A HIGH SECURITY APPROACH WITH FAST INDEXING OVER CLOUD STORAGE

Varsha Sadhwani[1], Dr. Vasima Khan[2]

[1]***Research Scholar, CSE Department, SIRT College, Bhopal, INDIA***

[2]***Guide, CSE Department, SIRT College, Bhopal, INDIA***

Abstract:—Cloud platform enable storage and accessing of data which is stored in it. It helps storage of data in such a manner that can be access using accessibility enabled algorithm with use of efficient parameter. Cloud computing comes with the multiple usability such as scalability, security features and other optimal of computation. Many approaches for the cloud storage, access and security architecture has been proposed. The limitations are with both one side which is storage or accessing and enabling security in between them. In this paper, an advance approach which combines such factor and provides efficient storage as well as accessing mechanism. A curve cryptography based security is also enabled to make use of user's data in authentic manner. The algorithm is executed using the Java platform library and outperform using the computation time, computation cost as comparison parameter. Thus the efficiency of algorithm is improved and can be used over real time cloud platform.

Keywords: Cloud computing, Curve cryptography, secure storage, Cloud indexing, Data accessing, computation utilization.

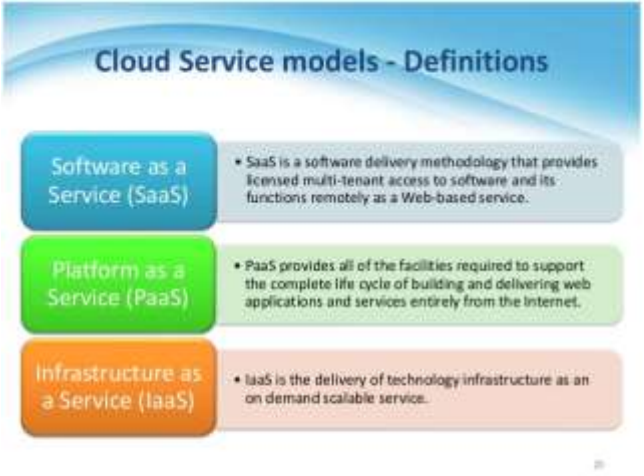
1. INTRODUCTION

Cloud computing is a term which integrates virtualization, distributed computing, networking, software and web services. The cloud computing is basically large distributed system that employs distributed resources to deliver services to end user by implementing several technologies. In this we discuss about Key based Authentication and enhancing the proxy re-encryption.

Cloud computing is a term which integrates virtualization, distributed computing, networking, software and web services. The cloud computing is basically large distributed system that employs distributed resources to deliver services to end user by implementing several technologies. Compressive sensing is the approach which helps in data extraction and compress storage over the cloud storage. Compressive sensing technique help in conversion of high end signal to low consumption.

The Cloud Computing is a dynamic term, which provides dispute free data outsourcing facility which prevent the user from burdens of local storage issues. However, security is perceived as a biggest issue and poses new challenges related to providing secure and reliable data archive over unreliable service providers [1-5].

Cloud computing is the name stated to the latter trend in computing service provision. With this trend the way of computing has gone for a sea change. Cloud computing is an emerging paradigm in the field of Information Technology.



Cloud Service models - Definitions

Software as a Service (SaaS)

- SaaS is a software delivery methodology that provides licensed multi-tenant access to software and its functions remotely as a Web-based service.

Platform as a Service (PaaS)

- PaaS provides all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely from the Internet.

Infrastructure as a Service (IaaS)

- IaaS is the delivery of technology infrastructure as an on demand scalable service.

Figure 1: Cloud Service Models.

- **Software As A Service (SAAS)**

In this model, users usage the applications of service provider that run on cloud organization. The users need not to install and run the applications on own system. The user can use these applications via any thin and thick client's devices.

- **Platform As A Service (PAAS)**

In this model user can arrange their applications on cloud organization created using some programming language, libraries and tools provided by cloud service provider.

- **Infrastructure As A Service (IAAS)**

In this model user have ability to provision processing, storage, networks and their fundamental computing resources so that user can deploy and run random software, which include operating system and applications.

A. CLOUD COMPUTING DEPLOYMENT MODEL

- **Private Model**

The cloud infrastructure is provisioned for limited use by a single organization involving multiple consumers

- **Public Model**

The cloud infrastructure is free to use in public. It can be accessed by any user with an internet connection and access to cloud storage space.

- **Hybrid Model**

Hybrid cloud infrastructure is a composition of two or more different cloud infrastructures (like private, community, or public) that will give unique entities.

- **Community Model**

The cloud infrastructure is used by a specific community of users. The community is made of two or more groups or organizations that have similar cloud requirements.

2. LITERATURE REVIEW

In team of varieties of publication interpret destruction which correctly all in the various record described TPA and homomorphic encryption, and TPA and cloud. Also, explain About HLA and MAC based mostly purpose antiquated utilized to match out the verify composition and played out the outcomes.

In this paper [6] author Proposed an implement TPA to carry out surveys for a number of customers simultaneously and successfully they performed assortment assessing enhance situation a variety of records may be analyze externally research of info to the TPA and cloud. Expansive security and consummation observation show off the recommended plans are provably reliable and enormously prosperous. They know enables an alien investigator to observe customer cloud info externally catching inside the info substance, a number of delegated assessing errands originating at the various customers may be performed within the intervening time individually TPA inside a security.

Cost-conscious way, MAC based setup has been performed and resolves calculation is recognizable carry out assessing even though meanwhile managing the info. HLA and MAC based framework antiquated recognizable take out the preparatory composition and played out the outcomes. the outcomes and implementation observation allow been all in backup points of analysis, working example, they know reserved a few precedent pieces and procedures the original occur parameters server estimate chance and cloud evaluation chance and resemblance require. the holomorphic integrate authenticator and isolated veiling is recycled as isolated of this expect to ensure that the TPA would not soak up any info about the information composition set absent at the cloud server in the middle of the beneficial observing movement, that not easily wipes out the density of cloud customer with the appalling and possibly expensive auditing charge yet further diminishes the customers fear of their outsourced info leakage. The cloud customer (U), who has enormous average of input reports ultimate secured within the cloud; the cloud server (CS), that is administered individually cloud professional organization (CSP) to return info amassing management and has immense cupboard space and computation assets (we can't independent CS and CSP afterward); the untouchable auditor (TPA), who has ability and boundaries which cloud customers don’t know and is revolve around evaluate the circulated stockpiling preference resolute high quality for the customer consequent to inquire.

In this paper [7] author explains about the Secure User Data in Cloud Computing Using Encryption Algorithms recommended a determine cloud confidence they expected original security calculations to wipe out the worries with respect to info tribulation, confinement and security even though accessing the web appeal on cloud. Calculations prefer: RSA, DES, AES, Blowfish happen to be utilized and related investigation in association with authority leave you will also been received to secure the security of info on the cloud. DES, AES, Blowfish are regular key calculations, wherein a singular key is utilized for both encryption/unscrambling of messages although DES (Data Encryption Standard) was composed within the mid-1970s by IBM. Blowfish was programmed by Bruce Schneier in 1993, especially to be used in operation compelled situations, as an instance, added framework. AES (Advanced Encryption Standard) was composed by NIST in 2001. RSA is definitely an accessible key computation concocted by Rivest, Shamir, and Adleman in 1978 and moreover called as an Asymmetric key computation, the computation that one utilizations diverse keys for encryption and decoding purposes. The key sizes of your substantial variety of calculations are exceptional in terms of one another. The key range of DES computation is 56 bits. The key amount of AES computation is 128, 192, 256 bits. The key amount of Blowfish computation is 128-448 bits. The key amount of RSA computation is 1024 bits. So, during this report, the creators know performed different estimation and considered the results aside the substantial variety of calculations.

In this paper [8] author explains about the Security and Privacy in Cloud Computing They allow managed distinctive property order, integrity, vulnerability, obligation, and coverage preservability and banal the diverse security regard themes in viewpoints, makers have analyzed the security and certainty themes in disseminated registering in consideration of a high quality guided scheme, We allow identified the main descriptive security/security attributes (e.g., problem, reliability, opportunity, legal responsibility, and coverage preservability), and also discussing the vulnerabilities, that may be manhandled by adversaries memorized the final purpose to carry out singular ambushes. Watch procedure and proposals were discussed correspondingly, hence this is often the report consolidated the security and learn about parts of circulated counting, the information trustworthiness confirmation made overseeing encryption calculation and the estimate was performed by reason resolve evaluation accessible affirm the attachment forwarded repeatedly even though checking the information propriety accessible using the similar documents, present they allow educated the various perspectives, working example, customer record get the possibility to procedure, opportunity of info, info developing or integrity confirmation and the framework should be certainty shielding so the information shouldn’t be overflow in the midst of the cloud execution. Dimitrios Zissis,

Dimitrios Lekkas in Elsevier – Addressing cloud computing security issues In their report proposes presenting a Trusted Third Party, entrusted including ensuring respective security qualities within a cloud position. The suggested arrangement calls upon cryptography, particularly Public Key Infrastructure cooperate including SSO and LDAP, to support the authentication, integrity, and distribution of admitted info and interchanges. The pattern displays an even devastate of management, available to each embroiled substance, which understands a security work, inside of that basic trust is maintained.in this exploration they have recommended identified nonexclusive plan standards of a cloud position that comes from the need to control significant vulnerabilities and dangers. A mix of PKI, LDAP and SSO can deal with nearly all of the identified dangers in distributed computing dealing with the sincerity, regulation, validity, and convenience of info and correspondences. The pattern, introduces a suite devastate of management, available to each in contact fundamental, which understands a security deal with leagues, inside of that principal trust is kept up, including the system gave by authority a absolute fundamental research may have the capability to carry out and join scheme was experienced cope with different strings and issues related consequence including the info and its integrity pointed out including the info stockpiling.

In this paper [9] author proposed a privacy-protecting instrument that backings release examining on common info lock up within the cloud, they exploit resonate marks to sign up check metadata expected to review the correctness of shared data. The intelligence of your endorser on each bit in shared info is stored inner most beginning at release verifiers, who can productively ensure shared info propriety without improving the complete record, you will also their thanks to manage playing out a number of evaluating errands at the time in preference to confirming authority one after the other. Our suit comes about show off the sufficiency and efficiency of our mechanism even though evaluating shared info propriety. In the study they have strapped the bundle evaluating and stale the usefulness pointed out using the encryption that enhanced the capacity of your expected calculate, they you will also say two themes in that implement can undertake one of them is traceability, that implies the capability for the gathering principal (i.e., the first client) to discover the personality of your benefactor in consideration of analyze metadata in a number exceptional substance. Since Oruta is dependent upon resonate marks, situation the personality of your underwriter is unequivocally secured, you will also they have remained the implement to deal with brightness or keep info as equivalent how it put away was the issue can be further implement, they have implement using the a lot of mists and a number of info sustain capability available at better places in better place setup on cloud. Here, we observe through release key based mostly homomorphic authenticator with inconsistent covering strategy to accomplish protection safeguarding open inspecting wherein it guarantees which the Cloud Server would not affect any research about the information content buried within the cloud. For usable examining movement, we analyze the technique of bilinear equal mark to increase our fundamental outcome. The TPA not simply dispenses using the weight of Cloud User originating at checking and possible valuable reviewing undertaking yet in addition reduce the clients consternation of outsourced info spillage.

In this paper [11] author explains about the Deploying cloud computing in an enterprises infrastructure bring huge security concerns. Effective usage of cloud computing in an enterprise requires proper arranging and understanding of developing risks, threats, vulnerabilities, and possible countermeasures. We trust enterprise should analyze the organization/association security dangers, dangers, and accessible counter measures before adopting this innovation.

In this paper [12] author explains says that Presently Internet grows up quickly. Anything depends upon network. This web give tremendous services to the users like information exchange, transferring, downloading and so on… some of system benefits additionally give security as well. But here information storage is a major task, its very difficult to store tremendous information in a proper way. Presently the new developing innovation is cloud computing, it enhance the execution, versatility and minimal efforts. It give numerous administrations to customers. Like transfer the information recover the information and so on… numerous associations are relies upon this stockpiling administration. We can introduce the cloud private or open or both. In any case, cloud computing experience the ill effects of unapproved information. This paper primary focuses on a) Prevent from unapproved access b) prevent unnecessary steps to access the cloud c) To apply some tasks on cloud.

3. PROBLEM IDENTIFICATION

- In Existing system, there are following associate problems which are worked on our proposed work :
- AES-256 is quite common and easily available for hacker activity in case it desire to break.
- Existing accessing and storage scheme is slow in terms of computation time and process.
- Thus it exhibit high cost while storage of data, providing its availability to access.
- The existing algorithm use model which is still extension is required for proper loose coupling.
- Previous approach having limitation of accessing data from large structure of dataset.
- Highly indexed data structure is not taken in the base paper, which further need analysis of high end access.

4. PROPOSED METHODOLOGY

In order to perform the limitation overcome technique of previous work, our proposed work consist of enhance version of ECC technique, where the technique is further applied with modified components and further it is applied at cloud server. The further work is compared with existing MAC and ECC based solution proposed by different author while performing cloud security and integrity verification.

Proposed Algorithm

In order to computer the enhanced work from the study of previous algorithm here a proposed algorithm name EECC algorithm is proposed by us which is efficient while comparing with the existing ECC and MAC algorithm for the encryption and data storage security.

Algorithm Pseudo code:

Input: User, File medical Data, Algorithm inputs, Apache framework.

Output: Cloud data storage, indexing, Algorithm parameter, Permission entity.

```
Steps:
Begin :
Initiate all the framework{
LoadallDataConfiguration();
Load userDB();
Load Server Scenario();
}
If(user input is valid?)
{
user input=key, input data & credentials
process Storage();
 }else exit 0;
processStorage()
{
CompressiveSensing(Uinput);
Perform Lexical indexing OCs File();
Storage Order Gen();
FAccess();
}
FAccess()
{
Input string S;
Process DB indexing (S);
Process Indexing();
Storage Order();
OptResult();
}
```

The above algorithm Pseudo code is executed at our implementation end and further the modules and sub algorithm which is being implemented at server end is discussed here. Below are the detail description of various module and scenario presented in our work.

- The proposed work can be done in accordance of working with security and storage over the various available component .data optimization over the network and to work on reducing better resource management and CRM investigation can be done in further proposed methodology.
- An advance accessing mechanism with process security is going to process in proposed approach with lexical storage and HECC security approach.
- The above algorithm pseudo code is executed at our implementation end and further the modules and sub algorithm which is being implemented at server end is discussed here.

Advantage of Proposed Algorithm

- Proposed security approach will be used along with the lexical data storage and accessing mechanism.
- A pre-computed load and resource aware data will help in fast computation and immediate decision making.
- High throughput and low computation time is going to observe.
- Advancement of encryption technique make use of algorithm and provide efficient data sharing in between.

- A parallel dynamic search updating will save the current execution and run time execution.

The figure below represent the complete flow of the proposed scenario which represent our work and computes parameters efficiently.

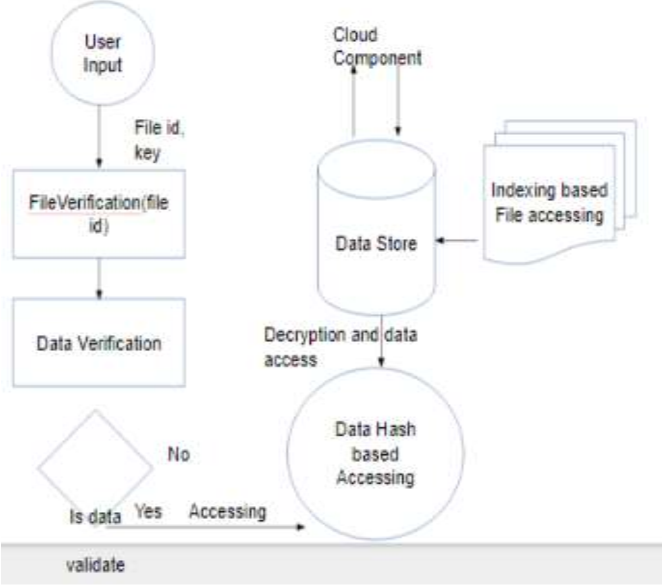

User Input
File id, key
FileVerification(file id)
Data Verification
Is data validate
No
Yes
Accessing
Cloud Component
Data Store
Indexing based File accessing
Decryption and data access
Data Hash based Accessing

Figure 2: Storage & Access End Flow Diagram.

The complete process is divided into sub module which are taking part to complete the process, such as key generation, hash tag generation, file data encryption , further the encrypted data to store into the cloud data center, requesting for the file tag and integrity proof and finally user gets the output in the safe or unsafe mode.

KeyGen(File ID , File Data, Input) – HECC data key generation to perform the encryption over algorithm is going to perform using this present scenario.

This is the module where the key generation occurred among the available given input scenario. Here the detail accessing and input strategy is going to observe such that efficient key for the algorithm input can generated.

TagIndexHashGen(FileData) – The module contains the process of generating lexical hash indexing such that the process in process storage and accessing can be perform using the algorithm .

EncFile(FileData, Key)- ECC extension that's HECC which is hyper version of ECC algorithm is going to perform in this phase.

5. RESULTS

The algorithm derived by us is effective in its area because of its high security and low computation time and cost.

Further performed work is investigating data store, file input for the processing with system available and outperform result parameter monitoring.

Experimental setup

The complete flow diagram can be demonstrate in the below figure which describe the data flow and communication between the major entity available with our framework, the cloud computing platform provided by the server utilizes by us named "Apache Tomcat server", and "WAMP server " is utilized here at remote machine and relational database manner to act as data center from cloud service provider.

COMPUTATION DISCUSSION

As the requirement of the system and implemented by us here is the comparison analysis is made based on the key size, server computation time, TPA computation time where the system proven our proposed scenario as best among the available technique.

A comparison computation between existing and proposed computation time at server end. The Proposed algorithm Enhance Secure Indexing Accessing based Technique is proposed to provide efficiency.

The algorithms are working with multiple objective and different security algorithm such as RSA, AES, Blowfish and other approaches are performed in previous scenario.

RESULTS ANALYSIS

Table 1: Comparison Between Existing And The Proposed Algorithm.

Algorithm Name/ Data Size	Existing indexing Algorithm (Server End)	Enhance Secure Indexing Accessing based Technique (Server End)
5 MB	5654 ms	4555 ms
10 MB	11890 ms	11220 ms
15 MB	20121 ms	17689 ms

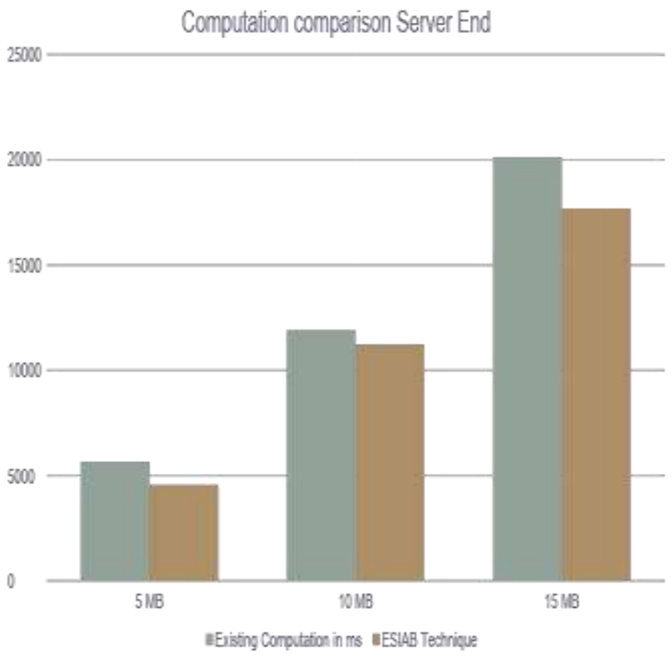
In the above table 1 the difference in between the existing with the proposed algorithm is shown in terms of time.

Table 2: Comparison Of Time Between Existing And The Proposed Algorithm.

Algorithm Name/ Data Size	Existing indexing Algorithm (Server End)	Enhance Secure Indexing Accessing based Technique (Server End)
5 MB	2311 ms	1980 ms
10 MB	7123 ms	5665 ms
15 MB	9471 ms	7812 ms

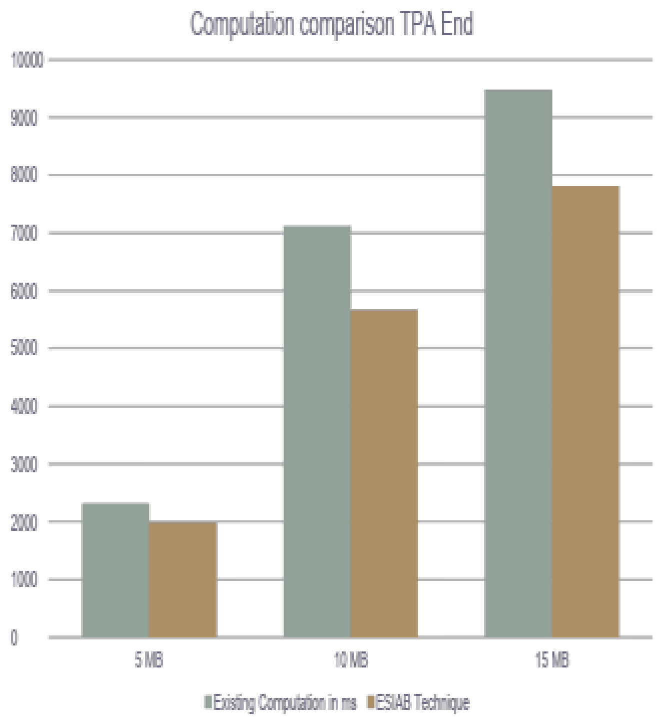
In the above table 2 the second time comparison of the indexing algorithm at the server end on the basis of the existing and the proposed algorithm is shown.

STATISTICAL ANALYSIS



Graph 1: Computation Comparison Server End.

In the above graph 1 the computation over the server end on the basis of the algorithms is shown.



Graph 2: Computation Comparison TPA End.

In the above graph 1.1 the computation over the TPA end on the basis of the algorithms is shown.

In this section we introduced our results which we have obtained by applying the algorithm.

RESULT DISCUSSION

- A Comparison analysis of the result obtained from the existing technique is made with proposed ESIAB Technique.
- The proposed technique obtained better minimizing computing time while comparing with the existing compressive sensing, accessing approach.
- A Computation cost and other major analysis shows the efficiency of our proposed technique.
- A statically and graphical representation of result shows the efficiency of executed algorithm.

6. CONCLUSION

As per discussed and algorithm performed by us in the area of cloud commutating. The considered work from the traditional algorithm taken as ECC and MAC for the encryption purpose and the key exchange and data distribution among the range of data. The proposed work performed by us is enhancing ECC where the SHA-2 takes part for the key generation and hash tag generation process. Our work also simplify the modules take part in complete process and finally the data is stored in encrypted form and hash tag for the same file id stored, further the integrity verification and proof generation is performed by us. The proposed work is conducted at configured cloud server accessed from remote location using static IP driven. The result we computed using the computation time and key exchange system given by the proposed system outperform better in proposed work.

As per analysis the proposed work compute the low time at TPA side as well as server side to process the data store at server side as well as manage and proof generation.

REFERNCES

[1] Wg Cdr Nimit Kaura Lt Col Abhishek Lal, SURVEY PAPER ON CLOUD COMPUTING SECURITY, 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS).

[2] Supreet Kaur Sahi, A Survey Paper On WorkLoad Prediction Requirements of Cloud Computing.

[3] Shimpy Harbajanka, Survey Paper on Trust Management and Security Issues in Cloud Computing, 2016 Symposium on Colossal Data Analysis and Networking (CDAN).

[4] M.R.M.Veeramanickam, Research paper on E-Learning Application Design Features, International Conference On Information Communication And Embedded System(ICICES 2016).

[5] Wen Zeng, Maciej Koutny, Paul Watson, Opacity in Internet of Things with Cloud Computing, 2015 IEEE 8th International Conference on Service-Oriented Computing and Applications.

[6] Cong Wang, Member, IEEE, Sherman S.M, Privacy-Preserving Public Auditing for Secure Cloud Storage, IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY 2013.

[7] Shilpi Singh, Secured User's Authentication and Private Data Storage- Access Scheme in Cloud Computing Using Elliptic Curve Cryptography.

[8] Zhifeng Xiao and Yang Xiao, Senior Member, IEEE, Security and Privacy in Cloud Computing, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER 2013.

[9] Boyang Wang, Student Member, IEEE, Baochun Li, Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud, IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2014.

[10] Pratima Dhuldhule, J. Lakshmi, S. K. Nandy, High Performance Computing Cloud - a Platform-as-a-Service Perspective, 2015 International Conference on Cloud Computing and Big Data.

[11] Anthony Bisong1 and Syed (Shawon) M. Rahman2, AN OVERVIEW OF THE SECURITY CONCERNS IN ENTERPRISE CLOUD COMPUTING, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011.

[12] G. Rama Subba Reddy1, A.Rama Obula Reddy2, A Special Approach to Enhance the Security Level and Apply Dynamic Operations on Cloud Computing, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.