Journal of Advances in Science and Technology
Vol. 18, Issue No. 2, September–2021, ISSN 2230-9659

A Study of Cloud Computing Security and Data Integrity

Surina Jaiswal[1]*, Dr. Tryamvak Hiwarkar[2]

[1] Research Scholar,Sardar Patel University Balaghat MP,School of Computer Science and Technology

[2] Professor, Sardar Patel University Balaghat MP, School of Computer Science and Technology

Abstract - Cloud computing security and data integrity are two critical aspects of cloud computing that are of utmost importance. The cloud offers many benefits, such as scalability, flexibility, and cost-efficiency, but it also poses several security risks. In this response, I will provide an overview of cloud computing security and data integrity and discuss some of the ways to ensure the security and integrity of data in the cloud. And the study in which discussed about Integrity, Cloud Security, and Cloud Computing. Proposed a Secure Authentication and Data Sharing Architecture in a Cloud-Enabled Big Data Environment, We presented a practical way for properly protecting and exchanging data in the cloud. Transmission speed and computation time for a multi-node Hadoop cluster was used to evaluate the task. The proposed method assures that big data outsourcing is authenticated and private. The methodology that assures the integrity of data as well as the accuracy of the cloud service provider's calculations was discussed. This research presents a suitable way for ensuring both the data integrity and the accuracy of computations performed by the cloud service provider. The cloud user should be able to verify the integrity of their data with the cloud service provider for the user to get the most of the cloud's storage capabilities.

Keyword - Cloud, Data, Integrity

- X -

INTRODUCTION

Cloud is a word established as a common paradigm in the current digital world. Cloud computing employs the virtualized platform containing the elastic resources including software, hardware, services, and data sets by enabling dynamic provisioning of the pool of virtual resources to the cloud users. The aim of cloud computing is to transform the conventional desktop computing towards service oriented computing employing huge clusters and data centers. Cloud computing affects its ease and cheap cost to the cloud clients utilizing the notion of virtualization.(Nandhini.P (2018)) Cloud computing known as Internet based computing has arisen from the principles of distributed computing, utility computing, grid computing. It incorporates the concepts like virtualization, multitenancy, service oriented architectures for offering infrastructure, platform, and software as the service rather than a product. A cloud model contains the five important elements to benefit the consumers and suppliers. On-demand, self-service: The cloud customers may automatically employ the computing resources such as servers, CPU cycles, and memory and network storage whenever required without intervening human involvement with the cloud service provider. A wide network access: The cloud services are constantly becoming accessible by heterogeneous thin or thick client devices such mobile phones, laptops, desktops, tablets and workstations. Resource pooling: The cloud service provider's computing resources are brought together to serve several cloud users utilizing a multi-tenant architecture. Rapid elasticity: The computer resources may be provided and released elastically, in certain circumstances frequently, to scale up and scale down according to the consumer's demand. Measured service: The utilization of cloud resources may be monitored, tracked, managed, and reported daily or weekly or monthly by both the service provider and the customer.

Integrity

Information is protected against tampering by integrity safeguards. These procedures guarantee the quality and completeness of the data they contain. Data that is kept on a system and data that is sent between systems, such as email, must be safeguarded from cyber-attacks. The integrity of a system can only be maintained by ensuring that system users are only allowed to edit information that they are officially permitted to alter, not just at the system level. As with the preservation of information's confidentiality, the integrity of its data is also guarded against unintentional disclosures. Z. Zhou and D. Huang (Zhou) In order to ensure the integrity of data, countermeasures must also defend against accidental changes, such as human mistakes or data loss due to a system breakdown. This intricate method comprised getting the appropriate credentials for withdrawals, as well as infecting the banking system to destroy the database records of transfers and then suppressing confirmation notifications which would have alerted banking authorities to fraud. More than $60 million was stolen from a plan that was found and shut down, yet the criminals still managed to get away with it. (K. Kumar and Y-H. Lu,) Protecting integrity may be accomplished by the use of a variety of strategies. Authorized users can't make unauthorized modifications with access control and strict authentication in place. In order to verify the authenticity of a transaction or a file, hash verifications and digital signatures are useful. In order to ensure the integrity of data, administrative measures such as the separation of responsibilities and training are equally necessary.

Cloud Security

Because critical services are often outsourced to a third party on the cloud, it also introduces an extra risk. When data is stored or processed in an external location, it becomes more challenging to maintain data and privacy security, ensure the availability of data and services, and prove compliance. Therefore, cloud computing removes most of the data and operating control from the client organization. The cloud service provider, rather than the end user, may be responsible for even the most fundamental responsibilities, such as software updates and firewall configuration. In order to safeguard themselves, customers need to establish trust with their service providers and get knowledge of the risks associated with their providers' security development, implementation, and maintenance.(Jia-Lun Tsai) Many companies avoid the risks associated with outsourcing by using private or hybrid clouds instead of public ones. There are plenty of other facets of cloud computing that need a security and risk assessment overhaul. The letter T is represented by the first letters of the names of four authors: When information is stored in the cloud, its location is difficult, if not impossible, to determine. Abstraction has been used to security measures that were previously obvious. This opacity may lead to a wide variety of compliance and security problems.

Since so much shared infrastructure is at the heart of cloud computing, its security model is fundamentally different from that of traditional information technology environments. In today's ever-evolving IT infrastructures, mis-configuration, data breach, and criminal behavior are all the more likely due to factors such as workload balancing and fluctuating Service-Level Agreements (SLA).

By eliminating the potential for operator error and supervision, an automated approach to infrastructure sharing may help remove operator error and supervision. The risks of a shared infrastructure mean that cloud computing solutions still need to put a premium on isolation, identity, and compliance.

Cloud Computing

Cloud computing is a technology offering services in which resources are provisioned on an on-need, pay per use basis through web-based tools and applications, as opposed to a direct connection to a server.(M. Bahrami and M. Singhal) Rather than keeping files on a proprietary hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database. As long as an electronic device has access to the web, it has access to the data and the software programs to run it. With the advent of cloud any business, organization, university, research centre etc. can reduce their capital expenditure and instead divert the investment to other areas thereby strengthening their organizations. The employees in an organization can share their data through cloud. The research community has benefitted a lot because of sharing their research works through cloud. The major features of the cloud are ubiquity, resource pooling and elasticity, adaptability, scalability, flexibility, multi-tenancy and high Quality of Service (QoS). Main reasons to use cloud computing are, maintaining or managing the network does not need any effort while it provides flexible capacity and Internet access from any place. Advantages of cloud computing include improved performance, instant software updates, quick deployment, easy access to information, efficient backup and recovery, reduced cost and does not require capital expenses. When it comes to providing cloud services the various corporate players are: Amazon web services, Google Cloud, Microsoft Azure, Sales force etc.

LITERATURE REVIEW

Sookhak et al. (2017) examined the many remote data auditing (RDA) methods used to audit the dispersed cloud environment's stored data. Cloud computing architectures may be classified into multi-server, single server and multi-server designs for distributed systems. In a distributed setting, auditing methods including replication-based RDA, erasure-based RDA, and network-based RDA are used. The survey categorizes numerous RDA approaches based on several themes. Security needs and problems have been examined. The lack of research in RDA has been brought to the fore.

Jianghong Wei et al. (2017) Encryption based on identity revocation and cypher text updating is possible using RS-IBE (Revocable-Storage Identity-Based Encryption). The degree of security in a security model is raised thanks to the solid design of RS-IBE. The RSIBE scheme resulted in a more cost-effective data exchange system with improved performance and efficiency. However, revocable-storage identity-based encryption does not improve data secrecy.

Cihan et al. (2017) NIST controls are configured and monitored continually as part of an autonomously configuring cloud security infrastructure. Virtual machines (VM) are created using a configuration engine, which applies the necessary security constraints and continually monitors each VM to determine its present status. Despite the novelty of this security architecture, there is no recourse in the event of a breach of the security controls.

Alhumrani & Jayaprakash Kar (2016) for cloud data encryption and safe communication, the cryptographic methods were examined and assessed. Communication in the Cloud (CC) is safe thanks to protocols like Secure Shell Protocol (SSH), Internet Protocol Security (IPSec), Kerberos, Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). The authentication, however, was not done utilizing cryptographic methods in an efficient way.

Jainish et al. (2016), the owner of the data would be alerted right away if someone tried to access it without authorization, according to a new logging approach that has been suggested. The data owner grants the data user access to the data he has saved. Key creation and integrity checking are performed using the RSA and MD5 algorithms, while encryption and decryption are carried out via hierarchical encryption. Without the owner's permission, the data cannot be altered. To encrypt and decrypt data, the AES algorithm is used on text encoded in the base 64 encoding format, which is the only one that can be decoded.

Ke Han et al. (2016) for cloud storage security, CP-ABE (Cipher text Policy Attribute-Based Encryption) are a cryptographic solution to the problem. CP-ABE methods, on the other hand, were unable to be used directly in cloud storage. Effective and safe access controls for shared data were implemented to solve the challenge of security. The CP-ABE-based system's security was further bolstered by the newly devised scheme. Secure access control technique, on the other hand, did not reduce encryption time.

Ali Gholami & Erwin Laure (2015) As a result of this paradigm change, the issues of In CC environments, multi-tenancy, loss of control, and trust were essential. The cloud security and privacy issues were solved by existing solutions. According to CC's privacy-preserving sensitive data techniques, the technologies may be divided into three categories: cloud reference architectures, cloud resource management systems, and cloud service management systems. However, there was no reduction in the amount of data that had to be stored. Decryption rights for any given set of cipher-texts were created and delegated. In a new cryptosystems technique, any secret keys were aggregated into a single key with the combined power of all the collected keys. Secretly sent and stored on a smart card, the aggregate keys used minimum storage space.

Abhilasha N Madde et al. (2015) decryption permissions for every given collection of cipher-texts were generated and delegated. Secret keys were combined into one key with a power of 40 in the new cryptosystems approach. The combined keys were transferred and stored on a smart card covertly and with little use of storage space. In order to get a query-biased snippet of data from the server, Ningduo Peng et al. (2013) developed a single-server and two-round approach based on searchable encryption principles. Making the text preview able under any cryptosystem and developing a safe index to handle dynamic computation for matching snippets when keywords are requested were the means of achieving this goal.

Jia-Lun Tsai & Nai-Wei Lo (2015) Distributed mobile CC services may now be authenticated using an effective authentication method. Using private key, mobile users may access CC services from a wide range of service providers, enhancing their security. Using a bilinear pairing cryptosystem and dynamic generation, the system was secure. Although cloud service provisioning efficiency may have been improved, it was not done so in an efficient manner.

Dharmendra et al. (2014) the use of multilayer encryption and two-level verification as a security architecture for cloud data at rest For sensitive data, a two-level verification is used; for typical data, a single-level verification is applied. This speeds up the verification process, since the sensitive data can be verified more quickly. Using this security architecture, users may choose whether or not their data should be encrypted at the user's or cloud service provider's end. A variety of encryption methods are supported, including block-level and file-level encryptions. Only data in the "rest" state is protected by the security framework. In-transit data is ignored.

Dong-junxin & Yen-Wei Chen (2013) Fuzzy k-means clustering methods were utilized to construct the conventional k-means cluster technique for digital picture segmentation and classification. With algorithm convergence, a SOR-based fuzzy k-means algorithm was developed. For solving linear systems of equations, SOR was an alternative to the Gauss-Seidel technique. Auto-stopped is a data mining technique. Patients with trajectories may be classified by Hongying Fei and Nadine Meskens (2013) using the bisecting K-Medoids clustering method. Two sorts of patient trajectories were distinguished by the method's design. Outpatient visits were used to categories patients in the first group. Trajectories were used to categories the groups at the beginning of the process in the second kind. Even still, the problem of computational complexity was not solved.

METHODOLOGY

Proposed a Secure Authentication and Data Sharing Architecture in a Cloud-Enabled Big Data Environment, We presented a practical way for properly protecting and exchanging data in the cloud. Transmission speed and computation time for a multi-node Hadoop cluster was used to evaluate the task. The proposed method assures that big data outsourcing is authenticated and private. The methodology that assures the integrity of data as well as the accuracy of the cloud service provider's calculations was discussed. Fingerprint was used as an authentication structure in the design and implementation of a novel remote fingerprint authentication technique based on Merkle hash tree. This remote authentication strategy was enable only authorized users to access the system. There was a demonstration of a technique for assuring the security of dynamic data storage. An appropriate CIA model for securing data stored in the cloud was also being established using the approaches for confidentiality, integrity, and authentication outlined in the study.

DATA ANALYSIS

This research presents a suitable way for ensuring both the data integrity and the accuracy of computations performed by the cloud service provider. The cloud user should be able to verify the integrity of their data with the cloud service provider for the user to get the most of the cloud's storage capabilities. Maintaining data integrity ensures that any information kept in a cloud server is authentic and has not been tampered with. This implies that only authorized users may make changes to the data, boosting the reliability of the cloud service providers.

SYSTEM MODEL FOR DATA INTEGRITY ASSURANCE

This architecture for secure cloud storage includes a Data Owner (DO), Data Users (DU), a Cloud Service Provider (CSP) with n cloud storage servers (s1, s2,.., sn), a number of compute intensive servers, a dedicated service for providing meta-data, and a Third Party Auditor (TPA), we see a schematic of the overall system paradigm for secure data storage.

Third Party Auditor (TPA): This term is used to describe a company or person who can confirm the safety of data kept in a cloud server.

The role of the auditor falls into two categories.

1. **Private auditability**: Here, only the data owner has access to verify that the server-stored data file is in fact intact.

2. **Public auditability**: This allows any interested party, including the TPA, to confirm the accuracy of the data.

Metadata generator: What this means in practice is that the Data Owners have control over some kind of business or service that is physically located on the premises of the cloud service providers. It is responsible for creating metadata from encrypted data blocks.

ASSURING THE INTEGRITY OF DATA AND COMPUTATION

An efficient method is presented here for checking the integrity of users' information saved on the cloud server. There are two major upsides to this plan.

- Obtaining evidence that data saved in the cloud has not been altered or removed by the cloud service provider without the owner's permission.

- Allowing data consumers to check the accuracy of calculations performed by the cloud service provider, hence preventing server misbehavior.

Computation security

The proposed computation security assurance scheme uses Merkle hash tree, for verifying correctness of computations performed by the CSP.

Merkle hash tree is a complete binary tree having the height of h and 2^h leaves. Each leaf node holds the value of the computed results and each internal node holds the hash of the concatenation of its children node as defined by the equation 4.1.

$$n_{parent} = hash(hash(n_{left})||hash(n_{right})) \qquad (4.1)$$

Merkle's hash tree was created from the ground up. Each parent node N can only have a maximum of two children nodes, much like a binary tree. In reality, there are always two child nodes for every non-leaf node. The data in a single MHT node, or "node N," is produced as follows. The calculated results are hashed, and that value is used to determine the leaf node's value. A parent node of leaves N1 and N2 is constructed as NP= {H(h(N1)||h(N2))}. Similarly all the parent nodes are constructed by combining the hash values of left child and right child. This process will be continued until the root of the Merkle hash tree is generated as illustrated in the Figure 1. This root is considered as the signature (Ω).

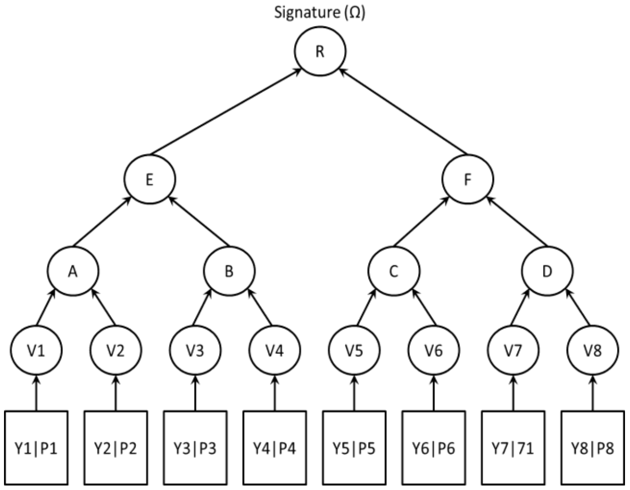

Figure 1: Merkle hash tree constructed by the cloud server

The process of assuring the computation integrity involves two phases, namely computation commitment generation phase and verification phase.

Computation commitment generation phase

1. As well as the data, cloud users also send in a number of computing jobs.

2. As soon as it receives them, the CSP does the calculations and creates the signature using the Merkle hash tree, with the computed results serving as the leaves.

3. When the calculation is complete, the CSP will deliver the user's signature together with the computed results.

Table 1: Hardware configuration required for eucalyptus cloud environment setup

Hardware	Server1	Server2	Client1
CPU	1 GHz	VT Extension	VT Extension
RAM	1 GB	1 GB	1 GB
Disk	5400 rpm	5400 rpm	5400 rpm
Disk space	40 GB	40 GB	40 GB
Networking	100 Mbps	100 Mbps	100 Mbps

Storage management

Eucalyptus offers a storage-only service known as walrus, which is competitive with Amazon's Simple Storage Service (S3). The permanent data is stored in buckets and objects in Walrus, which is a file level storage system as opposed to block level storage. Eucalyptus' Walrus storage solution is compatible with Amazon S3 (Simple Storage Service). Walrus's many storage choices may be accessible through its web-based user interface. The pictures for the virtual machines may be kept in the walrus's buckets and managed, deleted, and registered using various Amazon tools.

Table 2: Metadata values for the text “cloud computing”

Character	I	j	ASCII(Char)	Metadata
C	1	1	99	99
L	1	2	108	216
O	1	3	111	333
U	1	4	117	468
D	2	1	100	200
Space	2	2	30	120
C	2	3	99	594
O	2	4	111	888
M	3	1	109	327
P	3	2	113	678
U	3	3	117	1053
T	3	4	116	1392
I	4	1	105	420
N	4	2	110	880
G	4	3	103	1236

SECURITY ANALYSIS

Security model for assuring integrity

There are three potential vulnerabilities that might allow unauthorized access to the stored information. As a potentially untrustworthy, self-absorbed, and even malevolent actor, CSP is sometimes a necessary evil. Cloud service providers (CSPs) may retrieve seldom accessed data from cloud storage while falsely portraying and billing customers for all data stored in the cloud. (ii) CSP may be in the dark about how rogue people are misusing customer information. (iii) CSP may not report the Byzantine failure of the storage servers in order to get the economic advantages. More specifically, we divide assaults into two categories based on the adversary's role:

Internal attacks: Untrusted cloud service providers or insiders inside the firm are the source of these intrusions. They are knowingly exposing user information to other parties for financial advantage.

External attacks: These assaults are coming from people on the Internet who are not a part of the cloud service. Malicious users may compromise cloud service providers by accessing consumers' data for financial gain.

Replace attack: Whenever a block or its accompanying information is challenged, the cloud server has the option of discarding it and replacing it with a different legitimate, uncorrupted pair of original data and metadata blocks.

Replay attack: In order to avoid constantly downloading the challenged data block, the cloud server may instead create the proof by referencing the proof produced for the previous challenge.

Ensuring data integrity

By verifying these characteristics, the data integrity assurance system guarantees the following aspects of safe storage:

Public verifiability: Anyone, not only the data's owner, may use this system to ensure the reliability of their cloud-based information. In this case, both public and private verifiability are supported by allowing a TPA to do an integrity check.

Privacy of data: Despite the TPA doing the verification, data privacy is maintained by not disclosing any sensitive information to them. Because the data owner has the encryption keys, the TPA can only audit the encrypted text.

Block less verification: This feature requires that no whole data block be acquired by the TPA during the verification process. Thanks to this method, the TPA doesn't have to request the whole data block from the cloud server but rather only the two characters at the given point (MDB[i,j] and EDB[i,j]). This quality ensures that the system can be verified with no blocks being present.

Low computation: When it comes to checking the security of data kept in the cloud, the effort expended by the data's owner and the TPA is minimal.

Low storage overhead at TPA: To keep things simple, with this system the only information the TPA or data owner has to keep track of are the random function (RF) and the secret key (Sk). Because of this, the suggested architecture places little burden on TPA and data owner for storing their respective data.

Protection against salami attack: Since the data owner validates the CSP's calculations, the likelihood of salami attacks is reduced.

Probability of detection of data corruption (Pd): In this methodology for assuring data integrity, the issue of data corruption has been confidently recognized. Numerous types of data corruption caused by an unreliable server or an evil user were studied to determine the probability (Pd). Different types of data corruption include erasure, addition, alteration, and append. Here, the greatest possible chance of 1 has been identified for the probabilities of data insertion, data deletion, and data appending corruptions, with just a few obstacles in the way. The probability (Pd) of the replacement corruptions over the stored data can be computed using the equation 4.3.

$$\mathrm{Pd} = 1 - \left(1 - \frac{\mathrm{mb}}{\mathrm{nb}}\right)^{t*s} \qquad (4.3)$$

- The data file **F** comprises of nb data blocks and the probability to choose any one block is **1/nb**.
- The hacker modifies **mb** data blocks and the probability of modifying the data block is **mb/nb**.
- The number of challenges made by the TPA to the server to detect the data corruption is **t** .
- The number of characters in each data block is **s**.

CONCLUSION

Cloud computing is seen as a flexible computing paradigm due to its low cost and rapid deployment. The cloud's development and usage might be hampered, though, if security concerns aren't addressed adequately. On particular, this research focuses on the issue of how to safely save and manage sensitive information in the cloud. The findings of this study point to the importance of the Confidentiality, Integrity, and Authentication paradigm in cloud adoption. By leveraging 2-Keys symmetric encryption, this strategy guarantees the privacy of cloud-based data. The DO ensures the integrity of data and computations by using data and computation assurance mechanisms. Using the remote user authentication technique, we can ensure that only approved users have access to sensitive information and services.

REFERENCES

1. S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1 – 11, 2011.

2. M. T. Khorshed, A. S. Ali, and S. A. Wasimi, “A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing,” Future Generation Computer Systems, vol. 28, no. 6, pp. 833 – 851, 2012.

3. Z. Zhou and D. Huang, “Efficient and secure data storage operations for mobile cloud computing,” in Proceedings of the 8th International Conference on Network and Service Management. International Federation for Information Processing, 2012, pp. 37–45

4. K. Kumar and Y.-H. Lu, “Cloud computing for mobile users: Can offloading computation save energy?” Computer, no. 4, pp. 51–56, 2010.

5. M. AlZain, E. Pardede, B. Soh, and J. Thom, “Cloud computing security: From single to multi-clouds,” in System Science (HICSS), 2012 45th Hawaii International Conference on, Jan 2012, pp. 5490–5499

6. Talebian, E. Ahmed, A. Gani, and M. K. Khan, “A review on remote data auditing in single cloud server: Taxonomy and open issues,” Journal of Network and Computer Applications, vol. 43, pp. 121–141, 2014.

7. S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” Journal of network and computer applications, vol. 34, no. 1, pp. 1–11, 2011.

8. J. Yang and Z. Chen, “Cloud computing research and security issues,” in Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on. IEEE, 2010, pp. 1–3.

9. H. Aljahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, and J. Xu, “Multi-tenancy in cloud computing,” in Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium on, April 2014, pp. 344–35

10. R. A. Sana Belguith, Abderrazak Jemai, “Enhancing data security in cloud computing using a lightweight cryptographic algorithm,” ICAS 2015 : The Eleventh International Conference on Autonomic and Autonomous Systems, 2015.

11. Sookhak, M, Gani, A, Khan, MK & Buyya, R 2017, ‗Dynamic remote data auditing for securing big data storage in cloud computing', Information Sciences, vol. 380, pp. 101-116

12. Jianghong Wei, Wenfen Liu & Xuexian Hu 2017, „Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption", IEEE Transactions on Cloud Computing, vol. 99, pp. 1-13.

13. Cihan Tunc, Salim Hariri1, Mheni Merzouki, Charif Mahmoudi, Frederic J de Vaulx, Jaafar Chbili, Robert Bohn & Abdella Battou 2017, ‗Cloud Security Automation Framework', IEEE 2nd International Workshops on Foundations and Applications of Self Systems (FASW), pp. 307-312.

14. Alhumrani, SA & Jayaprakash Kar 2016, „Cryptographic Protocols for Secure Cloud Computing", International Journal of Security and Its Applications, vol. 10, Issue 2, pp. 301-310.

15. Jainish Rajesh Jain & Abu Asaduzzaman 2016, ‗A Novel Data Logging Framework to Enhance Security of Cloud Computing', SoutheastCon 2016, 978-1-5090-2246-5/16 IEEE 2016.

16. Ke Han, Qingbo Li & Zhongliang Deng 2016, „Security and efficiency data sharing scheme for cloud storage", Chaos, Solitons and Fractals, Elsevier, vol. 86, pp. 107-116.

17. Ali Gholami & Erwin Laure 2015, „Security and Privacy of Sensitive Data in Cloud Computing: A Survey of Recent Developments", NETCOM, NCS, WiMoNe, CSEIT, SPM, pp. 131-150.

18. Abhilasha N Madde, Priyanka R Powar, Tanvi S Bankar, Harshada M Somwanshi & Prof Amol Dhumane, 2015, „Highly Secure Data Sharing in Cloud Storage using Key-Pair Cryptosystem", IJCSMC, vol. 4, Issue 10, pp. 35-39.

19. Jia-Lun Tsai & Nai-Wei Lo 2015, „A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services", IEEE Systems Journal, vol. 9, Issue 3, pp. 805-815.

20. Dharmendra S Raghuwanshi & Rajagopalan, MR 2014 , ‗MS2: Practical Data Privacy and Security Framework for Data at Rest in Cloud', 2014 World Congress on Computer Applications and Information Systems (WCCAIS 2014), pp. 231-238

21. Dong-junxin & Yen-Wei Chen 2013, „SOR Based Fuzzy K-Means Clustering Algorithm for Classification of Remotely Sensed Image", Lecture Notes in Computer Science, Springer, vol. 7951, pp. 375-382.

22. M. Bahrami and M. Singhal, “A light-weight permutation based method for data privacy in mobile cloud computing,” in Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2015 3rd IEEE International Conference on, March 2015, pp. 189–19

23. Nandhini.P (2018) on “A Research on Big Data Analytics Security and Privacy in Cloud, Data Mining, Hadoop and Mapreduce” Shreyas Satardekar Int. Journal of Engineering Research and Application www.ijera.com ISSN : 2248-9622, Vol. 8, Issue4 (Part -III) April 2018, pp65-78

Corresponding Author

Surina Jaiswal*

Research Scholar,Sardar Patel University Balaghat MP,School of Computer Science and Technology