HYBRID CLOUD SECURITY - RISK & POSTURE ASSESSMENT

[1]RAHUL KUMAR, [2]RASHMI AGARWAL

[1, 2]REVA Academy for Corporate Excellence (RACE), REVA University, Rukmini Knowledge Park, Kattigenahalli Yelahanka, Bangalore 560064, India
E-mail: [1]rahul.cs02@reva.edu.in, [2]rashmi.agarwal@reva.edu.in

Abstract - Now a days, cloud computing has turned into a huge innovation pattern. The cloud computing innovation benefits incorporate expense investment funds, high accessibility of assets, and simple versatility. The cloud clients can remotely store their information and partake in the on-request great applications and administrations from cloud assets. The information security is one of the main issues as the clients of distributed storage benefits never again truly keep up with direct command over their information in cloud. In this manner, moving of all information over the cloud has suggestions for protection and security. One potential arrangement of this issue is to encode information before capacity over cloud however information encryption alone is deficient. Additionally, the cloud computing has best in class weaknesses because of the center advancements utilized in it. This paper makes sense of the possible dangers and weaknesses, challenges related with different administrations of cloud computing advances and prescribes techniques to relieve them. These security issues ought to be treated into account in a serious way to stay away from grievous for an association's standing and presence. The cloud specialist organization ought to give the Security as a Service and Data security as a Service to accomplish the trust of the client and feel them that their information will remain got and safeguarded in the cloud.

Keywords - Cloud Computing, Cloud Security, Risk Assessment in cloud, Security Threats

I. INTRODUCTION

Cloud computing is a virtual pool of assets like programming, stage and framework that is progressively versatile and reconfigured for an exceptionally minimal expense to address the issue of the client. All administrations of the distributed computing, for example, capacity, application advancement and access application are gotten to through Internet. It tends to be utilized on any sort of gadgets like PCs, PCs, cell phones, tablets. Cost saving, high accessibility of the assets, dynamic versatility is the couple of the benefits of distributed computing. Google, Amazon, Microsoft are the large players to offer different types of assistance to the cloud clients. Each cloud supplier sent a server farm that remembers different stages for the improvement of uses for cloud and equipment to help the application created and different frameworks like organization, information base. Cloud specialist organization utilizes the help level arrangements (SLA) with the customer to offer the types of assistance. Fundamentally, Cloud registering offers three sorts of types of assistance. These three administrations are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) model called SPI model. This model is called SPI model (Herman et al., 2020).

SaaS comes at top of the cloud stack. SaaS layer is essentially involved by the shopper for the utilization of the applications running on the cloud. The fundamental advantage of utilizing SaaS is that a client doesn't have to buy the expensive authorized programming. Everything the product on the cloud is authorized and completely upheld by their separate sellers. Buyer just pays for the product use. It replaces the utilization of programming from conventional to lease model, in this way decreasing the client's actual hardware sending and the board costs. Every one of the applications are gotten to through Internet utilizing internet browser and there is compelling reason need to locally introduce anything extra.

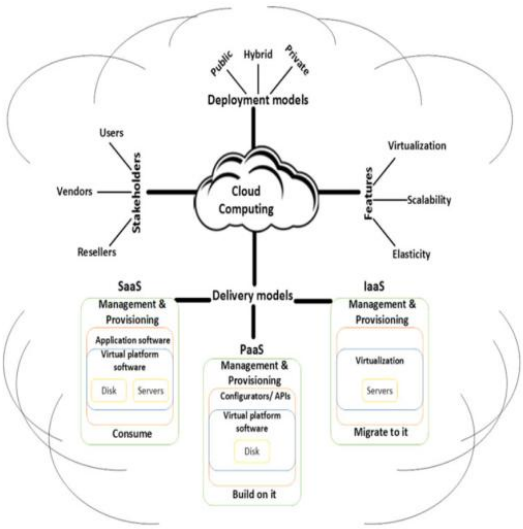

Figure 1: SPI Model

PaaS gives the climate to the application advancement. It is essentially utilized by application engineers, analyzers and managers to create and testing programming's. it upholds the whole programming advancement life cycle and gives the virtual machines, working frameworks, applications, administrations, improvement systems, exchanges, and control structures.

IaaS gives the framework like capacity, organization, CPUs on request, lease premise. It depends on the idea of virtualization. IaaS establishes a virtual climate and

let the clients to share an asset without them knowing to run their applications. Virtual climate incorporates virtual PCs, distributed storage, network framework parts, for example, firewalls and design administrations. Utilization charges are determined based on each CPU hour, information GB put away each hour, network data transfer capacity consumed, network foundation utilized each hour (Theebendra et al., 2014).

II. CLOUD SECURITY

The biggest problem on cloud computing is the security and privacy of the user data storage and management. All the user data is stored at the Cloud Service Provider (CSP). Although CSP take all measures to provide best security but still it is tough to have full faith on the CSP due to the state-of-the-art risks associated with the cloud. Virtualization which is the back bone of the cloud computing and is also a big threat to the security. Virtualization which allows having several machine images on a single server. If the two virtual machines are running on a server, it is quite possible that one can access both virtual machine and have unauthorized access to the data and application of the other user and also an attach launch to one virtual machine can also affect the other virtual machine on the same server. Security level agreement (SLA) is negotiated between CSP and the consumer that defines the risks associated with the cloud services. The major securities flaws exist on the cloud are due to DDoS, malware, IP vulnerabilities, insecure cryptography, Fraudulent Resource Consumption (FRC) and many more (Zhang et al., 2010).

III. METHODOLOGY

This paper revolves around scripts that are designed to return a series of potential risks and security misconfigurations. The initial steps included understanding of the key differences between security of on-premises services and that over the Cloud.

This research makes sense of the possible security risks, misconfigurations, and a weakness, challenges related with different administrations of cloud computing advances and prescribes techniques to relieve them. These security issues ought to be treated in a serious way to stay away from grievous for an association's standing and presence.

With the move to cloud infrastructure, compliance standards had to evolve. Cloud services and platforms are now required to comply with various federal, international, local and state security laws, regulations and standards. This tool generates reports to meet Compliance standards such as PCI DSS, HIPAA that have specific requirements for cloud environments. It also works similar to CIS Benchmarks that provide security configuration outlines based on best practices and are approved by business, government, academia, and industry bodies. The benchmarks for the reports are meant for application and system administrators, security experts, and auditors, as well as for platform deployment, help desk, and individual DevOps personnel, who wish to create, deploy, secure, or evaluate solutions within the cloud (Alturkistani et al., 2014).

IV. IMPLEMENTATION

Script is designed to allow detection of security risks in cloud infrastructure accounts, including: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure and (OCI). These scripts are designed to return a series of potential misconfigurations and security risks. Scripts works in two phases. First, it queries the cloud infrastructure APIs for various metadata about your account, namely the "collection" phase. Once all the necessary data is collected, the result is passed to the "scanning" phase. The scan uses the collected data to search for potential misconfigurations, risks, and other security issues, which are the resulting output. It saves the data queried from the cloud provider APIs in JSON format, which can be saved alongside other files for debugging or historical purposes (Jouini et al., 2016).

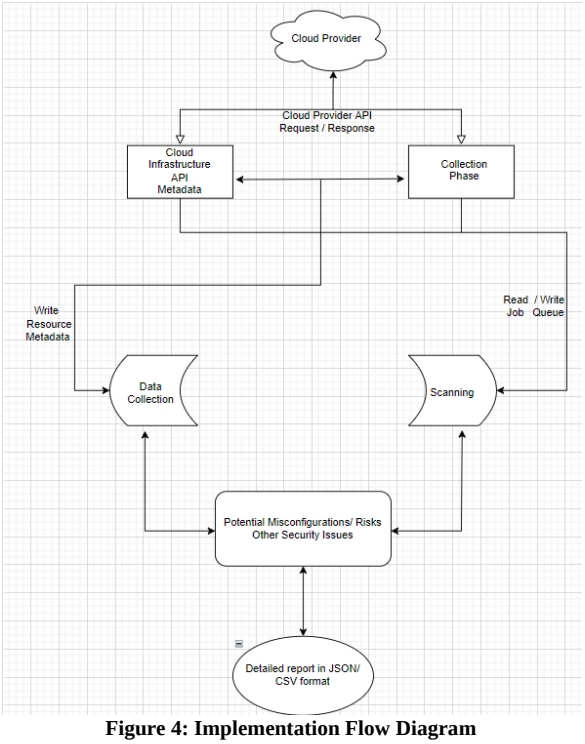

Figure 4: Implementation Flow Diagram

V. RISK ASSESSMENT

Risk evaluation implies surveying the current security and controls which incorporates the most common way of recognizing the security dangers to a framework and deciding their likelihood of event,

their effect, and the protections that would moderate that effect. The fundamental goal of hazard evaluation is to characterize proper controls for decreasing or disposing of those dangers. As the event of a gamble influences the framework as well as excessively affects the business cycle too contingent on the seriousness of the gamble.

A general cloud computing foundation comprises of the cloud, the client, the gadgets the clients use to interface with the cloud and the distinguishing proof strategy used to confirm the gadget and the client. At the point when we think about just the cloud, we see that there are essentially three spots where hazard can happen. One being compromised account, local malware on the application being utilized in the cloud or an information break (Joshi et al., 2019).

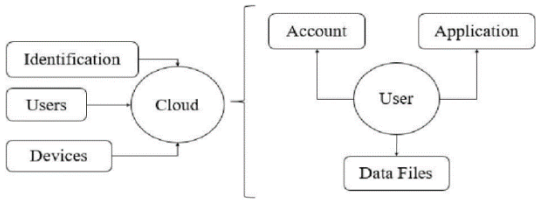

Figure 3: Basic Cloud Architecture

There a couple of chance evaluation techniques that accessible to us in the IT world, yet at this point they have not been organized explicitly for cloud computing conditions. The gamble appraisal strategies are as per the following: The Expression of Needs and Identification of Security Objectives (EBIOS) is a technique for assessing and treating chances, which plans to decide the security activities to execute and furthermore articulations wellbeing. Functionally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)is a technique for appraisal of weaknesses and dangers based on the working resources of the organization. MEHARI is a gamble evaluation strategy with regards to the security of data frameworks; this technique is intended to address the issues of each organization. These techniques are relevant in an ordinary IT climate however there are more elements to a cloud computing climate which builds the intricacy of hazard evaluation which these procedures neglect to really cover. Just considering either subjective or quantitative investigation won't give an exact outcome. In the evaluation of a perplexing data framework, subjective examination and quantitative investigation ought not be just isolated, in actuality, the two strategies ought to be coordinated (Herman et al., 2020).

Quantitative gamble and effect evaluation structure in view of NIST-FIPS-199 (QUIRC) centre around six vital classes of safety targets (SO) (for example Secrecy, uprightness, accessibility, multi-party trust, shared review capacity and convenience). The result of the likelihood of a danger happening faced characterized as quantitative challenge i.e., a happening danger occasion, and its possible effect or outcome. The danger occasion happened would can be categorized as one of the given SO classification would be the normal over the combined, weighted amount of n dangers which guide to that SO class.

This quantitative system positions the danger in view of well-qualified assessment on the probability and outcome of dangers, as a logical means to gather the data fundamental for evaluating security chances. Blow table is a fundamental model how a gamble could be estimated concerning effect, event and exposure. The tables contain five segments (table 1). The primary segment contains the name of occasion or chance the following three sections contains the effect, event and revelation of the that gamble. The result of these three classifications is the Risk Priority Number (RPN) which is kept in the fifth segment (Saripalli et al., 2010).

I-impact	Score
Barely Perceptible	1
Meaningless	2 – 3
Moderately Significant	4 – 6
Serious	7 – 8
Extremely Serious	9 – 10

Table 1: For measuring the risk impact

O-Occurrence	Score
Unlikely	1
Very Small	2 – 3
Small	4 – 6
Mild	7 – 8
High	9 – 10

Table 2: For measuring the occurrence of risk

D-Disclosure	Score
High	1
Mild	2 – 3
Small	4 – 6
Very Small	7 – 8
Unlikely	9 – 10

Table 3: For measuring the disclosure of risk

$$RPN = I \times O \times D$$

RPN takes a value in the range 1 – 1000. The severity of risk determines the size of RPN. The high value of the RPN has a great importance of risk.

While taking the fundamental parts of cloud, information is the centre resource that is getting put away in the cloud. The discussion of viable information administration as a way to moderate gamble in cloud computing frameworks particularly those issues connected with information at last contribution many advantages to cloud purchasers. They utilize the Otto Boris (2011) scientific hypothesis for deducting and understanding the significant cycles important to develop a powerful information administration plan structure.

VI. ISSUES IN CLOUD

Security is the main issue in distributed computing. We are dwelling all that in supplier's premises which makes the data profoundly unstable. It's a primary snag in reception of distributed computing. As per the IDC's study on the cloud administrations, security concerns are number one issue confronting cloud computing. Troubles or overheads before cloud computing are the risk of-Disrupts Services, Theft of Information, Loss of Privacy, Damage of data. These issues forestall the associations to embrace the cloud computing administrations. These can be taken out by applying profoundly confided in security conventions. IEEEtran.bst documents, while the Microsoft Word formats are independent. Causal Productions has utilized its earnest attempts to guarantee that the layouts have a similar appearance (Velev et al., 2011).

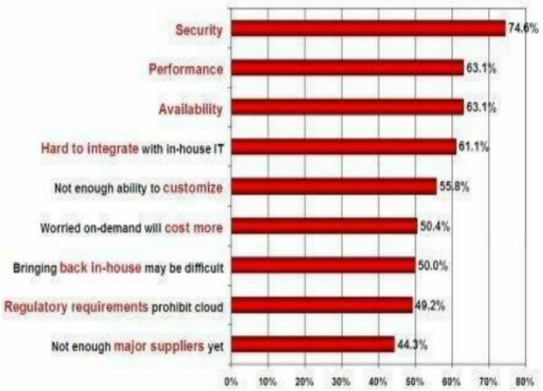

Figure 4: Major Issue's analysis of cloud computing

VII. SECURITY ARCHITECTURE OF CLOUD COMPUTING

The above discussion is on certain review literature by many research people on different aspects of security. The aspects went on describing the problems and threats in related to security in cloud. The literature in detail explains about the issues like security for data, virtualization security and prescribed format of SLA etc. There are many research people have keen interest in designing certain security architectures help for secure cloud computing. The following are described below: The author Gary Anthes has described the various security research works in cloud are discussed. He brought forward the research works done in popular companies like IBM, HP, and Microsoft (Gupta et al., 2019).

There are many security risks involved in cloud computing, and also some good solutions are also been designed by the researchers which are pointed below.

1. Researchers at HP laboratories are prototyping cells as a service to automate security management in cloud. A cell is single administrative domain using security policies containing virtual machines, storage volumes across physical machines
2. IBM research people doing virtual machine introspection which puts security inside protected VM running on same machine. This employs number of protective methods listing the kernel functions. It can make reduce of running virus scanners on system.
3. Microsoft research described about cryptographic cloud storage where the data is secured by user by encrypting format such that the provider cannot get what the data is present.

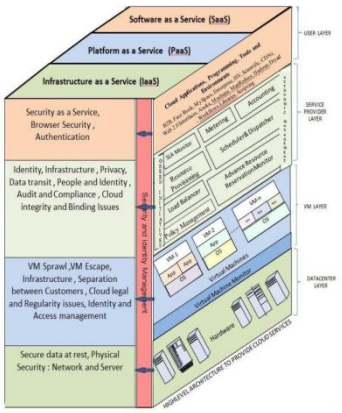

Figure 5: Security Architecture of Cloud Computing

VIII. PROPOSED SOLUTION AND SCOPE OF WORK

This paper is primarily centered around Cloud Security Posture challenges faced by organizations in security, compliance, misconfiguration, and vulnerabilities. The solution to all the above issues and for better management of their multi-cloud security posture, it is important to make it easy to operationalize cloud security and scale scarce cloud security resources, while enabling a deeper understanding of risks with intelligent insights, real-time detection, and more compliance benchmark capabilities (Driesen et al., 2012).

Organizational readiness, success metrics, and teams responsible for different aspects of cloud security posture management. Respondents with better interdepartmental alignment on security policy and/or enforcement policies are more likely to be confident in their ability to defend against a security breach. Automation of manual deployment and configuration of Information systems, orchestration of the security tools & achieve compliance in a Hybrid environment has played a pivotal role in the success of this tool.

A deeper understanding of risks with intelligent insights and real-time detection is of paramount importance in Multi-Cloud Security Posture. Misconfiguration of Information systems and non-Adherence to the compliance accompanied by auditing the configuration state of services in IaaS

accounts (AWS, Azure, etc.) for potential misconfigurations that lead to security breaches and monitoring activity in accounts in real-time helps mitigate insider threats (Goodin, 2012).

IX. CONCLUSION

However, cloud is another innovation there is an eternity expanding need for it. Work planning and asset allotment in cloud conditions are exceptionally powerful in nature and hard to foresee. Thus, customary IT risk evaluation strategies end up being inadequate in the cloud and the nature of administration gets impacted. Quantitative or subjective evaluation of chance in a cloud computing exclusively can't give precise outcomes however the reconciliation of both would be substantially more successful. Scarcely any models proposed in the above examined papers are hypothetical and may be inadequate in a constant climate. However, information administration can give a general perspective on the information being handled, it requires further examination on the off chance that the cloud is to hold enormous information. There is a requirement for an organized gamble evaluation technique devoted for cloud computing frameworks which can builds the trust between cloud clients and cloud specialist organizations.

REFERENCES

[1] D. Velev and P. Zlateva, “Cloud Infrastructure Security", Lecture Notes in Computer Science, pp. 140-148, 2011. Available: https://www.researchgate.net/publication/220865671_Cloud_Infrastructure_Security. [Accessed 2 November 2020].

[2] Driesen, V. And Eberlein, P., SAP SE, 2012. Brokered cloud computing architecture. U.S. Patent 8,250,135.

[3] Gautam, R. and Jain, M., 2020. Cloud Computing Security: Aws Data Security Credentials. Studies in Indian Place Names, 40(3), pp.6385-6389.

[4] Goodin, D., 2012. Why passwords have never been weaker-and crackers have never been stronger. Ars Technica.

[5] H. Gupta and D. Kumar, “Security Threats in Cloud Computing", 2019 International Conference on Intelligent Computing and Control Systems (ICCS), 2019. Available: https://ieeexplore.ieee.org/document/9065542. [Accessed 26 December 2020].

[6] H. Schulze, "AWS Cloud Security Report 2020 for | Cloud Security Alliance", Cloud Security Alliance, 2020. [Online]. Available: https://cloudsecurityalliance.org/blog/2020/10/14/aws-cloud-security-report-2020-for-management-managing-the-rapid-shift-to-cloud/. [Accessed 28 December 2020].

[7] Herman, M., Iorga, M., Salim, A.M., Jackson, R.H., Hurst, M.R., Leo, R., Lee, R., Landreville, N.M., Mishra, A.K., Wang, Y. and Sardinas, R., 2020. NIST Cloud Computing Forensic Science Challenges (No. NIST Internal or Interagency Report (NISTIR) 8006). National Institute of Standards and Technology.

[8] Theebendra, C. and Santhini, N., 2014. Cloud Computing Security-Data Storage and Transmission. International Journalof Research in Computer Applications and Robotics, 2(12), pp.27-35.

[9] Zhang, X., Wuwong, N., Li, H. and Zhang, X., 2010, June. Information security risk management framework for the cloud computing environments. In 2010 10th IEEE international conference on computer and information technology (pp. 1328-1334). IEEE.

[10] Alturkistani, F.M. and Emam, A.Z., 2014. A review of security risk assessment methods in cloud computing. New Perspectives in Information Systems and Technologies, Volume 1, pp.443-453.

[11] Jouini, M. and Rabai, L.B.A., 2016. Comparative study of information security risk assessment models for cloud computing systems. Procedia Computer Science, 83, pp.1084-1089.

[12] Joshi, S. and Kumari, U., 2019. Cloud computing: architecture & challenges. Mody University International Journal of Computing and Engineering Research, 1(1), p.6.

[13] P. Saripalli and B. Walters, "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security," 2010 IEEE 3rd International Conference on Cloud Computing, 2010, pp. 280-288, doi: 10.1109/CLOUD.2010.22.

★★★