International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A Proposed Model Architecture for Ensuring Security and Privacy in Public Cloud Computing Systems

Neerav Nishant *[1], Vaishali Singh [2]

Submitted: 26/01/2024 **Revised**: 04/03/2024 **Accepted**: 12/03/2024

Abstract: In recent scenario public cloud services has springing up as a widely embraced and effective proposal for the organizations seeking to process, save, and utilize data and application that uses internet to share resources and information. The purpose of this research is to look into the problems and security risks associated with public cloud computing. It is distinguished by five important characteristics: on-demand self-service, broad network access, resource pooling, measured service and rapid elasticity. However, the arising prevalence of the public cloud services, security considerations have become paramount in the authoritative processes. This study emphasis to scrutinize the information security concerns of public cloud services and pinpoint organizations potential penetrability and threats that may encountered. Specifically, the focus is on investigating the challenges pertaining to cloud databases and their security concerns. Additionally, it examines different cloud service models and potential information security issues. In summary, this study offers a comprehensive evaluation of available security solutions and presents recommendations for tackling the challenges posed by cloud security.

Keywords: *Cloud Computing, Security Service , Cloud Security*

1. Introduction

The web is a huge network where various resources connected around the world. It permits us to get any help or data that we require in a split second. This has brought about cloud computing, which alludes to remote admittance to processing assets given by outsider administrations associated with the public web. The market of cloud computing is the quickest developing portion in the world of IT business, and it is changing the manner in which organizations work. It has developed from different other registering models, for example, disseminated processing, utility figuring, lattice registering, P2P registering, virtualization, and server bunches [14]. Web-based applications are the primary focus of cloud computing, which also allows for the sharing of flexible IT resources like operating systems, hardware, and software on to the internet. The advantages of cloud computing incorporate speed and simplicity of sending, in addition the enhancements to the financial matters of different ventures. The Cloud administration models, distributed storage, and cloud suppliers like Amazon EC2, Microsoft Sky blue, Google Application Motor (GAE), Salesforce.com, IBM Blue Cloud, and so forth, empower this sharing of IT assets. It resembles having an enchanted PC that can able to give anything you want, similar to games or schoolwork help. Here we have three kinds of benefits that it can provide: infrastructure, software and platforms. Programming resembles applications we can use on web, as Google or Facebook.

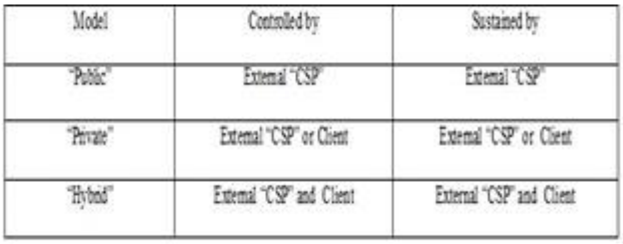
IaaS - Infrastructure as a Service (IaaS) provides network capacity, online processing and data storage in the virtual environment. It offers an assortment of the programming connection points for applications that let clients oversee and communicate involving the framework's parts in alternate ways and its advantages, in addition various sending distributed computing models for that[15]. IaaS incorporates capacity, network assets, and handling power, and is frequently alluded to as utility processing. Data security issues confront cloud users. This technology requires proper security to reduce user anxiety.

PaaS - PaaS refers to the cloud-based application creation and publishing platform and built on IaaS infrastructure. The developers also can use provider, programming languages and the tools to run applications using PaaS. This provides the prerequisite infrastructure that supports the entire lifecycle of application development and delivery of web applications and services over the Internet, as well as providing application of building blocks for defining new applications of business. Microsoft Azure, Google App Engine, and Engine Yard are just some of the platform providers. PaaS is a development platform that can supports the entire “SOFTWARE LIFECYCLE”, allowing cloud users to create cloud software and app in the PaaS cloud.

SaaS - SaaS is the very commonly used cloud service and can be used by almost anyone with the internet connection. SaaS stands for “On-Demand Software”. Cloud users or

[1] *Research Scholar, Department of Computer Science and Engineering, Maharishi University of Information Technology, Lucknow, india.*
[2] *Assistant Professor, Department of Computer Science and Engineering· Maharishi University of Information Technology, Lucknow, india..*
Corresponding Author E-mail : contactnnishant@rediffmail.com

customers, with the assistance of utility or application users, execute their program in the hosting of website domain that may be accessed via networks or internet by variety of the clients. Salesforce.com, Microsoft Online Services, and Google Docs are the few examples of numerous effective SaaS services targeting both domain that are businesses and consumers. This type of programs can be used by any thin client device such as a web browser.



Model	Controlled by	Sustained by
"Public"	External "CSP"	External "CSP"
"Private"	External "CSP" or Client	External "CSP" or Client
"Hybrid"	External "CSP" and Client	External "CSP" and Client

Table 1: Demonstrating the various cloud deployment techniques.

Platforms are similar to tools for creating your own apps and websites. Foundation resembles stuff that the makes web work, similar to servers and capacity. Private, public, and hybrid clouds are among the various cloud computing deployment models.

Public cloud - A public cloud is the service offered by a single service provider to multiple customers who share the cloud synchronously and its computing resources. Different classification levels are offered depending on the resource.

Private cloud – A private cloud is a cloud environment only for a single organization. The cloud could contain various different divisions, yet they belong all to same organisation. The cloud could contain a wide range of divisions, yet they all have a place with a similar organization. Virtualization is utilized in numerous confidential mists to amplify the utilization of the association and existing server framework [16]. This cloud provisioning and metering infrastructure makes it possible to decommission and provision resources quickly. There are numerous private cloud architectures currently in use as:

1. Devoted private cloud: These are overseen by inward IT groups and are situated in client claimed server farms or collocation offices.

2. Local area Private Cloud: These are facilitated somewhere else by a specialist organization liable for their upkeep and are limited by Administration Level Arrangements (SLA) and other legally binding arrangements that guarantee their consistence and security.

3. Private Cloud Managed: In this game plan, the hidden framework is claimed by the client, yet oversaw by an outsider.

Hybrid Cloud – The hybrid cloud is a combination of two or more deployment models. In order to give users a better overall experience, the hybrid cloud constructs the use of many cloud models. Utilizing a cross breed cloud design, clients can accomplish failover and high nearby accessibility without utilizing a Web association.

The study conducts a comprehensive literature review on public cloud security, as well as industry reports and case studies, in order to provide insight into actual issues and procedures. It examines significant security breaks and public cloud breaks and investigates their causes and examples learned. In view of the discoveries, this study gives suggestions for associations to reinforce their security openly cloud administrations. This highlights the requirement for an all encompassing and proactive way to deal with security that incorporates a blend of specialized controls, strategies and persistent checking. The review closes with an outline of future patterns and advancements in broad daylight cloud security, for example, the mix of man-made brainpower and AI in danger identification and counteraction. It provides organizations and decision-makers with useful data to help them make better decisions, lower risks, and guarantee the integrity, confidentiality, and availability of their cloud-based applications and data.

2. Literature Review

Securing the cloud computing set-up has emerged as very important priority for organizations and the businesses across all scales. With the increasing volume of cloud processed and stored data, the potential for data breaches and the cyber attacks escalates significantly. Implementing multi-factor authentication stands out as one of the best effective strategies to bolster cloud computing security. This approach mandates users to provide at least two authentication factors, such as a password and a biometric scan, to access the system. By doing so, it ensures that only authorized users gain entry, thus mitigating risk of the data breaches and unauthorized access. Additionally, encrypting all data are stored in cloud is paramount. It serves as a protective barrier against unauthorized access, even in cases of data theft or interception by the cybercriminals. The regular patches and the updates are also vital to sustain the cloud computing systems security. Therefore, maintaining the system with latest patches and security updates is imperative. Moreover, the businesses should enforce stringent password policies to thwart the cloud computing systems uncertified access. Such policies should mandate users for creating complex, difficult-to-guess passwords and regularly change them.

Furthermore, conducting routine security audits of cloud computing systems is crucial. These audits help in identifying potential vulnerabilities and threats, thereby enabling organizations to fortify their system security effectively. In today's digital landscape, cyber protection has become indispensable for providing any form of online service. As our daily activities increasingly migrate online, security measures have become paramount. Cloud computing, with its cost-saving benefits and the liberation of resources from IT infrastructure maintenance, presents a dynamic and demanding environment for cyber security management [25]. The growths of various new technologies also introduce new challenges, with ensuring adequate security being the foremost. Securing cloud computing infrastructure shares commonalities with securing traditional IT infrastructure, yet it presents unique risks attributable to the cloud service models, operating paradigms, and underlying technologies. In the cloud computing system there are essentially three important security goals:

Confidentiality: To sustain confidentiality, the data should be protected from any type of accidental or intentional disclosure. The IPR, traffic analysis, encryption, and the inference all of these plays very crucial role in the security and privacy of cloud-based systems.

Integrity: Ensures that data is not tampered with during transmission over a network and protects data from illegal deletion and modification.

Availability: Accessibility is guaranteed by its availability of cloud information. The accessibility of data can be threatened, for example, by a DOS attack.

Authentication: It confirms the identification of the person making that making communication.

Auditing: The two primary tools practiced by companies are System testing and monitoring to regulate operational assurance.

Finally, the disaster recovery strategy play very important role in event of the security breach or the data loss.

3. Proposed Cloud Security Architecture

Instead of security, resilience is the main goal of Internet design. Locally hosted applications have a much smaller attack surface than distributed applications. In addition to the inherent vulnerabilities in Internet-based applications, cloud computing now faces additional risks due to shared, virtualized, and outsourced resources. All the service models are not equal in context of cloud security [7]. We will get most from the SaaS provider and the least from the IaaS provider in terms of integrated security. Therefore, each cloud environment and cloud service model in which we deploy our applications has unique risks. Cloud providers and users must implement security measures. Protecting servers from external threats is the responsibility of the cloud service provider. A cloud service provider will only be considered suitable if it adequately manages customer security. Therefore, we here proposed a security architecture for the cloud-based systems based on security considerations to maintain privacy concerns and save data in the frameworks described in fig. below.

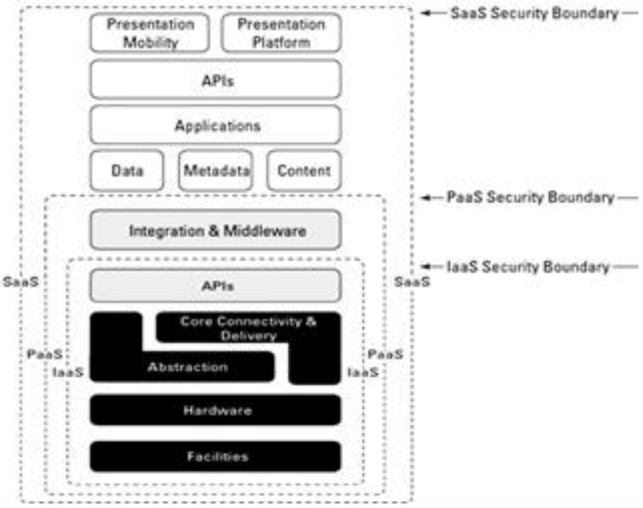


Fig.: Proposed cloud security architecture

The architecture of cloud reference models describes each specific cloud service delivery system along with security boundaries that indicate where customer and cloud service provider obligations begin and end [9] [11]. Security measures that fall below security limit must be integrated into the system, and those that exceed the security limit must be updated by the customer. Including security type and level in our SLAs is more important than ever as we move up the hierarchy. All of the basic security issues and risk and capacity considerations inherent to the model are inherited by each service model. While PaaS provides application development frameworks, control structures, and transactions, IaaS provides the infrastructure and SaaS is the operating environment with the management, applications and interfaces. As we move up the hierarchy, SaaS has the highest level of security and integrated features, while IaaS has the lowest [21]. In the SaaS model, security is provided by the vendor as part of a service level agreement, with levels of governance, compliance, and accountability specified in the contract for the entire system. The framework for software and middleware layer of the PaaS model can be protected by vendor-defined security barriers. High-level security for the application and user interface will be managed by the customer under the PaaS model, while following the IaaS approach.

4. Cloud Computing Security Issues

In cloud computing where several advantages, on the other hand it has also disadvantages. Among the challenges is security, a major hurdle that cloud computing must overcome. Cloud computing encompasses applications, platforms, and infrastructure, each serving distinct functions and offering diverse products globally. Various technologies, such as networking, databases, and virtualization, play crucial roles in cloud computing but also introduce security concerns. For instance, ensuring a secure network for cloud-connected systems is paramount, as is addressing security risks stemming from virtualization. Ensuring the secure mapping of virtual machines to physical ones is essential. Cloud location transparency is crucial for adaptability, as failure to identify data storage locations can lead to breaches of data protection laws in different regions. Protecting users' privacy in the cloud is imperative, requiring measures like data encryption and stringent data distribution rules. The key security and privacy issues inherent in cloud computing are as discussed below.

4.1. Multiple Safety Challenges

1. Data storage location

2. Restoration – For the data preservation of the customer, every cloud service have needs a plan of disaster recovery.

3. Support for inquisitiveness - If the customer detects the unfair behaviour by the provider and there several legal avenues may not be open to pursue any inquiry.

4. Data isolation - Since the data encrypted that are kept on the same hard drive from many firms, supplier should have the necessary data separation tools. Ownership of data necessitates dedicating significant time to understand as much as possible about the vendors they use and laws.

5. Regulatory compliance – In regulatory compliance there is option to choose the provider who welcomes the impartial audits.

4.2. Cloud Computing Privacy issues

The most well-known cloud applications are the consumer services such as email, virtual worlds, and social networks. Terabytes of sensitive data are collected and kept in data centres across many countries by the companies that provide these services. The right to privacy is a fundamental human right. The "right to be left alone" and "control over information about us" are just two instances of privacy [10]. To construct a benefit/risk analysis, it might be helpful to begin with a privacy grouping that focuses on the negative consequences of privacy breaches.

5. Managing Cloud Computing System Issues

To begin with, we should safeguard any gadgets that are straightforwardly associated with the Web from the standard gamble of unlawful access. On the other hand, we want to defend data while it traversed the organization, and lastly, we should focus on getting superior grade, reliable associations with the cloud.

5.1. Limiting access of network via safety groups

While firewalls are generally used to partition organizations, they can likewise act as a supportive strengthening layer when joined with other organization limitations.

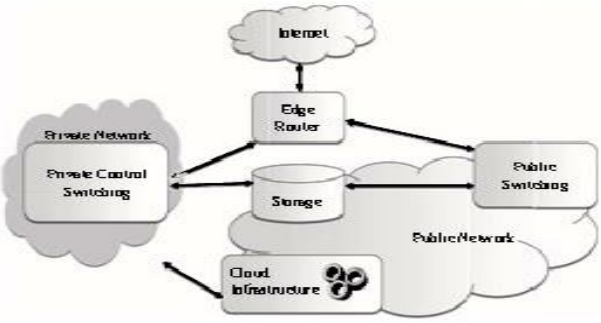


Fig.: Separation of network via the safety groups.

In above fig., we perceive how the organization is apportioned into the secure sub organizations. This is particularly valuable when numerous subnets utilize a similar catalog administration. In a PaaS environment, a security group (SG) can act as firewall, giving the control of customer over which ports and network protocols can be accessed from outside. And a security bunch in the Amazon EC2 is an assortment of the firewalls acknowledges the rules for approaching UDP, ICMP parcels, or TCP. The rules for the distributed internal firewall of a particular Security Group (SG) are applied to an instance when it is launched with that SG [17].

5.2. Prevention of physical access to applications and servers

The most striking elements of the cloud computing is, it empowers clients to "self-administration." It's a method for accessing enormous queues of servers on web. Regularly, just immediate, or on-premises associations are permitted among chairmen and the traditional servers server farms. Monitoring and restricting administrative access is essential for determining who and why modifies the system. Issues with information access ordinarily come from careless safety efforts taken to safeguard client data [22].

5.3. Data Security within cloud

The challenges in Cloud security rotate around delicate information. Despite that data put away in the cloud may be normal, private, or touchy, anyone can get to it whenever, anyplace. Cloud-based registering requires information uprightness strategies. Furthermore, the information can be harm or lost or undermined because of catastrophic event, miss occurring, and fire. Because of these conditions, information may not be open to clients. This framework encodes information start to finish for enormous clients.

5.3.1. Virtual protection

One of the essential cloud component is virtualization. The virtual machines are dynamic in nature, meaning they might be promptly stopped, continued, and quickly got back to before cases. One of the principal errands of virtualization is to ensure that few occasions running on a similar actual PC stay secluded from each other [24]. Thus due to its dynamic nature, developing and maintaining continuous security is challenging.

5.3.2. Providing the security to network

The framework and organization that are utilized in a standard endeavour setting can be obviously characterized with regards to usage. Since traffic is unsurprising, setting up an extremely static organization arrangement that main allows the anticipated kinds of traffic while hindering all others is conceivable. The probability of being a survivor of unfriendly attacks by different occupants (or against them) is, obviously, nothing in a solitary inhabitant situation [26]. The principal thing to acknowledge is that a universally useful organization will not at any point work as typically and effectively as a devoted organization for a specific reason.

6. Cloud Safety and Security Monitoring

It can be suggested that all organization gadgets, applications and servers have their security logs consequently gathered. For lawful reasons thus that they might be questioned in case of a ready, keeping these records in their unique formats is significant. Dangers can be distinguished, weaknesses can be unveiled, a review trail can be kept up with, and legal sciences might be made conceivable with the assistance of safety checking. Logs from the working framework, (for example, occasion syslogs and logs), applications, IPS/IDS frameworks, antivirus programming, network gadgets, and capacity gadgets are probably going to contain data on integrity occurrences. These integrity and security occasions are packaged into the streams and shipped off to a unified gathering administration, frequently a Security Data and Occasion The executives (SIEM) framework, over an organization. Fig. given below showing every one of the lifecycle stages of safety observing.

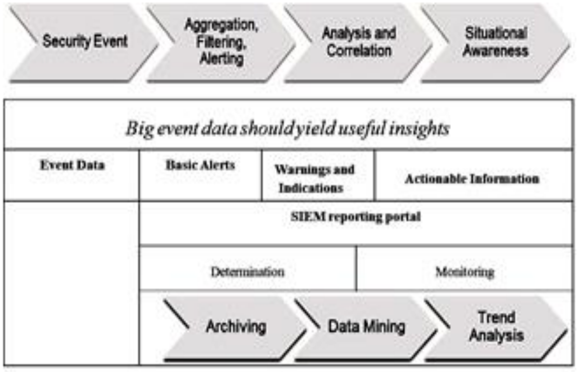


Fig.: Security Monitoring Lifecycle

In the cloud the data security is vital due to the sheer volume of clients and delicate idea of the data put away there. Encryption calculations serve a urgent job in guaranteeing safe web-based correspondence. It's the essential technique for guarding touchy data. Encryption calculation takes "the key" and changes the information or plaintext message into figure message, which then may be unscrambled by client. The same key is mostly used for both the encryption and unscrambling activity in the symmetric key encryption. Whereas, asymmetric key encryption is another choice; this strategy utilizes a couple of keys, called a confidential key and another a public key, to encode information. The encryption is performed utilizing public key, and decoding utilizes the confidential key [12]. In this study we have outlined the numerous concerns regarding cloud computing security and privacy as well as future research directions. The report additionally offered answers for these issues. Additionally, general recommendations for cloud security were made in the paper. Taking everything into account, getting cloud computing frameworks is crucial for safeguarding delicate information and forestalling digital assaults. By carrying out powerful safety efforts, for example, multifaceted validation, encryption, normal updates and fixes, solid secret key arrangements, security reviews, and calamity recuperation plans, organizations can guarantee the security and wellbeing of their cloud computing frameworks

7. Conclusion

The cloud computing is a growing field of technology. Experts in this field of safety are attempting to deal with new dangers that continually arise. To exploit the modest expense and expanded adaptability given by this progressive innovation, organizations who are thinking about a transition to the cloud ought to tread carefully and cautiously dissect the risks. There are security worries as the quantity of organizations utilizing cloud administrations keeps on developing quickly. Security of shared the assets and information is a central issue with the distributed computing idea. We have outlined the numerous concerns regarding cloud computing security and privacy as well as future research opportunities in this study. The report additionally offered answers for these issues. Additionally, general recommendations for cloud security were made in the paper. Taking everything into account, getting distributed computing frameworks is crucial for safeguarding delicate information and forestalling digital assaults. By executing vigorous safety efforts, for example, multifaceted verification, encryption, normal updates and fixes, solid secret word strategies, security reviews, and calamity recuperation plans, organizations can guarantee the security and wellbeing of their cloud computing frameworks.

Author contributions

Neerav Nishant : Conceptualization, Methodology, Field study, Writing-Original draft preparation, Validation

Vaishali Singh : Visualization, Investigation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Buyya R., Broberg J., Goscinski A. (2010). Cloud Computing: Principles and Paradigms, John Wiley & Sons, Vol. 87.

[2] Mohammed M. (2014). Alani: Securing the cloud: threats, attacks and mitigation techniques, Journal of Advanced Computer Science and Technology, Vol. 3, No. 2, pp. 202-213.

[3] Buecker A., Lodewijkx K., Moss H., Skapinetz K., Waidne M. (2009). Cloud security guidance, IBM Red Paper 2009, p. 12.

[4] Padhy R.P., Patra M.R., Satapathy S.C. (2011). Cloud computing: security issues and research challenges, IRACST- International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 11.

[5] Tiwari P.K., Mishra B. Cloud computing security issues, challenges and solution, International Journal of Emerging Technology and Advanced Engineering. Vol. 2.

[6] Prince Jain: security issues and their solution in cloud computing, International Journal of Computing & Business Research.

[7] Anantwar R.G., Chatur P.N., Anantwar S.G. (2012), cloud computing and security model: a survey, International Journal of Engineering Science and Innovative Technology (IJESIT), Vol. 1.

[8] Tim M., Subra K., Shahed L. (2009). Cloud security and privacy: an enterprise perspective on risks and compliance, O' Reilly Media, USA.

[9] Barrie S. (2011). Cloud Computing Bible, Wiley Publishing Inc.

[10] Pearson S., Azzedine B. (2010). Privacy, security and trust issues arising from cloud computing, 2010 IEEE Second International Conference Cloud Computing Technology and Science (CloudCom), pp. 693-702.

[11] Hamouda S.K., Glauert J. Security, Privacy and Trust Management Issues for Cloud Computing, Taylor & Francis Group.

[12] Shakeeba S.K., Tuteja R.R. (year). Security in cloud computin using cryptographic algorithms, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3.

[13] Oztemel, E., Gursev, S. Literature review of Industry 4.0 and related technologies. J Intell Manuf 31, 127–182 (2020). https://doi.org/10.1007/s10845-018-1433-8

[14] P. D. Kaur and I. Chana, "Unfolding the Distributed Computing Paradigms," 2010 International Conference on Advances in Computer Engineering, Bangalore, India, 2010, pp. 339-342, doi: 10.1109/ACE.2010.80.

[15] Jouini, M., & Rabai, L. B. A. (2019). A security framework for secure cloud computing environments. In Cloud security: Concepts, methodologies, tools, and applications (pp. 249-263). IGI Global.

[16] Dhaya, R., Kanthavel, R., & Venusamy, K. (2021). Dynamic secure and automated infrastructure for private cloud data center. Annals of Operations Research, 1-21.

[17] Bolívar, H., Parada, H. D. J., & Roa, O. (2019, October). Modeling cloud computing security scenarios through attack trees. In 2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI) (pp. 1-6). IEEE.

[18] Barrett, P. (2000, December). Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor. In Advances in Cryptology—CRYPTO'86: Proceedings (pp. 311-323). Berlin, Heidelberg: Springer Berlin Heidelberg.

[19] Hamouda, B. E. H. H. (2020). Comparative study of different cryptographic algorithms. Journal of Information Security, 11(3), 138-148.

[20] Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.

[21] Josyula, V., Orr, M., & Page, G. (2011). Cloud computing: Automating the virtualized data center. Cisco Press.

[22] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102.

[23] Pandey, S., & Farik, M. (2017). Best symmetric key encryption-A Review. International Journal of Scientific & Technology Research, 6(6), 310-312.

[24] Kosta, S., Aucinas, A., Hui, P., Mortier, R., & Zhang, X. (2012, March). Thinkair: Dynamic resource allocation and parallel execution in the cloud for

mobile code offloading. In 2012 Proceedings IEEE Infocom (pp. 945-953). IEEE.

[25] Nishant, N. ., & Singh, V. . (2023). Distributed Infrastructure for an Academic Cloud. *International Journal on Recent and Innovation Trends in Computing and Communicat*ion, 11(6), 34–38. https://doi.org/10.17762/ijritcc.v11i6.6769

[26] Varghese, B.etal : Cloud Futurology Computer. 52, 9, 68–77(2019). https://doi.org/10.1109/MC.2019.2895307.

[27] Nishant, N. ., & Singh, V. . (2023). Distributed Infrastructure for an Academic Cloud. International Journal on Recent and Innovation Trends in Computing and Communication, 11(6), 34–38. https://doi.org/10.17762/ijritcc.v11i6.6769.