iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41591

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 IV Apr 2022- Available at www.ijraset.com

Security in Cloud: From Individual to Multi Cloud

Kapil Kumar Sahu[1], Mohd Tajammul[2]
[1]*MCA Scholar,* [2]*Associate Professor, School of CS and IT Dept of MCA Jain(Deemed-to-be university)-560069, Bangalore, Karnataka, India*

Abstract: ***The use of cloud technology has increased in many businesses.Cloud providers should handle privacy and security concerns as a top priority. Customers are increasingly less interested in dealing with "individual cloud" suppliers due to potential issues such as availability and performance failure and the threat of hostile intruders in the individual cloud. This study focuses on the problems regarding cloud computing's data security. Usage of cloud computing wish to avoid using an unscrupulous cloud provider because their information and data will be transferred with a third party. Protecting sensitive and confidential information from attackers or malicious insiders.***
Keywords: Security, Individual cloud, Multi-cloud.

I. INTRODUCTION

Users of technology can consume services whenever they want, based on the unique requirements. Customers no longer need to make the choice or expensive software, and availability on demand across the network is simple thanks to cloud computing. Users of technology can consume services anyway they want, based on their specific interests. It must devise a method of safeguarding the documents. Cloud content might be hacked or lost. It can encrypt things before exporting them to the cloud, which eliminates the possibility of release. It has the possibility of storing several cloud services and authenticating them before submitting them off.They'll have same file. Cloud provides incredibly fast data retrieval and availability. The transition from a individual cloud to a virtualized environment is investigated, as well as studies on challenges in individual and multicloud cloud computing. The server responses are authenticated by adjusting the hash of the data collected and compared it to the remotely stored data. Resource optimization has now become the task of cloud providers.

II. PROPOSED STATEMENT

Cloud providers should approach privacy - related concerns as a primary concern. Customers are becoming increasingly less interested in dealing with "single cloud" providers due to potential issues such as service level breakdown and the potential of hostile insiders in the single cloud. Data storage in Cloud Applications is the focus of the inputs. The following aspects of our effort can be articulated:he research project focuses on data storing and smart data block operations. Unauthorized users are prohibited from obtaining virtualized data by encoding and decoding, and the admin can also prohibit such visitors' Port numbers. Clients will not be able to access or retrieve resources stored on the server unless the supervisor grants authority to the appropriate users.

III. SYSTEM DESIGN

While global online online services offer huge amounts of digital and customisable computation capabilities, this compute platform change also lifts the duty for information systems from local devices. As a result, consumers' cloud computing and integrity will be at the mercy of their cloud service providers. Cloud computing is a cloud platform in which a large number of indicators are linked together in private or public networks to create a dynamically network stack for saving application data and files.

Data integrity:Computation authenticity refers to the ability of a programme to run as intended while being protected against virus, an outsider, or an unauthorized user who could alter the network's execution and produce an inaccurate output. Information stored may be harmed during transmission to and from the cloud storage system. Data integrity could aid in the recovery of digital evidence or the detection of computation. At the huge computational levels, integrity should be tested. Data integrity refers to the protection of data against illegal alteration.

Data intrusion:Computation authenticity refers to the ability of a programme to run as intended while being protected versus infection, an outsider, or an unauthorized user who could alter the network's execution and produce an inaccurate conclusion. Information stored may be harmed during transmission to and from the cloud services. Data integrity could aid in the recovery of digital evidence or the detection significant computation. At the computing and storage resources levels, integrity should then be tested. Data integrity ensures the safety of data against illegal changes.

A. *Service Availability*

In terms pf cloud computing security, service availability is crucial. Amazon has previously stated in its license agreement that the service may be unavailable from periodically. Any time any user's files infringe the cloud storage policy, the user's web service may be stopped for any reason.

B. *Architecture Diagram*

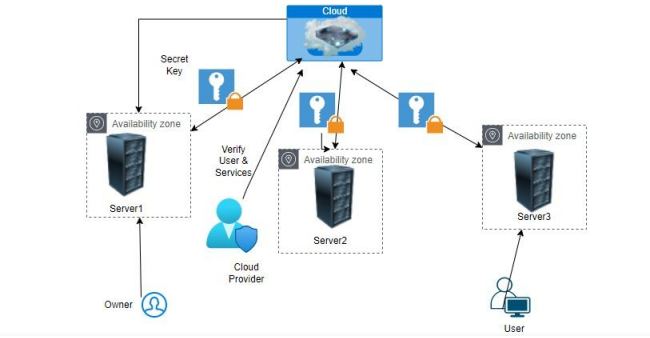


Fig:1 Work flow diagram of our system

IV. LITERATURE REVIEW

In [1] This tool was invented to be utilised with the web and includes features such as data storage, remote monitoring, and more. Cloud computing has shown to be an excellent tool for all the services offered, but it also arrives with a variety of risks. Different fire assaults and data theft have been identified as a critical factor over the years of its development, because the data held in the cloud by an organisation or an individual user is generally secret and private. Many hackers illegally obtain these data, which will then be exploited to fire attacks on the user. This paper specifically aims to spread awareness of such threats and recommend changes for attempting to deal with data failing to uphold issues. In this paper [2] The algorithm that is utilized to enhance cloud security is discussed. Based on numerous methodologies, the suggested algorithm has been developed and implemented for bringing together different keys in cloud computing. The proposed technique in intelligent machines was employed to implement these procedures in our proposal, which included codes, variants, and reordering bits. The original key is also expanded employing linear equation. The method can manage clients by producing private keys of varied lengths and causing the key to be damaged after quite a period of use. Furthermore, using a variety of strategies, the suggested block cypher algorithm has been developed and implemented to secure information exchanged amongst clients with high complexity.

In this paper[3], The aim of this paper is to give a quick overview of cloud technology, with a focus on multi-cloud systems. The fundamentals of cloud computing technologies are first addressed. Following that, we'll go through some of obstacles that enable digital faces and how multi-cloud.products. Our purpose is to have a current look at multi-cloud computing's state-of-the-art and to discuss open concerns in the industry. The purpose of this paper is to assist the reader comprehend cloud computing's problems, how multi-cloud technology resolves some of these concerns, and to arouse community interest in multi-cloud platforms' potential integration with other unique technologies. In this paper[4], The number of cloud users and providers using cloud-based services is steadily increasing, demonstrating that the cloud computing technology has delivered on its promise. Yet, the cloud economy's unstoppable growth is providing significant hurdles to its members. On the supplier side, the capacity to orchestrate resources to maximise profitability while not struggling to achieve customer demand is a cause of concern. The efficient material selection from a multiplicity of digital programs advertised by a variety of suppliers is an interesting question on the customer side. The focus of this research is to offer the reader with a methodical analysis and comparison of the most significant CROFs discussed in the study, as well as to underline the cross technology open topics that the research community should solve in the coming years. In this paper [5], Many cloud providers pool their compute resources, workstations, and types of facilities in a federated cloud environment to meet customer requirements. Distributed network computing is a concept that refers to the combination of services based on interchange features, which allows several cloud provider to work together based on geographic location. By partially outsourcing work various computer resources and capabilities from a nearby cost-effective state, it enhances performance, facility occupancy, reaction time, and pricing structure.Terms and conditions made between cloud vendors and intermediator cloud brokers benefit customers as well.

The goal of this study is to look at the federal cloud infrastructure, its many architectural kinds, the benefits of federation, the obstacles of federation, and recommendations for further studies in the distributed sdn computing field. In this paper[6], The security issues that enable digital presents are discussed in the report. It looks over the current security approaches, procedures, and limitations for virtualized environment. Alibaba and amazon were early adopters of cloud computing, which began in the mid-1990s. In the domain of computer engineering, it is rapidly expanding. Cloud computing is now used by a large number of people. Cloud computing is connected to internet and has the most advanced computer architecture. The largest concern when a person has installed his or her cloud-based system is security. Many companies have begun to offer cloud services to their clients, and security has now become a main priority in their ventures. Most security specialists, but at the other part, are working hard to improve security products. Despite the fact that security is improving all the time, attackers continue to find new opportunities to cheat a certain cloud. This paper[7] Our study's goal is to learn about cloud systems, security challenges, and threats, as well as new solutions that could help alleviate cloud problems. It is a well-known fact that the cloud has been a feasible following section introduces since 2008; yet, the opinion of cloud security is that it requires considerable upgrades in order to accomplish maximum mputing has to be resolved asap. Although the cloud computing industry has grown tremendous progress in combating risks, there is still work to be done..In this paper[8],This paper's important aim would provide a virtualized approach for dealing with security vulnerabilities in existing database systems. Current storage technologies face a variety of cyberspace security concerns as a result of their ancient buildings and procedures for collecting information in Bahrain. Bahrain has discovered that migrating local storage services to the cloud environment solves a slew of related cyber security challenges. On the other end, as a result of this movement, a variety of cyberthreats have emerged, such as public network exposure and heterogeneous distributed shared infrastructure. Due to the vulnerabilities introduced by this migration, data breaches occur, posing a threat to the fundamental private information. In [9-14], The writers have provided numerous meanings of cloud services as well as security procedures. In [15] Via the purpose of information broadband connections, sharing of data in cloud storage is gaining a lot of traction since it can provide subscribers with enhance efficiency storage services. Cryptographic techniques are frequently used to ensure the anonymity of shared sensitive material. Information security, but in the other hand, continues to be a problem in cloud computing for information exchange. The essential concern is how to keep and revoke the key for encryption. Our concept is efficient and robust, as per the security analysis and performance evaluation. In this paper[16] we offer an architecture positioning for processes in multiclouds that is outlay for INTaaS players while also maintaining their customers' changeable security restrictions. The solution is reduced using information retrieval heuristics to make it tractable for larger, more productive INTaaS processes. The technique is tested on authentic merging procedures for money and operational efficiency, and intriguing market are explored.In this paper[17] To address this, multiple offsite data verification mechanisms for proving data access and accessibility have been developed. These approaches, therefore, seem to have a high cost or are unable to correct offsite abuses of power. The tri based data security checking and recovery (MRVR) scheme is proposed in this study to achieve public monitoring and ability to recover in a multi-cloud ecosystem. On the basis of component, interpolation map, and binary accumulation tree approaches, homologous recombination evaluation and recovery strategies are given (BAT). MRVR has been proven to be secure and private information, with good data account receivable and uptime, according to security study. in this paper[18] There is no reliance on a specific service insurer's resources in multi cloud. Plan is important in multi cloud since it delivers resources to various users. The two types of multi - tenant cloud optimization techniques are free or macro task rescheduling and contingent or workflow programming methods.

This article focuses solely on an isolated job scheduling method. The number of iterations of Swarm Optimization (PSO) is lower than that of other combinatorial optimization. in this paper[19] We investigate the problem of a privacy preservation client number disclosure attack in a multi-cloud context in this work.

Essentially, data files and requests are dispersed among multiple cloud servers, allowing each web server to only have a quantity of information about searches and their outcomes. We formulate the record and query assignment as an optimization problem, which we solve using the minimum st cut algorithm to minimise query response time while protecting information leakage. In this paper [20], To address these issues, this paper gives a technique for effectively storing and managing data in a multi-cloud appropriate assessment tools on the affect the potential algorithm. The multi-cloud storage in this scheme is done to avoid any single cloud from failing, the geometric encryption scheme is used to encode and decode file types, the secret key is reliably scattered using Shamir's lower limit key exchange protocol, and and at last the firewall parties affected algorithm is used to promote exchange of encrypted information via clouds. The scheme's prototype is developed in the Programming language framework and tested in a simulated number of co setting.in this paper[21]To address that issue, this paper gives a methodology for effectively storing and managing data in a multi-cloud strong cultural on the affect the potential algorithm.

The multi-cloud collection in this scheme is done to avoid any single cloud from failing, the coplanar encryption scheme is used to encode and decode file types, the secret key is confidently scattered using Shamir's lower limit key exchange protocol, and and at last the backdoor parties affected automated system is used to sustain gifting of encryption keys via clouds. The scheme's prototype is developed in the Programing framework and verified in a simulated cross context.

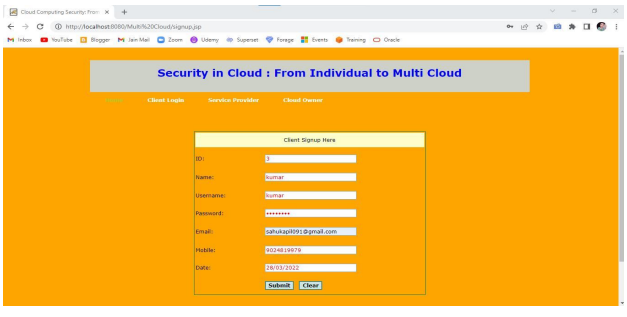
V. IMPLEMENTATION

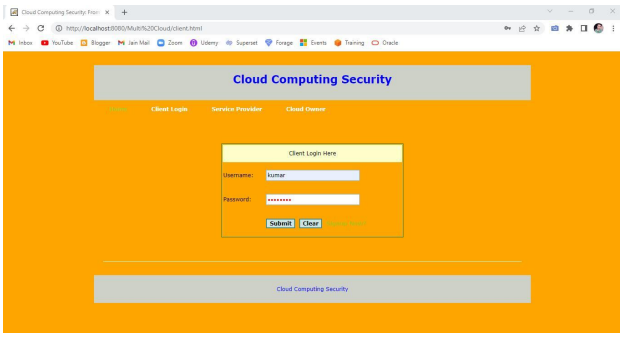
In this paper, we have implemented a system we successfully executed in this system we have use two types of module,backend and fronted. In the fronted part we have used,Javascript, Java frameworks AWT, Springs. We have used Java frameworks like spring,AWT,RMI for the designing of the webpage. Javascript for the authentication and we have used tomcat apache as a server for providing cloud services to online.and we have used database mysql and its connectivity with tomcat apache with the help of javascript.

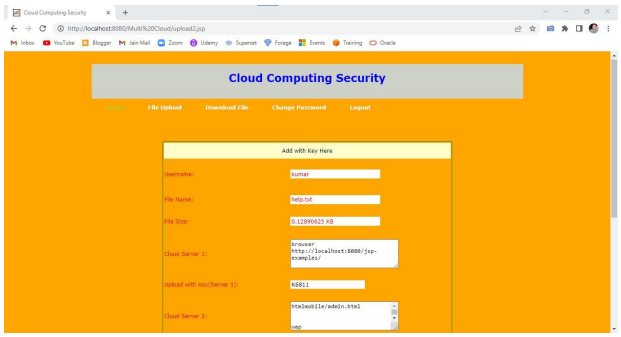
A. Algorithm

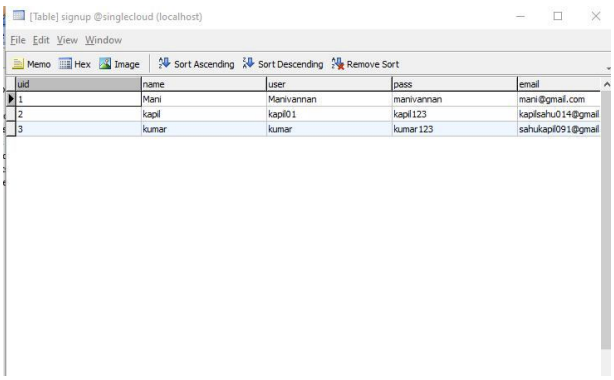
1) *Step: 1* In this step we need to start to Apache tomcat for this we need bin directory we do this in order to start a server in which we will be able to store file and protect in cloud.
2) *Step: 2* In this Navicate Lite for Mysql it is a type of MySQL server which is used to provide database to our program this step help the owner of the cloud to look what are available from anywhere in The world it is on the name as Single cloud that the name we had given to our file in which it is stored and the create a table on it.
3) *Step:3* In this we will go the table we have created that is single cloud from Navicate Lite for Mysql then right click on table then select table single cloud the select the batch file then enter c/singlecloud./open it will connect your data from the NavicateLitefor Mysql and apache tomcat server
4) *Step:4* There we will type its localhost name and then its frontend will open there we will give the username and its password and some more details then if the user is correct it will tell welcome with the username.
5) *Step: 5* In this step click on file upload from the top of the webpage we had used then upload the file and click okay.
6) *Step: 6* In this system the system will automatically divide the file into three server for its security as mention it can we view by cloud owner not user the cloud owner will click on verify and then it will okay.
7) *Step: 7* In this we had cloud user will be able to download only when the cloud owner will be allowed user to download.
8) *Step: 8* In this there is cloud provider the user is the mediator between cloud owner and user it take our verifying the user as well what types of key the user has provided whether it a premium or basic.

B. Screenshot









VI. CONCLUSION

The goal of this paper is to review current findings on single and multi-cloud computing. Encrypted and selective encryption algorithms are two of the most common methods for securing data. In addition, encryption methods were proposed in this paper to make virtualized data secure, highly susceptible, and to give consideration to security risks, issues, and comparisons between AES techniques to discover the perfect encryption method should be used in public cloud to keep virtualized information safe and not be infected with malware by hackers.Encryption techniques are vital for cloud cybersecurity, and an evaluation of several values used in algorithms discovered that the Asymmetric encryption takes the shortest time to process cloud data. The DES algorithm uses the least amount of time to encrypt files. RSA uses the most bandwidth and takes the longest fully encrypt.We discovered that such a lot of study has gone into ensuring the protection of single clouds and file storage, but multi clouds have gained less security attention.

VII. FUTURE SCOPE

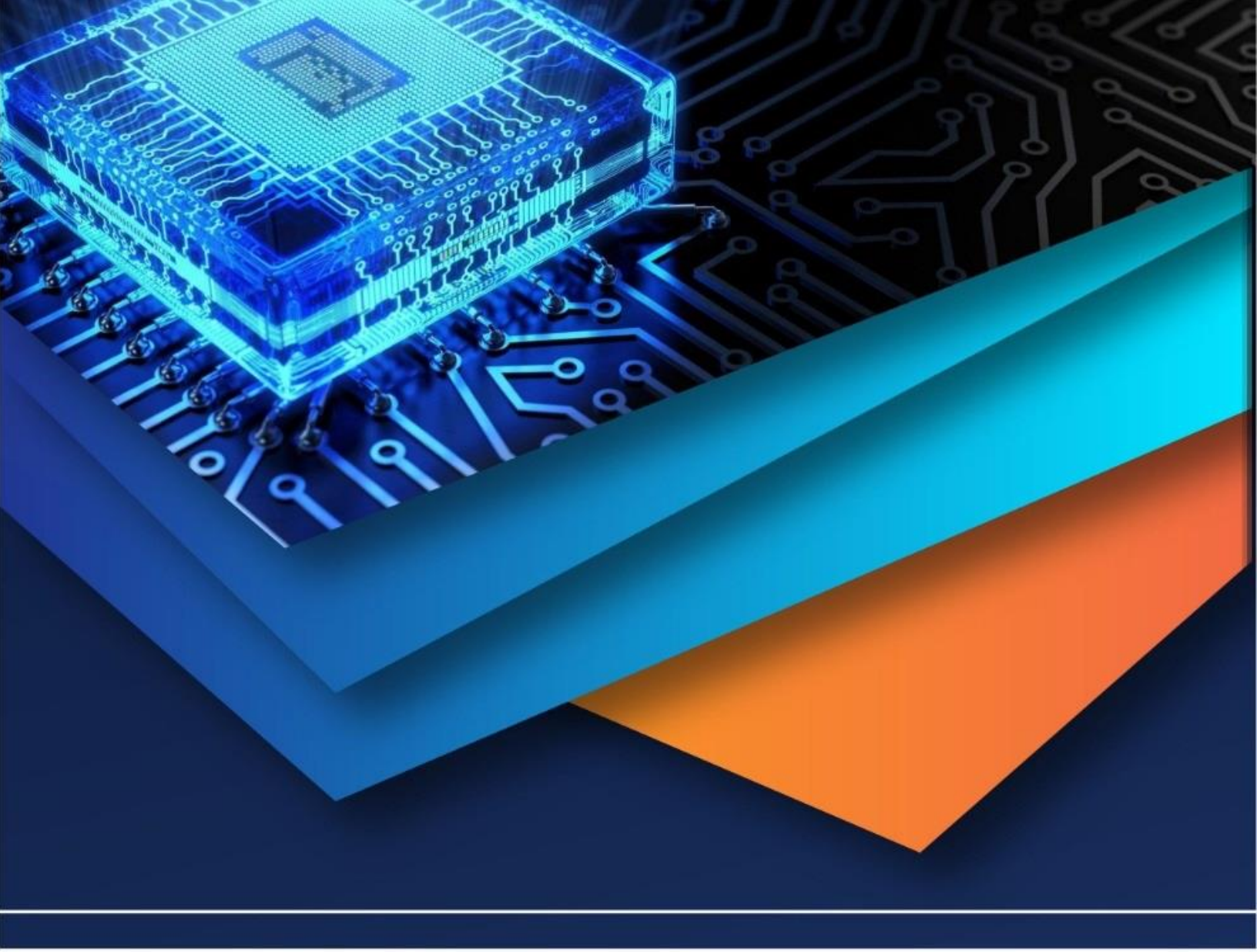
The Future scope this project,Users with destination mobile devices can seek information about their settings at any time and from everywhere with location-based services. While this cloud computing paradigm provides a great deal of utility in terms of information acquisition, it also raises issues about possible suspect into user location anonymity. To ensure user privacy, cloaking user locations into voxels provides a self privacy criteria and transforming location-based inquiries into region-based queries is a common strategy. We identify and solve three new difficulties related to this location cloaking strategy in this work. First, we look at how cloaking regions are represented, and we show that a spherical region produces a minimal result size for region-based searches.

REFERENCES

[1] Sasubilli, Manoj Kumar, and R. Venkateswarlu. "Cloud computing security challenges, threats and vulnerabilities." 2021 6th International Conference on Inventive Computation Technologies (ICICT). IEEE, 2021.
[2] Namasudra, Suyel. "An improved attribute-based encryption technique towards the data security in cloud computing." Concurrency and Computation: Practice and Experience 31.3 (2019): e4364.
[3] Hong, Jiangshui, et al. "An overview of multi-cloud computing." Workshops of the international conference on advanced information networking and applications. Springer, Cham, 2019.
[4] Tomarchio, Orazio, Domenico Calcaterra, and Giuseppe Di Modica. "Cloud resource orchestration in the multi-cloud landscape: a systematic review of existing frameworks." Journal of Cloud Computing 9.1 (2020): 1-24.

[5] Habibi, Moslem, MohammadAmin Fazli, and Ali Movaghar. "Efficient distribution of requests in federated cloud computing environments utilizing statistical multiplexing." Future Generation Computer Systems 90 (2019): 451-460.
[6] Basu, Srijita, et al. "Cloud computing security challenges & solutions-A survey." 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2018.
[7] Ramachandra, Gururaj, Mohsin Iftikhar, and Farrukh Aslam Khan. "A comprehensive survey on security in cloud computing." Procedia Computer Science 110 (2017): 465-472.
[8] Tajammul, M., Parveen, R., & Tayubi, I. A. (2021, March). Comparative Analysis of Security Algorithms used in Cloud Computing. In 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 875-880). IEEE.
[9] Tajammul, M., Shaw, R. N., Ghosh, A., & Parveen, R. (2021). Error Detection Algorithm for Cloud Outsourced Big Data. In Advances in Applications of Data-Driven Computing (pp. 105-116). Springer, Singapore.
[10] Tajammul, M., & Parveen, R. (2020, December). To Carve out Private Cloud with Total Functionality. In 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN) (pp. 831-835). IEEE.
[11] Tajammul, M., & Parveen, R. (2020). Auto encryption algorithm for uploading data on cloud storage. International Journal of Information Technology, 12(3), 831-837.
[12] Tajammul, M., & Parveen, R. (2019). Algorithm for Document Integrity Testing Pre Upload and Post Download from Cloud Storage. International Journal of Recent Technology in Engineering, 973-979.
[13] Tajammul, M., & Parveen, R. (2019). Two pass multidimensional key generation and encryption algorithm for data storage security in cloud computing. International Journal of Recent Technology in Engineering.
[14] S Awad, Wasan. "A framework for improving information security using cloud computing." International Journal of Advanced Research in Engineering and Technology 11.6 (2020).
[15] Zuo, Cong, et al. "Fine-grained two-factor protection mechanism for data sharing in cloud storage." IEEE Transactions on Information Forensics and Security 13.1 (2017): 186-196.
[16] Ritter, Daniel. "Cost-efficient integration process placement in multiclouds." 2020 IEEE 24th International Enterprise Distributed Object Computing Conference (EDOC). IEEE, 2020.
[17] Pei, Xin, et al. "Ensuring replication-based data integrity and availability in multicloud storage." 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD). IEEE, 2016.
[18] Shanthan, BJ Hubert, et al. "TCAMTSA: Time and Cost based Scheduling Algorithm for Multi Cloud Systems." 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS). Vol. 1. IEEE, 2021.
[19] Dou, Yi, and Henry CB Chan. "Access pattern hidden query over encrypted data through multi-clouds." GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE, 2017.
[20] Feng, Kaiying, and Junxing Zhang. "Improving availability and confidentiality of shared data under the multi-cloud environment." 2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA). IEEE, 2017.
[21] Zaveri, Vandik, et al. "Mining User's Browsing History to Personalize Web Search." 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT). IEEE, 2018.

.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY