Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Comp. Engg. 81 (2015) 32036-32039

ISSN: 2229-712X

# An Efficient Methodology for Cloud Computing to Retrieve Data

Kapil Dev Raghuwanshi and Sitendra Tamrakar

Department of Computer Science Engineering, NRI Institute of Information Science & Technology, Bhopal, India.

**ARTICLE INFO**

**Article history:**

Received: 15 November 2014;

Received in revised form:

19 April 2015;

Accepted: 28 April 2015;

**Keywords**

IaaS,
PaaS,
SaaS,
Hybrid Cloud,
TRSE,
SSE.

**ABSTRACT**

Cloud computing is an efficient data sharing technique where users can directly store and access information through internet. Hence the chances of unauthorized access and security of data is an important issue in cloud computing, hence various techniques are implemented for the security of cloud data. Encryption is a technique of providing a secure access of data over internet, but chances of attack is still possible. Hence an efficient technique is implemented using the concept of multi-keyword based data retrieval in cloud computing with encryption [1]. Although the technique is efficient in terms of communication overhead and security from various attacks but further enhancements can be done in the technique to make it for secure and easy, hence a new and efficient technique is implemented in cloud computing using attribute based encryption and verification, the proposed technique implemented provides security from various attacks and provide less storage and communication overhead.



## Introduction

Cloud computing is now a promising technique for data outsourcing and high-quality data services. Cloud computing delivers the services of the computing rather than delivering a product. With the help of cloud computing computers or machines are given with software's, shared resources and other information and other devices are given as utility over the network. Clouds are classified on the basis of public, private and hybrid [1]. Considering the modern era and technology most of the e-business is conducted over the internet i.e. via internet network. Cloud computing provides data storage, platform, and various IT services through internet. Cloud computing can manage multiple data centres but needs to be deployed efficiently. The basic area to be focused upon is the data security i.e. data privacy. The enterprises provides services like rapid resource elasticity, ubiquitous network access, usage based pricing etc. for which cloud computing enables the enterprises. [2].

- **Public Cloud:** Mainstream web browsers allow users to access cloud through interfaces.
- **Private Cloud:** resides in an organization's internal enterprise datacenter. Thus the cloud setup is deployed inside the organization.
- **Hybrid Cloud:** it is a combination of more than one cloud type.
- **Community Cloud:** Specific community uses this cloud. The community is of the consumers who are from organizations that contain shared apprehensions [2]. Coherent and economic sale is achieved by cloud computing through resource sharing. It maximizes or enhances the effectiveness of shared resources. The resources by cloud are shared by multiple users and are reallocated as per the demand dynamically which thereby helps in allocating resources to users. Cloud computing services and resources can be shared at different hours in different parts of the world. Thus use of computing power increases and environmental damage can be reduced as use of less power, air conditioning, rack space, etc.

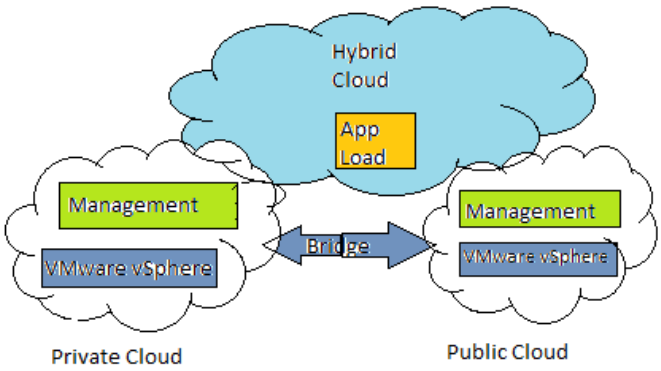


**Figure 1. Types Of Clouds In Cloud Computing**

which are used to deploy variety of functions. Cloud computing, allows different users to access single server for retrieval and updation of the data without the requirement of licenses for different applications. Cloud computing enables the companies to focus upon the business projects rather being worried about the infrastructure and its cost. With the services of cloud computing the organizations can have applications early and running faster and are easier to maintain and manage enabling IT towards adjustment of resources to meet fluctuating and unpredictable demands in business. Through high-capacity networks, low cost computers and multiple storage devices due to widespread adoption of hardware virtualization, service oriented architecture and autonomic and utility computing cloud computing technology is rapidly growing.Clouds are the pools of virtualized resources which are easily usable and accessible. To obtain optimum resource utilization the resources in cloud are dynamically reconfigured. Strong cloud architectures with its mass computing and storage centers various organizations and individuals are benefited when utilizing the services. It consists of virtualization, on-demand deployment, Internet delivery of services, open source software etc. [3]. The data and applications are maintained using remote servers and internet by cloud computing.

Tele:
E-mail addresses: dev_2988@yahoo.co.in

It helps the consumers and businesses to use clouds applications and resources without the need of installing and accessing the personal files on any other computer via internet. Cloud Computing provides efficient computing through various services like centralizing storage, service availability memory, processing and bandwidth promising lower costs, rapid scaling, easier maintenance. The main focus needs upon the data security and privacy. There are various Services provided by cloud computing which are [4].

- Providing Services to multiple distinct end users in opposition to bulk data processing or workflow management for a single user.
- It uses data model containing sharable units in which all data objects have access control lists (ACLs) with one or more users.
- Developers can run applications on a separate and different computing platform with physical infrastructure, job scheduling, user authentication, base software environment etc. and without implementing th platform by themselves..

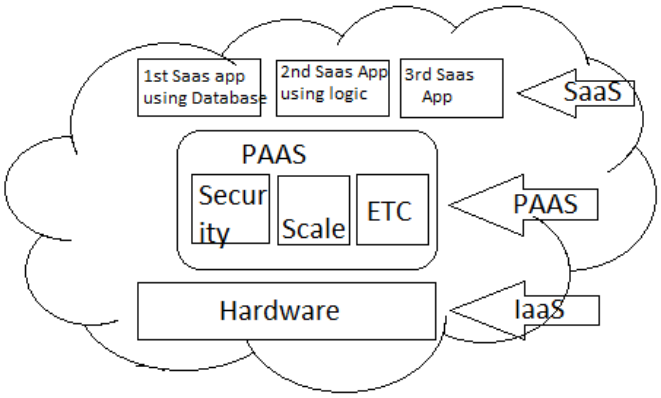


**Figure 2 . Cloud Computing Services**

With the help of cloud computing user can shift his/her work and resources from the personal computers or say individual enterprise applications on to a set of cloud computers. Cloud Computing resolves the problems related with hardware, machine failures etc. with the elasticity property of cloud computing users, capacity or applications can be added at any time without any prior notice and with the pay as you go approach the small and medium sized enterprises can use elasticity property in case when vendor has many customers thereby lowering the per-unit cost to each customer. Whereas larger companies can manage collaborations easily in the cloud.

With the help of Cloud computing environment the individuals and businesses work with applications. The data of the entity is stored and maintained on shared machines in a web based environment and does not physically reside in organizations/individuals home or in the corporate environment. Cloud Computing enables convenient and on-demand network access providing multiple configurable computing resources like networks, servers, storage, applications, services etc. which can be shared and can be provisioned and released without any extra management effort. Service provider has no concern, relation and interaction when resources are released and services are withdrawn. Cloud Computing is based on particular architecture responsible for providing various services and can be categorized as:

- Infrastructure as a Service (IaaS) is foundation of cloud services providing clients to access server hardware, use various storage services, analyze and obtain bandwidth usage and information and other computing resources.
- Platform as a Service (PaaS) is build upon IaaS. Clients can access basic operating software through this. It gives optional services for the development and usage of software applications in the form of database access and payment service. These services are thus not required for purchasing and the computing infrastructure needs not to be managed.
- Software as a Service (SaaS) is builds upon IaaS and PaaS which provides clients to access the software applications [5].

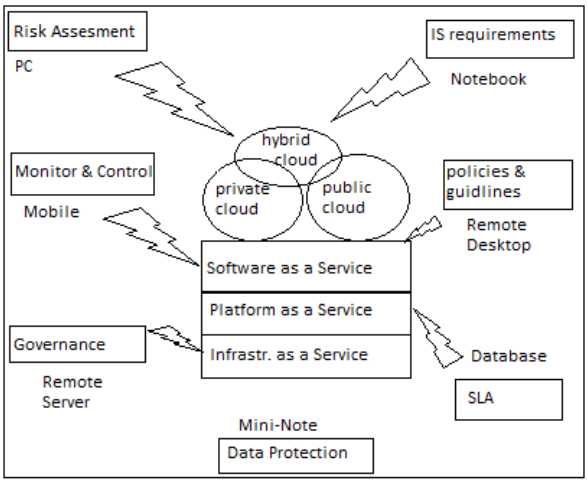


**Figure 3. Cloud Computing Models**

**Literature Survey**

Jiadi Yu [1] et.al. provided with the services which are associated with cloud computing in the form of data outsourcing and data services. Prevention of data is possible through encryption but it is not a efficient procedure. They explained that with the help of Searchable symmetric encryption (SSE) retrieval of encrypted data over cloud is possible. They focused on data privacy issues which are related with SSE and formulated privacy issue from similarity relevance and scheme. Robustness is offered in the case of data privacy leakage when server side ranking based on order preserving encryption (OPE) is used. They presented two round searchable encryption (TRSE) scheme which supports top-k multi keyword retrieval. Employing vector space model and homomorphism encryption scheme search accuracy is enabled and users can involve in ranking thereby fulfilling major concern for security and its requirement of multi-keyword top-k retrieval. The work when being executed on server side with the help of operations on cipher text, information leakage can be eliminated or prevent and thus ensuring data security [1].

Mrs. P.S. Priya [6] et.al. provided that in cloud computing multiple computers are connected through a communication network which is somewhat similar to utility computing and the distributed computing concepts. With the help of cloud computing an application can be executed on multiple machines simultaneously. They explained Searchable symmetric encryption (SSE) which helps to retrieve encrypted data over cloud and for preventing the leakage two round searchable encryption (TRSE) scheme is visualized. TRSE supports top-k multikeyword retrieval and generate a log file module. This enhances the efficient retrieval of data providing search accuracy. It provides the homomorphic encryption enabling the users for ranking and computation work being performed on server side by cipher text operations. Their scheme solved the problem related with secure multi-keyword top-k retrieval over encrypted cloud data by homomorphic encryption provided by TRSE. In the result analysis a log file is generated at the server for each action performed by user on any file [6].

Issa M. Khalil [7] et.al. Explained the benefits provided by cloud computing in the form of configurable computing

resources, economic savings and flexibility of services provided etc. Concepts of cloud comprises of multi-tenancy, resource sharing and outsourcing. This leads in generation of security challenges which requires tuning of security measures. The proposed scheme provides security policies, protocols etc. for cloud security challenges. They identified vulnerabilities associated with the clouds and classified security threats and attacks, presenting state of the art practices to control vulnerabilities, neutralize threats and calibrate the attacks etc. They provided cloud security framework presenting lines of defence identifying the dependency levels and identified various cloud security threats which are then classified into categories. Various cloud security issues like misconfigurations, malicious insiders, multi tenancy, side channels, weak browser security, mobility etc. are analyzed and monitored thereby classifying as categories of security standards, network, access, cloud infrastructure and data. Various attacks are suggested and the countermeasures associated with them with analysis, study and short comings of the solutions giving the measures for cloud security attacks, intrusion detection systems, autonomous systems and federated identity management systems etc.[7]

P. Shanmuga Priya [8] et.al. explained cloud computing as unity of users or cloud customers who can remotely store data on clouds and can retrieve the applications and services from shared pool of resources provided by cloud computing. As the data is stored on shared cloud it's privacy should be protected for an effective data utilization service. They focused on these issues related with data privacy by SSE and proposed that server-side ranking based on order-preserving encryption (OPE) causes leakage in privacy which is resolved by TRSE supporting top-k multi-keyword retrieval. TRSE is employed with vector space model and fully homomorphism encryption (FHE). The vector space model provides search accuracy and FHE is an encryption system providing arbitrarily complex computation on encrypted data [8].

Cong Wang[9] et.al. explained that cloud computing though being economical data service outsourcing needs to focus upon cloud data security by encrypting it before outsourcing the data into public cloud. This is done for protection of data privacy. The problem of secured ranked keyword search over encrypted cloud data is explained and resolved. They explained that with the help of traditional techniques of searchable encryption users are able to securely search the encrypted data with the help of keywords, but this process is insufficient for data utilization in huge number of data files in cloud because the approaches provide support to Boolean search only. File retrieval accuracy is obtained by search result relevance ranking as the usability of the system is increased by ranked search. Relevance score measurement for building secure searchable index is deployed and one to many order preserving mapping technique for the protection of sensitive secure information. In their scheme loss of keyword privacy is prevented by facilitating server side ranking. Solution to efficient ranked keyword search problem is proposed achieving effective utilization stored encrypted data (remotely) in Cloud Computing. They investigated the efficient support of relevance score dynamics, authentication of the ranked search results and reversibility of one-to-many order preserving mapping technique [9].

Mohamed Hamdi [10] et.al. knowledged that Cloud architectures constitutes cost efficient backbones supporting transmission, storage, and computing of the applications contents. Cloud computing is used for business, scientific, and pervasive computing fulfilments. Due to such diverse application area of cloud computing it is also vulnerable to security threats and issues and various concerning features confidentiality, privacy, authentication, anonymity, dependability and fault tolerance conflicts. They explored the fundamental concepts associated with cloud computing its security in the form of cloud security services, cloud security principles, cloud security requirements and various testing techniques.

W. Jansen [11] et.al. remarked that cloud computing provides various services to the people in different ways which are capable of doing multiple operations in the form of on demand scalability and reliability of available pooled computing resources, secure access to metered services, relocation or dislocating the data from inside to outside of the organization etc. Proposing the challenges of privacy and security associated with cloud computing and its services and gave instructions for organizations to take when data is outsourced from applications to public cloud. Multiple organizations requires with various services provided with cloud computing as well as the privacy and security issues associated with it suggesting that public cloud computing is still important information technology solution set that organizations should adopt. They made it clear to ensure that cloud computing solution is configured, deployed and managed for security and privacy concerns of organization thus preventing the data with policies in organization's cloud. Risk management tasks for assessing and identifying the risks are proposed which are related with managing the risks in cloud computing [11].

Ning Cao [12] et.al. remarked cloud computing provides flexibility and economic savings to the data owners while outsourcing their complex data management systems to more commercial public cloud. But this data needs to be encrypted for privacy protection removing the use of traditional approach for data utilization based on plaintext keyword search. Cloud consists of large number of files and documents thus therefore are needed with multiple keyword searches and should return documents in the order of the relevance to these searched keywords. They solved the problem of privacy preserving multi-keyword ranked search (MRSE). Their technique contained efficient similarity measure of coordinate matching which explains to capture relevance of data documents to search query in which all of the possible matches are considered. They proposed MRSE schemes and its idea on secure inner product computation. Similarity measure is computed with the help of inner product similarity and thereby through MRSE schemes achieving stringent privacy requirements which guarantees privacy and efficiency, low overhead on computation [12].

Qi Zhang [13] et.al. explained that cloud computing provide holding and delivering of services and eliminating the requirement for users to plan for future prospects about the provisioning, allowing organizations to start with small resources and increase them when there is high demand for service. They recognized that technology of cloud computing is at its start and still consists of some issues which are needed to be addressed thereby explained its architectural principles, state of the art implementation, research challenges, concepts, design challenges, research directions etc for the proper understanding of cloud technique. With the help of cloud computing utility computing is now a reality. They focused their research on automatic resource provisioning, power management, security management. Cloud computing services contains several features which makes them attractive to business owners in the form of lowering operating cost, no upfront investment, high scalability, easy access, reducing risks and reduced maintenance expenses etc. [13].

M. A. Vouk [14] et.al. explained that cloud computing is obtained from versatile research in fields of virtualization, distributed computing, utility computing, networking, web, software services etc. which gave service oriented architecture. Cloud has reduced information technology overhead by providing flexibility, on demand services, lowered owner cost etc. They remarked the issues associated with cloud computing and presented cloud implementation based on VCL technology. The components and concepts of cloud computing are proposed and explained like computing through service oriented architectures (SOA), component-based system engineering, orchestration of multiple services through workflows, virtualization etc. Cloud computing through Cyber infrastructure increases efficiency, quality, and reliability among applications by analysing and identifying the common features in application which provides efficient and enhanced sharing of services and equipments between the applications [14].

**Proposed Work**

1. Setup the cloud environment with a number of users and data centres and brokers having their individual physical characteristics.
2. User 'Ui' when sends the data to the data centre will generate a keyword and create a string 'str'.
3. User 'Ui' using his public key encrypt the data and send to the storage repository in the form of tupple (keyword, cipher text).
4. User 'Ui' also allots a unique id and password for the receiver for the access of the data.
5. Te receiver needs to authenticate first for the data to access.
6. After authentication receiver 'R' sends query in form of keyword to the central authority where on the basis of keyword the queries are fetched with the match keyword.
7. Receiver accesses the data in encrypted form and performs decryption using private key.
8. Receiver also verifies the message is valid or not using Message Authentication Code.

**Conclusion**

The methodology that we propose here provides security from various types of attacks. The methodology also provides less computational time since the technique doesn't depends on the searching of the multi-keywords in the storage panel. The methodology also provides authentication and validity of the message.

**References**

[1] Jiadi Yu, Peng Lu, Yanmin Zhu, Guangtao Xue and Minglu Li "Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, 2013

[2]P. Mell and T. Grance, "The NIST definition of cloud Computing", 2012.

[3] Pankaj Arora, Rubal Chaudhry Wadhawan and Er. Satinder Pal Ahuja "Cloud Computing Security Issues in Infrastructure as a Service", International Journal of Advanced Research in Computer Science and Software Engineering, 2012.

[4] Dawn Song, Elaine Shi, Ian Fischer and Umesh Shankar "Cloud Data Protection for the Masses", IEEE 2012

[5] Kim-Kwang Raymond Choo "Cloud computing: Challenges and future directions", 2010

[6] Mrs. P. Shanmuga Priya, Preethi.D, Priya.J and shanthini.B, "Retrieval of Encrypted Data Using Multi Keyword Top –K Algorithm", International Journal of Scientific and Research Publications, 2014

[7]Issa M. Khalil, Abdallah Khreishah and Muhammad Azeem "Cloud Computing Security: A Survey", Computers, 2014.

[8] P. Shanmuga Priya and R. Sugumar, "Multi Keyword Searching Techniques over Encrypted Cloud Data", IJSR, 2014.

[9]Cong Wang, Ning Cao, Kui Ren and Wenjing Lou "Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, 2012.

[10] Mohamed Hamdi, "Security of Cloud Computing, Storage, and Networking", IEEE, 2012

[11]Wayne Jansen and Timothy Grance "Guidelines on Security and Privacy in Public Cloud Computing", Draft NIST Special Publication, 2011

[12]Ning Cao, Cong Wang, Ming Li, Kui Ren and Wenjing Lou "Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data", 2010

[13]Qi Zhang, Lu Cheng and Raouf Boutaba "Cloud computing: state-of-the-art and research challenges" Springer, 2010.

[14]Mladen A. Vouk "Cloud Computing – Issues, Research and Implementations", Journal of Computing and Information Technology, 2008