iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** XI **Month of publication:** November 2020

DOI: https://doi.org/10.22214/ijraset.2020.32244

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: 7.429
Volume 8 Issue XI Nov 2020- Available at www.ijraset.com

Network Security in Cloud Computing

Sachin Gupta
Department of Information Technology, B.K. Birla College of Arts, Commerce and Science, Kalyan, Maharashtra, India. Student of Information Technology, B.K. Birla College

Abstract: Cloud computing is being alternate choice of pc and mobile users for knowledge and provide storage and access. Cloud computing is that the development of parallel computing, distributed computing, grid computing and virtualization technologies that outline the form of a brand new era. Virtual Machine Introspection (VMI) has been verified to be a good tool for malware detection and analysis in virtualized environments.
Cloud-based good producing paradigm facilitates a brand new type of applications and services to research an outsized volume of knowledge and modify large-scale producing collaboration. Cloud Service providers (CSP) offers access to scalable , reliable computing resources model. analysis into the protection of the Cloud focuses principally on protective legitimate users of Cloud Services from attacks by external, malicious users. Cloud computing offers many advantages to users and organizations, in terms of cost and savings in operational expenditure.
Keywords: cloud computing, cloud computing network security, malware detection, VMI, several attacks.

I. INTRODUCTION

Cloud computing a new technology-supported distributed processing, parallel computing and grid computing, and is one among the most well-liked topics within the field of data technology. Academic circles, industrial circles and governments have also paid close attention there too.

There are 4 types of cloud computing:

1) Private Cloud
2) Public Cloud
3) Hybrid Cloud
4) Community Cloud

Security in Cloud is considered, it should not be constrained within the limits of data security but the corresponding Virtual Machine (VM) security should also be considered equal.
Many cloud operators are now active on the market, providing an upscale offering, including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) solutions. The cloud technology stack has also become the most stream in enterprise data centres, where as private and hybrid cloud architectures are increasing adopted by cloud computing. Even though the cloud has greatly simplified the capacity provisioning process, it poses several novels challenges within the area of Quality-of-Service (QoS) management. QoS denotes the quantity of performance by these Computing and reliability and available offered by an application and by the platform or infrastructure. QoS is prime for cloud users, who expect providers to deliver the advertised quality characteristics, and for cloud providers, who need to find the right tradeoffs between QoS levels and operational costs.

II. OBJECTIVES OF STUDY

1) *H1:* If trust issue comes then some of the significant challenges faced by cloud computing environments towards addressing the problem of trust management because These potential challenges once efficiently addressed will provide a roadmap for trustworthy ecosystems.
2) *H2:* If Process of backing up and recovering data is simplified then reside on the cloud and not on a physical device because various cloud providers offer reliable and flexible backup/recovery solutions.
3) *H3:* If privacy and network security issues facing by the several user because there are no response sometime from server or failure of network connection .

©IJRASET: All Rights are Reserved

III. LITERATURE REVIEW

The paper highlighted kaur et. al. [1] Cloud computing network security and challenges in the area of Quality-of-Service (QoS) management, QoS application can be improved by using many techniques such as scheduling by managing the supply and demand for cloud services. The paper highlighted subramanian et. al. [2] there are several benefits to users and organization, Studying the causes and effects of various cyber-attacks in the challenges related to it in all the three layers, Virtual layer, Virtualization Layer and Physical layer are addressed, effect of issues at the computational level specifically Virtual Machine level, Hypervisor level and Hardware level. The paper proposed Muhasili et. al. [3] In Cloud Computing there are some attacks in Cloud Services from attacks by external and malicious usersnattacks include launching a DDoS the attack, sending spam and perpetrating click fraud. There are huge data is one of the greatest basic rising innovations, horrendous circumstances of the cloud and huge actualities. The paper highlighted Butt et. al. [4] Author compare the performance of each technique based on their features, advantages, and disadvantages, cloud security, security threats, VM-based attacks. The author got the results, security threats and attacks as the most challenging issues and several research directions that need more investigations. The paper highlighted Morsy et. al. [5] Author explain Cloud Computing Architecture and Security Implications and cloud computing security management. Capture different stakeholders security requirements, Deliver feedback about the current security status to the cloud providers and consumers. The paper highlighted Rakotondravony et. al. [6] general classifications of related attacks on cloud computing, detection and mitigation mechanisms, attacks on Virtual Machines (VMs), classification of malware attacks in IaaS cloud environments, VMs and the cloud provider can be both source and target of attacks, statistical analysis of CVE reports on popular virtualization products. The paper proposed Qi et. al. [7] Author explain in this Cloud-based manufacturing systems architecture and the study of stored and analyzed of big data, probabilities of service downtime, ensuring the robustness of the smart manufacturing system, fog computing and cloud computing cooperate for better meeting requirements. The paper highlighted Khan et. al. [8] Author explain study of fog computing & security, security issues regarding data, virtualization, segregation, network, malware and monitoring. The Author Purposed possible security solution categories with respect to various components of Fog infrastructure, residing between IoT devices and Cloud. developers can prevent the occurrence of vulnerabilities pro-actively and save the Fog platform from potential damage. The paper highlighted Afzal et. al. [9] The author proposed Real-time implementation of load balancing is very less and should be encouraged, deal with load unbalancing problem effectively like nature-inspired algorithms, machine learning and mathematical derived algorithms. The paper highlighted Endo et. al. [10] The Author purposed, Cloud provides looks solutions for high availability even in failure cases, High availability is a great challenge for Cloud providers due to its complexity, many issues found by Author like portability, feasibility, and security. The paper highlighted Nathiya et. al. [11] DDOS attack was using an attacking internal the network IP address for a legitimate user, Author says when A critical system is affected in loss of economic network resources, loss of processing time in working times. The paper proposed Wang et. al. [12] cloud computing environment, promote computer network security, the connotation of cloud computing achieve security development and application of computer network, development of computer network security technology, accelerate the solution of the problem. The paper highlighted Jabbar et. al. [13] security and integrity aspect of the cloud, cloud environment are required to provide rapid development, dynamic resources and economies of scale. Most of cloud computing services fall into three broad categories: IaaS, PaaS, and server less and SaaS. The paper proposed park et. al. [14] Blockchain Security in Cloud Computing secure solutions of security and attacks on a database, Blockchain connection structure. The blockchain has a distributed structure and utilizes the peer network and the computing resources of peers, efficiency are also needed beside security, providing security by presenting a method of secure blockchain. The paper highlighted Fan et. al. [15] Author purposed system Model and Framework, address the revocation issue and verifiable outsourced multi-authority access control scheme, analysis and simulation of data access control in fog-cloud computing system proposed a verifiable the outsourced multi-authority access control scheme, named VO-MAACS, analysis and simulation results show that our scheme is both secure and highly efficient. The paper highlighted Stergiou et. al. [16] Author purposed Security issues in IoT and Cloud Computing integration. Cloud Computing technology offers many possibilities but also gives several limitations as well as, Cloud Computing and Internet of Things develop rapidly, Cloud Computing technology improves the function of the IoT. The paper purposed Jing et. al. [17] Author explain connotation of cloud computingsnd Optimization strategy of computer network security technology under cloud computing, Network Security Policy of Cloud Computing. There are three aspects of security risks: the technical level, security, policy guarantee level, we should strengthen the awareness of computer network security, achieve security development and application of computer network policy of cloud computing. The paper proposed Mukherjee et. al. [18] an overview of existing security and privacy concerns. state-of-the-art to deal with the fog computing-related security and privacy challenges, Author purpose to solve differently challenges in privacy and security in fog computing. The paper highlighted Tapale et. al. [19]

©IJRASET: All Rights are Reserved

Three service models (SaaS, PaaS and IaaS) and four deployment models (private, public, hybrid and community cloud), address security issues such as data transfer across the gateway, long-term viability, compromised services, regulatory compliance, virtualisation in cloud computing paradigm. The paper highlighted Khadim et. al. [20] Author purposed security of the information can be confirmed by distributing the operator's information between obtainable service providers instead of storing the whole information on a single service provider location, the bandwidth of network station is impacted by the obtained data. The paper highlighted Hepsiba et. al. [21] Cloud Service Providers (CSP) delivers security policies for cloud storage, Cloud Computing business model still has some security issues, the author says the research will be encompassed by providing a new mechanism for security issues in Cloud Environment. The paper proposed Paul et. al. [22] Cloud model is applicable in different types of organizations and institutions including government organizations and bodies, for a better security both Cloud Service providers and customers joint initiatives are much important. The paper highlighted Sheikh et. al. [24] Nodes or virtual machines (VMs) are the virtual resources that are assigned to consumers for running the service and executing tasks, Executing and running tasks over the allocated resources raises some security issues that need to be considered such like data security, and service security. The paper highlighted Nora et. al. [29] Security issues are most challenges in cloud computing, therefore, the encryption algorithms have been applied in cloud data to make cloud data more secure, compared and tested the two algorithms using different file size that results in the AES is faster than DES in the encryption time but in decryption the DES is faster than AES on small files.

IV. RELATED WORK

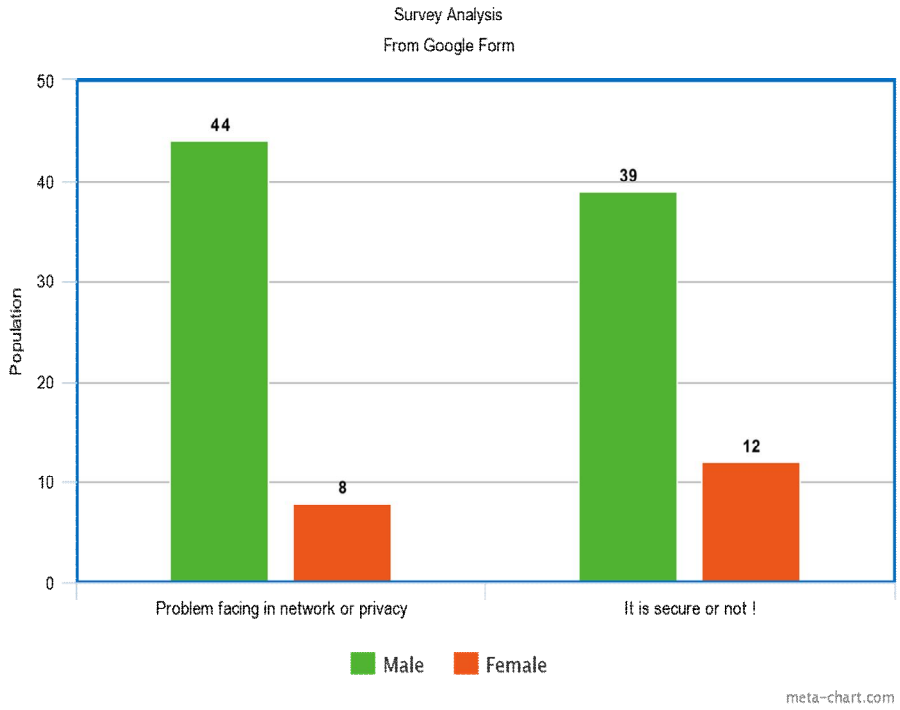


Fig. Survey Analysis

We collected 65 samples out of 70 population with male and female responses. A data is collected using the google form we prepared a questionnaire for response and analysis for network security in cloud computing. It is a quantitative-based analysis collected nominal based data, 65 samples in which 52 are males and 13 are females are responded. In each graph green represent males and red represents female. In the above graph figure, we see that 44 male says yes and 8 male say no whereas 8 female says yes and 5 female says no response to face any problem in the privacy and network security in cloud computing.
We see that in another question cloud computing Secure or not According to you, In this 39 male says yes and 13 male say no whereas 12 female says yes and 1 female says no, According to the graph, we see the response of having problems problem in privacy and network problem.

©IJRASET: All Rights are Reserved

We calculated a chi-square test based on a hypothesis in which created an observed table than expected a table and after this we calculated chi-square and find a degree of freedom to get a tabular chi-square value. If chi-square calculated is greater than chi-square tabular it except alternative hypothesis and rejects the null hypothesis.

A. Table of Observed Value

Table(a)

Response	Male	Female	Total
Yes	44	8	52
No	8	5	13
Total	52	13	65

Formula for finding expected value
(Observed Value-Expected value)^2 % Expected value

B. Table of Expected Value

Table(b)

Response	Male	Female
Yes	41.6	10.4
No	10.4	2.6

C. Calculation of X^2

Table(c)

Observed value (O)	Expected value (E)	(O-E)	(O-E)^2	(O-E)^2 % E
44	41.6	2.4	5.76	0.131
8	10.4	-2.4	5.76	0.72
8	10.4	-2.4	5.76	0.72
5	2.6	2.4	5.76	1.152

Chi-square calculated= 2.723
Degree of freedom =(column-1) (row-1)
(2-1) (2-1)
1×1=1
Chi-square tabular=1
Chi-square calculated= 2.723
Chi-square calculated > Chi-square tabular,
After getting this result, we accept alternative hypothesis

V. RESULT

We performed chi-sqare tesingy data analysis by collecting relevant data from the given questionnaire(Google Form) and performed on it. So according to the experiment H3 hypothesis is accepted that is having problems in privacy and network security in Cloud Computing.

VI. CONCLUSION AND FUTURE SCOPE

In this paper, we presented Network security in cloud computing, There are Various attacks on cloud computing network security, we are given various types and it's solutions which issue are arise, cloud security issues such as firewall misconfigurations, malicious insiders, tampered binaries, multi-tenancy, side channels, weak browser security, and mobility. Then, we classify these issues into five security categories, namely: security standards, network, access, cloud infrastructure, and data.
we added a focus on network security, There are some attacks that directly involve VMs as both source and target of attacks. Our classification supports practitioners at an early stage of the design of VMI-based mitigation mechanisms by identifying relevant attacks which threaten their VM or by which it can harm co-located VMs.

©IJRASET: All Rights are Reserved

A statistical analysis of CVE reports on popular virtualization products highlighted how most vulnerabilities allow attackers to exploit flaws in the product design, especially to achieve DoS attacks which, from economically perspective remains the most damaging attack and most expensive regarding financial loss for the victim or cloud provider. In the future, research will be encompassed by providing a new mechanism for VMI and network security issues in Cloud Computing.

VII. ACKNOWLEDGMENT

I'm extremely grateful to Prof. Swapna Augustine Nikale, Department of Information Technology, B.K. Birla College (Autonomous), Kalyan for encouragement and guidance for carrying out this research work.

VIII. GLOSSARY

1) VMI: Virtual Machine Introspection
2) VMM: Virtual Machine Manager or Hypervisor
3) CSP: Cloud Service Provider
4) IaaS: Infrastructure-as-a-service
5) PaaS: Platform-as-a-service
6) SaaS: Software-as-a-service

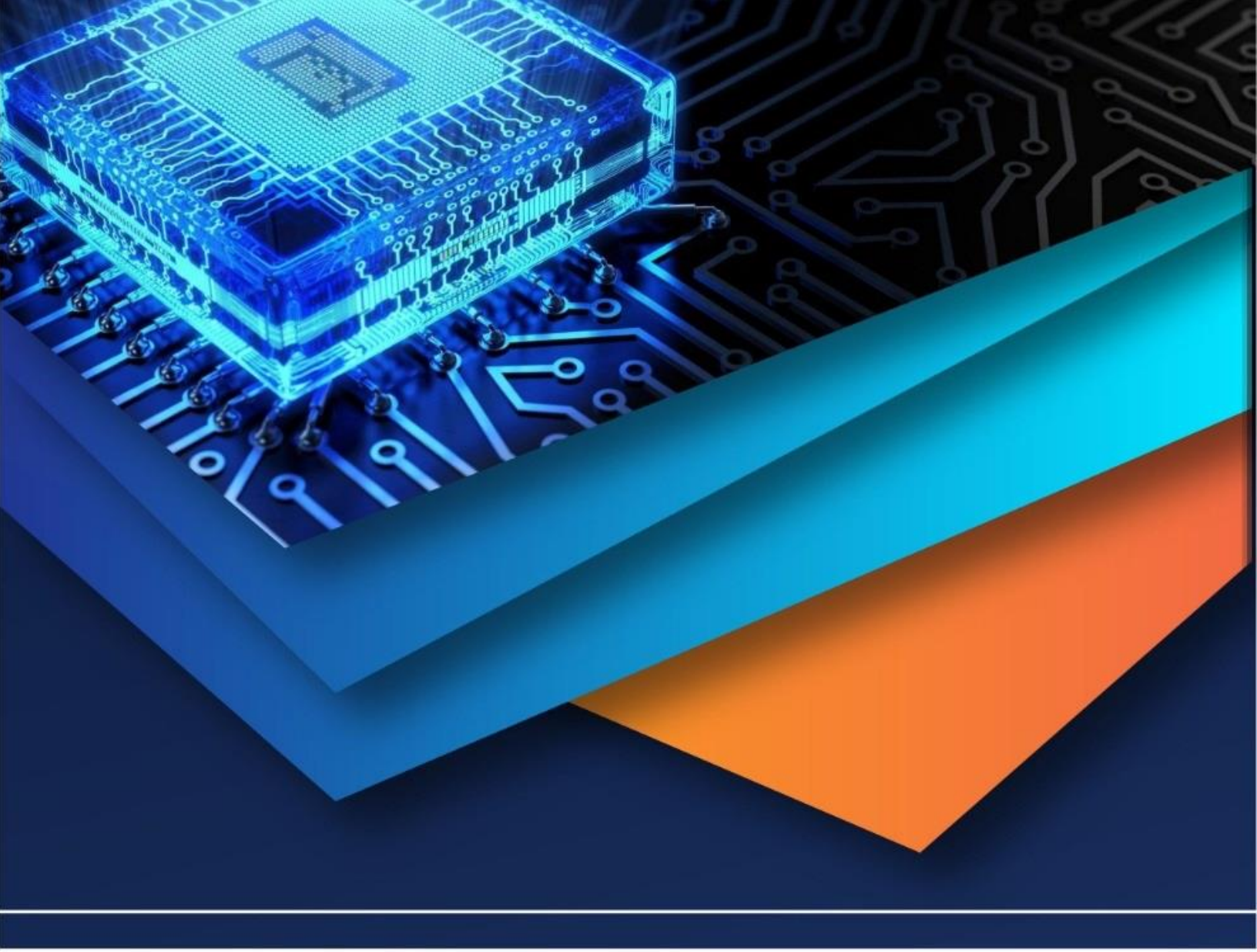
REFERENCES

[1] Cloud computing network security for various parameters, and its application. (2019). International Journal of Advanced Science and Technology, 28, 897–904. https://scholar.google.com/scholar?as_ylo=2016&q=cloud+computing+network+security&hl=en&as_sdt=0,5#d=gs_qabs&u=%23p%3DVOBLPvfG9b8J
[2] Recent security challenges in cloud computing, Subramanian, N., & Jeyaraj, A.(2018). Computers & Electrical Engineering, 71, 28–42. https://doi.org/10.1016/j.compeleceng.2018.06.006
[3] A STUDY OF CLOUD COMPUTING AND ITS ARCHITECTURE, 2020, 675–678. https://scholar.google.com/scholar?as_ylo=2016&q=A+STUDY+OF+CLOUD+COMPUTING+AND+ITS++ARCHITECTURE&hl=en&as_sdt=0,5#d=gs_qabs&u=%23p%3DTP8bY4uozKsJ
[4] A Review of Machine Learning Algorithms for Cloud Computing Security, Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., Suh, D. Y., & Piran, M. J. (2020). Electronics, 9(9), 1379. https://doi.org/10.339/electronics9091379
[5] An Analysis of the Cloud Computing Security Problem (2016).Mohamed Al Morsy, John Grundy and Ingo Müller, Computer Science & Software Engineering https://arxiv.org/abs/1609.01107
[6] Classifying malware attacks in IaaS cloud environments,2017.Noëlle Rakotondravony, Benjamin Taubmann, Waseem Mandarawi, Eva Weishäupl, Peng Xu, Bojan Kolosnjaji, Mykola Protsenko, Hermann de Meer, Hans P. Reiser, 10.1186/s13677-017-0098-8, Journal of Cloud Computing
[7] A Smart Manufacturing Service System Based on Edge Computing, Fog Computing, and Cloud Computing, 2019.Qinglin Qi, Fei Tao 10.1109/access.2019.2923610, IEEE Access
[8] Fog computing security: a review of current applications and security solutions., 2017, Saad Khan, Simon Parkinson, Yongrui Qin 10.1186/s13677-017-0090-3, Journal of Cloud Computing
[9] Load balancing in cloud computing – A hierarchical taxonomical classification, 2019, Shahbaz Afzal, G. Kavitha 10.1186/s13677-019-0146-7, Journal of Cloud Computing
[10] High availability in clouds: a systematic review and research challenges, 2016, Patricia T. Endo, Moisés Rodrigues, Glauco E. Gonçalves, Judith Kelner, Djamel H. Sadok, Calin Curescu, 10.1186/s13677-016-0066-8, Journal of Cloud Computing
[11] Reducing DDOS Attack Techniques in Cloud Computing Network Technology, 2017, T. Nathiya, 10.29027/ijirase.v1.i1.2017.23-29, International Journal of Innovative Research in Applied Sciences and Engineering
[12] Research on Computer Network Security Policy of Cloud Computing, 2020, Xiaojing Wang, 10.1088/1742-6596/1533/3/032044 of Physics: Conference Series
[13] INTEGRITY AND SECURITY IN CLOUD COMPUTING ENVIRONMENT: A REVIEW, 2020Safa S. Abdul-Jabbar, Ali Aldujaili, Saja G. Mohammed, Hiba S. Saeed10.35741/ISSN.0258-2724.55.1.11Journal of Southwest Jiaotong University
[14] Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions, 2017, Jin Park, Jong Park10.3390/sym9080164Symmetry
[15] A Secure and Verifiable Outsourced Access Control, The scheme in Fog-Cloud Computing, 2017, Kai Fan, Junxiong Wang, Xin Wang, Hui Li, Yintang Yang10.3390/s17071695Sensors
[16] Secure integration of IoT and Cloud Computing, 2018, Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta10.1016/j.future.2016.11.031Future Generation Computer Systems
[17] Research on Computer Network Security Policy of Cloud Computing, 2020, XiaoJing Wang10.1088/1742-6596/1533/3/032044Journal of Physics: Conference Series
[18] Security and Privacy in Fog Computing: Challenges, 2017, Mithun Mukherjee, Rakesh Matam, Lei Shu, Leandros Maglaras, Mohamed Amine Ferran, Nikumani Choudhury, Vikas Kumar10.1109/access.2017.2749422IEEE Access
[19] Cloud computing review: concepts, technology, challenges and security, 2017, Manisha T. Tapale, Mahantesh N. Birje, Praveen S. Challagidad, R.H. Goudar10.1504/ijcc.2017.10004732International Journal of Cloud Computing
[20] Storage Architecture for Network Security in Cloud Computing, 2018, Qusay Kanaan Kadhim, Hamid Sadeq Mahdi, Haitham Ail10.24237/djps.1401.205cDiyala Journal For Pure Science

©IJRASET: All Rights are Reserved

[21] Security Issues in Service Models of Cloud Computing, (2016), International Journal of Computer Science and Mobile Computing Research, 5(3), 610–615., https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Security+Issues+in+Service+Models++of+Cloud+Computing&btnG=#d=gs_qabs&u=%23p%3DC-gowxiwOjYJ
[22] Cloud Security: An Overview and Current Trend, 2019, Prantosh Paul, P. S. Aithal10.2139/ssrn.3497705SSRN Electronic Journal
[23] A Survey on Cloud Security Issues, 2019, Foram Suthar, Samarat V.O. Khanna, Jignesh Patel10.26438/ijcse/v7i3.120123International Journal of Computer Sciences and Engineering
[24] Systematic Literature Review (SLR) of Resource Scheduling and Security in Cloud Computing, 2019, Abdullah Sheikh, Malcolm Munro, David Budgen10.14569/ijacsa.2019.0100404International Journal of Advanced Computer Science and Applications
[25] Information Security in Cloud Computing: A Systematic Literature Review and Analysis, (2017), International Journal of Scientific Engineering and Technology, 6(1), 50–55.https://doi.org/10.17950/ijset/v6s1/110
[26] Hybrid Data Encryption Technique for Data Security in Cloud Computing, (2017), Sinhgad Institute of Management & Computer Application (SIMCA), 221–224. https://scholar.google.com/scholar?q=Hybrid+Data+Encryption+Technique+for+Data+Security+in+Cloud+Computing&hl=en&as_sdt=0,5#d=gs_qabs&u=%23p%3DrVtS4ulm4dkJ
[27] Accountability in Cloud Computing by Means of Chain of Trust, (2017). International Journal of Network Security, 19(2), 251–259., https://doi.org/10.6633/IJNS.201703.19(2).10
[28] A survey of Cloud Computing Security challenges and solutions, (2016). International Journal of Computer Science and Information Security (IJCSIS), 14(1), 52–56.https://scholar.google.co.in/scholar?hl=en&as_sdt=0%2C5&as_ylo=2016&as_vis=1&q=A+survey+of+Cloud+Computing+Security++challenges+and+solutions&btnG=#d=gs_qabs&u=%23p%3D8E0722kltmAJ
[29] Comparative Study of Database Security In Cloud Computing Using AES and DES Encryption Algorithms, 2019, Nora Abdullah Al-gowany, Sultan Almotairi10.26735/16587790.2019.004Journal of Information Security and Cybercrimes Research.
[30] The Importance of Authentication and Encryption in Cloud Computing Framework Security, (2018), Pedro Ramos Brandão10.11648/j.ijdst.20180401.11International Journal on Data Science and Technology

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)