JCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

A Survey on Cloud Data Security

S.Renuka[1*], N. Suresh Kumar[2]

[1] Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, India
[2] GITAM Institute of technology, Visakhapatnam

Corresponding Author: renuka.csit@gmail.com, Tel.: +91-7731934302

DOI: https://doi.org/10.26438/ijcse/v7i4.8895 | Available online at: www.ijcseonline.org

Accepted: 16/Apr/2019, Published: 30/Apr/2019

Abstract— Dispersed processing is pool of organizations that are provided for customer. Conveyed stockpiling data may be gotten to from wherever at whatever point due to cloud works in remote zone. It manhandles the organizations given by the cloud supplier. There are shifting sorts of cloud benefits particularly, PC code as a Service, Platform as an organization, Infrastructure as an organization, Network as a Service, Identity as an organization. Getting ready models of cloud encapsulate Intra cloud, lay cloud, arrange Cloud and lay cross cloud. By virtue of the organizations of disseminated registering, there's a gigantic measure of learning hold tight cloud .Hence it's required to supply the acceptable security to the information in Clouds. Consequently the conveyed stockpiling has expanded additional thought from each the teachers and mechanical shared attributes. It likewise gets new troubles keeping up learning genuineness and unwavering quality in data accumulating .Deviating the cloud from single to multi-cloud is imperative to accomplish the information security. Multi cloud is very proposed appreciation to the soundness that fragile data shouldn't be dispatched to one cloud, to avoid oppression on only one cloud supplier. Data to be held tight is part into varied squares and scattered among absolutely extraordinary disseminated stockpiling suppliers. To deal with all the outline we will when all is said in done gift an audit paper. This diagram paper relies upon the propelled examination related with single and multi-cloud esteem, security and handiness based generally describe. This work mean to drive crafted by multi spread over single cloud to decrease the vulnerability demanding inside the cloud

Keywords— Cloud Computing, Data Privacy, Multi-Clouds, Security, Confidential Data, Cloud Service Provider.

I. INTRODUCTION

Distributed computing incorporates dissecting and putting away data.It is an electronic model for giving a reasonable domain to share the resources.Cloud suppliers give the applications by means of internet.It is request based system

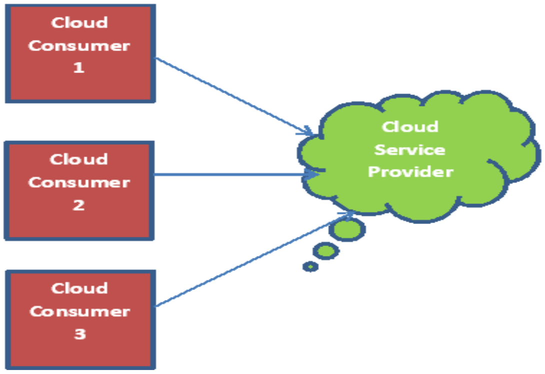

Fig.1 Overview of Cloud computing

Figure 1 describes the overview of cloud computing as follows.

The element of the security issue on appropriated registering is occupied with the SPI exhibit for instance Programming as a Service (SaaS), Platform as a Service (PaaS) and Web as an organization (IaaS) and id discussed in detail in this paper. The Software is the organization given to the customer to using application running on the cloud. The Platform is the organization offered by the master center to present customer's very own application on the authority community's cloud establishment without presenting any additional gadgets and programming on their close-by machines. The Infrastructure is the organization given to the customer to utilize the workplace of limit, taking care of and frameworks organization with the goal that customer can run and send any item or device on this stage.

A. Factors Of Cloud Computing

There are different factors of cloud computing that should be looked into it

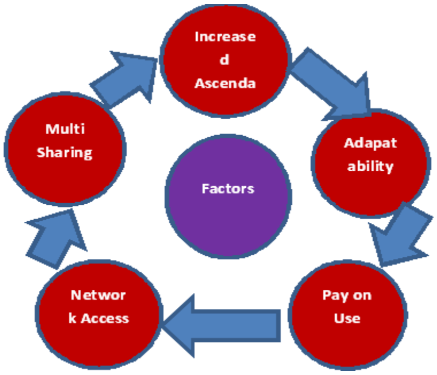

Fig.2 Factors of Cloud computing

Figure 2 describes the factors of cloud computing as follows.

1.Multi-sharing :
It incorporates sharing pool of assets, stockpiling administrations and applications with the co inhabitants remaining on a similar stage.

2.Increased ascendable:
It expands the adaptability as far as space for capacity, transfer speed and so on.

3.Adapatability:
It gives the adaptability in diminishing or expanding the assets on need premise.

4. Pay on use:
Clients will pay dependent on the use of assets on cloud.

5. System Access:
Cloud administrations can be gotten to utilizing pc, PC or portable device.SaaS(Software as a Service)

B. Cloud Service Models:

There are three models

Fig.3 Service Models of Cloud computing

Figure 3 describes the service models of cloud computing. It is explained below.

SaaS(Software as a Service)
It is completely on intrigue application administration. Client can get to databases and application programming's on intrigue or need of customers. It presents and run applications in solitude PCs or in their own server ranches. This discards the expense of hardware getting, provisioning and upkeep, similarly as programming allowing, foundation and backing

PaaS (Platform as a Service)
It is totally on intrigue arrange organization to have costumer application. Stage as an organization (PaaS) is organization in which an untouchable vender gives gear and programming devices. A PaaS provider has the gear and programming without any other individual structure. In this manner, Users need not to present in-house gear and programming to make or run another application.

IaaS (Infrastructure as a Service)
It joins sorting out system organizations, data amassing and handling organizations. The IaaS provider furthermore gives the organizations to run with those establishment fragments. The organizations look like charging, watching, getting to, security, support, replication and recovery.

C. Cloud Formation Models:

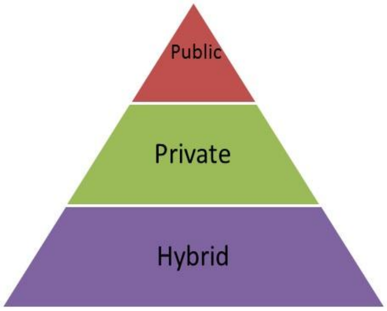

Fig.4 Formation Models of Cloud computing

Figure 4 describes the models of cloud computing .It is as follows

1. Private Cloud:
This is gotten to by the general customers and guaranteed by single affiliation. It suggests a model of disseminated processing where IT organizations are passed on over arranged IT system for the submitted usage of a singular affiliation. It is completely constrained by a single affiliation who has all out bearing over the applications continue running on the foundation, where they run, and the comprehensive network or on the other hand affiliations utilizing it - essentially over each bit of the foundation. A private cloud can be gotten to through web assets.

2. Open Cloud:
A private cloud can be gotten to through web assets. The organizations may be for nothing or on enthusiasm, for instance, CPU cycles, amassing or information exchange limit they use, etc. An open cloud is in a general sense the web and is executed utilizing a commonplace server farm foundation of equipment and programming that is shared by different clients. The server farm is off-premises. Open Cloud master networks use the web to give assets, for

example, applications and capacity to the general people, or on an 'open cloud.

3. Mixture Cloud:
Mixture cloud is a mix of two mists which combines off-premises and on-premises getting to of benefits. In this way, affiliations can profit by versatile IT assets offered by outside Cloud suppliers while keeping express applications or information inside the firewall. A blended Cloud condition fuses multifaceted nature concerning the vehicle of jobs transversely over various conditions, seeing of within and outside foundation included, security and protection, and may as such not be reasonable for applications requiring complex databases or synchronization.

II. ADVANTAGES OF CLOUD

It is advantageous in terms of
It is invaluable as far as

Organization:
1. Programming can be gotten to effectively
2. Recuperation of Data should be possible effectively.
3. Administrator work can be diminished.
4. Organization is done rapidly

Cost
1. Capital Investment isn't genuinely necessary.
2. Rather Capital costs can be changed to working costs.
3. Less IT Staff is required.

Organization
1. Joint effort is improved.
2. It is anything but difficult to have an association with different associations.

Information
1. Information is verified in the cloud.
2. Client's information will be leveled out of cloud specialist co-ops.

As Cloud Computing has picked up considerations from all association, there are potential Security Concerns in Cloud Computing which should be tended to. This incorporates Outsourcing,

Shared Responsibility, Virtualization, Multi-tenure, Service Level Agreement.

D. Issues in Cloud Computing:

1. Data capacity
Normally cloud specialist organizations give stockpiling as an administration (SAAS).They get the information from the client and set in the server farms which implies a capacity administration. Yet, the issue is whether the information which is put away in the cloud ids safe or not. Since we have a few issues where the information is lost because of security openings.

2. Data Security
There are a few situations where the information is left amid exchange from neighborhood server to cloud .It causes the security risk in distributed computing.

3. Data Integrity
Information trustworthiness is one of the basic issues in distributed computing. Since it guarantees that the information is of value, and verified. In any case, it might get flopped as the information may get modified or erased.

4. Cost
Cost is likewise one of the serious issue in distributed computing. Here the information estimate is legitimately relative to the expense in light of the fact that the more the information is put away the more sums the client needs to pay. There is another issue that putting away the information in single cloud.

III. LITERATURE SURVEY

Emir Erdem et al.[1] proposed a cloud based OTP architecture which includes three modules namely User, Service Provider, Cloud Based OTP Provider. Here user enrolls and logins into the system with username, password, OTP. These three are sent to the service provider and then sent to the cloud provider. Then cloud will matches the OTP of the user with its file. Then the login will be successful.

Yucai Zhou et al.[2] proposed a new architecture in which the data is collected and categorized into two models. One is cloud layer which handles all core information and the other one application layer which takes care about the virtualization process. It creates highway platform the cloud is splitting into many computable units through a network and analysis is based on data.

Himel Dey et al.[3] proposed a new model on integration of cloud security with multi tenanacy.In this model new server is included for distributing keys to the users.This server handles two servers one is for authentication and the other is for giving ticket to the user for further procedure.A main server called file server which provides the resources by taking Ticket from thr user.To get that ticket user has to register and request for the ticket from distribution server.After verifying ticket the resources will be allocated to the user.

HONGBO LI et al.[4] proposed a Identity Based Encryption with Flexible Authorization which provides more efficiency in filtering the encrypted data with the respective keys. It has modeled with four levels of authorization. One is to compare the encryption between any users on the cloud. Second level includes comparison of cipher text of any users on the cloud. Third Level tells the comparison of cipher text of specific user. Fourth is hybrid approach.

Andrei Tchernykh et al[5] proposed multi cloud based storage system which is called weight access scheme. Though this model information loss got reduced a lot .Based on the weight of the key the resources will be saved.

Prof. Amit R. Gadekar et al[6] proposed a model to classify the data into categories based on the importance of the data. The data is categorized into three levels high level, medium level, low level. The encryption will be done based on the level of the data. The encryption will be more secured for the high level data, no encryption will be done on for the low level data.The data is segmented into either horizontal or vertical.

Jayachander Surbiryala et al.[7] extended the exisisting model by extending with a new module called User Shredder Module(USM).This is used in some scenarios like when the user wants to shift from one provider to other provider in the cloud then all the services should be stopped.Before stopping the services the data of the user should be used by other users.SO USM will be used to change the data of the user into unrelated information.

Talal Halabi et al[8] proposed a new model of allocation of resources satisfying the security parameters(C,A,I). It is used to provide the security satisfaction to the users' requests and assigning the requests to the appropriate data centers, which will then perform the internal distribution of resources and workload management according to other parameters such as physical servers' resource capacity, power efficiency, and load balancing.

D. N. WU et al. [9] proposed verifiable public key encryption in which it has four modules namely Key generator, cloud server, clients and Data Holders. Key generator is responsible for creating the encrypted keys based on requirements. Data Holders are responsible for handling the confidential data and then sent to the authorized users. Cloud Servers maintain a huge amount of data that should be shared among the users based on searchable cipher text. Users should register for the keyword encryption for to search for the specific files.

Jianyi Zhang et al.[10] proposed a work on Searchable Asymmetric Ciphertext (SAC) which can be used in Multi Data Holders (MDH).Here there will be multiple data holders who want to sent their the data to the specific user. Before sending the files to the user MDH should create their privacy based searchable indexes for respective files.If the user wants to search for the file he has to enter the trapdoor (which is encoded version of keywords to search) then the cloud server will match with that keyword and the result will be given to the user.

Mohd. Aman Kalyankar et al.[11] proposed a trusted cloud computing platform where the manual work is transformed into digital where all the documents are uploaded into the cloud for the digital process.Instead of working in a physical way working with digital way is more easily accessible.

Mu Yang et al.**[12]** proposed a block chain-based privacy and preserving of data.It does not allow the outsourced services like providing own privacy services, tracing the sharing services etc.It mainly concentrates on storing and verifying the data and then assigning the budget assumptions through independent block chain contracts based on the data owner requirements.

Nikhil Shrivastva et al[13] Cloud provides many benefits in terms of cost and accessibility of data. Providing **security** to the data which is uploaded by the user is a **major** factor. Users will store the confidential data in the cloud which is being handled by the third party people called as Service Providers….untrusted. The data will be stored in a **Single cloud** which is risky in terms of security as well as server crashes. To overcome this problem A movement of **clouds–of-clouds** has started. The **solution** is data is distributed and replication for storage and retrieval on multiple clouds. Here the user will get registered then uploads the data on cloud which is distributed on three cloud servers. After uploading the data respective keys are being generated from respective clouds and a generalized key is encrypted using byte substitution encryption technique. This encrypted key is then provided to the user/client. For downloading the same data from the servers, the client uses the encrypted key which is decrypted and the three keys are again generated and are being given to clouds and the data is retrieved.

P. Raja Kaushik et al [14] provides confidentiality for the messages in storage servers user has to encrypt his message by using some cryptography methodology. After that user has to apply associate erasure code methodology to encode and store messages. When he needs to use the message he must retrieve the code word symbols from storage servers and then rewrite them. Here there are three issues raised. First one is User will create more communication and computation traffic between users and servers. Second one is user has to manage cryptographic keys i.e; If user lost his device of cryptographic keys then safety will be broken.SO storage servers cannot directly support different functions. That means one user's message cannot be directly forwarded to another user by storage servers. The owner of messages should retrieve, decode, and rewrite so forward them to a different user. In this paper, we are proposing to address the matter of forwarding information to a different user by storage servers directly below the command of the information owner. Since storing cryptologic keys in a very single device is risky, a user distributes his cryptologic key to key servers that performs cryptographic functions on behalf of the user which is protected by security mechanisms. To work with the distributed structure of systems, we need servers perform all operations many times. With this thought, we propose a brand new threshold proxy encryption theme and integrate it with a secure localized code to make a secure distributed storage system. The encoding theme supports cryptography operations over encrypted messages and forwarding operations over encrypted and encoded messages.

Dayanand Sagar Kukkala et al[15] proposed an architecture called as **Information-centric security architecture** to overcome these security concerns. The existing problems are **cheap data analysis**, **cost-effective** and **increased authentication demands**.SO the proposed system is **Developing Information centric security** framework for cloud computing to minimize all these problems. Below is the example for how the **Information centric security framework works for a pharmaceutical company**.

The chief scientist will hire a university professor as a part time consultant. He is given access to confidential documents for review. Since these documents should be kept as top secret documents, stored and transmitted in cipher text. Below are the steps for architecture

1. The policy created for access/usage rules for “Top Secret” documents.
2. Document is classified as “Top Secret” and tagged accordingly
3. University professor hired as consultant and given access to “Top Secret” document
4. An encrypted copy is sent to the professor with authorization rules. Professor can only read the document while the chief scientist is allowed to save it to a flash drive.
5. After 30 days, the professor’s local encryption key is destroyed and he can no longer access the file.

Mohamad Reza Khayyambashi et al.[16] proposed a new cloud which is been divided in two categories one **is Cloud by Personal Access** which is used to save personal data and **Cloud by Group Access** which is used to work at different levels accessing for data. This is used by organizations who can put their data for their employees to read edit the data.

Maha TEBAA et al.[17] proposed a needed technology which became popular for sharing resources, maintenance etc. But there is never ending problem with the **cloud security.** There is a problem with data transfer security. When the data is being transferred to the cloud we use encryption methods to secure the and store data. But to process the data on a server, the cloud provider need to access the raw data which is untrustworthy. In this we propose a method of executing the operations on encrypted data. We are introducing the concept of Cloud Computing and the necessity to adopt Homomorphic Encryption to secure the calculation of data hosted by the Cloud provider. The Homomorphic Encryption method is able to perform operations of encrypted data without decrypting them.

IV. PROPOSED WORK

A. Multi Cloud

Multi cloud alludes to mix of different mists from the numerous cloud suppliers.

It has a capacity to choose distinctive cloud administrations from various cloud suppliers dependent on the client's information. Multi-cloud is the place an affiliation use something like two dispersed processing stages to perform distinctive errands. Affiliations that would lean toward not to depend upon a lone cloud provider may use resources from a couple of providers to get the best preferences from each remarkable organization..

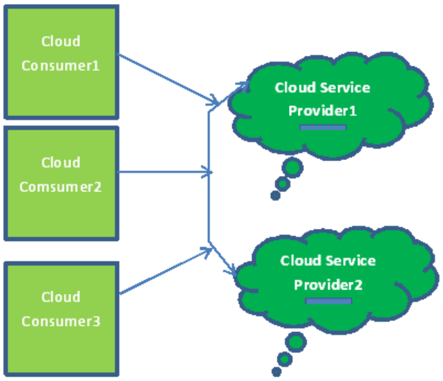

Fig.5 Overview of Multi Cloud

Figure 5 describes the overview of multi cloud computing as follows.

B. Analysis of Multi-Clouds

Multi mists approach is a distributed storage engineering that builds a virtual cloud by consolidating distinctive Cloud stockpiling administrations. Information put away will be separated into different squares and conveyed them among various distributed storage suppliers in a repetitive way.To dodge reliance on a solitary cloud supplier Multi mists is profoundly required. The reason that the client can't believe a solitary cloud information to store the information. Henceforth exchanging the distributed computing from single to multi is basic for the information security.

Here the customer information (C1 ,C2,C3) is isolated into parts, put away in Cloud An and B and the metadata is put away in a private cloud.

The accompanying table demonstrates the diverse strategies utilized in multi cloud Data

Table 1: Literature Review.

S.No	**Method**	**Author Name**	**Implementaion**	**Benefits**
1	Homomorphic Encryption	Mark D.Ryan etal.	High authentication level,High Security through auditing the data,Robust Data Sharing with Key.	Data Security is achieved.
2	CP-ABE/KP-ABE	Sherif H. Nour El-Din	KP-ABE and CP-ABE. KP-ABE enables data owner to encrypt a given message using specific attributes	Enables the data owner specific data user without affecting other existing users
3	Identity-Based Broadcast Encryption (IBBE)	Ling Liu	Usage of convergent encryption (CE) and ID-based broadcast encryption (IBBE)	It assures the confidentiality of data files and the security of convergent keys.
4	ID Crypt	GUOFENG LIN	Searching the encrypted data and shared that encrypted data among users.	Improves the security strength and efficiency of searching
5	Hierarchical Identity Based Encryption	Yang et al	Implemented for decryption and revocation	Improves the efficiency of In-cloud Storage
6	**SecRA**	Yun Tian et al.	Uses Shamir Secret key alogorithm for data integrity,confiedentiality.	Improves the security,reliability and performance of cloud storage
7	Trust management	Weijuan Fan et al.	It distributes the group of Trusted Service Providers	Improves the multi-cloud trust
8	Multi-Agent System (MAS)	Amir Mohamed Talib et al	Providing interaction on a cloud network	Provides a security framework
9	Distribution based, Cryptography based and Hybrid based solutions	Tara Salman et al.	It is implemented for security	To strengthen the multi-cloud security
10	Message locked Encryption (MLE)	HassanO. Karame et.al.	Fault tolerance protocol	Cloud Data Security is achieved.
11	CHARM	C. Divya Shaly et al.	Data Hosting Scheme	It is cost efficient
12	DEPSKY	Ouadia Zibouth et.al	Implements convergent encryption to encrypt user's personal data with a unique key.	High efficient encryption is applied.
13	Shamir Secret	M.Muhil et al.	Storing the data in multiple clouds and encrypt them before transferring.	To reduce the risk of data attacking
14	SDSMC Framework	F.Leo John et al.	It implements file splitting, encryption, decryption and merging.	To reduce the risk of process tampering.
15	DTBAC	R.K. Banyal et al.	Feasible Access control solution for cloud.	TO deter the risk of unauthorized activities.
16	EPDP	A. Manimaran	Data integrity verification	Improves the scalability service.

V. CONCLUSION

There are different methods to look into the security of multi cloud. Each approach discusses briefly about the algorithm used and the architecture needed to enhance the security. The purpose of this work is to overcome the security issue related with single cloud as well as multi cloud. Much research has been done on the single cloud and more research is going in the area of multi cloud to overcome the security issue as well. It is observed that Multi-Cloud is one of the best scheme can be used in solving or managing the cloud security issues.

REFERENCES

[1] Emir Erdem and Mehmet Tahir Sandıkkaya , Member, IEEE," OTPaaS—One Time Password as a Service", IEEE Transactions On Information Forensics And Security, Vol. 14, No. 3, March 2019.

[2] Yucai Zhou ; Kejun Long ; Peng Xu ; Wang Liu, ," Design of a Cloud Platform for Digital Highway", International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS), March,2019.

[3] Himel Dey , Rifat Islam ,Hossain Arif," An Integrated Model To Make Cloud Authentication And Multi-Tenancy More Secure", 2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST), February,2019.

[4] Yucai Zhou, Kejun Long ,Peng Xu , Wang Liu, ," Authorized Equality Test on Identity-Based Ciphertexts for Secret Data Sharing via Cloud Storage", **IEEE Journals & Magazines**, volume 7, Page s: 25409 – 25421, February,2019.

[5] Andrei Tchernykh ,Mikhail Babenko , Vanessa Miranda-López, Alexander Yu. Drozdov , Arutyun Avetisyan," WA-RRNS: Reliable Data Storage System Based on Multi-cloud 2018 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW),August,2019.

[6] Prof. Amit R. Gadekar, Dr. M V. Sarode, Dr. V M. Thakare," Cloud Security and Storage Space Management using DCACrypt", International Conference on Information, Communication, Engineering and Technology (ICICET),August,2018

[7] Jayachander Surbiryala, Bikash Agrawaly, Chunming Rong," Improve Security over Multiple Cloud Service Providers for Resource Allocation", 1st International Conference on Data Intelligence and Security,2018

[8] Talal Halabi, Martine Bellaiche, and Adel Abusitta," Online Allocation of Cloud Resources based onSecurity Satisfaction, 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering",2018

[9] D. N. WU, Q. Q. GAN, AND X. M. WANG," Verifiable Public Key Encryption With Keyword Search Based on Homomorphic Encryption in Multi-User Setting,IEEE Translations,Vol.6,August,2018.

[10] Jianyi Zhang, Chenggen Song, Zhiqiang Wang, Tao Yang And Wenming Ma, "Efficient And Provable Security Searchable Asymmetric Encryption In The Cloud",IEEE Translations,vol.6,December,2018

[11] Mohd. Aman Kalyankar, CRS Kumar, "Aadhaar Enabled Secure Private Cloud with Digital Signature as a Service", 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018) IEEE Conference Record # 42487,2018.

[12] Mu Yang, Andrea Margheri, Runshan Hu, and Vladimiro Sassone, "Differentially Private Data Sharing in a Cloud Federation with Blockchain", Copublished by the IEEE CS and IEEE ComSoc,November/December 2018.

[13] Mohamad Reza Khayyambashi,Sayed Mohammad Hossein, Mirshahjafari, EhsanShahrokhi, , "Design And Implement A New Cloud Security Method Based On MultiClouds On Open Stack Platform" ,David C. Wyld et al. (Eds) : CCSEA, CLOUD, DKMP, SEA, SIPRO – 2016.

[14] C. Divya Shaly, R. Anbuselvi, " Multi-Cloud Data Hosting for Protection Optimization and Security"-International Journal of Computer Science and Mobile Computing. April 2016.

[15] A. Manimaran and K. Somasundaram."An efficient Data Security Mechanismin Cloud Computing Using Anonymous ID algorithm. 2016.

[16] Ms Vrushali K Gaikwadl, Prof. Ramesh Kagalkar. "Data Security & Availability in Multi-clouds Storage with Cooperative Provable Data Posession".–IJES February 2015.

[17] Yun Tian, Xiao Qin, Yafei Jia." Secure Replica Allocation in Cloud Storage with Heterogeneous Vulnerabilities",IEEE

[18] Tara Salman. "On Securing Multi-Clouds: Survey on Advances and Current Challenges", Nov 2015.

[19] Ms Vrushali K Gaikwadl, Prof. Ramesh Kagalkar. "Data Security & Availability in Multi-clouds Storage with Cooperative Provable Data Posession".–IJES February 2015.

[20] Maha Tebaa, Said El Hajji, " From Single to Multi-Clouds Computing Privacy and Fault Tolerance". Elsevier 2014.

[21] P. Raja Kaushik1 , G. Praveen Bab," Data Security Issues in Distributed Cloud System", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.9, September- 2014, pg. 357-360.

[22] Farrukh Shahzad, " State–Of–the–art Survey on Cloud Computing Security Challenges, Approaches and Solutions". Elsevier 2014.International Journal of Pure and Applied Mathematics Special Issue.

[23] He Kai, Huang Chuanhe, Wang Jinhai, Zhou Hao, Chen Xi, LuYilong ZhangLianzhen, Wang Bin, Computer School, Wuhan University, Wuhan, China "AnEfficient Public Batch Auditing Protocol for Data Security in Multi-CloudStorage"-IEEE/978–0-7695–5058-9/13 2013

[24]Cong Wang,student member,ieee,Qian Wang,student member,ieee, Kui Ren,member,ieee,Ning Cao,student member,ieee and Wenjing Lou,senior member,ieee,"Towared secure and dependable storage in cloud computing" 2012.

[25]Maha Tebaa ; Said El Hajji ; Abdellatif El Ghazi," Homomorphic encryption method applied to Cloud Computing, National Days of Network Security and Systems,2012.

[26] Yashaswi Singh,Farah Kandah,Weiyi Zhang," secure cost effective multi cloud storage in cloud computing"2011.

[27] A.Bessani, M. Correia, B.Quaresma, F.Andre and P.Soura "Depsky:dependable and secure storage in cloud computing."2011.

[28] E.Grosse, J.Howie, J.Ransome, J Reavis and S.Schmidt, " Cloud computing roundtable", IEEE Security & Privacy,8(6),2010.

[29]W.Itani, A.Kayssi, A.Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures" Eight IEEE International Conference on Dependable, Autonomic ans Secure Computing,Dec 2009.

[30] R.Gellman, "Privacy in the cloud: Risks to privacy and confidentiality from cloud computing",Prepared for theWorld Privacy Forum Feb 2009.

[31] B.R.Kandukuri, R.V.Paturi and A.Rakshit, "Cloud Security Issues," 2009 IEEE International Conference on Service Computing, 2009.

[32] Scalable Security Solutions, Check Point Open Performance Architecture, Quad-Core Intel Xeon Processors,"Delivering Application-Levels Security at Data Centre Performance Levels,"Intel Corporation, 2008.

ABOUT AUTHORS

S.Renuka is currently working as an Assistant Professor in Information Technology Department, Gokaraju Rangaraju Institute of Engineering & Technology, Hyderabad. Currently She is pursuing Ph.D.(C.S.E) in GITAM,Vizag. She has 6 years of experience in current college. She has total 7 years of teaching experience.

N. Suresh Kumar is currently working as an Assistant Professor in Information Technology Department, GITAM Institute of Technology,Vizag .He was awarded with Ph.D. in Andhra University in the year 2018.He has total 17 years of teaching experience