ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)
Vol. 3, Issue 1 (Jan. - Mar. 2016)
International Journal of Advanced Research in Education & Technology (IJARET)

Enhanced Security and Privacy to Outsourced Data Using Hash Function

[I]Mohd Asadullah, [II]Umesh Chandra, [III]R K Choudhary
[I]Ph.D. Scholar, [II]Assistant Professor, [III]Professor
[I,II,III]Dept. of Computer Science, Sri Venkateshwara University, Meerut, UP, India

Abstract
As Cloud Computing grow into ubiquitous, more and more sensitive data are being integrated into the cloud. It is quite difficult to keep up all necessary data in secure manner where it has the necessity for various usages for users in cloud. Cloud service is centred on Web Service area, and it will go through all types of security issues comprising what online services aspect. Security is the main concern for development of the cloud services. For the safety of data privacy, sensitive data typically have to be encoded before outsourcing, which marks better service utilization a very complex task. On the other hand, encrypted data must be searchable for client or user (registered) in relevant manner to minimize the cost and overhead and maximize the utilization of data. In this paper, we discuss the mechanism of data security before outsourced and make it usable through allowing clients or users to safely search over scrambled data.

Keywords
Security; Privacy; Outsourced Data; Cloud computing;

I. Introduction

Cloud computing, the innovative terminology for the extensive imagined vision of computing as a service [1], empowers appropriate, on-demand control access to an integrated place of configurable computing resources (e.g., webs, requests, application, facilities and information) that can be quickly arrayed with strong proficiency and nominal supervision overhead [2]. The remarkable benefits of Cloud Computing comprise: on-demand self-service, global network access, position independent resource assembling, quick resource resistance, pay as you go facility, transferral of risk, etc. [2]-[3]. Thus, Cloud Computing could simply assistance its consumers in evading outsized principal amounts in the organization and managing of both software and hardware. Unquestionably, Cloud Computing carries specific paradigm flowing and assistances in the area of IT. The applications of web and novel technologies today, for commerce and for these clients, is even now a part of living. Any data is accessible at any place within the world at any time. Few years ago that wasn't probable [4]. Today it has risen lots of prospects of right to use to public and personal data like web speed access or the readying of mobile dispositive that enable the joining to web from virtually all over. Nowadays lots of individuals are accessing their mail on-line through webmail shoppers, writing cooperative documents victimization net browsers, making computer-generated albums to transfer their pictures of the vacations. They're active apps and storage data in servers situated in web and not in their own terminals. Something as straightforward as enter in an exceedingly web content is that the solely thing a user must begin to usage the services that exist in on a far off server and lets him share non-public and personal info, or expending computing cycles of a mound of servers that he can ever see with his own eyes [5]. And each day its getting used a lot of these facilities that are known as cloud workstation service area. That term is given as a result of the trope regarding web, as one thing than the client see sort of a cloud and can't see what's within.

Cloud computing is a global source where user wish to keep all his data with safety dimension, and outsourced his data in secure manner through this many application, program and computational concepts can grow complete profits via this technology without any confined physical storage device and server for his data storing. These facilities and services are generally distributed into three classes as:

- Infrastructure-as-a-Service.
- Platform-as-a-Service and
- Software-as-a-Service [6]-[7]

As Cloud Computing grow into ubiquitous, more and more sensitive data are being centralized into the cloud, such as emails, individual health records, private albums and images, corporation business figures and facts, official and legal record, etc. By keeping their data into the cloud, the data vendors can be reassured from the load of data storage and management so as to enjoy the on-demand great eminence data storage facility. However, the point that data holders and cloud server are not in the identical confidential domain may put the contract out data at risk, as the cloud server may no lengthier be wholly trusted in such a cloud environment due to a sum of reasons: the cloud server may disclosure data facts to unlicensed bodies or be scythed. It follows that sensitive data generally should be encoded prior to contract out for data confidentiality and opposing unauthorized accesses.

However, data typically have to be encoded before outsourcing, which marks better service utilization a very complex task assumed that there could be a huge volume of outsourced data records. Furthermore, in Cloud Computing, data vendors may provide access of their outsourced data with an enormous number of users. The particular users might require to only access certain particular documents they are concerned for the time of a specified period. One of the most common techniques for access or retrieve the particular file and document is through keyword-based search rather than repossessing all the encoded documents which is totally unfeasible in cloud computing concepts. These keyword-based search method permits users to individually retrieve required documents and is being used frequently in plain-text search circumstances, such as Google search. Regrettably, data encryption limits customer's capability to accomplish keyword search and thus creates the classical plain text search procedures inappropriate for Cloud Computing. Moreover this, data encryption also requires the security of keyword privacy since keywords typically comprise with significant information correlated to the original data. Although keyword privacy can be

ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

secured by encryption of keyword, it more reduces the classical plaintext search methods unusable in this phenomenon.

II. Properties of Cloud Computing

1. Minimum Investment
At the start, any business has to get the complete structure that wants for starting to run an assignment. It suggests that lots of expense in PC setup. If this business has all the in-house it implies that it ought to get few servers and personal computers powerful sufficient to help all the requiring of the business. If this business starts to usage some services within the cloud, it will cost less cash during this organization and capitalize it in different regions of the plan.

2. Cost Minimization
As of expense by requirement, simply fee what's being employed, and since it's not essential to own establishments targeted on the up keep and capability of the organization or package that's employed by cloud computing.

3. New Functionalities and Actualizations
The code informs area unit monitored by the supplier of the service, this supplier are going to be fascinated by actualize all the merchandise that they provide as shortly as doable to draw in additional purchasers. That the organization don't ought to be disturbed regarding these items and don't would like special staff centred in this [8].

4. Organization focused in Business
Organization can emphasis their energies a lot of in business space and not most within the technical one. The main aim of any organization should be cost effective services and products with quality.

5. Data Sharing
As this services are net centered, it's easy to right to use to any or all information of any other party or to his information through each straightforward stratagem with net affiliation, thus it's terribly suitable for that parties that have various access points. Specialists regarding cloud computing recognizes next points as potential issues regarding the utilization of cloud computing [9].

6. Service Availability
There's a giant obsession within the clients of cloud computing, it's however trustworthy is the service, as a result of the enterprises desires information and alternative services twenty four hours day. Suppliers cannot provide full assurance of sharing however their degrees of obtainability of service are high. Supplier's deals an agreement, SLA (however, generally it's tough to grasp however critics are often lose a service for some time).

7. Data Lock-in
The application interface of cloud computing are still no standardized, therefore it's tough to share information among suppliers in simplified method. additionally it's tough to usage in similar method completely to other suppliers and additionally signify consumer to see that suppliers have additional power than themselves, as a result of if enterprise needs to alter of supplier it'll be tough to alter all services and knowledge and this generates, making disbelief in purchasers [9].

8. Low accountability within the security of data
Information is that the one amongst the foremost value vigorous in enterprise, therefore it's an awfully necessary call the way to have it. It's traditional to assume that have this information outer of the business will be a drag. Additionally managers of businesses are sometimes conventional during this reasonably selections therefore it's still a drag. Commonly organizations arrange to find non-crucial information within the cloud and save the private one hosted within the business.

9. Low performance/Points of failure
The speed and latency problem of the networks is a blockage simply. The throughput of our system is affected especially within the IaaS deal, wherever we want huge volume of knowledge transmission. Additionally we have a tendency to get a lot of completely different points of letdown: the affiliation of the individual business and also the affiliation of the supplier.

10. Difficult to customize the application
Services provided within the open cloud are centered to many clients, don't seem to be centered specifically issues, simply centered generally resolutions and frequently don't disclose a lot of personalization. It describes it's exhausting to search out focused applications related to the in-house code arcade wherever we will results to the majority requirements.

III. Issues and Challenges

1. Security
The procedure of keeping data on the cloud and access that data from the cloud, the main things are intricate: the customer, server, and network among them [10]. These three components must keep robust security to make mandatory of data security. User is liable for guaranteeing that no another party can approach to the model. In this case when consider the security issue of cloud store house, our motive is more about another two components i.e. server and the network among server and client.
All cloud server storing sources are handled by high achievement and high accessibility store house capacity system. Several cloud results work on personal hard-disks from the host network, which describes any computational or storage let-down can cause in down period and probable data loss. As cloud servers are self-directed, if there occurs any server crash in kept data, these can be endangered against in-house and external attacks.

2. Authentication and Identity Administration
By using cloud services, clients can simply access their private information and make it accessible to several services across the web. An identity management (IDM) tool can support to validate users and services based on identifications and individualities.

3. Access Control and Accounting
Heterogeneity and variety of service area, as well as the domains' diverse access necessities in cloud computing surroundings, request fine-grained access control strategies. In individual, access control services should be flexible sufficient to detention dynamic, framework, or feature- or identity-based access requests and to impose the attitude of least honour. Such access control services might essential to incorporate privacy-protection necessities conveyed through composite guidelines.

4. Trust Management and Policy Integration

Although various service suppliers coincide in clouds and co-operate to deliver numerous services, they might have diverse security methodologies and privacy policies, so we must address heterogeneity among their mechanisms. Cloud service suppliers might require comprising numerous services to empower superior application amenities. Therefore, mechanisms are compulsory to confirm that such a dynamic association is controlled securely and that security breaks are successfully scrutinized during the interoperation procedure.

5. Secure Service Management

In cloud computing environments, cloud service providers and service integrators compose services for their customers. The service integrator avails a platform that helps independent service providers to orchestrate and interwork services and cooperatively provide additional services that fulfil customers' protection requirements.

6. Privacy and Data Protection

Privacy is an essential concern in all the issues we've deliberated so far, containing the requirement to secure individuality facts, strategy mechanisms during incorporation, and operation accounts. Many administrations aren't contented storing their data and records on systems that exist in outside of their own premise data centres.

7. Data Integrity and Confidentiality

Confidentiality and uniformity of data can be confirmed on the both adjacent of server i.e. server side and user side. Communication among user and server must be through a protected network, means the data should be private and uniformity during the transmission over server and user. Several protocols such as SSL [11] to attain to a secure communication.

8. Data Availability

Availability of resources as well as stored data and information to the server is confirmed, and then the server should always guarantee that kept information are available for clients [10]. The final component of significance also is the network among the server and the user.

9. Dynamic Environment

Data used on cloud computing should be in a dynamic auditing structure. The central theory in this self-motivated atmosphere is that all regulated and flexible setup should have lively action such as updation, add, and remove. The cloud podium which has virtualized circumstances also should have some definite autonomous environments.

IV. Related Work

In cloud computing, data security is the most important concern before outsourced it. Many researchers provide different security model for data privacy and confidentiality.

In Key-Policy Attribute-Based Encryption (KP-ABE), [12] each cipher text is characterized by the encryptor with a frame of expressive attributes. Each private key is related with an access framework that identifies which kind of cipher texts the key can decode. The method is named as Key-Policy Attribute-Based Encryption, since the access configuration is itemized in the private key, while the cipher texts are normally tagged with a set of descriptive attributes.

In CP-ABE [13] structures attribute strategies are allied with attributes and data are related with keys. Whereas, Decryption is allowed only those keys which are related with attributes fulfill the technique related with the data. The encryptor must be capable to elegantly select who should or should not have access to the data that she/he encrypts. Thus, this approach is conceptually nearer to classical access control model such as Role-Based Access Control (RBAC).

The Fuzzy Identity-Based Encryption [14] views an identity as set of descriptive attributes. A Fuzzy IBE policy permits for a private key for an identity a, to decrypt a cipher text encoded with an identity a', if and only if the identities a and a', are near to each other as measured by the set overlap distance metric. Therefore, the scheme permits for a definite quantity of error-acceptance in the individualities.

V. Problem Formulation

The motivation behind all the discussed methodology is to provide secure data before outsource it but these approaches may lead to maintain complicated access hierarchy for security mechanism which increase overhead. And after outsourced this encrypted data it may also complicated task to search over on this encrypted data for the user and find out the optimum solution according to his/her requirement.

So, in this paper we proposed a framework to provide a secure data over cloud in which the data owner needs to maintain only a few secrets and the data is also modified by owner as well as auditor to minimize the overhead. And we also provide a mechanism to search data on encrypted data to increase the usability and relevancy of data.

VI. Proposed Work

Among all security and management necessities of cloud computing, key management and it's overhead is one of the important requirements in order to its security and handle its dynamic nature avoid securely management issues. In this work, we will introduce a model which provides the security on data before outsource it.

The basic idea of this proposed approach is to create the data block encryption keys by a hierarchy. Each key in the hierarchy can be resulting by conjoining its parent node and some public data. Since the derivation process uses a one-way function, we cannot determine the secret keys of the parent node and sibling nodes. In this manner, the data owner will require to maintain only the source nodes of the hierarchies. During the key circulation process, the owner can refer the secrets in the hierarchy to end consumers based on their admittance rights. The end user will originate the leaf nodes in the hierarchy to decode the data blocks. The charge of this method is the calculation of one way functions during key derivation which minimize the communication overhead.

Although there are various selections of the association of key hierarchies and key derivation tasks, below we proposed a methodology using a binary tree structure and hash functions. Without losing generality, we assume that the outsourced data hold n blocks and $2^{p-1} \leq n \leq 2^p$. Therefore, we can figure a binary tree with height p as follows. The data owner will choose a root secret $k_{0,1}$. Here the first index of the key represents its level in the hierarchy, and the second index represents its sequence in the level. For example, for level x in the hierarchy, the sequence numbers are from 1 to 2^x. In this way, for node $k_{i,j}$ in the hierarchy,

its parent is $k_{(i-1),(\lceil j/2 \rceil)}$ (when $i \neq 0$), and its children are $k_{(i+1)(2*j-1)}$ and $k_{(i+1),(2*j)}$ (when $k_{i,j}$ is not a leaf node). The keys in level p will be used to encrypt the data blocks. The hierarchy is illustrated in Fig. 1.

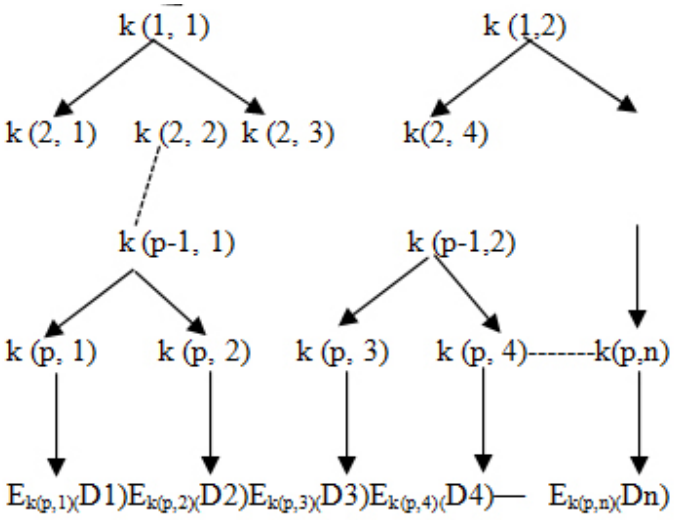

Fig.1 Key derivation hierarchy

Left child of k (i, j):

$$k((i+1),(2*j-1)) = \text{hash}(k(i,j)\|(2*j-1)\|k(i,j))$$

Right child of k (i, j):

$$k((i+1),(2*j)) = \text{hash}(k(i,j)\|(2*j)\|k(i,j))$$

Now we discuss the key derivation process as the above figure described. The data owner selects a public hash function h (). For any node $k_{i,j}$ in the hierarchy, its left child can be computed as $k_{(i+1),(2*j-1)} = h(k_{i,j}\|(2*j-1)\|k_{i,j})$. Here we `sandwich' the sequence number of the child node with the parent's key and then apply the hash function. We can calculate the right child of $k_{i,j}$ in a same manner. Through continually applying this function, a node can calculate the secrets of all of its children. When we reach level p of the hierarchy, the hash results can be used as keys to encrypt the data blocks.

After encryption of data; searching and indexing the data becomes problematic. For example, if data is stored in clear-text, one can efficiently search for a document by specifying a keyword. This is impossible to do with traditional, randomized encryption schemes. Cryptographers have recently invented versatile encryption schemes that allow operation and computation on the cipher text. Searchable encryption allows the data owner to compute a capability from his secret key. A capability encodes a search query, and the cloud can use this capability to decide which documents match the search query, without learning any additional information. For this evaluation we addressed two cryptographic primitives such as homomorphic encryption and Private Information Retrieval (PIR) perform computations on encrypted data without decrypting. As these cryptographic techniques mature, they may open up new possibilities for cloud computing security.

From the above encryption we provided security of data before outsource and maintain at less overhead of key management at owner as well as owner end.

VII. Result analysis

For the performance of this work, the result of proposed approach is compared with existing approach. The results clarify that the proposed work helps in increasing the security on cloud when outsourced. Therefore the proposed work has higher security and less overhead. The comparison of existing approach [12], [13], [14] and proposed work on the basis of below parameters is depicted in table 1.

Table.1 Comparative Analysis

Parameters	Existing Approach(s)	Proposed Approach
Security	High	High
Computational Overhead	High	Low
Fine grain Access Control	Average	High
Collision Resistant	Average	Low
Cloud Security	Average	High
Key Size	Linear	Constant
Data Sharing	Allow	Allow
Encrypted searching	NA	Allow

VIII. Conclusion

In this paper, the methodology provide a secure mechanism over data on cloud with minimum overhead through maintain a few secrets by the owner and give the responsibility to auditor also to edit the data base if authorized to minimize the computational overhead. And we also addressed the searchable scheme on encrypted data to increase the usability of data in the aspect of user.

The proposed work can be further elongated to analyse the addressed searchable scheme and find out the optimum solution for searchable index and provide the relevant result to the user with minimum overhead.

References

[1] *D. Parkhill, "The challenge of the computer utility," Addison-Wesley Educational Publishers Inc., US, 1966.*

[2] *P. Mell and T. Grance, "Draft nist working definition of cloud computing," Referenced on June. 3rd, 2009*

[3] *M. Armbrust and et.al, "Above the clouds: A berkeley view of cloud computing," Tech. Rep., Feb 2009.*

[4] *Y. G. Min, Y. H. Bang, "Cloud Computing Security Issues and Access Control S5.olutions," Journal of Security Engineering, vol.2, 2012.*

[5] *E. Yuan and J. Tong, "Attribute Based Access Control (ABAS) for web Services," Conference on Web Service, IEEE, 2005.*

[6] *Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Springer-Verlag Berlin Heidelberg -2009.*

[7] *G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 598–609.*

[8] *M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE Transactions on Parallel and Distributed Systems, vol 24, no 1, Jan 2013.*

[9] *Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion," IEEE Transactions on Dependable and Secure*

Computing, vol 9, no 6 NOV/DEC 2012.

[10] B. S. Bindu, B. Yadaiah, "Secure Data Storage In Cloud Computing," International Journal of Research in Computer Science, Vol 1 Issue 1, pp. 63-73, 2011.

[11] M. Zhou, Y. Mu, W. Susilo, M. H. Au, "Privacy-Preserved Access Control for Cloud Computing," IEEE International Joint Conference, 2011

[12] S. Subashini, V. Kavitha," A Survey on Security issues in Service delivery models of Cloud Computing," ELSEVIER, 2011

[13] L. Wang, D. Wijesekera and S. Jajodia, "A logic based framework for attribute based access control. Proceeding of ACM workshop on formal methods in Security Engineering. pp. 45-55, ACM press.2004.

[14] M. Raykova, H. Zhao, and S. M. Bellovin, "Privacy Enhanced Access Control for Outsourced Data Sharing," Columbia University, Department of Computer Science,New York.

[15] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and efficiently searchable encryption," inProceedings of Crypto 2007, volume 4622 of LNCS. Springer-Verlag, 2007.

[16] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc.of IEEE Symposium on Security and Privacy'00, 2000.

[17] E.-J. Goh, "Secure indexes," Cryptology ePrint Archive, Report 2003/216, 2003,

[18] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keywordsearch," in Proc. of EUROCRYP'04, 2004.

[19] B. Waters, D. Balfanz, G. Durfee, and D. Smetters, "Building an encrypted and searchable audit log,"in Proc. of 11th Annual Network and Distributed System, 2004.

[20] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data,"in Proc. of ACNS'05, 2005.

[21] C. Danwei, H. Xiuli, and R. Xunyi, "Acess Control of Cloud Computing service based on UCON," Nanjing University of posts & Telecommunications, Springer 2009.

[22] S.Yu, C.Wang, K.Ren, W.Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Journel from Illinois Institute of Technology.

[23] A. Pimlott and O. Kiselyov, "A Logic Based Trust Management System," Proceeding of 8th international symposium on Functional and Logic Programming, Springer, Japan. 2006, pp. 130-144.

[24] E. Damianiet al., "New Paradigm for Access Control in Open Environment," Proceeding of 5th IEEE International Symposium on Signal Processing and Information.2005

[25] P. Bonatti and P. Samarati, "A unified framework for regulating access and information release on the web," Journal of computer Security. 10(3): 241-272.2002.