Cloud Computing Security Challenges

[1]Sonu Airen, [2]Puja Gupta

Assistant professor
Department of Information Technology
Shri G.S. institute of technology & science
Indore, India.

Abstract:
Cloud computing might change Internet consumption in the ever-changing technological environment. This study carefully explores Cloud computing security issues, from data privacy to service delivery model dynamics. The problem is creating SLAs that are precise enough to cover critical features and simple to comprehend. This is much more complicated when working with IaaS, PaaS, and SaaS cloud services. The diversity of cloud providers makes it important to carefully consider SLA detail, according to the report. In a broad market with several cloud services, interoperability is crucial. According to the "Hazy Cloud" phenomenon, vendor locking occurs because each cloud provider has a distinct methodology that hinders smooth interaction.
The study proposes balancing Cloud computing's transformational potential with watchful security measures to shape IT solutions. It highlights the security dangers of Cloud computing and stresses the need for a deliberate and educated approach to reap its advantages.

Keywords: Cloud Computing, Security issues, Services, Deployment model.

INTRODUCTION:

The concept of cloud computing emerged around 2008, marking a significant shift in the way computing resources are accessed over the Internet. Represented by a cloud symbol on network diagrams, cloud computing encompasses various activities, including social networking and interpersonal computing. However, its primary focus lies in accessing online software applications, data storage, and processing power. Unlike traditional methods, cloud computing enables the dynamic expansion of capacity and capabilities without the need for substantial investments in new infrastructure, personnel training, or software licensing. It essentially extends the capabilities of Information Technology (IT).

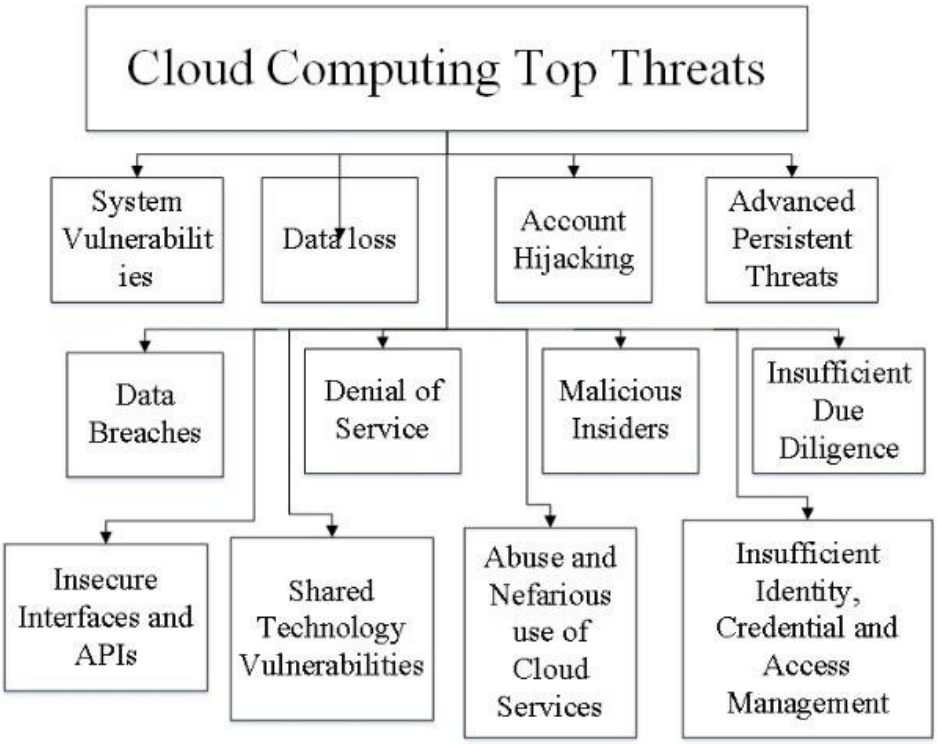


FIGURE 1: Top Cloud Computing Threats [9]

In recent years, cloud computing has transformed from a hopeful business idea into one of the fastest-growing sectors in the IT industry. However, with this growth, worries have emerged, especially regarding the safety of the cloud environment. This concern is amplified as more confidential information about individuals and companies finds its place in the cloud. Even though cloud computing brings scalability and flexibility, security problems have emerged as a notable obstacle, hindering its widespread acceptance. Despite the enthusiasm surrounding cloud services, many businesses remain hesitant to fully embrace them. Security concerns stand out as the primary challenge, with figure 2 illustrating that security is the top-ranked issue affecting the acceptance and implementation of cloud computing. In this report, we will delve into the specific security challenges faced by cloud computing and explore potential solutions to mitigate these concerns. Examining the security implications of cloud computing reveals a nuanced perspective. On one hand, the centralization of data and the increased allocation of security-focused resources could potentially enhance overall security measures. However, lingering concerns persist, particularly regarding the potential loss of control over sensitive data and the security of kernels stored with cloud providers.

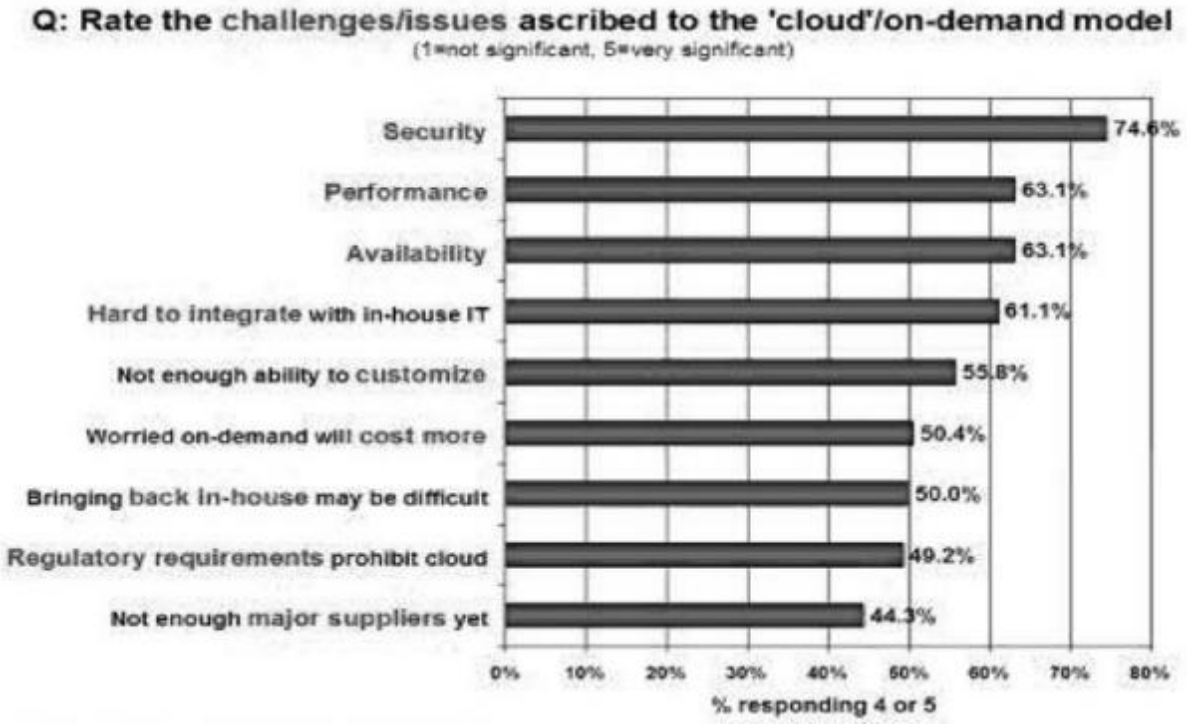


FIGURE 2: Results of IDC survey ranking security challenges, 2008 [1]

RELATED WORKS

In the ever-evolving landscape of cloud computing, an extensive array of research initiatives has played a pivotal role in unraveling the intricate fabric of its security landscape. The pivotal year of 2008 marked a watershed moment with Gartner's identification of seven critical security concerns, laying the foundation for enterprises venturing into the transformative journey of cloud computing [1]. These concerns, encompassing privileged user access, regulatory compliance, data location, data segregation, recovery mechanisms, investigative support, and long-term viability, underscored the multifaceted challenges inherent in this paradigm shift.

Going beyond Gartner's seminal insights, a diverse tapestry of research endeavors has delved deep into the multifaceted dimensions of cloud computing security. Notably, the Cloud Computing Use Case Discussion Group has distinguished itself by exploring a myriad of scenarios and corresponding requirements, providing invaluable perspectives from the vantage points of customers, developers, and security engineers. Concurrently, the European Union Agency for Cybersecurity (ENISA) conducted meticulous investigations, thoroughly examining the security risks associated with the adoption of cloud computing. This comprehensive analysis considered affected assets, risk likelihood, impacts, and vulnerabilities, contributing significantly to our understanding of the intricacies involved [4].

As the tapestry of cloud computing security unfolds, these research initiatives collectively contribute to a nuanced comprehension of the challenges and opportunities presented by this transformative technology. The insights derived from these endeavors not only guide enterprises in navigating the complexities of cloud adoption but also inform policymakers and technologists in shaping a secure and resilient future for cloud computing.

In the intricate realm of security intricacies encapsulated in Service Level Agreements (SLAs), the seminal work of Balachandra et al (2009) stands out as a beacon, making noteworthy contributions by delving into the nuanced aspects related to data locations, segregation, and data recovery [5]. Their insightful exploration paved the way for a deeper understanding of how these elements interplay within the framework of SLAs, shedding light on crucial considerations in cloud computing security.

Taking the baton in 2010, Kresimir et al embarked on a profound dive into the high-level security concerns embedded within the cloud computing model [6]. Their comprehensive exploration addressed critical facets such as data integrity, payment processes, and the privacy of sensitive information. By navigating these complex terrains, Kresimir et al provided valuable insights that not only heightened awareness but also laid the foundation for refining security practices in the evolving landscape of cloud technology.

Building on this foundation, Bernd et al (2010) further enriched the discourse by identifying and categorizing security vulnerabilities in the cloud platform [7]. Their classification into technology-related, cloud characteristics-related, and security controls-related vulnerabilities offered a structured lens through which the intricate security challenges of cloud computing could be systematically understood and addressed.

Shifting the spotlight to the cloud service delivery model, Subashini et al (2010) undertook a thorough exploration of inherent security challenges, with a specific emphasis on the Software as a Service (SaaS) model [8]. Navigating through the intricacies of SaaS security, their work contributed significantly to the broader understanding of how service delivery models influence and shape security considerations in cloud computing.

In the continuum of insightful contributions, Ragovind et al (2010) added depth to the discourse by engaging in discussions about the management of security in cloud computing [9]. Drawing insights from Gartner's list and findings from the International Data Corporation, their work provided a practical perspective on the challenges and solutions surrounding security management in the cloud.

Morsy et al (2010) took the baton and embraced a comprehensive, multi-dimensional approach to cloud computing problems [10]. Their consideration of architectural nuances, characteristics, stakeholders' interests, and service delivery model perspectives offered a holistic view of the challenges and opportunities inherent in the cloud computing landscape.

As these scholars collectively expanded the horizons of knowledge in cloud computing security, their works not only addressed immediate concerns but also laid the groundwork for ongoing exploration and refinement of security practices. The collaborative efforts of these researchers have significantly shaped our understanding of security intricacies in the cloud, contributing to the ongoing evolution of robust and resilient cloud computing ecosystems.

In a recent collaborative survey orchestrated by the esteemed Cloud Security Alliance (CSA) and IEEE, a spotlight was cast on enterprises' eager inclination to embrace the vast potential of cloud computing. This pivotal research, however, concurrently emphasized a critical imperative—the pressing need for fortified security measures. The survey brought to light not only the enthusiasm within the business sector for integrating cloud solutions but also the paramount importance of bolstering security protocols. This dual revelation serves as a poignant reminder that the journey towards widespread adoption of cloud computing must be guided by a judicious balance between innovation and security, especially in response to the ever-evolving landscape of regulatory requirements [11].

SECURITY ISSUES IN CLOUD COMPUTING

1 Cloud Deployment Models

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on demand, as depicted in Figure 2. The Cloud Computing model comprises three main deployment models:

1.1 Private Cloud

The term "private cloud" refers to offerings that emulate cloud computing on private networks. It is established within an organization's internal enterprise datacenter. In a private cloud, scalable resources and

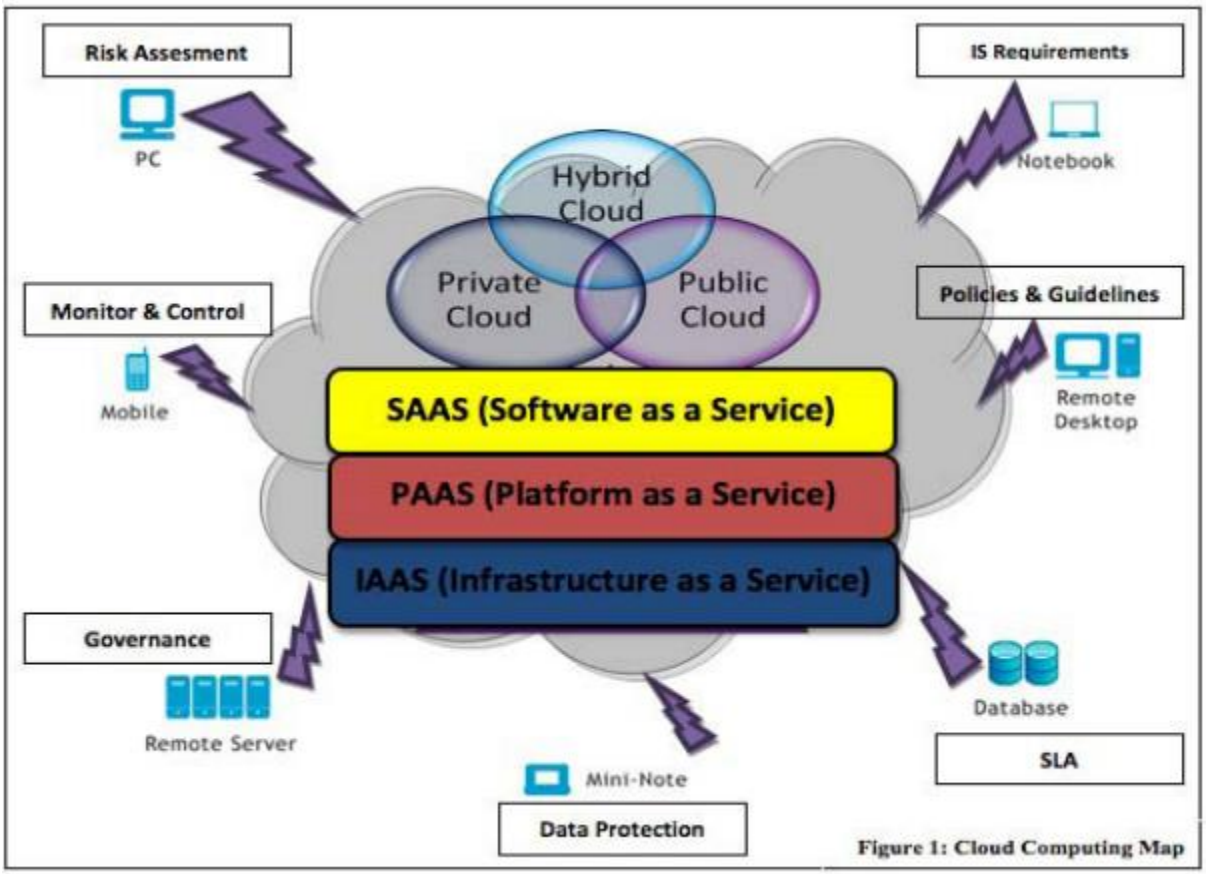
virtual applications provided by the cloud vendor are pooled together and made available for cloud users to share and use. Unlike the public cloud, all cloud resources and applications in the private cloud are managed by the organization itself, akin to Intranet functionality. Private clouds offer a potentially more secure environment compared to the public cloud due to their specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific private cloud [12].

1.2 Public Cloud

The public cloud embodies cloud computing in the traditional sense, where resources are dynamically provisioned on a fine-grained, self-service basis over the Internet. This is typically done via web applications or web services from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. Public clouds operate on a pay-per-use model, similar to a prepaid electricity metering system, offering flexibility to accommodate spikes in demand for cloud optimization [13]. However, public clouds are perceived as less secure than other cloud models due to the added responsibility of ensuring that all applications and data accessed on the public cloud are protected from malicious attacks.

1.3 Hybrid Cloud

The hybrid cloud integrates a private cloud with one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network [14]. It combines virtual IT solutions through a mix of both public and private clouds. Hybrid clouds afford more secure control over data and applications, enabling various parties to access information over the Internet. Additionally, they feature an open architecture that facilitates interfaces with other management systems. The hybrid cloud configuration can describe combinations involving a local device, such as a Plug computer with cloud services, or configurations combining virtual and physical, collocated assets. For instance, a mostly virtualized



environment that requires physical servers, routers, or other hardware, such as a network appliance acting as a firewall or spam filter.

FIGURE 3: Cloud deployment model [13]

2 Cloud Computing Service Delivery Models

Building upon the cloud deployment models, the next critical security consideration pertains to the various cloud computing service delivery models. The three main cloud service delivery models are Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

2.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service involves a single-tenant cloud layer where the cloud computing vendor's dedicated resources are exclusively shared with contracted clients at a pay-per-use fee. This minimizes the need for substantial initial investments in computing hardware, such as servers, networking devices, and processing power. IaaS offers varying degrees of financial and functional flexibility not commonly found in internal data centers or with colocation services. Computing resources can be added or released more quickly and cost-effectively than in an internal data center or with a collocation service [2]. IaaS has empowered startups and businesses to focus on their core competencies without the burden of provisioning and managing infrastructure. While IaaS provides a compelling cost advantage, it inherently offers only basic security features (e.g., perimeter firewall, load balancing). Applications migrating to the cloud demand higher levels of security at the host level.

2.2 Platform as a Service (PaaS)

Platform-as-a-Service (PaaS) constitutes a set of software and development tools hosted on the provider's servers. Positioned one layer above IaaS on the stack, PaaS abstracts everything up to the operating system, middleware, etc. It offers an integrated set of developer environments, allowing developers to build applications without concerning themselves with the underlying infrastructure. PaaS provides a comprehensive software development life cycle management, covering planning, design, application building, deployment, testing, and maintenance.

2.3 Software as a Service (SaaS)

Software-as-a-Service is a software distribution model where applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS has gained prominence as the underlying technologies supporting web services and service-oriented architecture (SOA) mature, and new developmental approaches become popular. Often associated with a pay-as-you-go subscription licensing model, SaaS leverages increasingly available broadband services to support user access from diverse areas globally.

SaaS implementation is often accompanied by considerations of information security. Security officers need to explore various methods to secure SaaS applications, including Web Services (WS) security, Extensible Markup Language (XML) encryption, Secure Socket Layer (SSL), and other available options for enforcing

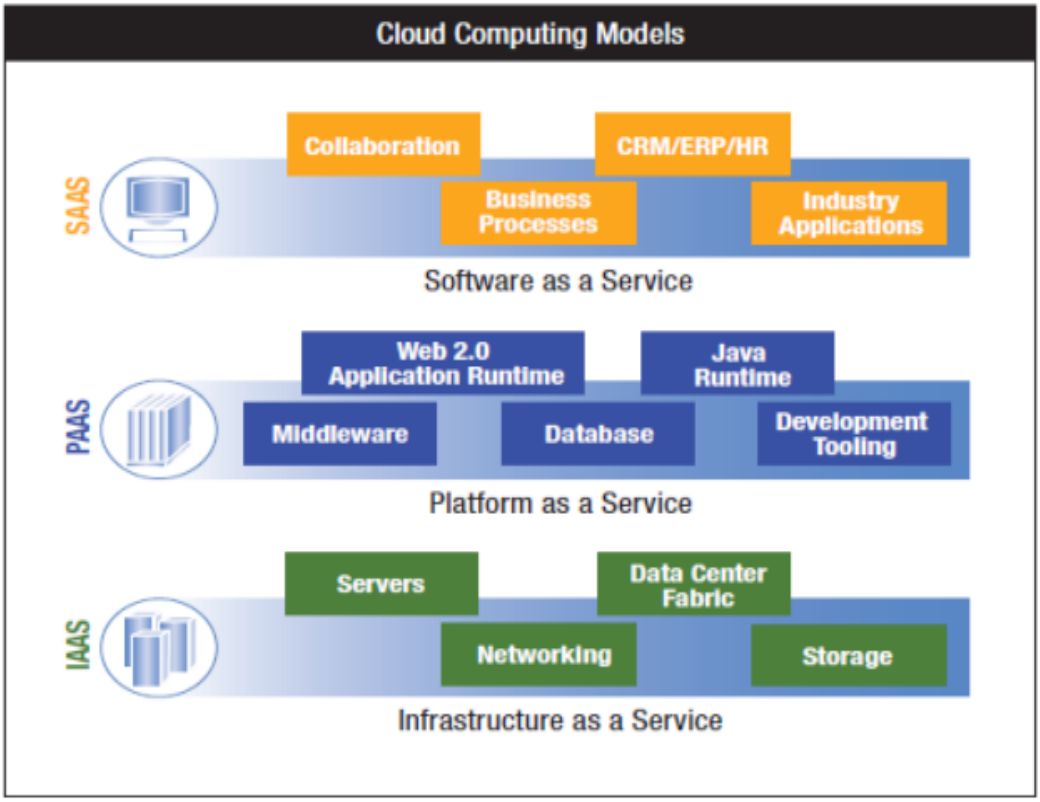


FIGURE 4: Cloud computing service delivery models [15]

data protection transmitted over the Internet [8]. Combining the three types of clouds with the delivery models results in a holistic cloud illustration, as seen in Figure 3, surrounded by connectivity devices and information security themes. Virtualized physical resources, virtualized infrastructure, virtualized middleware platforms, and business applications are provided and consumed as services in the Cloud [15]. Both cloud vendors and clients must prioritize maintaining security at all interfaces within the Cloud computing ecosystem. The next section of the paper introduces challenges faced in the Cloud computing domain.

Cloud Computing Challenges

The current adoption of cloud computing faces several challenges, primarily due to user skepticism about its authenticity. A survey conducted by IDC in 2008 highlighted major challenges recognized by organizations that hinder the widespread adoption of Cloud Computing:

A. Security:

The paramount challenge hindering Cloud computing acceptance is security. Entrusting data and running software on someone else's hardware using someone else's CPU raises significant concerns. Well-known security issues such as data loss, phishing, and botnets (running remotely on a collection of machines) pose serious threats to organizational data and software. The multi-tenancy model and pooled computing resources in cloud computing introduce new security challenges that require novel techniques to address. For instance, hackers can leverage the Cloud to organize botnets due to the reliable infrastructure services it provides at a relatively lower cost, facilitating attacks [9].

B. Costing Model:

Cloud consumers must carefully consider tradeoffs among computation, communication, and integration. While migrating to the Cloud can significantly reduce infrastructure costs, it raises the cost of data communication, especially in scenarios where the organization's data is distributed across various public/private/community clouds in the hybrid cloud deployment model. The cost per unit of computing resource used may also be higher, particularly for CPU-intensive tasks. Evaluating the cost-effectiveness of on-demand computing becomes crucial [9].

C. Charging Model:
The elastic resource pool in cloud computing complicates cost analysis compared to regular data centers. The cost of instantiated virtual machines becomes the unit of analysis instead of the underlying physical server. For SaaS cloud providers, the cost of implementing multi-tenancy within their offerings can be substantial, involving the redesign and redevelopment of software originally used for single-tenancy. Additionally, costs include providing new features for intensive customization, enhancing performance and security for concurrent user access, and managing complexities induced by these changes. SaaS providers need to carefully weigh the trade-off between providing multi-tenancy and the cost-savings yielded by it, considering factors like reduced overhead through amortization and fewer on-site software licenses. Establishing a strategic and viable charging model is crucial for the profitability and sustainability of SaaS cloud providers [9].

D. Service Level Agreement (SLA):
Cloud consumers lack control over the underlying computing resources but must ensure the quality, availability, reliability, and performance of these resources once their core business functions are migrated to the entrusted cloud. Obtaining guarantees from providers on service delivery is crucial. Typically, these guarantees are outlined in Service Level Agreements (SLAs) negotiated between providers and consumers. Defining SLA specifications presents challenges, requiring an appropriate level of granularity that balances expressiveness and simplicity. The specifications should cover most consumer expectations and be easily weighted, verified, evaluated, and enforced by the resource allocation mechanism on the cloud. Different cloud offerings (IaaS, PaaS, and SaaS) need distinct SLA metaspecifications, posing implementation challenges for cloud providers. Advanced SLA mechanisms must continuously incorporate user feedback and customization features into the SLA evaluation framework [16].

E. What to Migrate:
Based on a survey conducted by IDC in 2008 with a sample size of 244, the seven IT systems/applications most migrated to the cloud are IT Management Applications (26.2%), Collaborative Applications (25.4%), Personal Applications (25%), Business Applications (23.4%), Applications Development and Deployment (16.8%), Server Capacity (15.6%), and Storage Capacity (15.5%). The survey highlights that security and privacy concerns deter organizations from moving their data to the cloud, leading them to migrate peripheral functions such as IT management and personal applications first. There is a conservative approach to employing Infrastructure as a Service (IaaS) compared to Software as a Service (SaaS), with marginal functions often outsourced to the cloud while core activities remain in-house. The survey also anticipates a shift in the next three years, with 31.5% of organizations planning to move their Storage Capacity to the cloud. However, this number is relatively low compared to Collaborative Applications (46.3%) at that time [1].

F. Cloud Interoperability Issue:
Presently, each cloud offering has its unique approach to how cloud clients, applications, and users interact with the cloud, contributing to the "Hazy Cloud" phenomenon. This significantly impedes the development of cloud ecosystems by promoting vendor locking. Vendor locking restricts users from choosing alternative vendors or offerings simultaneously, hindering the optimization of resources at different levels within an organization. Proprietary cloud APIs further complicate integration with an organization's existing legacy systems, such as an on-premise data center for highly interactive modeling applications in a pharmaceutical company.

Cloud interoperability is crucial for realizing seamless fluid data flow across clouds and between cloud and local applications. Several levels of interoperability are essential for effective cloud computing. First, to optimize IT assets and computing resources, organizations often need to retain in-house assets and capabilities related to their core competencies while outsourcing marginal functions (e.g., human resource systems) to the cloud. Second, for optimization purposes, organizations may need to outsource various

marginal functions to cloud services offered by different vendors. Standardization emerges as a potential solution to address interoperability issues. However, as cloud computing gains traction, interoperability problems have not yet become a top priority on the agenda of major industry cloud vendors [9].

Conclusion

While Cloud computing represents a new phenomenon poised to revolutionize Internet usage, caution is essential. The rapid emergence of new technologies, each with its advancements, holds the potential to simplify human lives. However, understanding the security risks and challenges associated with these technologies is imperative, and Cloud computing is no exception. This paper has emphasized key security considerations and challenges currently faced in Cloud computing.Despite these challenges, Cloud computing has the potential to emerge as a frontrunner in promoting secure, virtual, and economically viable IT solutions in the future. The transformative impact of Cloud computing on how we utilize technology is undeniable, but a balanced approach that addresses security concerns is vital to fully realize its benefits. Vigilance, strategic planning, and continued advancements in security measures will be crucial for the successful and secure integration of Cloud computing into our technological landscape.

REFERENCES:

[1] F. Gens. (2009, Feb.). “New IDC IT Cloud Services Survey: Top Benefits and Challenges”, IDC eXchange, Available: [Feb. 18, 2010].
[2] J. Brodkin. (2008, Jun.). “Gartner: Seven cloud-computing security risks.” Infoworld, Available: [Mar. 13, 2009].
[3] Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0," 2010.
[4] ENISA. (2009, Feb) "Cloud computing: benefits, risks and recommendations for information security."[Jul. 10, 2010].
[5] R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. “Cloud Security Issues.” In PROC ‘09 IEEE International Conference on Services Computing, 2009, pp 517-520.
[6] P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.
[7] B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 2010.
[8] S. Subashini, and V. Kavitha. (2010) “A survey on security issues in service delivery models of cloud computing.” J Network Comput Appl doi:10.1016/j.jnca.2010.07.006. Jul., 2010.
[9] S. Ramgovind, M. M. Eloff, E. Smith. “The Management of Security in Cloud Computing” In PROC 2010 IEEE International Conference on Cloud Computing 2010.
[10] M. A. Morsy, J. Grundy and Müller I. “An Analysis of the Cloud Computing Security Problem” In PROC APSEC 2010 Cloud Workshop. 2010.
[11] Cloud Security Alliance (CSA).[Mar.19, 2010]
[12] S. Arnold (2009, Jul.). “Cloud computing and the issue of privacy.” KM World, pp14-22.[Aug. 19, 2009].
[13] A Platform Computing Whitepaper. “Enterprise Cloud Computing: Transforming IT.” Platform Computing, pp6, 2010.
[14] Global Netoptex Incorporated. “Demystifying the cloud. Important opportunities, crucial choices.” pp4-14.[Dec. 13, 2009].
[15] M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. “What’s Inside the Cloud? An Architectural Map of the Cloud Landscape.” IEEE Xplore, pp 23-31, Jun. 2009.
[16] C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser. “Business Models in the Service World.” IT Professional, vol. 11, pp. 28-33, 2009.
[17] N. Gruschka, L. L. Iancono, M. Jensen and J. Schwenk. “On Technical Security Issues in Cloud Computing” In PROC 09 IEEE International Conference on Cloud Computing, 2009 pp 110-112.
[18] N. Leavitt. “Is Cloud Computing Really Ready for Prime Time?” Computer, vol. 42, pp. 15- 20, 2009.

[19] M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, "On Technical Security Issues in Cloud Computing." in PROC IEEE ICCC, Bangalore 2009, pp. 109-116.
[20] C. Soghoian. “Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era” The Berkman Center for Internet & Society Research Publication Series.[Aug.22, 2009].