ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

AssuringSecured Data Storage in Cloud Computing

Vinayak R. Kankate[1] ,Varshapriya J. N[2]

Abstract:-Cloud Computing provides new vision to the world. The approach of cloud computing is totally different from traditional system. In traditional system for any service, we need purchase, install, maintain, update by own. But in cloud environment we just pay for that service according to our usage basis & here no need to worry about purchase, install, maintenance and update. It is beneficial with respect to cost, flexibility, scalability. We require only good bandwidth network for better performance. Cloud provides different kinds of services like Software as a service, Platform as a service, Infrastructure as a service, Storage as a service etc. But still cloud is not fully mature. Cloud computing facing following problems like Data Security, Monitoring and Latency Issues. This paper focuses on cloud data storage security, which has been an important aspect of quality of service and we hereby present an effective and user friendly distributed scheme with explicit dynamic data support to ensure the correctness of cloud data. Cloud computing provides computation, software, data access and storage services that hides the physical location and configuration of the system that delivers the services from users. The system must design mechanisms that not only protect sensitive information by enabling computations with encrypted data, but also protect users from malicious behavior by enabling the validation of the computation result by using different algorithms- Shamir's secret sharing- is defined for a secret, File Distribution, Challenge Token precomputation,Correctness Verification and Error Localization, File Retrieval & Error recovery algorithms. The new scheme also provides secure and efficient dynamic operations on data blocks say for example - update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and server colluding attacks.

*Keywords:-***Cloud Computing, Data Storage, Security, Quality of Service etc.**

I. INTRODUCTION

Cloud computing provides computation, software, data access and storage services that hides the physical location and configuration of the system that delivers the services to users or clients. Also the clients cannot only use the services provided by the cloud provider rather they can also use the applications provided by the other clients those are registered on the same cloud. Cloud computing receives more and more attention, from both industrial and academic community. Cloud computing separates usage of IT resources from their management and maintenance, so that users can focus on their core business and leave the expensive maintenance of IT services on cloud service provider. Internet-based online services like Amazon Simple Storage service (S3) and Amazon Elastic Compute Cloud (EC2) provides huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. Cloud Computing proposes new challenges and threats related to security:

1) Traditional cryptographic primitives for data security and protection cannot be directly adopted, due to the user's fear of losing data under Cloud Computing.
2) Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc.

Cloud Computing is powered by data centers running simultaneously as cooperated and distributed organization. Each user's data is redundantly stored in multiple physical locations to reduce further data integrity threats. Therefore, distributed protocols for proper storage should be assured, is of at most importance so as to achieve a secure and robust cloud data storage system in the real world. The new scheme also provides secure and efficient dynamic operations on data blocks say for example - update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and server colluding attacks. The system must design mechanisms that not only protect sensitive information by enabling computations with encrypted data, but also protect users from malicious behavior by enabling the validation of the computation result.

II. RELATED WORK

Existing System for data security in cloud computing which has always been important part of Quality of service, Cloud Computing poses new challenges and threats to security for different reasons Traditional cryptographic primitives for data security and protection cannot be directly adopted, due to the user's fear of

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

losing data under Cloud Computing. Hence, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kinds of data for each user stored in the cloud. Secondly, the data stored in the cloud may be updated by the users, including insertion, deletion, modification, appending, reordering, etc. By using these techniques, to ensure the storage correctness without having users possessing data, cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations.

The proposed **"Assuring Secured Data Storage in Cloud Computing"** system designed to fulfill the drawbacks of the existing data storage security system. Efforts are made to remove drawbacks as many as possible. In this paper, we focus on cloud data storage security, which has always been an important aspect of quality of service, and we suggest an effective and user friendly distributed system with explicit dynamic data support to ensure the correctness of users data in the cloud, providing redundancies and guarantee data dependability on erasure correcting code in the file distribution preparation.

By using this construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the homomorphic token with distributed verification of erasure-coded data, our system achieves the storage correctness insurance and data error localization: whenever data corruption has been detected during the storage correctness verification, our system can almost guarantee the simultaneous localization of data errors. The challenge-response protocol in our project further provides the localization of data error, as compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers. The new system supports secure and efficient dynamic operations on data blocks, including: insert, update, delete and append. As per the extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and server colluding attacks. Proposed system avoids server failure and any unexpected error we should put one server restore point in cloud server database for efficient data back up or restore using multi server data comparison method. It is one of the major advantages of our proposed system.

III. ALGORITHMS

The system must design mechanisms that not only protect sensitive information by enabling computations with encrypted data, but also protect users from malicious activities by enabling the validation of the computation result. It supports secure and efficient dynamic operations on data blocks, including data update, delete and append. In the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance, since it can be the first step to fast recover the storage errors. The procedure for file retrieval and error recovery based on erasure-correcting Code.

A. File Distribution Preparation:-

The erasure-correcting code may be used to tolerate multiple failures in distributed storage systems. In cloud data storage, we rely on this technique to disperse the data file F redundantly across a set of d distributed servers. The layer interleaving technique is used to determine the c redundancy parity vectors from r data vectors in such a way that the original r data vectors can be reconstructed from any r out of the r + c data and parity vectors. By placing each of the r + c vectors on a different server, the original data file can survive the failure of any c of the r + c servers without any data loss, with a space overhead of c/r. The unmodified r data file vectors together with c parity vectors are distributed across r + c different servers. The user obtains the encoded file by multiplying FbyA

that is , G = F · A= (G(1),G(2), . . . , G(m),G(m+1),. , G(n))

= (F1, F2, . . . ,Fm, G(m+1), . . . , G(n)),

where F is the actual file and A is derived from a Vander monde matrix, is a matrix with the terms of a geometric

progression in each row. For a interleave index of 3, the first block containing data packets numbered (0,3,6,...(r-1).c), the second with data packets numbered (1,4,7,..,((r-1).c)+1) and the third with data packets

numbered (2,5,8,...((r-1).c)+2).

B. Challenge Token precomputation:

The main idea is - when a file is distributed to the cloud, the user pre-computes a certain number of short verification tokens on individual vector G(j) (j □ {1, . . . , n}), each token covering a random subset of data blocks that would be distributed to the different cloud servers. Later, when the user wants to make sure the storage correctness for the data in the cloud, he challenges the cloud servers with a set of randomly generated

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

block indices. Upon receiving challenge, each cloud server computes a short "signature" over the specified blocks and returns those signatures to the user. The values of these signatures should match the corresponding tokens pre-computed by the user. Suppose if the user wants to challenge the cloud server t times to ensure the correctness of data storage, the user must pre-compute x verification tokens for each G(j) (j □ {1, . . . , n}), a challenge key *kchal*and a master permutation key *KPRP*. To generate the *ith*token for server j, the user acts as follows,

1. Derive a random challenge value αi and a permutation key k(i)
Prpbased on *KPRP*.
2.Compute the set of r randomly-chosen indices.
3.Calculate the token v(j)i using the random challenge value αi.
After token generation, the user has the choice of either keeping the pre-computed tokens locally or storing them in encrypted form on the cloud servers.

C. Correctness Verification and Error Localization:-

Error localization is a key prerequisite for eliminating errors in storage systems. However, many previous schemes do not explicitly consider the problem of data error localization, thus only provide binary results for the storage verification. Our scheme outperforms those by integrating the correctness verification and error localization in our challenge-response protocol: the response values from servers for each challenge not only determine the correctness of the distributed storage, but also contain information to locate potential data error(s).

D. File Retrieval and Error Recovery:-

Information is usually added to mass storage devices to enable recovery of corrupted data. The redundancy allows the receiver to detect limited numberof errors that may occur anywhere in the message, and often to correct these errors without retransmission. Since our layout of file matrix is systematic, the user can reconstruct the original file by downloading the data vectors from the first m servers, assuming that they return the correct response values. Notice that our verification scheme is based on random spot-checking, so the storage correctness assurances a probabilistic one. However, by choosing system parameters (e.g., r, l, t) appropriately and conducting enough times of verification, we can guarantee the successful file retrieval with high probability.

Algorithm:-Error Recovery

1: procedure
% Assume the block corruptions have been detected
among
% the specified r rows;
% Assume s ≤ k servers have been identified misbehaving
2: Download r rows of blocks from servers;
3: Treat s servers as erasures and recover the blocks.
4: Resend the recovered blocks to corresponding servers.
5: end procedure

Algorithm:-Shamir's Secret Sharing

A secret sharing scheme is a means for n parties to carry shares or parts si of a message s, called the secret, such that the complete set s1, . . .sn of the parts determines the message. The secret sharing scheme is said to be perfect if no proper subset of shares leaks any information regarding the secret. Shamir's scheme is defined for a secret.Shamir has introduced a simple and elegant wayto split a secret A 2 GF(2^l) into n shares such that no tuple of shares with cardinality lower than a so-called threshold d < n depends on A.

Shamir's protocol consists in generating a degree-d polynomial with coefficients randomly generated in GF(2^l), except the constant term which is always fixed to A.

Shamir's Reconstruction protocol is used for to re-construct A from its sharing, polynomial interpolation is first applied to re-construct PA(X) from its n evaluations Ai.

Then, the polynomial is evaluated in 0. Those two steps indeed leads to the recovery of A since, by construction, we have A = PA(0). Actually, using Lagrange's interpolation formula, the combined two steps are,

A = $\sum_{i=0}^{n-1} Ai.\beta i$

Where,

βi can be considered as a public values.

Properties of Shamir's secret Sharing:-

1) **Perfect Security –** information theoretic security. Given any *t* shares, the polynomial is uniquely determined.
2) **Ideal-**Each share is exactly the same size as the secret.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

3) **Extendable-**additional shares may easily be created, simply by calculating the polynomial in additional points.
4) **Flexible-**can assign different weights (by the number of shares) to different authorities.
5) **Homomorphic property-**Shamir's secret sharing scheme has the (+,+) homomorphism property.
6) **Efficient Distributed Mechanism For Arithmetic Calculations**

IV. DYNAMIC DATA OPERATIONS

A. Update Operation:-

In cloud data storage, sometimes the user may need to modify some data block(s) stored in the cloud, from its Current value fij to a new one, fij + δfij . We refer this operation as data update. Due to the linear property of Reed- Solomon code, a user can perform the update operation and Generate the updated parity blocks by using δfij only, without involving any other unchanged blocks.

B. Delete Operation:-

Sometimes, after being stored in the cloud, certain data blocks may need to be deleted. The delete operation we are considering is a general one, in which user replaces the data block with zero or some special reserved data symbol. From this point of view, the delete operation is actually a special case of the data update operation, where the original data blocks can be replaced with zeros or some predetermined special blocks.

C. Append Operation:-

In some cases, the user may want to increase the size of his stored data by adding blocks at the end of the data file, which we refer as data append. We anticipate that the most Frequent append operation in cloud data storage is bulk append, in which the user needs to upload a large number of blocks (not a single block) at one time.

D. Insert Operation:-

An insert operation to the data file refers to an append operation at the desired index position while maintaining the same data block structure for the whole data file.

V. SECURITY ANALYSIS AND PERFORMANCE EVALUATION

Security analysis of this paper focuses on the adversary model. We evaluate the efficiency of our system via implementation of both file distribution preparation and verification token pre-computation. In this system, servers are required to operate on specified rows in each correctness, verification for the calculation of requested token. We will show that this "sampling" strategy on selected rows instead of all can greatly reduce the computational overhead on the server, while maintaining the detection of the data corruption with high probability. Suppose nc servers are misbehaving due to the possible compromise or Byzantine failure. nc ≤ n. Assume the adversary modifies the data blocks in z rows out of the l rows in the encoded file matrix. Let r be the number of different rows for which the user asks for check in a challenge. Let X be a discrete random variable that is defined to be the number of rows chosen by the user that matches the rows modified by the adversary.

VI. EXPERIMENTAL RESULTS

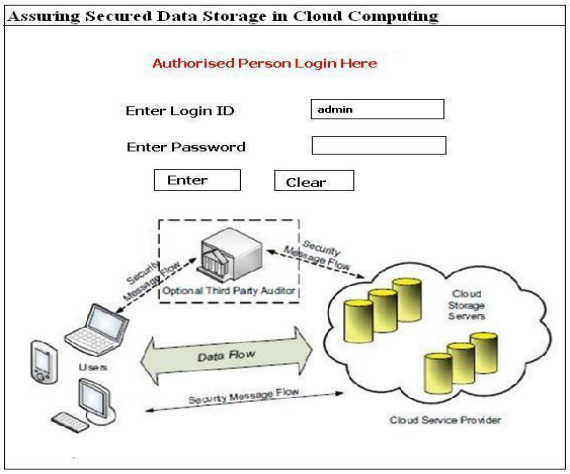

Fig 1:- Server Login

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

The server program which is used to store the client data for security.

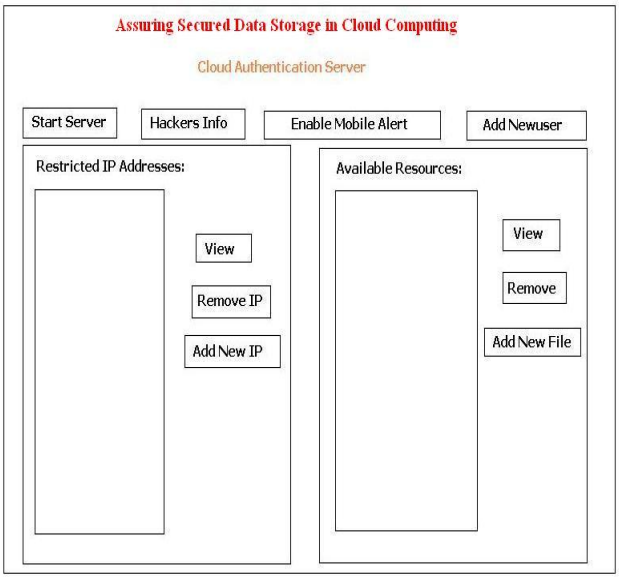

Fig 2:-Server module where the files must be added. The entire sever operations will be done here.

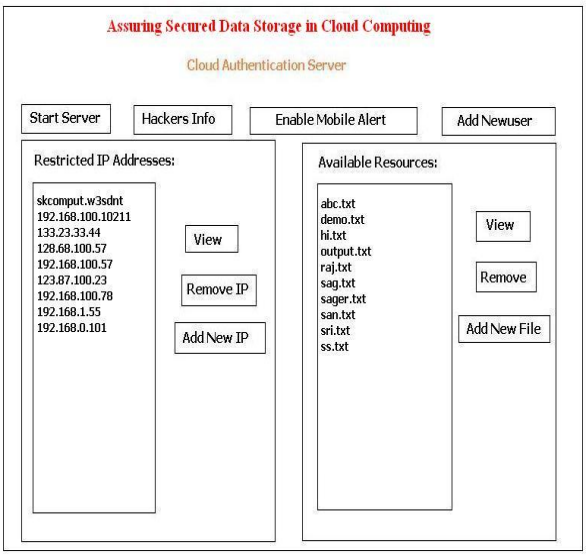

Fig 3:-The server is started and the files that are present in the server are shown Adding, deleting of the files, Restricted IPs will be done

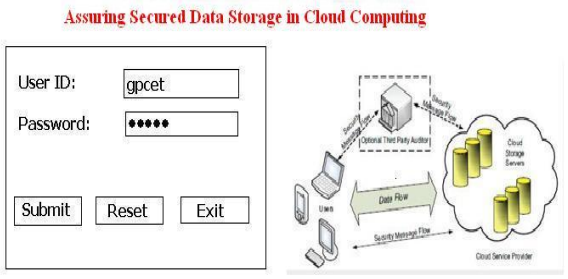

Fig 4:-The Client login program to authenticate the users.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

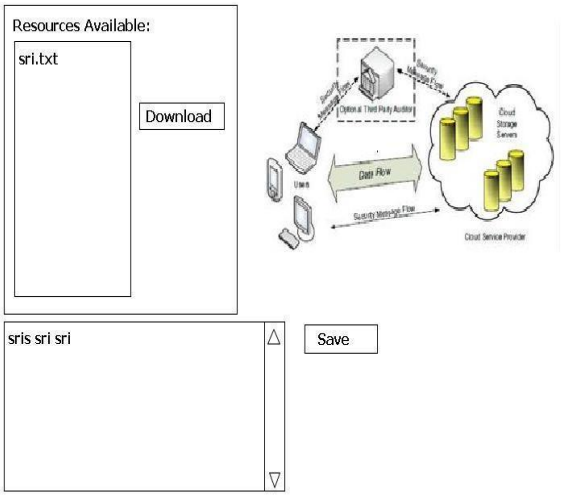

Fig 5:- The list of files that are allocated for the IP address are shown here and the can be downloaded by proper password provided

Assuring Secured Data Storage in Cloud Computing

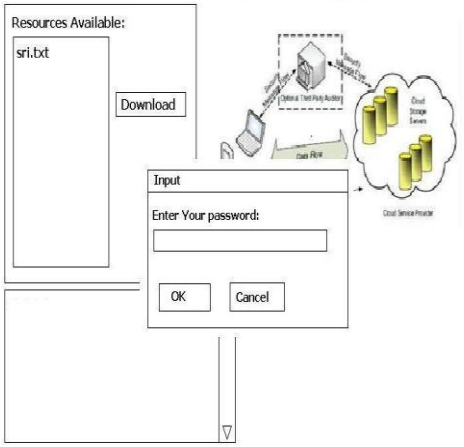

Fig 6:-Asks for the password if the IP address is added in the Restricted IP address list, they cannot download the file until the IP address is deleted

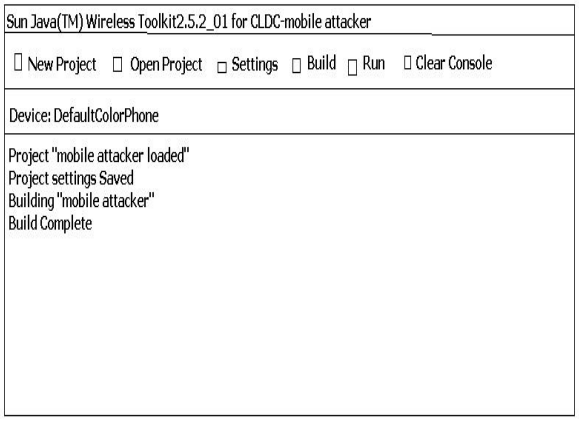

Fig 7:-Wireless Tool Kit is used as a Third party user to authenticate the userMobile Attacker is the program used to trace the Hacker

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

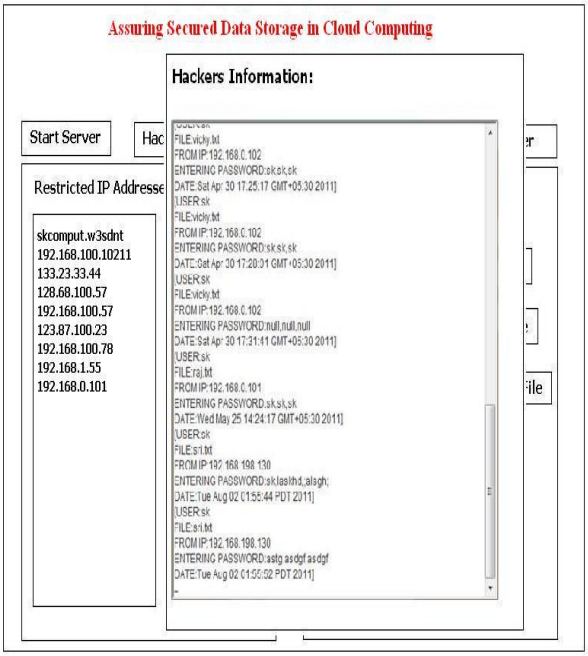

Fig 8:-The list of information traced while restricted IP is trying to download the file

VII. CONCLUSIONAND FUTURE WORK

In this paper, we have proposed tothe best of our knowledge and described the system "Assuring Secured Data Storage in Cloud Computing." Security and storage of data are the major concerns of client in the cloud storage network. We have proposed an effective and flexible distributed system with explicit dynamic data support, including block update, delete, and append. We rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability. By utilizing the homomorphic token with distributed verification of erasure coded data, our system achieves the integration of storage correctness insurance and data error localization. One of the future enhancement idea includes whether we can construct a system to achieve both public verifiabilityand storage correctness assurance of dynamic data. Besides, along with our research on dynamic cloud data storage, we also plan to investigate the problem of fine-grained data error localization.

REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, from Illinois Institute of Technology angw.lou from Worcester Polytechnic Institute on the paper of "Ensuring data storage security in cloud computing," in Proc. Of IWQoS'09, July 2009, pp. 1–9.

[2] Venkatesa Kumar V and Poornima G from Anna University of Technology, Coimbatore, Coimbatore, Tami Nadu on the paper of" Ensuring Data Integrity in Cloud Computing" in Journal of Computer Applications ISSN: 0974 – 1925,Volume-5, Issue EICA2012-4, Feb 2012.

[3] Dinesh.C, P.G Scholar, Computer Science and Engineering, Mailam Engineering College, Mailam, Tamilnadu. On the paper of "Data Integrity and Dynamic Storage Way in Cloud Computing".

[4] K.ValliMadhavi, R.Tamilkodi and R. Bala Dinakar from Dept of MCA GIET,RajahaMundry on the paper of "Data Storage Security in Cloud Computing for Ensuring Effective and Flexible Distributed System" in International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X.

[5] Wang Shao-huiP Chang Su-qinP Chen Dan-weiP Wang Zhi-weiP from College of Computer, Nanjing University of Posts and Telecommunications, Nanjing210046, China; on the paper of "Public Auditing for Ensuring Cloud DataStorage Security With Zero Knowledge Privacy".

[6] Amazon.com, "Amazon Web Services (AWS)," Online at http://aws.amazon.com, 2008.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

[7] N. Gohring, "Amazon's S3 down for several hours," Online athttp://www.pcworld.com/businesscenter/article/142549/amazons s3 down for several hours.html, 2008.

[8] A. Juels and J. Burton S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. of CCS '07, pp. 584–597, 2007.

[9] Cong Wang, Qian Wang, KuiRen, Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE transactions on Services Computing, 06 May 2011.

[10] Sun Microsystems, Inc., "Building customer trust in cloud computing with transparent security," Online at https://www.sun. Com/offers/details/sun transparency.xml, November 2009.

[11] Cloud security defense to protect cloud computing against HTTP-DoS and XML-Do attacks, Ashley Chonka, YangXiang n, WanleiZhou, AlessioBonti, and Elsevier.

[12] Towards Secure and Dependable Storage Services in Cloud Computing Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, KuiRen, Member, EEE, Ning Cao, Student Member, IEEE, and Wenjing Lou, Senior Member, IEEE- 2011.

[13] M. Einar, N. Maithili, T. Gene. Authentication and integrity in outsourced databases [J]. ACM transactions On Storage. 2006, 2(2): 107-138.

[14] J. Hendricks, G. Ganger, and M. Reiter, "Verifying Distributed Erasure coded Data," Proc. 26th ACM Symposium on Principles of Distributed Computing, pp. 139–146, 2007.

[15] "On the Use of Shamir's Secret Sharing Against Side-Channel Analysis" by Jean-SebastienCoron, Emmanuel Prouff, and Thomas Roche Tranef jscoron@tranef.com , ANSSI, 51, Bd de la Tour-Maubourg, 75700 Paris 07 SP, Francefirstname.name@ssi.gouv.fr.

[16] Shamir, Adi (1979), "How to share a secret", Communications of the ACM 22 (11): 612–613, doi:10.1145/359168.359176.

[17] Dawson, E.; Donovan, D. (1994), "The breadth of Shamir's secret-sharing scheme", Computers & Security 13: 69–78, doi: 10.1016/0167-4048(94)90097-3.

AUTHOR BIOGRAPHY

Mr. Vinayak R. Kankatehas received the B.E. degree from Pune University, Nasik in 2011. He is currently pursuing M.TECH degree in the Computer Science and Engineering at VJTI, Mumbai under Mumbai University, Mumbai. His area of interest is security, data storage, integrity and privacy in Cloud Computing, and Secure Mobile Cloud as well as Cryptography and Network security. He is currently doing his project in cloud computing area.

Varshapriya J. N
Assistant Professor
Department of Computer Science
VeermataJijabai Technological Institute, Mumbai