iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44064

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 10 Issue VI June 2022- Available at www.ijraset.com

A Semantic Study on Emerging Risk and Security Management in Cloud Computing

Pratik Gaikwad[1], Dhanashri Patil[2]
[1, 2]*Department of Computer Science and Engineering, Sanjay Ghodawat University, Kolhapur,*

Abstract: Cloud computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. However, cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. One of the most significant problems that has hampered the expansion of cloud computing is security. It complicates data privacy, and data protection continues to have an impact on the market. Users must be aware of the dangers of data breaches in the cloud. This study focuses on cloud computing security concerns.
Keywords: Cloud Security, Cloud Threats, Cloud Computing, Cloud Risk and Management

I. INTRODUCTION

Cloud Computing has recently emerged as new paradigm for hosting and delivering services over the Internet. Cloud Computing is the use of computing resources such as hardware and software that are delivered as service over the internet. The security and privacy of cloud data is a major problem.

The integrity, privacy, and protection of data are critical requirements for cloud services. Several service providers use various policies and mechanisms for this goal, which vary depending on the nature, kind, and scale of data. When using the cloud to store data, one of the most important decisions to make is whether to engage a third-party cloud provider or build an internal organisational cloud.

As a result, data that is more sensitive to be maintained on a public cloud, such as defence and national security data or more confidential future product specifics, must be stored on a private cloud. For questions on paper guidelines, please contact us via e-mail. Cloud computing security is controlled by different mechanisms such as deterrent control, preventive control, detective control, and collective control. Cloud Vulnerability and Penetrating Testing are very much important for secure and healthy cloud security practices. Cloud Computing is an important name in the IT and Computing domain and this is rising in different organizations and institutions. In this paper different areas of Cloud Computing have been described. There are different models and architecture for cloud computing security and different rules, regulation, and framework.

The Organization of paper is as follows: Section I presents Introduction. In Section II Security Risks are described. Section III presents the The Security Management in Cloud. Section IV describes the Services of Cloud Security, and we conclude this paper in section V.

II. SECURITY RISK

Cloud Computing is used to store and access business information with the help of the internet. It allows users to easily access necessary files and use various cloud applications from anywhere using any electronic device. It is an internet-based service that provides servers, storage as well as a number of applications. The data stored in the cloud can sometimes be critical. This can pose as a huge security risk for the business.

As your data is held on a publicly accessible server, its security is not in your own hands. The company running the cloud service (and its servers) has complete control over your information. In a way, it is more secure than a personal computer. A single hardware fault cannot jeopardize your entire data. But at the same time, it also exposes the information to outside threats. A hack that compromises the cloud servers can leak your personal data.

More concurringly, you need to trust the cloud service provider itself to respect your privacy. And in this age of Big Data, that is hardly a given. Tech giants have routinely come under fire for violating the privacy of user data they have access to, making it a risk to store important information on the cloud. Then there are the security vulnerabilities even cloud services are exposed to. Like any web service, cloud computing can be subject to Distributed-Denial-of-Service (DDoS) attacks that cripple its capabilities. This forces the affected service to go offline, making your application unavailable for an unknown period of time.

A. List of Security Risks in Cloud

ID	Risks	Description
R01	Account or service hijacking	An account theft can be performed by different ways such as social engineering and weak credentials. If an attacker gains access to a user's credential, he can perform malicious activities such as access sensitive data, manipulate data, and redirect any transaction [].
R02	Data scavenging	Since data cannot be completely removed from unless the device is destroyed, attackers may be able to recover this data [ ].
R03	Data leakage	Data leakage happens when the data gets into the wrong hands while it is being transferred, stored, audited or processed [].
R04	Denial of Service	It is possible that a malicious user will take all the possible resources. Thus, the system cannot satisfy any request from other legitimate users due to resources being unavailable.
R05	Customer-data manipulation	Users attack web applications by manipulating data sent from their application component to the server's application []. For example, SQL injection, command injection, insecure direct object references, and cross-site scripting.
R06	VM escape	It is designed to exploit the hypervisor in order to take control of the underlying infrastructure [].
R07	VM hopping	It happens when a VM is able to gain access to another VM (i.e. by exploting some hypervisor vulnerability) []
R08	Malicious VM creation	An attacker who creates a valid account can create a VM image containing malicious code such as a Trojan horse and store it in the provider repository [].
R09	Insecure VM migration	Live migration of virtual machines exposes the contents of the VM state files to the network. An attacker can do the following actions:
		a) Access data illegally during migration []
		b) Transfer a VM to an untrusted host []
		c) Create and migrate several VM causing disruptions or DoS
R10	Sniffing/Spoofing virtual networks	A malicious VM can listen to the virtual network or even use ARP spoofing to redirect packets from/to other VMs [].

There are several security risks to consider when making the switch to cloud computing. Here are the security risks your organization should be aware of:

1) Privileged user access. Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs. Get as much information as you can about the people who manage your data.

2) Regulatory compliance. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are signaling that customers can only use them for the most trivial functions.

3) Data location. When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.

4) Data segregation. Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. Encryption accidents can make data totally unusable, and even normal encryption can complicate availability.

5) Recovery. Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure. Ask your provider if it has the ability to do a complete restoration, and how long it will take.

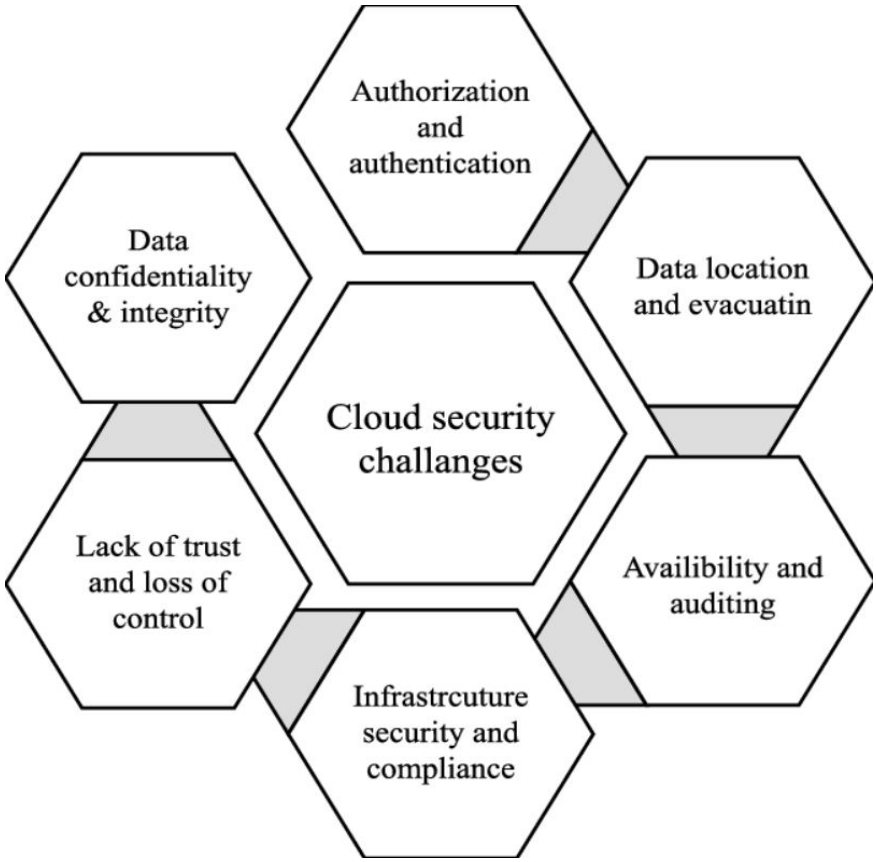
6) Investigative support. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centres. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then you're only safe assumption is that investigation and discovery requests will be impossible.

7) Long-term viability. Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application.

8) CSP Supply Chain is compromised. If the CSP outsources parts of its infrastructure, operations, or maintenance, these third parties may not satisfy/support the requirements that the CSP is contracted to provide with an organization. An organization needs to evaluate how the CSP enforces compliance and check to see if the CSP flows its own requirements down to third parties. If the requirements are not being levied on the supply chain, then the threat to the agency increases.

9) Insufficient Due Diligence Increases Cybersecurity Risk. Organizations migrating to the cloud often perform insufficient due diligence.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com



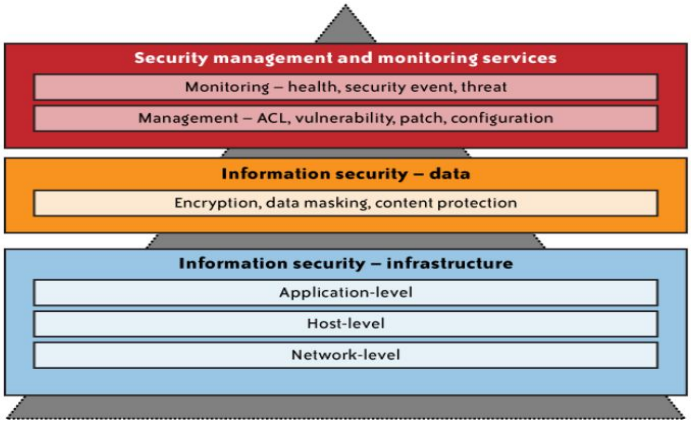
III.SECURITY MANAGEMENT IN CLOUD

A LARGE PART OF The NETWORK, SYSTEM, APPLICATIONS, AND DATA WILL BE CONTROLLED BY A THIRD-PARTY PROVIDER IF YOU USE PUBLIC CLOUD SERVICES. The cloud services delivery model will establish virtual perimeter islands (clouds), as well as a security paradigm in which the client and the cloud service provider share responsibilities (CSP). The IT operations team will face new security management problems as a result of this shared responsibility approach. With this in mind, the first question a chief information security officer (CISO) must answer is whether she has enough transparency from cloud services to manage governance (shared responsibilities) and security management processes (preventive and detective controls) to ensure the business that data in the cloud is properly protected. The answer to this issue is divided into two parts: what security controls the client must offer in addition to those built into the cloud platform, and how must an enterprise's security management tools and procedures adapt to manage security in the cloud. Both responses must be re-evaluated on a regular basis based on the sensitivity of the data and changes in service levels over time.

Cloud based services have become an integral part of several organizations, with technology providers adhering to privacy and data security norms for ensuring the confidentiality of user data. Although efforts are being taken to develop cloud security standards, CSPs are implementing a blend of privacy and security controls. This has created confusion among users in terms of the security measures that they expect from their providers.

The adoption of the cloud is estimated to see a continued upward spiral in the foreseeable future. However, organizations are still wary of cloud computing as an accurate delivery environment for their applications. The most dominant concern among them is security. The question that crawls upon the minds of businesses is if their sensitive data is secure in the cloud and the ways they can employ on-demand services while maintaining industry and regulatory compliance.

As a cloud customer, you should begin with the exercise of determining the trust boundary of your cloud services. You should be familiar with all of the layers of the cloud service that you own, touch, or interact with, including the network, host, application, database, storage, and web services, as well as identity services (see Figure). You should also be aware of the extent of your IT system administration and monitoring duties, which include access, change, configuration, patch, and vulnerability management.



A. Security Management Policies

1) Identifying and assessing cloud services - First, you need to spend time identifying which cloud products and services are being used in your organization, and which ones might be considered in the future. Then, you'll need to assess and audit those items, analysing their security and potential vulnerabilities.

2) Auditing and adjusting native security settings - Within each application, you'll have full control of your own privacy and security settings. It's on your cloud security team to understand which settings are available, and take full advantage of them to grant your organization the highest possible level of security.

3) Encrypting data - In many cases, you'll need to take extra efforts to prevent data loss and preserve data integrity by encrypting your data and securing your connections. It's your responsibility to allow legitimate network traffic and block suspicious traffic.

4) Managing devices - Cloud applications allow you to reduce the amount of physical infrastructure you maintain, but you and your employees will still be accessing data and services with specific devices. You'll need some way to manage and monitor those devices to ensure only authorized devices can access your data.

5) Managing user - Similarly, you'll need to consider user-level controls. Establish varying levels of user permissions, to restrict access to your most valuable or sensitive information, and change user permissions as necessary to allow secure access.

6) Reporting - It's also important to monitor cloud activity from a high level, and report on that activity so you can better understand your risks and ongoing operations

B. Security Management Standards

Based on the authors' assessment, the standards that are relevant to security management practices in the cloud are ITIL and ISO/IEC 27001 and 27002.

1) ITIL

The Information Technology Infrastructure Library (ITIL) is a set of best practices and guidelines that define an integrated, process-based approach for managing information technology services. ITIL can be applied across almost every type of IT environment including cloud operating environment. ITIL seeks to ensure that effective information security measures are taken at strategic, tactical, and operational levels. Information security is considered an iterative process that must be controlled, planned, implemented, evaluated, and maintained. *Title and Author Details.*

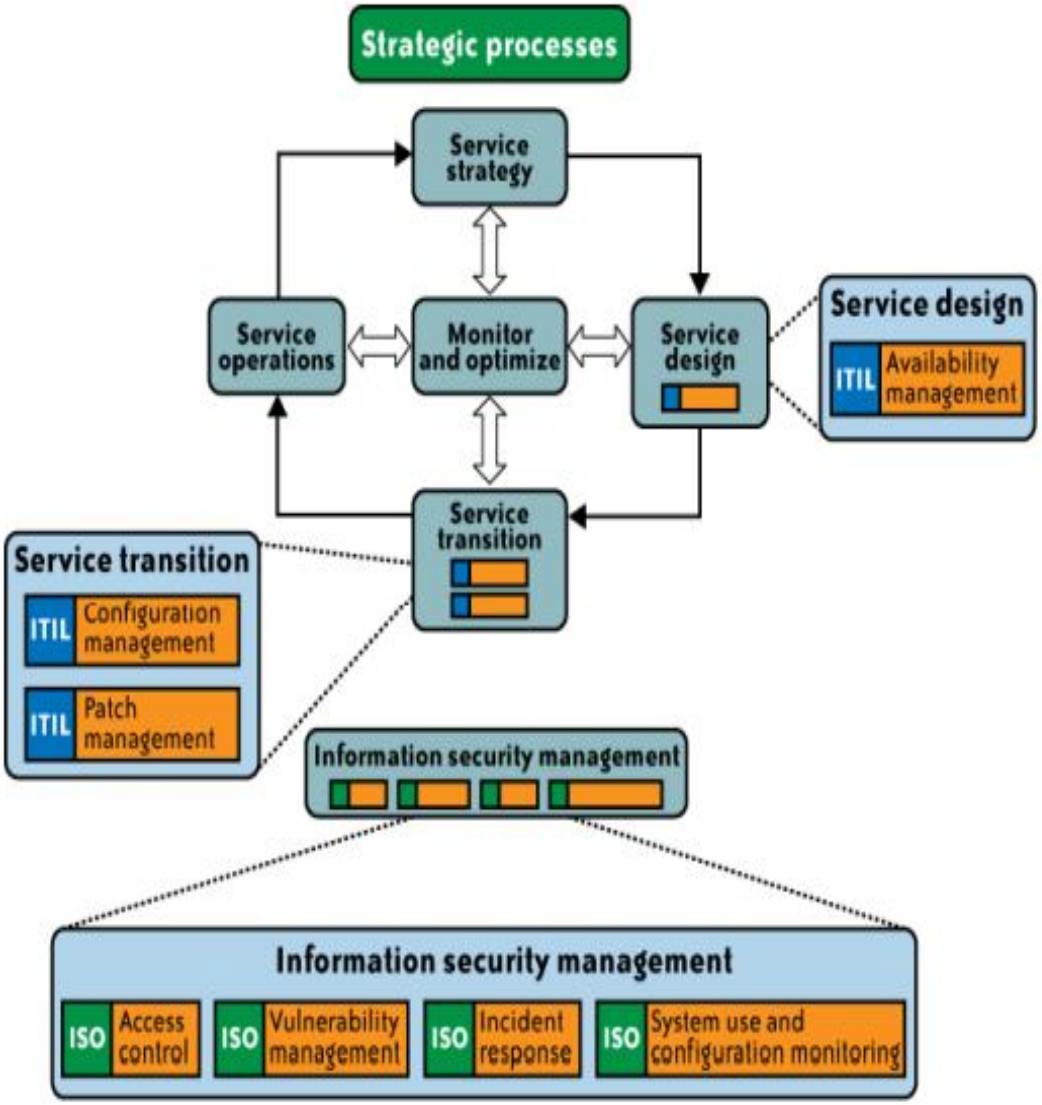
2) ISO 27001/27002

ISO/IEC 27001 formally defines the mandatory requirements for an Information Security Management System (ISMS). It is also a certification standard and uses ISO/IEC 27002 to indicate suitable information security controls within the ISMS. However, since ISO/IEC 27002 is merely a code of practice/guideline rather than a certification standard, organizations are free to select and implement controls as they see fit. Given the current trend of organizations moving toward ISO/IEC 27001 for information security management, there is a general consensus among information security practitioners to revise the ITIL security management best practices with the goal of strengthening the application and logical security in the Information and Communication Technology (ICT) infrastructure domain.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

C. Security Management Lifecycle

Although you may be transferring some of the operational responsibilities to the provider, the level of responsibilities will vary and will depend on a variety of factors, including the service delivery model (SPI), provider service-level agreement (SLA), and provider-specific capabilities to support the extension of your internal security management processes and tools. Mature IT organizations are known to employ security management frameworks, such as ISO/ IEC 27000 and the Information Technology Infrastructure Library (ITIL) service management framework. These industry standard management frameworks provide guidance for planning and implementing a governance program with sustaining management processes that protect information assets. For example, ITIL gives a detailed description of a number of important IT practices with comprehensive checklists, tasks, and procedures that can be tailored to any IT organization. A key tenet of ITIL, and one that is applicable to cloud computing, is that organizations (people, processes) and information systems are constantly changing. Hence, management frameworks such as ITIL will help with the continuous service improvement that is necessary to align and realign IT services to changing business needs. Continuous service improvement means identifying and implementing improvements to the IT services that support business processes such as sales force automation using a cloud service provider. Given the dynamic characteristics of cloud computing services, the activities present within the security management processes must be continually revised to remain current and effective.



The ITIL life cycle in a enterprise

D. Security Deploy Management

The three most common types of cloud deployment models are Private Cloud, Public Cloud, and Hybrid Cloud.

Deployment Type	Description	Implications	Challenges
Private Cloud	In a private cloud, the cloud service provider pools together scalable resources and virtual applications and makes them available to the cloud consumers. In this deployment model, the resources are dedicated to a single or a set of organizations and treated as an intranet functionality. The billing usually is on a subscription basis with a cloud consumer making minimum commitments	Positive security implications are relatively high and the organization has significant influence on the architecture, processes, and tools used in the deployment.	Security challenges include high cost of implementation and management, skills requirement, and vulnerability management. In this deployment model, cost and return on investment are key factors and the security implementation is usually based on risk assessment and hence, the security cover is not comprehensive
Public Cloud	In a public cloud, resources are dynamically committed on a fine-grained, self-service basis over the Internet or a portal10. Billing is usually consumption based and is charged on a pay per use basis.	Positive security implications are that due to a large number of cloud consumers and volumes of transactions involved. The cloud service provider normally has a comprehensive & layered security system, which can potentially provide a high degree of security due to its implement once and use multiple times model, which significantly reduces the cost of security implementation for the consumer.	Security challenges are heightened, as the resources are not committed but leveraged across multiple cloud consumers. This not only adds additional burden of ensuring all applications and data accessed on the public cloud, but also has to manage the multitude of external influences such as legislative, data protection etc.
Hybrid Cloud	Hybrid cloud is a deployment model where a private cloud is linked to one or more external cloud services while being managed centrally. It provides the cloud consumers a flexible and fit-for-purpose solution with a relative ease of operations. The hybrid clouds have a higher degree of complexity in terms of billing and commercials.	Positive security implications are that security can be purpose-built for vulnerabilities, threats, and risks that are assessed. This makes it costeffective and targeted.	Security challenges are relatively high as the deployment model is complex with heterogeneous environment, multiple orchestration, and automation tools. This will require additional administrative overhead, with any oversight resulting in significant risk exposure

E. Cloud Delivery Management

The three cloud delivery models proposed by NIST and adapted by the industry are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)

Delivery Type	Description	Risk and responsibility
Infrastructure as a Service (IaaS)	Infrastructure as a Service is a multi-tenant cloud layer where the cloud service provider dedicated resources are only shared with contracted clients at a pay-per-use fee. This typically means that Operating System is presented to the cloud consumer. The cloud service provider's responsibility ends with the operating system	This is a great model where the cloud consumer builds the application without worrying about the infrastructure requirements. The security responsibility is equally divided between the cloud service provider and the cloud consumer. In this model, the risk is segregated and layered. It is also a shared risk model.
Platform as a Service (PaaS)	Platform as a Service is one of the more popular delivery services where the cloud provider provisions not just the operating system but also a development stack. It is a common practice for providers in this model to provide database and application administration along with development services. Just as in IaaS, PaaS is a pay-per-use model.	This is an appropriate model, where the cloud consumer brings the application expertise along with licenses, data, and resources, and consumes the platform shell. This model is used by consumers who either lack infrastructure skills or want to save on high capital expenditure (capex) spend required to build the infrastructure. In this delivery model, the security responsibility starts to tilt more towards the cloud provider. Similar to IaaS, this is a shared risk model, however, the service provider bears higher risk than consumer as the provider supports more layers.
Software as a Service (SaaS)	In a Software as a Service model, the complete application stack is hosted by the cloud provider, who provides end-to-end resources, including licensing, application, networking etc., The cloud consumer, typically brings the data and business processes to consumes the services in a web service or software-oriented architecture.	This model is very effective in cases where the cloud consumer does not have the necessary skills, time, or resources to setup an application ecosystem and manage it. This model also provides the best commercial benefit with no upfront capex requirement. The security responsibility is mostly with the cloud provider. The consumer is mainly responsible for securing the client-side vulnerabilities. In this model, the service provider bears most risk.

IV. SECURITY VULNERABILITY, PATCH, AND CONFIGURATION MANAGEMENT

The ability for malware (or a cracker) to remotely exploit vulnerabilities of infrastructure components, network services, and applications remains a major threat to cloud services. It is an even greater risk for a public PaaS and IaaS delivery model where vulnerability, patch, and configuration management responsibilities remain with the customer. Customers should remember that in cloud computing environments, the lowest or highest common denominator of security is shared by all tenants in a multitenant virtual environment. Hence, the onus is with the customers to understand the scope of their security management responsibilities. Customers should demand that CSPs become more transparent about their cloud security operations to help customers understand and plan complementary security management functions.

By and large, CSPs are responsible for the vulnerability, patch, and configuration (VPC) management of the infrastructure (networks, hosts, applications, and storage) that is CSP managed and operated, as well as third-party services that they may rely on. However, customers are not spared from their VPC duties and should understand the VPC aspects for which they are responsible. A VPC management scope should address end-to-end security and should include customer-managed systems and applications that interface with cloud services. As a standard practice, CSPs may have instituted these programs within their security management domain, but typically the process is internal to the CSP and is not apparent to customers. CSPs should assure their customers of their technical vulnerability management program using ISO/IEC 27002 type control and assurance frameworks.

A. *Security Vulnerability Management*

Vulnerability management is an essential threat management element to help protect hosts, network devices, and applications from attacks against known vulnerabilities. Mature organizations have instituted a vulnerability management process that involves routine scanning of systems connected to their network, assessing the risks of vulnerabilities to the organization, and a remediation process (usually feeding into a patch management program) to address the risks. Organizations using ISO/IEC 27002 are known to address this program using a technical vulnerability management control objective, which states:

Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.

Technical vulnerability management should be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems, and any other applications in use.

Both the customer and the CSP are responsible for vulnerability management of the cloud infrastructure, depending on the SPI service in context.

B. *Security Patch Management*

Similar to vulnerability management, security patch management is a vital threat management element in protecting hosts, network devices, and applications from unauthorized users exploiting a known vulnerability. Patch management processes follow a change management framework and feeds directly from the actions directed by your vulnerability management program. Security patch management mitigates risk to your organization by way of insider and outsider threats. Hence, SaaS providers should be routinely assessing new vulnerabilities and patching the firmware and software on all systems that are involved in delivering the *aaS service to customers.

The scope of patch management responsibility for customers will have a low-to-high relevance in the order of SaaS, PaaS, and IaaS services—that is, customers are relieved from patch management duties in a SaaS environment, whereas they are responsible for managing patches for the whole stack of software (operating system, applications, and database) installed and operated on the IaaS platform. Customers are also responsible for patching their applications deployed on the PaaS platform.

C. *Security Configuration Management*

Security configuration management is another significant threat management practice to protect hosts and network devices from unauthorized users exploiting any configuration weakness. Security configuration management is closely related to the vulnerability management program and is a subset of overall IT configuration management. Protecting the configuration of the network, host, and application entails monitoring and access control to critical system and database configuration files, including OS configuration, firewall policies, network zone configuration, locally and remotely attached storage, and an access control management database.

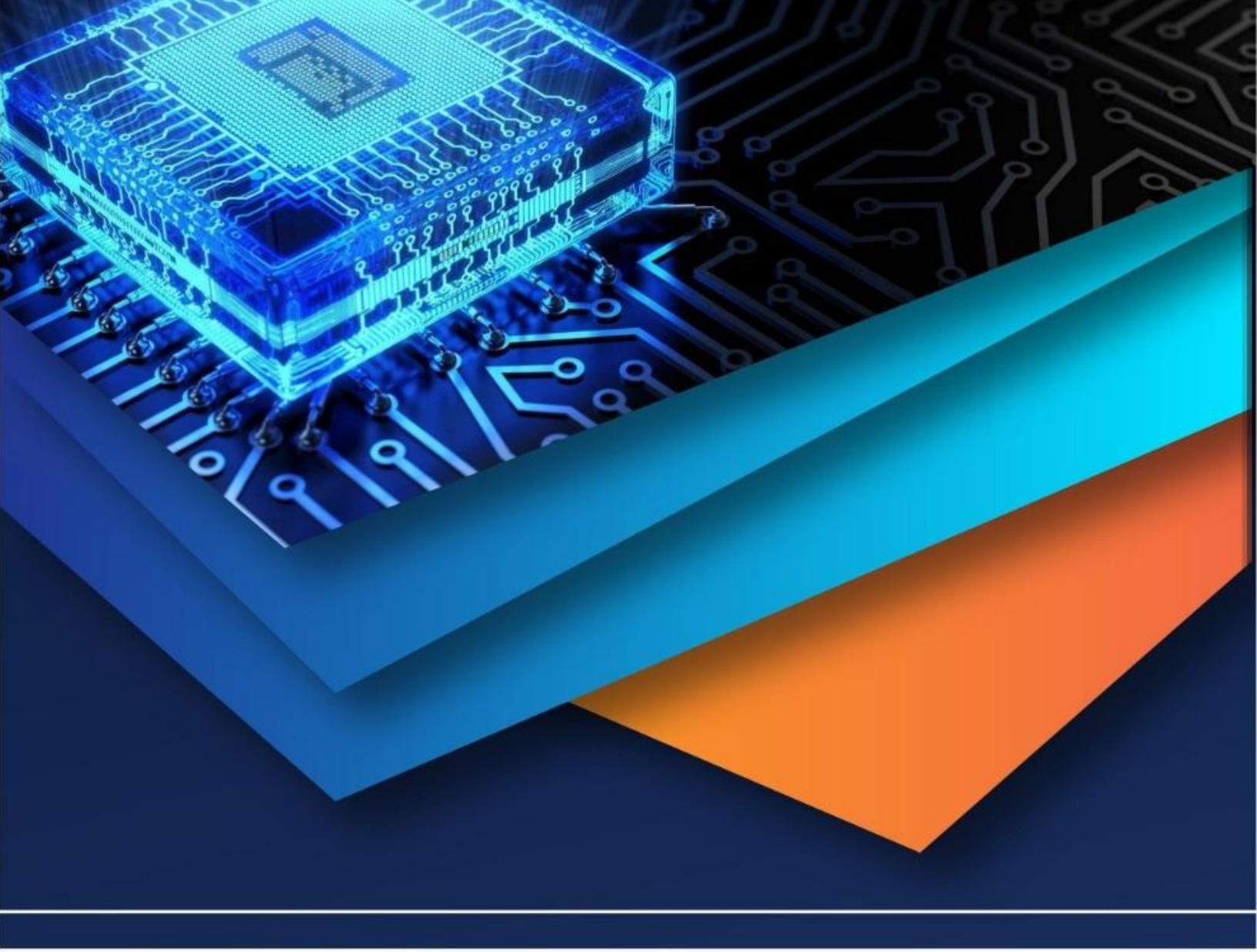
In the SPI service delivery model, configuration management from a customer responsibility perspective has a low-to-high relevance in the order of SaaS, PaaS, and IaaS services—that is, SaaS and PaaS service providers are responsible for configuration management of their platform, whereas IaaS customers are responsible for configuration management of the operating system, application, and database hosted on the IaaS platform.

V. CONCLUSIONS

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or inexistent. We have presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. As described in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Some surveys have discussed security issues about clouds without making any difference between vulnerabilities and threats. We have focused on this distinction, where we consider important to understand these issues. Enumerating these security issues was not enough; that is why we made a relationship between threats, Risks and vulnerabilities, so we can identify what vulnerabilities contribute to the execution of these Risks and make the system more robust. Also, some current solutions were listed in order to mitigate these threats. However, new security techniques are needed as well as redesigned traditional solutions that can work with cloud architectures. Traditional security mechanisms may not work well in cloud environments because it is a complex architecture that is composed of a combination of different technologies.

REFERENCES

[1] A Comprehensive Survey on Security in Cloud Computing, GururajRamachandra, https://www.sciencedirect.com/.
[2] Moulika Bollinadi, Cloud Computing: Security Issues and Research Challenges, Journal of Network Communications and Emerging Technologies (JNCET)
[3] Tim Mather, Subra Kumaraswamy, and Shahed Latif; Cloud Security and Privacy, Orilly
[4] Khurana Sand Verma A G, "Comparisons of cloud computing service model: S-a-a-S, P-a-a-S, I-a-a-S," published in International Journal of Electronics and Communication Technology (IJECT), vol.4, 2013, 2932.
[5] National Institute of Standards and Technology, (2011). NIST Cloud Computing Reference Architecture. https://www.nist.gov/publications/nist-cloud-computing-reference-architecture
[6] Abhijeet Chinchole, What is the Need for Cloud Security Standards, https://cloudlytics.com/the-need-for-cloud-security-standards/
[7] Prantosh Paul, Cloud Security: An Overview and Current Trend, International Journal of Applied Engineering and Management Letters (IJAEML), 3(2), 53-58. ISSN: 2581-7000, 2019.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY