IEEE Cloud Computing, vol. 3, no. 1, pp. 88–91, 2016.

[10] H. Hu, Y. Wen, T.-S. Chua, J. Huang, W. Zhu, and X. Li, "Joint content replication and request routing for social video distribution over cloud cdn: A community clustering method," IEEE transactions on circuits and systems for video technology, vol. 26, no. 7, pp. 1320–1333, 2015.

[11] M. Eldred, A. Good, and C. Adams, "A case study on data protection and security decisions in cloud hpc," in 2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom). IEEE, 2015, pp. 564–568.

[12] K. T. Rao et al., "Client-awareness resource allotment and job scheduling in heterogeneous cloud by using social group optimization," International Journal of Natural Computing Research (IJNCR), vol. 7, no. 1, pp. 15–31, 2018.

[13] P. Sherubha, S. Sasirekha, A. Dinesh Kumar Anguraj et al., "An efficient unsupervised learning approach for detecting an anomaly in cloud," Comput Syst Sci Eng, vol. 45, no. 1, pp. 149–166, 2023.

[14] S. P. Praveen and K. T. Rao, "An effective multi-faceted cost model for auto-scaling of servers in cloud," in Smart Intelligent Computing and Applications. Springer, 2019, pp. 591–601.

[15] Y. Yang, X. Chen, G. Wang, and L. Cao, "An identity and access management architecture in cloud," in 2014 Seventh International Symposium on Computational Intelligence and Design, vol. 2. IEEE, 2014, pp. 200–203.

[16] C. Banerjee, A. Kundu, M. Basu, P. Deb, D. Nag, and R. Dattagupta, "A service based trust management classifier approach for cloud security," in 2013 15th International Conference on Advanced Computing Technologies (ICACT). IEEE, 2013, pp. 1–5.

[17] S. P. Praveen, T. B. M. Krishna, S. K. Chawla, and C. Anuradha, "Virtual private network flow detection in wireless sensor networks using machine learning techniques," International Journal of Sensors Wireless Communications and Control, vol. 11, no. 7, pp. 716–724, 2021.

[18] S. Liu, J. Wu, Z. Lu, and H. Xiong, "Vmras: A novel virtual machine risk assessment scheme in the cloud environment," in 2013 IEEE International Conference on Services Computing. IEEE, 2013, pp. 384–391.

[19] A. Madhuri, V. E. Jyothi, S. P. Praveen, S. Sindhura, V. S. Srinivas, and D. L. S. Kumar, "A new multi-level semi-supervised learning approach for network intrusion detection system based on the 'goa'," Journal of Interconnection Networks, p. 2143047, 2022.

[20] K. M. Sudar, P. Deepalakshmi, A. Singh, and P. N. Srinivasu, "Tfad: Tcp flooding attack detection in software-defined networking using proxybased and machine learning-based mechanisms," Cluster Computing, pp. 1–17, 2022.

[21] R. Lalitha and P. N. Srinivasu, "An efficient data encryption through image via prime order symmetric key and bit shuffle technique," in Computer Communication, Networking and Internet Security. Springer, 2017, pp. 261–270.

[22] Praveen, S. Phani, et al. "A Hybrid Gravitational Emulation Local Search-Based Algorithm for Task Scheduling in CloudComputing." Mathematical Problems in Engineering 2023 (2023).

[23] Praveen, S. Phani, et al. "A robust framework for handling health care information based on machine learning and bigdataengineering Techniques." International Journal of Healthcare Management (2022): 1-18.

[24] Praveen, S. Phani, et al. "An Adaptive Load Balancing Technique for Multi SDN Controllers." 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS). IEEE, 2022.