Secure and Efficient Data Retrieval in Cloud Computing

Mrs.Pushpalata S.Patil.
Lecturer Dept of Information Technology
Shantiniketan Vidyamandir Sec & high Sec School[Junior College],sangli.

Abstract- *Cloud computing changed the world around us. Now people are moving their data to the cloud since data is getting bigger and needs to be accessible from many devices. Cloud computing has formed the conceptual and infrastructural basis for tomorrow's computing. The global computing infrastructure is rapidly moving towards cloud based architecture. While it is important to take advantages of could based computing by means of deploying it in diversified sectors, the security aspects in a cloud based computing environment remains at the core of interest. Cloud based services and service providers are being evolved which has resulted in a new business trend based on cloud technology. With the introduction of numerous cloud based services and geographically dispersed cloud service providers, sensitive information of different entities are normally stored in remote servers and locations with the possibilities of being exposed to unwanted parties in situations where the cloud servers storing those information are compromised. This paper reviews the existing technologies and a wide array of both earlier and state of-the-art projects on cloud security and privacy.*

The cloud server may fail to keep up the integrity of the cloud data due to hacking or entry of unauthorized entities. While searching the data in the cloud the attackers prefer the keyword which is not secured properly Traditional searchable encryption techniques allow users to securely search over encrypted data through keywords,, they support only Boolean search and are not yet Sufficient to meet the effective data utilization demanded by large number of users and large amount of data files in cloud. In this paper implement secure ranked keyword search over encrypted cloud data.

Keywords- Cloud computing, cloud service, cloud security, computer network, distributed computing, security, IAAS, OPSE, PAAS.

I. INTRODUCTION

Cloud computing is the next generation in computation. Maybe Clouds can save the world; possibly people can have everything they need on the cloud. Cloud computing is the next natural step in the evolution of on-demand information technology services and products. The Cloud is a metaphor for the Internet, based on how it is depicted in computer network diagrams, and is an abstraction for the complex infrastructure it conceals. It is a style of computing in which IT-related capabilities are provided "as a service", allowing users to access technology-enabled services from the Internet (i.e., the Cloud) without knowledge of, expertise with, or control over the technology infrastructure that supports them.

In some cases, it might be required or at least possible for a person to store data on remote cloud servers. These give the following three sensitive states or scenarios that are of particular concern within the operational context of cloud computing:

1) The transmission of personal sensitive data to the cloud server,
2) The transmission of data from the cloud server to clients' computers and
3) The storage of clients' personal data in cloud servers which are remote server not owned by the clients.

All the above three states of cloud computing are severely prone to security breach that makes the research and investigation within the security aspects of cloud computing practice an imperative one.

This paper presents an overview of the research on security and privacy of sensitive data in cloud computing environments. We identify new developments in the areas of orchestration, resource control, physical hardware, and cloud service management layers of a cloud provider. We also review the state-of-the-art in privacy-preserving sensitive data approaches for handling sensitive data in cloud computing such as privacy threat modelling and privacy enhancing protocols and solutions. The ownership of data is decreasing while agility and responsiveness are increasing. Organizations now are trying to avoid focusing on IT infrastructure. They need to focus on their business process to increase profitability. Therefore, the importance of cloud computing is increasing, becoming a huge market and receiving much attention from the academic and industrial communities.

Cloud computing was defined in [2] by the US National Institute of Standards and Technology (NIST). They defined a cloud computing in [2] as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

II. LITERATURE REVIEW

Cong Wang, Ning Cao, KuiRen, Wenjing Lo,In this paper, addresses Ranked Searchable Encryption technique that allow users to securely search over encrypted datathrough keywords. Ranked search greatly enhances system usability by enablingsearch result relevance ranking instead of sending undifferentiated results, and further ensures the file retrieval accuracy. But here efficiency of data retrieval ispreferred more over security and authorization of users is not mentioned.[1]

Mahbub Ahmed, Yang Xiang, In this paper introduce a new mechanism of ensuring trust and security in Software as a Service (SaaS) CC. Trust Ticket mechanism is used that helps a data owner in establishing a link between a CSP and a registered user. Thus gain control over data by managing users' access to the data on cloud. The algorithmic protocol for Trust Ticket deployment establishes a data owner's trust. This trust is established through a data owner's control over data and a registered user; because a data owner through Trust Ticket links a registered user with a CSP.[2]

Boneh D, Crescenzo G, Ostrovsky R, Persiano G, In this paper propose that**,** Public key encryption with keyword search enables the service provider to determine whether a document contains a specified keyword without getting any information about the document or keyword. It supports multi user requirements with user authentication and also avoids statistical attack on keywords. It also enables the service provider to participate in partial decipherment thus reducing the users computational overhead. In the proposed scheme, user authentication is provided before giving the secret key for decryption of document. Here when a user is revoked, all the documents in which the user has access needs to be re-encrypted. This introduces heavy computation overhead for the owner of the document.[3]

Sultan Aldossary, William Allen, this paper propose that, Cloud computing changed the world around us. Now people are moving their data to the cloud since data is getting bigger and needs to be accessible from many devices. Therefore, storing the data on the cloud becomes a norm. However, there are many issues that counter data stored in the cloud starting from virtual machine which is the mean to share resources in cloud and ending on cloud storage itself issues. In this paper, we present those issues that are preventing people from adopting the cloud and give a survey on solutions that have been done to minimize risks of these issues.[4]

Monjur Ahmed1 and Mohammad Ashraf Hossain, In this paper, Cloud computing has formed the conceptual and infrastructural basis for tomorrow's computing. The global computing infrastructure is rapidly moving towards cloud based architecture. While it is important to take advantages of could based computing by means of deploying it in diversified sectors, the security aspects in a cloud based computing environment remains at the core of interest. Cloud based services and service providers are being evolved which has resulted in a new business trend based on cloud technology. With the introduction of numerous cloud based services and geographically dispersed cloud service providers, sensitive information of different entities are normally stored in remote servers and locations with the possibilities of being exposed to unwanted parties in situations where the cloud servers storing those information are compromised.[5]

Ali Gholami and Erwin Laure,in this paper, they state that, Cloud computing is revolutionizing many ecosystems by providing organizations with computing resources featuring easy deployment, connectivity, configuration, automation and scalability. This paradigm shift raises a broad range of security and privacy issues that must be taken into consideration. Multi-tenancy, loss of control, and trust are key challenges in cloud computing environments. This paper reviews the existing technologies and a wide array of both earlier and state-of-the-art projects on cloud security and privacy.[6]

III. METHODOLOGY

AES algorithm is a symmetric encryption algorithm, same File Encryption Key (FEK) will be used to encrypt and decrypt the files. Both encryption and decryption of files will be done at client side. Different Files are encrypted with different keys.FEK is encrypted with the user's public key and stored in the Data Decryption Field (DDF) in the header of the file. When a user opens an encrypted file, the user's private key decrypts the FEK in the DDF; then the FEK decrypts the file.

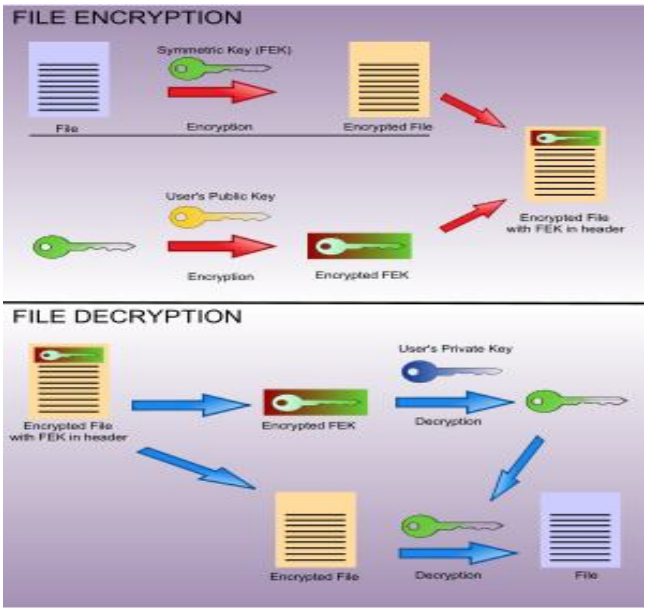

Figure 2: File Encryption and Decryption

Only the private key from the user who encrypted the file can decrypt the FEK, ensuring the file remains secure. Multiple users in the group are allowed to access a file, by storing multiple copies of the FEK in the file's DDF. Each copy is encrypted with public key of exactly one user.

IV. SIMULATION OF THE SYSTEM.

a. Security Analysis:

We evaluate the security of the proposed scheme byanalyzing its fulfillment of the Security guarantee that is to prevent cloud server from learning the plaintext of either the data files or the searched keywords, and achieve the "as-strong-as-possible" security strength. The scheme embeds theencrypted relevance scores in the searchable index inaddition to file ID. Thus, the encrypted scores are the onlyadditional information that the adversary can utilize againstthe security guarantee, i.e., keyword privacy and fileconfidentiality. Due to the security strength of the fileencryption scheme, the file content and keyword privacy is clearly well protected.

b. Performance of System

i. Index Construction:

To allow for ranked keyword search, an ordinary inverted index attaches a relevance score to each posting entry.

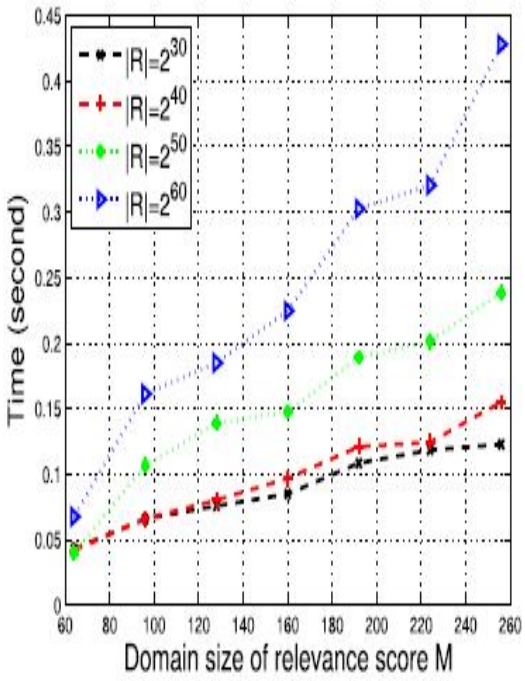

Figure: construction time based on different domain size

The indexsize and construction time listed were both per keyword,meaning the posting list construction varies from one keyword to another. Since we are asking the owner himself to enter the keywords that will be used in future to search the documents before uploading them, most of the storage cost is reduced. Note that the additional bit of encrypted scores is not a main issue due to the cheap storage cost onnowadays cloud servers.

ii. Efficiency of Search

The search time includes fetching the posting list in theindex, decrypting, and rank ordering each entry. Ourfocus is on top-k retrieval. As the encrypted scores are orderpreserved, server can process the top-k retrieval almost asfast as in the plaintext domain. Note that the server does not have to traverse every posting list for each given trapdoor,but instead uses a tree-based data structure to fetch thecorresponding list. Therefore, the overall search time cost isalmost as efficient as on unencrypted data. Following figure list oursearch time cost against the value of k increases, for thesame index constructed above.

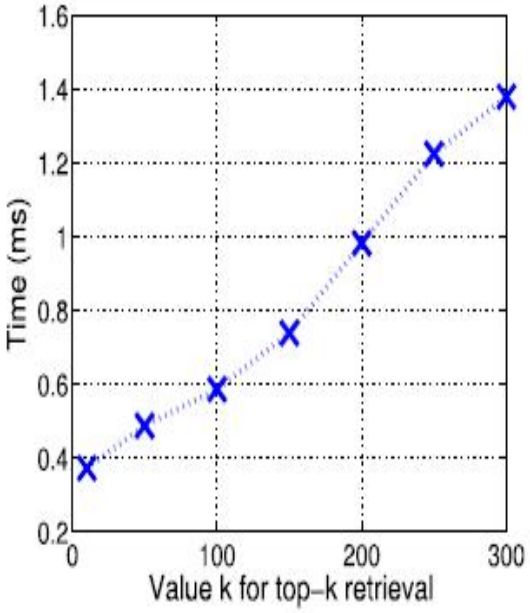

Figure :Time cost for top-k retrieval

VI. CONCLUSION

In this paper, as an initial attempt, we motivate and solve the problem of supporting efficient ranked keyword searchfor achieving effective utilization of remotely storedencrypted data in Cloud Computing. We first give a basicscheme and show that by following the same existing searchableencryption framework, it is very inefficient to achieve ranked search. We investigate some furtherenhancements of our ranked search mechanism, includingthe efficient support of relevance score dynamics and theauthentication of ranked search results. Through thorough security analysis, we showthat our proposed solution is secure and privacy preserving,

While correctly realizing the goal of ranked keywordsearch. Extensive experimental results demonstrate theefficiency of our solution.

REFERENCES

[1] Cong Wang, Ning Cao, KuiRen and Wenjing Lou. "Enabling Secure and Efficient Keyword Search over Outsourced Cloud Data" IEEE Transaction on Parallel and Distributed Systems, VOL. 23, NO. 8, August 2012.

[2] Ahmad. M. and Yang Xiang "Trust Ticket Deployment: A Notion of a Data Owner'sTrust in Cloud Computing" IEEE Security & Privacy, 16-18 Nov. 2011.

[3] Boneh D, Crescenzo G, Ostrovsky R, Persiano G. Public Key Encryption withKeyword Search. In: Proceedings of Eurocrypt 2004, Lecture notes in computer science, vol.3027; 2004.p. 506-22.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Scalable Secure FileSharing on Untrusted Storage," in Proc. of FAST'03, 2003.

[5] https://devcenter.heroku.com/articles/quickstart

[6] 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.

[7] P. Mell and T. Grance, "The nist definition of cloud computing," 2011.

[8] 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.

[9] 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.

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

[11] 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.

[12] M. Sookhak, H. 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.

[13] E. Aguiar, Y. Zhang, and M. Blanton, "An overview of issues and recent developments in cloud computing and storage security," in High Performance Cloud Auditing and Applications. Springer, 2014, pp. 3–33.

[14] I. Gul, M. Islam et al., "Cloud computing security auditing," in Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference on. IEEE, 2011, pp. 143–148.

[15] E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, "Enhanced data security model for cloud computing," in Informatics and Systems (INFOS), 2012 8th International Conference on. IEEE, 2012, pp. CC–12.