A Secure- Search- Scheme over encrypted data By Attaining a close grained query result verification techniques

P.Nikshiptha
B.Tech IV CSE , VITS (N6), Karimnagar, JNTUH, Hyderabad, TS, INDIA
soniya78933@gmail.com

M.Ranadheer
B.Tech IV CSE , VITS (N6), Karimnagar, JNTUH, Hyderabad, TS, INDIA
ranadheer.muriki09@gmail.com

J.Tejaswi
B.Tech IV CSE , VITS (N6), Karimnagar, JNTUH, Hyderabad, TS, INDIA
tejaswijanagama@gmail.com

N.Sindhuja
B.Tech IV CSE , VITS (N6), Karimnagar, JNTUH, Hyderabad, TS, INDIA
sindhunampally70@gmail.com

N.Premalatha
B.Tech IV CSE , VITS (N6), Karimnagar, JNTUH, Hyderabad, TS, INDIA
naredlapremalatha6264@gmail.com

P.Pradeep Kumar
HOD-CSE, Department of CSE, VITS, Karimnagar, JNTUH, Hyderabad, TS, INDIA
pkpuram@yahoo.com

ABSTRACT

Cloud computing is the on-demanding delivery of resources that are retrieved from the internet through Web-based tools and applications. Cloud computing is advantageous to the whole world but at the same time facing the problem of security. Encrypting the data in the cloud is not the solution as it is not meeting up the requirements of user. A secure search technique was developed over encrypted cloud data which allow an authorized user to query data files of interest by submitting encrypted query keywords to the cloud server in a privacy – preserving manner, but practically encounters a problem of incorrectness in the dishonest cloud environment by omitting some qualified results and communications overhead. Thus a well –functioning secure query system should be provided for query result verification. A Mechanism that allows the data user to verify the results. In this paper, we design a secure

,easily integrated and closed –grained query result mechanism by which the query user not only can verify the correctness of each data file in the set, but can also check the correctness of qualified data files returns, how many or which qualified data files are not returned in the set thereby knowing the incomplete information before decryption. The added advantage of this scheme is its loose coupling to concrete secure search techniques and can be easily integrated into any secure query scheme. In this paper we develop a verification object for encrypted cloud data and also a signature technique with extremely small storage cost .

1.Introduction

Cloud computing is a recent technology that uses the Internet, central servers to organize the data and applications, which the user can access. It allows individual users and other business peoples to use application without the necessity to install in their computer. They can access their files, which is located in other computer using Internet. This technology allows for more inefficient computing by centralizing storage, processing memory, and bandwidth. Cloud computing comes in three categories such as Software as a Service (SAAS), Infrastructure as a service (IAAS), Platform as a Service (PAAS).The SAAS provides application software which the user can use. The PAAS provides the platform for the user to do his operation The IAAS provide physical or virtual devices for user. And each provides different services to the user. The cloud is available in four-deployment model namely.

1. Public Cloud

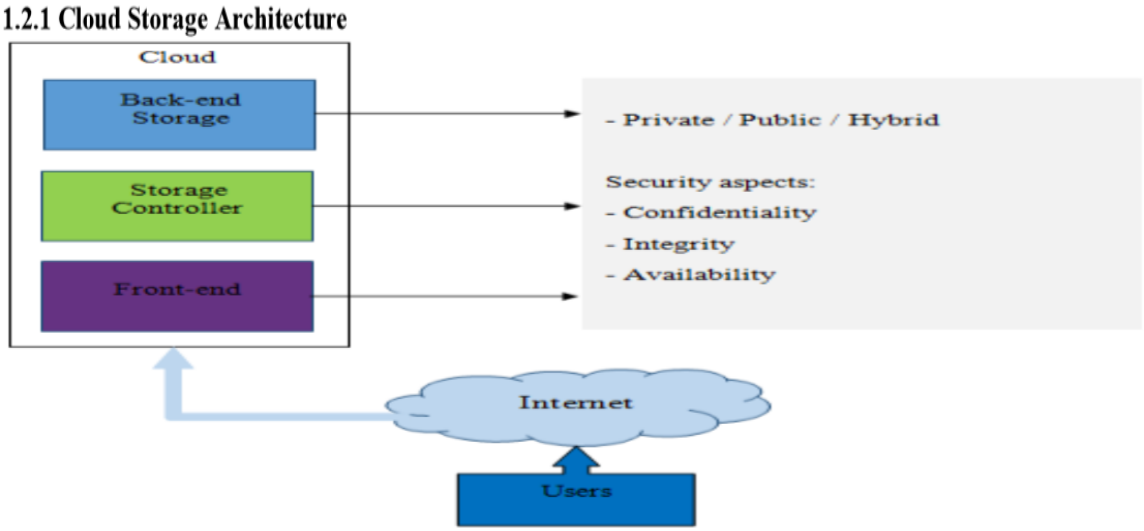
2. Private Cloud

3. Hybrid Cloud

Public Cloud: If the cloud computing resides outside an organization and any one access it is called public cloud. Third party hosts the files. Example: Amazon Elastic Compute Cloud (EC2), Google App Engine, Windows Azure Services Platform.

Private Cloud: If the cloud computing resides inside an organization and file or application accessed through a secure network is called private cloud.

Hybrid Cloud: Combination of public, private and community cloud is called hybrid cloud.



"Figure 2: Generic Cloud Storage Architecture[4]"

1.1Cloud storage

Cloud computing is popular which is booming now-a-days and it is mainly used for storage purpose with high demand .It is a virtual storage areas over a network It is purely based upon Quality-Of-Service (QOS) .

It consists of many fabricates but yet it acts has a single system, The data which is generating from IT Companies are theoretically growing by that, we can't use our hardware, So instead of that we are using cloud storage

Cloud is mainly used to backup the data and it can be maintained regularly. It allows users to access high range of applications immediately uploaded by others.

Advantages:

- Cloud storage avoids the need to buy storage equipment.
- We have to just pay for the amount of storage we are using.
- Cloud storage allows user to access broad range of application and resources immediately, which are hosted by others.

Disadvantages:

- As data is redundant it leads to be hacked by unauthorized users.
- Cloud storage is costly for day users.
- Security is not guaranteed completely for our data.

2. Security Requirements:

- In cloud storage security is the main issue in order to protect the information.
- In this cloud the vast use of technology, it is the service that includes inherint problems, by taking the cloud model all the users misplace there control over physical security.
- Because of many users the data can be shared over the different clouds.

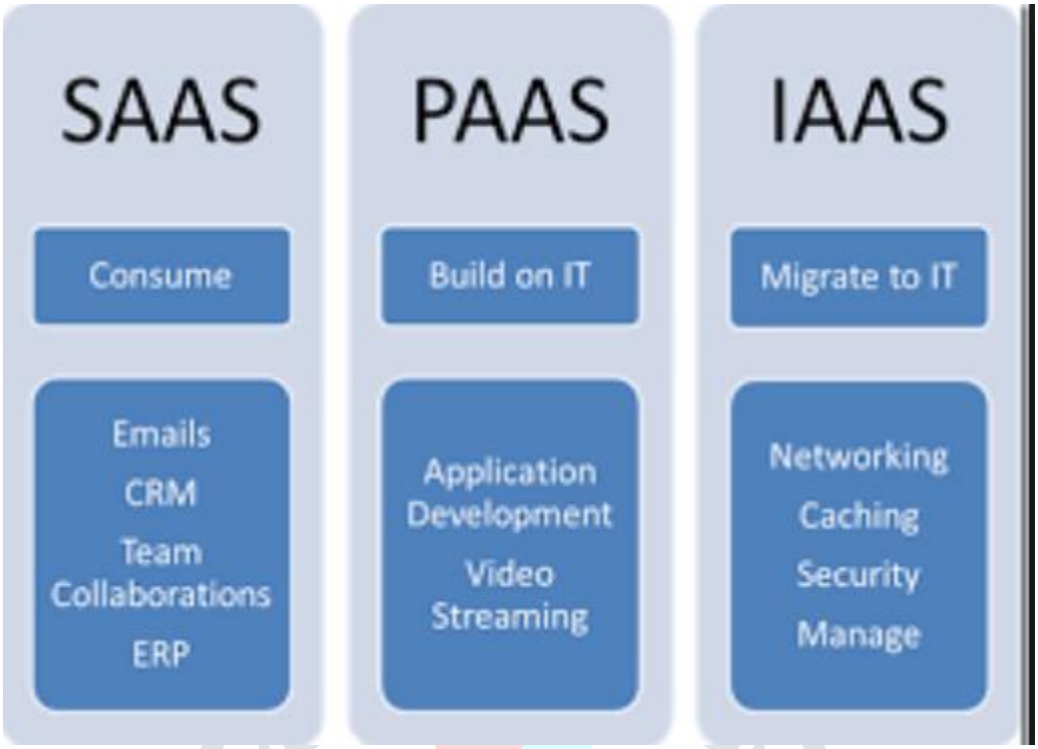
Confidentiality: Protecting data and information from disclosure to unauthorized person.

Integrity: Protecting data and information from being modified by unauthorized person.

Availability: Authorized people are able to access and use data and information whenever require.

2.2Cloud services

Cloud computing comes in three categories such as Software as a Service (SAAS), Infrastructure as a service (IAAS), Platform as a Service (PAAS).The SAAS provides application software which the user can use. The PAAS provides the platform for the user to do his operation The IAAS provide physical or virtual devices for user. And each provides different services to the user. The cloud is available in four-deployment model namely.



Infrastructure as a Service IAAS): gives business access to vital web architecture, such as storage space, servers, and connections, without the business need of purchasing and managing this internet infrastructure themselves. Because of the economies of scale and specialization involved, this can be to the benefit of both the business providing the infrastructure and the one using it. In particular, IAAS allows an internet business a way to develop and grow on demand. Both PAAS and SAAS clouds are grounded in IAAS clouds, as the company providing the software as service is also providing the infrastructure to run the software. Choosing to use an IAAS cloud demands a willingness to put up with complexity, but with that complexity comes flexibility. Amazon EC2 and rack space Cloud are examples of IAAS.

Platform as a Service (PAAS): clouds are created, many times inside IAAS Clouds by specialists to render the scalability and deployment of any application trivial and to help make your expenses scalable and predictable. Some examples of a PAAS system include: Moss, Google App Engine, and Force.com. The chief benefit of a service like this is that for as little as no money you can initiate your application with no stress more than basic development and maybe a little porting if you are dealing with an existing app. Furthermore, PAAS allows a lot of scalability by design because it is based on cloud computing as defined earlier in the article. If you want a lean operations staff, a PAAS can be very useful if your app will capitulate. The most important negative of using a PAAS Cloud provider is that

these services may implement some restrictions or trade-offs that will not work with your product under any circumstances.

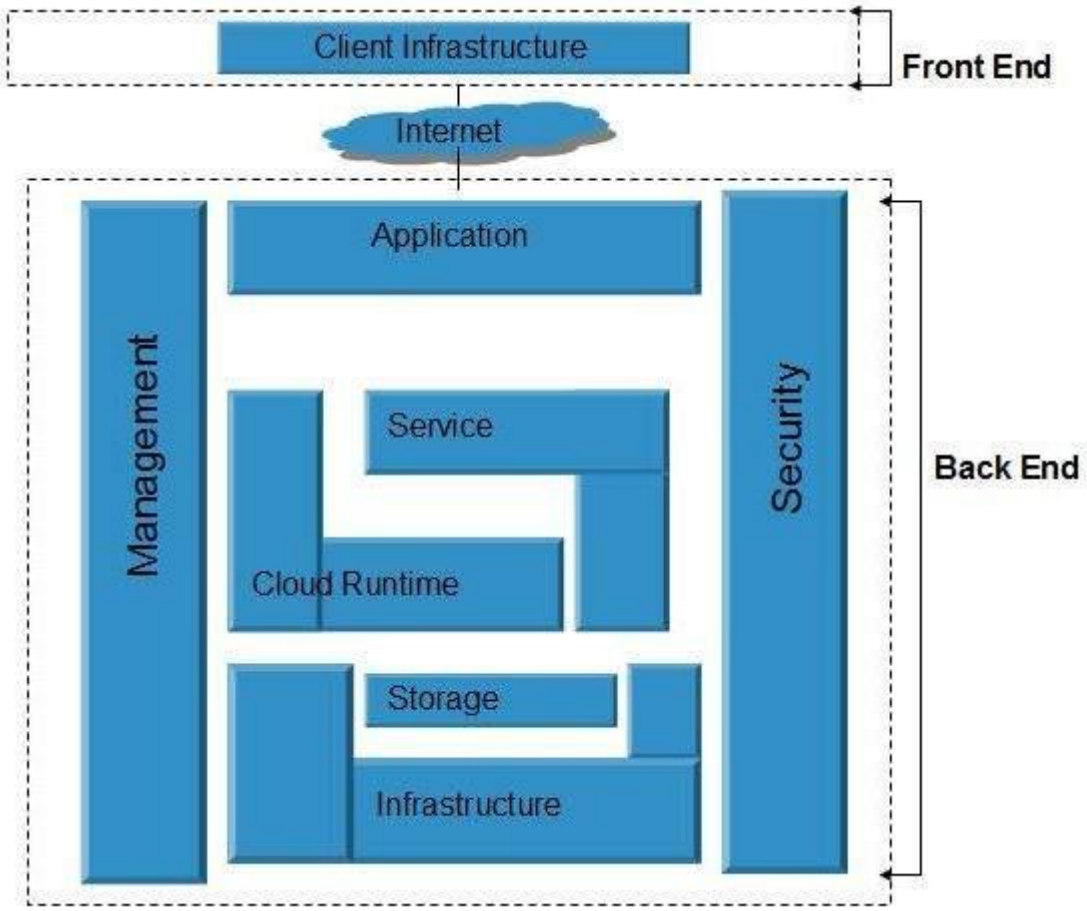
Software as a Service (SAAS): is relatively mature, and the phrase's use predates that of cloud computing. Cloud applications allow the cloud to be leveraged for software architecture, reducing the burdens of maintenance, support, and operations by having the application run on computers belonging to the vendor. Gmail and Sales force are among examples of SAAS run as clouds, but not all SAAS has to be based in cloud computing.

- **Cloud Computing Architecture:**

Cloud Computing architecture comprises of many cloud components, which are loosely coupled. We can broadly divide the cloud architecture into two parts:

- Front End
- Back End

Each of the ends is connected through a network, usually Internet. The following diagram shows the graphical view of cloud computing architecture:



Front End

The front end refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, Example - Web Browser.

Back End

The back End refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc.

3. Existing system:

- Recently, with the growing popularity of cloud computing, how to securely and efficiently search over encrypted cloud data becomes a research focus
- Some approaches have been proposed based on traditional searchable encryption schemes in which aim to protect data security and query privacies with better query efficient for cloud computing.
- However, all of these schemes are based on an ideal assumption that the cloud server is an ”honest-but-curious” entity and keeps robust and secure software/hardware environments. server
- As a result, correct and complete query results always be unexceptionally returned from the cloud server when a query ends every time. However, in practical applications, the cloud server may return erroneous or incomplete query results once he behaves dishonestly for illegal profits such as saving computation and communication cost or due to possible software or hardware failure of the system

Disadvantages:

- Encrypted data make effective data retrieval a very challenging task.
- Security problem

4. Proposed system:

- We formally propose the verifiable secure search system model and threat model and design a fine-grained query results verification scheme for secure keyword search over encrypted cloud data.
- We propose a short signature technique based on certificate less public key cryptography to guarantee the authenticity of the verification objects them-selves.
- We design a novel verification object request technique based on Parlier Encryption, where the cloud server knows nothing about what the data user is requesting for and which verification objects are returned to the user.
- We provide the formal security definition and proof and conduct extensive performance experiments to evaluate the accuracy and efficiency of our pro-posed scheme

Advantages:

our scheme can verify the correctness of each encrypted query result or further accurately find out how many or which qualified data files are returned by the dishonest cloud server

Conclusion:

We proposing here close grained query results verifications scheme foe secure search over encrypted cloud data this scheme was easily integrated with all secure schemes that are implemented on cloud data

This scheme can verify the correctness of each encrypted query results are accurately find out how many are which qualified data files are returned by the dishonest cloud server

A short signature technique is designed to guarantee the authenticity of verification by object itself by which the cloud server knows nothing about which verification object is requested by the data user and return by the cloud server

REFERENCES

[1] P. Mell and T. Grance, "The nist definition of cloud computing," http://dx.doi.org/10.602/NIST.SP.800-145.

[2] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[3] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Springer RLCPS, January 2010.

[4] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in IEEE Symposiumon Security and Privacy, vol. 8, 2000, pp. 44–55.

[5] E.-J.Goh, "Secure indexes," IACR ePrint Cryptography Archive, http://eprint.iacr.org/2003/216, Tech. Rep., 2003.

[6] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public-key encryption with keyword search," in EUROCRYPR, 2004, pp. 506–522.

[7] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetricencryption:improveddeinitionsandefficientconstructions," in ACM CCS, vol. 19, 2006, pp. 79–88.

[8] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and efficiently searchable encryption," in Springer CRYPTO, 2007.

[9] K. Kurosawa and Y. Ohtaki, "Uc-secure searchable symmetric encryption," Lecture Notes in Computer Science, vol. 7397, pp. 258– 274, 2012.

[10] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," IEEE Transactions on Computers, vol. 62, no. 11, pp. 2266–2277, 2013.

[11] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," in Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2013, pp. 258–274.

[12] M. Naveed, M. Prabhakaran, and C. A. Gunter, "Dynamic searchable encryption via blind storage," in IEEE S&P, May 2014, pp. 639–654.

[13] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in IEEE ICDCS, 2010, pp. 253–262.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2017.2709318, IEEE Transactions on Cloud Computing

[14] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keywordrankedsearchoverencryptedclouddata,"inIEEE INFOCOM, 2011, pp. 829–837.

[15] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in ACM ASIACCS, 2013.

[16] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud," in IEEE INFOCOM, 2014, pp. 2112–2120.

[17] W. Zhang, S.Xiao, Y. Lin, J. Wu, and S. Zhou, "Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing," IEEE Transactions on Computers, vol. 65, no. 5, pp. 1566–1577, May 2016. [18] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keywordrankedsearchschemeoverencryptedclouddata," IEEE Transactions on Parallel and Distributed System, vol. 27, no. 2, pp. 340–352, 2015.

[19] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Transactions on Communications, vol. E98-B, no. 1, pp. 190–200, 2015.