Providing Confidentiality, Integrity and Atomicity for data storage in the cloud storage: A Survey

Akanksha Bansal
Research Scholar, M.tech (Computer Science& Engineering)
ITM Group of Institutions, Gwalior (M.P.), India.

Arun Agrawal
AssistantProfessor, Department of Computer Science & Engineering
ITM Group of Institutions, Gwalior (M.P.), India.

Abstract –Cloud computing is only of the most growing area of research, there are lots of work in cloud like security and data base. In this paper we study about cloud architecture or cloud security concerns and their solution at the completion of paper we compare DES or RSA and then compare the result.We propose a secure the Cloud means secure the treatments and storage "databases hosted by the Cloud provider". Security goals of data include three points namely: Confidentiality, Integrity, and Availability (CIA). Confidentiality of data in the cloud is accomplished by encryption/ Decryption process.

Index Terms –DES;RSA;NAS;EC2;SaaS;PaaS;IaaS

1. INTRODUCTION

Cloud computing is a set of IT (information technology) facilities that are provided to a customer above a network on a lease basis and through the capacity to scale down or up their service requests. Usually cloud services are delivered by the intermediary provider who owns the infrastructure. It is a ideal for conveying calculate and storing resources on demand. The fundamental theory of the cloud is to available a platform for sharing funds which contain infrastructure and software with the assist of virtualization in order to provide quality of service, this environment make attempt to be reliable and dynamic.

Cloud storage is a significant service in the cloud computing, which allocate individuals with companies to keep their data in the cloud computing. Like that (Amazon S3) It is provide storage as a service (Saas). Cloud storage is provides a equivalent lower investment expenditure, on demand service, locality self-sufficient service to the users. Yet this service of cloud storage also suffers from various security challenges and issues. The cloud comes with many challenges and issues for the causes that are "Lack of control" and "Lack of trust". The Users are giving their data to the cloud computing which is not the reliable one and so data can be changed, detected, stolen or also corrupted. Some of the recently data loss events occur that are associate cloud disaster in 2009 and the break of (EC2) Amazon Elastic Computing Cloud.

In spite of the major benefits that cloud computing has, there are still various other security concerns like as confidentiality and data integrity. In the growth of the cloud raised lots of query about risks and data security upon data expose; thus, cloud storage provider should make sure confidentiality, data availability and integrity.

Cloud computing are in three kinds for example Infrastructure as a Service (IaaS), Platform as a service (PaaS), Software as a Service (SaaS).The SaaS is provides application software It is used by the user. The PaaS provides computing platform to do his development for the user It is used by developers and deploys. The IaaS provides virtual or physical devices for user.

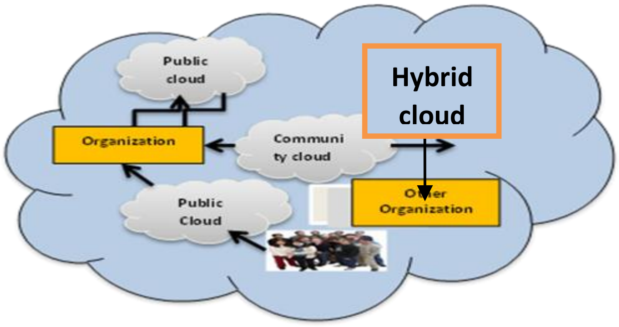


Figure 1: Deployment model

The cloud is available in four-deployment model namely.

1. Public Cloud

2. Public Cloud

3. Community Cloud

4. Hybrid Cloud

1.1Public Cloud

It is managed by the single organization. It is hosts the file by the third party and it is also called on premise and internal cloud

1.2Private Cloud

It is manage by the government organization or combination of them and may be owned this is also called as multi-tenant or external cloud

1.3Community Cloud

It is refer to an special purpose cloud environment which is managed and shared by lots of associated organization participating in a vertical market or common domain.

1.4Hybrid Cloud

It is the permutation of the two or more cloud private, public and community cloud is called hybrid cloud.

2. RELATED WORK

In this section, we existent counter measure solutions that have been proposed in the conferences and scientific journals pertaining to securing for the data storage in the cloud computing.

Pawar et al. (2014) have proposed that extensively emerging technology in the recent years in adopted by most of the organizations and IT industries. It is stored huge amount data by the user in the LAN may cost the user heavily. We use various electronic storage device like file servers, SAN and Network Area Storage (NAS) which available high performance and many valuable aspects to the user however, the electronic storage has several disadvantages like it life time is less require or cost further and data in the virtual pool hosted by the TPA. In this paper we provide method to save our data in cloud storage secure and provide an integrity check for our data to verify if integrity is preserved or not whereas we retrieve our data.

*Al-Jaberi et al. (2014)*have proposed that presented a model that keeps confidentiality, integrity and data privacy. The main weakness of surviving data integrity inspecting techniques is that they introduce privacy gaps through integrity checking. In this paper introduced a model to facilitate attends to privacy preservation and data integrity confirmation simultaneously. Cloud computing is the future technology of cloud computingand it has three most important security features which are Confidentiality, Availability and Integrity.

Choubey et al. (2015) have proposed that a rapid encryption solution that should be altered in every piece of the cloud and also provide entire solution of the data security & (SaaS) security as a service . Cloud computing is a network base technology as security concerns like as data security confidentiality, privacy etc. are encountered. It has a numbers of users, who are via cloud computing conveniences like email, file sharing, social network, and others which are raising the data load in cloud storage usually. It is also increasing the risk of data susceptibility.

*Kumar et al. (2015)*In this paper have proposed designed a cloud storage context (framework) that make available safe data outsourcing and retrieval of client data to authenticate the integrity of the data. We developed a cloud storage context (framework) has checked for real time data sets. The framework has checked for security, confidentiality and availability. Further, the security setup also tested against required parameter of time complexity and space. The storage framework and meets our initial parameter to meet end to end protection of the client data. But this type of security framework best archival of data.

Vaid et al. (2014) demand of falling the computing cost has led the novelty of the cloud computing. With the rising number of companies restoring to utilize resources in the cloud computing, security of the users' data is becoming a main issue of concern. This research plan is a focused on user performance founded anomaly detection for malevolent activities in case of illegal transactions or unauthorized access above cloud data. In order to attain vastly protected transactions in future, the scheme can be extended to implement the detection for network actions with many others applications at “Saas” layer of Cloud.

*Mittal et al. (2014)*This paper proposed a process to solved the privacy issues of the cc. It assume that the user data is share on two hosts and performs a connected k-means clustering use the Pallier Holomorphic encryption system for the safety purpose in order to avert any interpretation of intermediary results by an attacker. We proposed a secured k-means data mining method assume the data to be shared between diverse hosts preserving the protection of the data. The approach is capable to retain the accurateness and validity of existing k-means to generate final results even in the shared environment.

Shanmugakani et al. (2015) we tested the difficulty of the data security in the cloud data storage. We used the explicit integrity verification scheme, which reduces the data block confirmation, the quantity of computation on the server or client and also no require using Third Party Authority. Our design meets the focus of the data security and the data integrity conformation (verification) and Since of the easily interactions, our scheme can be executed quietly and efficiently. We proposed a new scheme to achieve integrity objectives and we explore how to authenticate the integrity and accuracy of the data storage in the cloud computing. The single feature of this scheme is finding out which data portion is changed or attacked by the malevolent user.

Kaur et al. (2014) we proposed a security model, imply cloud storage security, which provides security base on diverse encryption algorithms with integrity verification method. We start with the storage division selection phase divided into three diverse sections Private, Public and Hybrid mention in cloud analyst sections Private, Public, and Hybrid mentioned in Cloud Analyst to constrict the stage of many encryption techniques are implemented in all three sections founded on the security sections things namely confidentiality, security, integrity privacy, authentication and nonrepudiation. Unique token generation mechanism implemented in Private section helps to make sure the authenticity of the user.

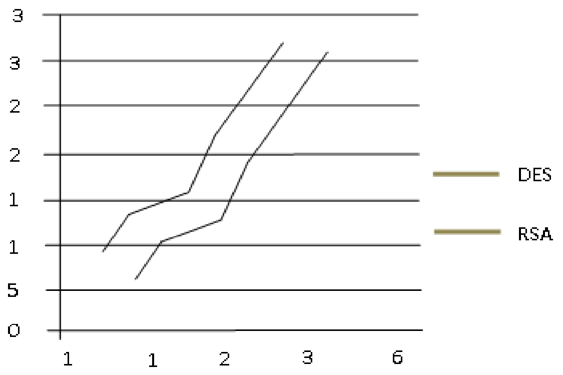
*Malviya et al. (2015)*we proposed a novel approach which is founded on Explicit Exact Minimal Storage Regenerating Code by hash function which provides Integrity, Reliability and Availability. We proposed a novel approach founded on EEMSR through cryptographic hash to ensure Integrity and Availability of the data stored in the cloud computing. From the security analysis we have shown that our approach is secure sufficient from many kinds of attack at last this approach build the storage service of the cloud computing more secure by ensuring Integrity Availability of the data stored in the cloud with less running time overhead. This data storage service introduces security challenges, such as reliability of the data and Confidentiality, Integrity and Atomicity.

Table.1 the comparatively study

Author	Proposed Soln.	Algorithm
Pawar	We save our the data in the cloud storage secure	RSA Algorithm
Al-Jaberi	Address data integrity verification and privacy preserving simultaneously	MD5, AES and RSA
Choubey	Fast encryption solution & Comp solution of data privacy &security, as a security	(Encrypt & Decrypt techniques)
Kumar	Design a cloud storage framework that provide secure data outsourcing sourcing	SSL , PBE , MAC
Vaid	Anomaly based unauthorized access or illegal transaction	BOAT Algorithm
Mittal	We sol. privacy issues cloud using Homomorphic encryption	Homomorphic encryption
Shanmungkani	We testing a problem of the data secure in cloud storage using explicit integrity verification	Explict integrity verification
Kaur	A security model is planned implemented in cloud analyst	Novel Encryption Techniques
Malviya	EEMSR through cryptographic hash to ensure Integrity and Availability data stored cloud	Exact regenerating code

In my propose work we use DES (Data Encryption Standard) algorithm for security issue and my base paper use RSA (Rivest-Shamir-Adleman) for security issues. Both are cryptographic Algorithm. In this graph represents a comparison between DES and RSA encryption algorithm.

Graph 1. Comparison between DES and RSA



3. DATA MINING ROLE IN CLOUD COMPUTING

In the Cloud Computing the data mining permit administrations to centralize the managing of the data storing and software. By data mining throughout Cloud Computing reduce the barriers that keep small industries from advantage of the data mining instrument. Data mining in the Cloud permit administrations to centralize the administration of the data storage and software, with reliable, secure service and assurance of capable, for their users. The techniques of data mining implementation over Cloud Computing will permit users to get back meaningful information from virtually incorporated data warehouse that reducing the charge of storage and infrastructure.

In the cloud computing "DM Cloud" cloud data mining offer tremendous prospective for analyzing and extracting the valuable information in many fields of human activities: economics, business, biology, health care medicines, pharmacy, advertising, heredity etc. This technology are use should permit that with just a little click of the mouse one can achieve the chosen information about behavior, clients, purchasing power, welfare and uniformity of purchases assured items and so on. Data mining Cloud is, from technical point of sight, a very dull process that needs a unique infrastructure based on application of processing, new storage technologies and handling.

In the cloud computing model are desperately required data mining applications and techniques. Since cloud is petering increasingly in all ranges of scientific computing and business it become a big area to be purposeful by data mining. "Cloud computing denote the novel trend in internet services relay on clouds of servers to handled task. DM in the cloud computing is the method of extract structure information from un structured or semi structured web data causes. Data mining is described as a "type of database" analysis that efforts to determine useful relationships and patterns in a group of data. The analysis used superior statistical process, such as at times employs artificial intelligence, cluster analysis or neural network (NN) techniques.

Data mining is individual of the rapidly developing field in computer industry that agreement with discovering patterns from huge data sets. It is the part of (KDD) knowledge discovery of database process and is utilize to extract human being explicable information. Mining is preferably use for a large quantity of the data and associated algorithms often need vast data sets to produce quality models.

The relationship between cloud and DM is value to discuss. Cloud providers used data mining provide customers better service. If customers are uninformed of the information being composed moral issues individuality and privacy are desecrated. This can be critical data privacy issues if the cloud providers exploitation information. Yet again attackers exterior cloud providers containing illegal accessed to the cloud, also contain the chanced to extract cloud data. In this mutually cases, invaders can use low-cost and uncooked computing power provide by the use of cloud to extract data and hence obtain valuable information from data. In the cloud data mining permit administrations to centralize the managing of the data storage and software with assurance of well-organized consistent and safe service for their user.

In the data mining the major effect of the data mining tools being deliver by Cloud are the clients imply pay for data mining tools that he requirements - that reduce his costs As he does not have to paid for compound data mining suites that he is not using in-depth. The customer does not have to retain a hardware infrastructure, as he may apply data mining through a browser that means he has to pay only expenditure that are produced by using Cloud computing. Data mining using through Cloud computing reduce the barriers that maintain small industries from advantaging of data mining tools. Data mining task consist of: Detect Types Fill from example, Analysis Key Influencers, Highlight Exceptions, Shopping Basket Analysis, Forecast, Scenario Analysis, and Prediction Calculator.

It is used to exploration important patterns of data from large quantity of data In the cloud famous areas in the Data mining are and regular pattern mining and association pattern mining etc. In the cloud computing cloud stand for network or Internet. In other words which is current at the remote location It services are provide available on VAN, LAN or WAN. Like as email, web conferencing etc. The relationship between data mining and cloud computing have their own pros and cons. Two causes are involved of data interaction one is appropriate quantity of the data and other is suitable mining algorithms. There are lot of mining algorithms which are useful to interact with private data and thus threat to data security. Like that association rule mining algorithms may be used business transaction records.

4. CLOUD SECURITY ISSUES & CHALLENGES

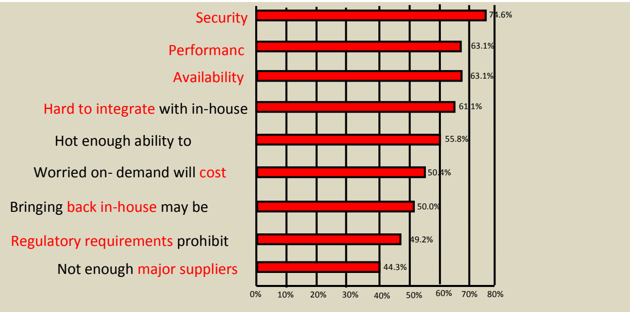


Figure 2: Study of major issues of the cloud computing

In the cloud computing lots of security concerns as it encompass various technologies contain resource allocation, virtualization ,traditional management database, cloud networks, OS, memory management and concurrency control For example, In the cloud network security that to be linked the systems in the cloud has to be safe. Virtualization paradigm in the cloud computing outcome in various security concerns. For example, the protection of the network that be linked the systems in the cloud computing must be much secured. Also, containerization and virtualization paradigm in cloud bring about various security concerns. Such as, the mapping of containers and VM to the physical machines has to be done in a secured way.

Clients use the entire services which are server oriented and all methods have to be entire on the server Due to server computing, entire data of client is saved at server which can be known as data center. However, some issues may be growing in the regular of security. Access control is one when client saved his entire data to the server and he is not accessing it for a long period because of any cause. An unauthorized access will use that data prohibited due to lack of authorized privileges of access control.We inhabit everything in providers premises which compose the information highly unprotected. This is a main barrier in acceptance of the cloud. According to the IDC's survey on the cloud services, security issues are number one problem facing cloud computing. Overheads or Difficulties ahead of the cloud are the risk of-Interrupt Services, Loss of Privacy, Damage of information and Theft of Information. This issue prevents organizations to adopting the cloud facilities.

Data security is the important security issue in the cloud computing. In the service provider's data center, securing data security and managing fulfillment are critical by using managing encryption keys of the data in transmit to the cloud. Encryption keys shares safely between cloud services provider and consumer and encryption of mobile media is a significant and frequently overlooked require. Platform as a Service based applications, Data-at peace is the economics of the cloud and a multitenant architecture used in SaaS. In other words, when stored data for exploit by procedure by the cloud-founded applications or a cloud founded application, is commingled with additional customer data.

There are the many issues and challenges.

4.1 Security

4.1.1Confidentiality

Top vulnerabilities are to be ensuring that data is secured from any attacks. So security analysis has to be done to safe data from spiteful user such as Cross-site Scripting and Access control mechanisms etc.

4.1.2 Integrity

To give protection to client data, thin clients are used where only some assets are available. Users should not storage their private data such as passwords so that integrity can be certain.

4.1.3 Availability

It is the chief issue in various organizations facing downtime as a main issue. It depends on the deal between client and vendors.

4.2 Data Storage

Data storing in VM have various issues one such issue of the data storage is reliability. Virtual machines requests to be storage in the physical infrastructure which may reason security threat.

4.3 Data Breaches

This is another vital security issue to be intense in the cloud computing. As huge data from many users are storage in the cloud computing, there is a chance of spiteful user entering the cloud like that the whole cloud environment is level to a high value attacks. A breach can arise caused by much accidental broadcast issue or due to insider attacks.

4.4 Locality

The data is distributed above the number of area and to find the position of data is complicated in the cloud computing. When the data is stimulated to diverse geographic locations the law governing on that data can also modify. So there is an issue of fulfillment and data privacy rules in the cloud computing. Customers should recognize their data place and it is to be intimated by the service provider.

4.5 Accession

It is refers to the data protection policies. In an association, the employees will be given accessed to the choice of data based on their business security policies. The same data can't be accessed by others employee work in same association users. User can use data protection and encryption mechanisms to avoid security threat.

5. CLOUD SECURITY SOLUTIONS

Encryption is recommended as a best solution to protected information. Before data storing in the cloud server. Data is encrypting to improve. Data Owner can give approval to particular group member like that data can be simply accessed by them. Heterogeneous data centric security is to be makeuse of obtainable data accessed control. A model of the data security includes of authentication, data encryption, data recovery and data integrity, user safety has to be planned to recover the data security above cloud. To make sure privacy and data protection can be used as a service. This method can be used to compute large files with dissimilar sizes and to address remote data security Rivest-Shamir-Adleman (RSA) based storage security.

This solution are based on cryptography a method are propose to constructed a reliable computing environment for the cloud system by providing protected cross stage into cloud system. The Network are proposed consist of the three backup sites for improvement behind disaster. The backs up sites are placed at the remote location from the vital server. If anyone of the path be unsuccessful, it will be use alternating path working. The encrypted file will be producing through back up sites and data are condensed. The data will be decrypted through revival operation. They planned a cross-stage integration model by used secure communication via internet and the utilization of a key for security to encrypt data (SHA) Secure Hash Algorithm is using for compression or GZIP algorithm is use for symmetric split of files and the implemented of SFSPL algorithm.

In this security solution is achieving when here is a shared trust between the consumer and provider they harmonize each other and the support security like that entire system works seamlessly. To attain this proper authorization, accounting controls and authentication, should be implementation by cloud service customer and providers. The identification to access information on cloud should be particular, secure (one time password or RSA tokens and should not be mutual among the entities of the consumer association. Be assured the consumer's access devices or indicate such as Virtual terminals, Personal Computers, gazettes, mobile phones and pamphlet are secured sufficient. The loss of an end point accessed to the device or access device by an unlicensed user can cancel even the better security protocols in the cloud. Be assured the user computing devices are supervised properly and protected from malware supporting and functioning advanced authentication features.

Following approaches can be useful for secure cloud computing

5.1 Backing

Natural disaster may be harmful the physical devices that may reason of data loss. To escape this difficulty backup or backing of information is the key of assurance of service make available by vendors.

5.2 Encryption Algorithm

Clearly cloud service providers encrypt the user's information via strong encryption algorithm. Although, difficulty is that encryption accident can make data entirely unusable and encryption also make difficult the ease of use. To solve this problem the cloud provider must provide proof that encryption representation were tested and designed by skilled specialists.

5.3 Client Satisfaction

Very hard for the client to actually confirm the presently implemented security initiatives and practices of a cloud computing providing by the service providers for the reason that customer usually has no accessed to the provider's service which can be included of various facilities spread around the sphere. Result for this Provider should find some standard certificate from some governing or uniform institution that make sure users that provider has establish adequate internal switch and these control are operating efficiently.

5.4 Analysis support

To determine audit tools are provide to the users. how their data is protected , stored, verify policy enforcement and used. However, analysis of prohibited activity is rather difficult. Since data for compound customers may be collocated and may also be organically spread across set of hosts and data centers. To determine this audit tools must be contractually dedicated along with the proof.

5.5 Network Protection

A user can repudiate the access of some Internet based service by using IP Spoofing which can be origin of security damage. We can used to Digital Signature technique for solve it. Secure Socket Layer (SSL) Protocol is used for managing security of message broadcast on the Internet. Which also ignore resource hacking

6. CONCLUSION

In this paper we study about cloud and its security issue or security related algorithms at the end of paper we conclude that DES algorithm performs well in compare to RSA.In my propose work we use DES (Data Encryption Standard) algorithm for security issue and my base paper use RSA (Rivest-Shamir-Adleman) for security issues. Both are cryptographic Algorithm.

REFERENCES

[1] MegnaUnnikrishnanandLipiArun " Comparative Study of Cloud Computing Data Security Methods" International Journal of Computer Applications (0975 – 8887) , Advanced Computing and Communication Techniques for High Performance Applications (ICACCTHPA-2014.

[2] AdityaRanjanMalviya , P. Shayam Kumar "On Security of Data Storage in Cloud Computing via Exact Regenerating Code" International Conference on Computing, Communication and Automation (ICCCA-2015) , IEEE,2015.

[3] DimpiRani , Rajiv Kumar Ranjan "A Comparative Study of SaaS, PaaS and IaaS in Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE -2014)

[4] CH.Sekhar1, S Reshma Anjum2 "Cloud Data Mining based on Association Rule"International Journal of Computer Science and Information Technologies (IJCSIT -2014)

[5] R.Kabilan, Dr.N.Jayaveeran "A Review on Data Mining in Cloud Computing Environment" International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE -2015), DOI: 10.15680/IJIRCCE.2015. 0310127.

[6] SakshiAggarwal ,Dr.RituSindhu "A Survey on Cloud Mining with Privacy Protection" International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE -2014) Vol 4, Issue 10, October 2014

[7] HimelDev, TanmoySen, MadhusudanBasak and Mohammed Eunus Ali " An Approach to Protect the Privacy of Cloud Data from Data Mining Based Attack" Department of Computer Science and Engineering (CSE) Bangladesh University of Engineering and Technology (BUET)

[8] Mr.A.Srinivas, M. KalyanSrinivas, A.V.R.K.HarshaVardhanVarma "A Study On Cloud Computing Data Mining"International Journal of

Innovative Research in Computer and Communication Engineering (IJIRCCE-2013) Vol. 1, Issue 5, July 2013

[9] C.Edward Jaya Singh , Dr.E.Baburaj "Starring role of Data Mining in Cloud Computing Paradigm" International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882 Vol 4, Issue 9, September 2015

[10] Anuja R. Yeole1, Poonam Borkar2 "Survey Paper on Data Mining in Cloud Computing" International Journal of Science and Research (IJSR) 2013

[11] RandeepKaur ,JagroopKaur "Cloud Computing Security Issues and its Solution: A Review" IEEE 2015

[12] Shade Kuyoro, Awodele.O" Big Data and Cloud Computing Issues" International Journal of Computer Applications https://www.researchgate.net/publication /290791630, Vol. 133 – No.12, Jan 2016

[13] Jitender Grover, Shikha ,Mohit Sharma "Cloud Computing and Its Security Issues - A Review" 5th ICCCNT – 2014, IEEE, july 11-13

[14] Umesh Kumar Singh, Rajesh Piplode "Study of Security Issues & Challenges in Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE-2012) www.ijarcsse.comvol 2, Issue 9 September 2012

[15] Rabi Prasad Padhy, ManasRanjanPatraand Suresh Chandra Satapathy "Computing: Security Issues and Research Challenges" IRACST-International Journal of Computer Science and Information Technology & Security (IJCSITS-2011) Vol. 1, No. 2, December 2011

[16] R. VelumadhavaRaoa,*, K. Selvamanib,* "Data Security Challenges and Its Solutions in Cloud Computing"International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015), ELSEVIER,2015, (http://creativecommons.org/licenses/by-nc-nd/4.0/)

[17] R. VelumadhavaRaoa,*, K. Selvamanib,* "Data Security Challenges and Its Solutions in Cloud Computing"International Conference on Intelligent Computing, Communication &onvergence (ICCC-2015),ELSEVIER,2015, (http://creativecommons.org/licenses/by-nc-nd/4.0/).

[18] Y. Ghebghoub, S. Oukid, and O. Boussaid "A Survey on Security Issues and the Existing Solutions in Cloud Computing" International Journal of Computer and Electrical Engineering (IJCEE-2013) Vol. 5, No. 6, December 2013

[19] Manas M N1, Nagalakshmi C K2, Shobha G3 "Cloud Computing Security Issues And Methods to Overcome" International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE-2014), Vol 3, Iss 4, Apr 14

[20] Prince Jain "Security Issues and their Solution in Cloud Computing" International Journal of Computing & Business Research (IJCBR-2012)

[21] Umesh Kumar Singh, Rajesh Piplode "Study of Security Issues & Challenges in Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE-2012) www.ijarcsse.com, vol 2, Issue 9 September 2012

[22] Mr.Chandrashekhar S. Pawar ,Mr.Pankaj R. Patil "Providing Security and Integrity for Data Stored in Cloud Storage" ICICES2014 - S.A. Engineering College, Chennai, Tamil Nadu, India , IEEE 2014

[23] Mohammed faez AL-Jaberi, AnazidaZainal "data integrity and privacy model in cloud computing" International Symposium on Biometrics and Security Technologies (ISBAST), IEEE, 2014

[24] SiddharthDuttChoubeyandMohit Kumar Namdeo"Study of Data Security and Privacy Preserving Solutions in Cloud Computing"International Conference on Green Computing and Internet of Things(ICGCloT) , IEEE 2015

[25] Malay Kumar, JasrajMeenal, Rahul Singh2, Manu Vardhan"Data Outsourcing: A Threat to Confidentiality, Integrity, and Availability"International Conference on Green Computing and Internet of Things (ICGCloT), IEEE 2015

[26] ChetnaVaid#, Harsh K Verma# "Anomaly-based IDS Implementation in Cloud Environment using BOAT Algorithm" IEEE 2014

[27] Deepti Mittal, DamandeepKaur, AshishAggarwal"Secure Data Mining in Cloud using Homomorphic Encryption" IEEE 2014

[28] N. ShanmugakaniandR.Chinnaa "An Explicit Integrity Verification Scheme for Cloud Distributed Systems" 9th International Conference on Intelligent Systems and Control (ISCO), IEEE 2015

[29] R. Kaur and R.P. Singh "Enhanced cloud computing security and integrity verification via novel encryption techniques" International Conference on Advances in computing, communication and informatics (ICACCI), IEEE 2014

[30] AdityaRanjanMalviya , P. Shayam Kumar "On Security of Data Storage in Cloud Computing via Exact Regenerating Code" International Conference on Computing, Communication and Automation (ICCCA-2015) , IEEE,2015.

Author

Akanksha Bansal was born in 21th August 1992. She received the Bachelor of Engineering in Computer Science & Engineering from Shriram College of Engineering & Management (Banmour) Gwalior, India in 2014, and she is currently pursuing M.tech in Computer Science & Engineering from ITM Universe, Gwalior, India. Her main area of research interest as Data mining, cloud computing & cloud databases.