International Journal of advancement in electronics and computer engineering (IJAECE)
Volume 10, Issue3, March. 2021, pp.107-110, ISSN 2278 -1412
Copyright © 2012: IJAECE (www.ijaece.com)

Survey Efficient Multi-User Searchable Encryption Scheme without Query Transformation over Outsourced Encrypted Data

Neha Mishra [1], Rakesh Kumar Lodhi[2]
[1]*M.Tech Scholar,TIT(RGPV), Bhopal,nehamishra2292@gmail.com India;*
[2,] *Assistant Professor, Scholar,TIT(RGPV), Bhopal, rakeshlodhi21@gmail.com , India;*

Abstract – Cloud computing could be a revolutionary mechanism that ever-changing way to enterprise hardware and software system style and procurements. Key encryption is initial topology to classify multiple user and provide security. Searchable Encryption (SE) schemes provide security and privacy to the cloud data. The existing SE approaches enable multiple users to perform search operation Cloud information's are keeping and accessed during a remote server with the help of services provided by cloud service suppliers. Providing security could be a major concern because the information is transmitted to the remote server over a channel (internet). Before implementing Cloud computing in a company, security challenges has to be addressed initial. This study identifies the problems associated with the cloud information storage.

Keywords*: Content based image retrieval, Joint equal contribution, low level features, High level features, Color histogram*

I. Introduction

Cloud computing could be a revolutionary mechanism that ever-changing way to enterprise hardware and software system style and procurements. The cloud computing provides made advantages to the cloud clients like complimentary services, elasticity of resources, easy accessibility through net, etc. From little to massive enterprises poignant towards cloud computing to extend their business and tie-ups with different enterprises [1]. Although cloud computing has huge advantages, cloud user are unwilling to place their confidential or sensitive information, it includes personal health records, emails and government sensitive files. Suppose once information is placed in cloud information center; the cloud consumer lost their direct control over their data sources. The Cloud Service supplier (CSPs) has promise to confirm the information.

Security over hold on information of cloud shoppers by using strategies like firewalls and virtualization. These mechanisms wouldn't offer the entire information protection due to its vulnerabilities' over the network and CSPs have full command on cloud applications, hardware and client's information. Encrypting sensitive information before hosting will be information privacy and confidentiality against CSP. A typical drawback with encryption scheme is that it's impractical due to large quantity communication overheads over the cloud access patterns. Therefore, cloud desires secure strategies to storage and management to preserve the information confidentiality and privacy [2].

Cloud Computing security is that the major concern to be addressed these days. If security measures aren't provided properly for information operations and transmissions then information is at high risk [3]. Since cloud computing provides a facility for a group of users to access the stored information there's an opportunity of getting high information risk. Strongest security measures are to be implemented by characteristic security challenge and solutions to handle these challenges [4].

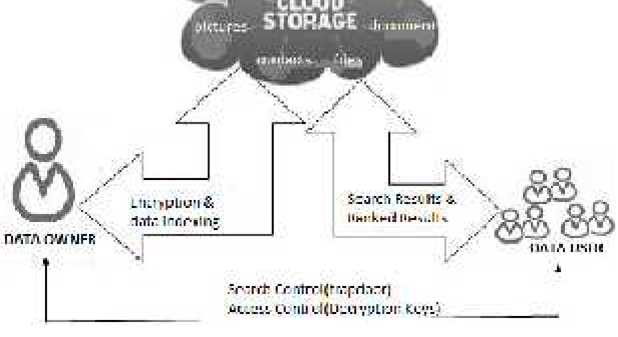

Fig.1 Cloud data storage model

II. Literature Survey

Day by day technology will grow with internet but internet maturity is big issue so here we analysis some paper to enhanced security.

Deepthi Rao et. al. [1] "An Efficient Multi-User Searchable Encryption Scheme without Query Transformation over Outsourced Encrypted Data" This paper Proxy server based approach for supporting search operation over the data of multiple owners is proposed. Different from the existing approaches, the data user's query in this approach can be used to search over the multiple owners' data without transforming the query. In order to bypass the query transformation, the idea of partial encryption is used, i.e., half of each of the both index keyword and query keyword are encrypted by using the secret key of the data owner and the data user respectively and the other half of the index keyword and query keyword is encrypted by using common secret key of the proxy server. The experimental results confirm that the proposed approach is efficient. Future work could be to include a module for addition and revocation of data users and also to enhance the security functionalities of the proposed approach..

Yu Zhang et al.[2] "FEACS: A Flexible and Efficient Access Control Scheme for Cloud Computing", In this paper, we tend to propose a flexible and efficient Access control scheme (FEACS) supported KP-ABE, that is appropriate to protect sensitive data underneath cloud computing setting. It permits users to enrol and leave from cloud surroundings at any time, and it conjointly permits them to vary their access policies on-demand. Moreover, once enrollment, revoking and update occur, only the connected user desires actions. For simple to explain the access policy, full logic expression is additionally supported in FEACS. These benefits build FEACS a lot of efficient and a lot of flexible for practical applications in cloud computing setting. We conjointly formally proved the safety of our scheme under the CCA-DM model and analyze the performance in numerous phases.

Stefano Russo et al.[3] "Editorial: Security and Dependability of Cloud Systems and Services", SERVICE-BASED cloud computing systems are used today in several business- and mission-critical situations. Because the service-oriented paradigm progressively spreads during a big selection of application fields, as well as massive information, cloud storage, mobile cloud computing, and sensor cloud, there's a growing would like for sound methodologies, algorithms and techniques for building services during which corporations, organizations and citizens will trust and depend upon. Security and responsibility are so changing into more and more relevant issues for such systems, whose quality, heterogeneity, and quick ever-changing dynamics bring difficult challenges to the analysis and trade communities.

Kazi Zunnurhain et al.[4] "Security Attacks and Solutions in Clouds", Cloud computing is revolutionizing how information technology resources and services are used and managed, but the revolution always comes with new problems. Authors have depicted some crucial and well known security attacks and have proposed some potential solutions in this paper, such as utilizing the FAT table and a Hypervisor.

Alexander Lawall et al.[5] "Resource Management and Authorization for Cloud Services", In the age of cloud computing, corporations still have the problem to manage access rights for resources. This can be very true, if corporations are combined to virtual organizations and need to share resources that are set at cloud suppliers. For an even authorization model, an up thus far information regarding partner organizations is indispensable. This contribution proposes an approach to request the automated preparation of resources from a cloud supplier. The access rights to the resources are managed and administered by the proprietary company, though partner organizations are concerned. They're not revealed to the cloud supplier; however stay within the owning company. This establishes a separation of resources (i.a. systems) and authorization that alleviates security risks. Attackers of resources cannot access them because the authorization model isn't implemented on identical location because the resources. This makes the intrusion far more advanced.

III. Methods to Secure Data in Cloud

A. Authentication and Identity

Authentication of users and even of communication systems is performed by varied ways; however the most common is cryptography [6]. Authentication of users takes place in varied ways that like within the kind of passwords that's known separately, within the kind of a security token, or within the kind a measurable amount like fingerprint. One drawback with using traditional identity approaches in a very cloud surroundings is faced once the enterprise uses multiple cloud service suppliers (CSPs)[6]. In such a use case, synchronizing identity data with the enterprise isn't scalable. Different issues arise with ancient identity approaches once migrating infrastructure toward a cloud-based resolution.

B. Data Encryption

If you are aiming to store sensitive data on an oversized information store then you would like to use data encryption techniques. Having passwords and firewalls is good; however people will bypass them to access your information. Once information is encrypted it's a type that can't be scan while not an encoding key.

The information is completely useless to the intruder. It's a way of translation of information into secret code. If you would like to scan the encrypted information, you ought to have the secret key or password that's conjointly known as encryption key [7].

C. Information integrity and Privacy

Cloud computing provides data and resources to valid users. Resources are accessed through internet browsers and may even be accessed by malicious attackers [2]. A convenient resolution to the matter of data integrity is to supply mutual trust between supplier and user. Another resolution is providing correct authentication, authorization and accounting controls therefore the method of accessing data ought to go through numerous multi levels of checking to confirm approved use of resources [8]. Some secured access mechanisms ought to be provided like RSA certificates, SSH primarily based tunnels.

D. Availability of Information(SLA)

Non availableness information or data could be a major issue concerning cloud computing services. Service Level agreement is employed to produce the data regarding whether or not the network resources are accessible for users or not. It's a trust bond between client and supplier [9].An way to give convenience of resources is to possess a backup set up for local resources similarly as for many crucial data. This allows the user to possess the data regarding the resources even when their unavailability.

E. Secure Information Management

It is a method of data security for a group of information into central repository. It comprised of agents running on systems that are to be monitored and so sends info to a server that's known as "Security Console". The protection console is managed by admin WHO could be a person WHO reviews the data and takes actions in response to any alerts. Because the cloud user base, dependency stack increase, the cloud security mechanisms to resolve security problems additionally increase, this makes cloud security management rather more difficult. It's additionally referred as a Log Management. Cloud suppliers additionally give some security standards like PCI DSS, SAS 70. Data Security Management Maturity is another model of data Security Management System [10].

F. Data Stealing Solution

At the end of every session, the customer will send an e-Mail about the usage and duration with a special number to be used for log in next time. In this way, the customer will be aware of the usage and charges as well as be availed with a unique number to be used every time to access the system. In Amazon EC2, a key pair is used to verify the authenticity of the customer, but this approach only needs the special number appended with the UserName. There will be an overhead for sending e-Mail to all the customers with a randomly generated number when their session will expire. Eventually, as mentioned earlier, the PID generator inside the Hypervisor can be appointed to commit the task [10, 11].

G. Flooding Attack Solution

All the servers in cloud are thought-about as a fleet of servers. One fleet of server is considered for system kind requests, one for memory management and last one for core computation connected jobs. All the servers in fleet will communicate with each other. once one in every of the server is full, a replacement server is brought and utilized in the place of that server and an another server that's referred to as name server has all the record of current states of servers and can be used to update destinations and states. Hypervisor will be used for managing jobs [10]. Hypervisor additionally do the authorization and authentication of jobs. A certified customer's request will be known by PID. RSA may be accustomed code the PID.

IV. Conclusion

This paper has is detail study of user key allotment and data sharing in cloud architecture. This survey is essentially done to review all the issues like attacks, information loss and unauthenticated access to information and conjointly the ways to remove those issues. However, these approaches incur huge computational burden on PS due to the repeated encryption of the user queries for transformation purpose so as to ensure that users' query is searchable over the encrypted data of multiple owners.

References

[1] Deepthi Rao, D.V.N. Siva Kumar and P. Santhi Thilagam "An Efficient Multi-User Searchable Encryption Scheme without Query Transformation over Outsourced Encrypted Data" 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS) IEEE 2018.

[2] Zhang, Yu, et al. "Feacs: A flexible and efficient access control scheme for cloud computing." Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on. IEEE, 2014.

[3] Wang, Cong, et al. "Toward secure and dependable storage services in cloud computing." IEEE transactions on Services Computing 5.2 (2012): 220-232.

[4] Zunnurhain, Kazi, and Susan V. Vrbsky. "Security attacks and solutions in clouds." Proceedings of the 1st international conference on cloud computing. 2010.

[5] Lawall, Alexander, Dominik Reichelt, and Thomas Schaller. "Resource management and authorization for cloud services." Proceedings of the 7th International Conference on Subject-Oriented Business Process Management. ACM, 2015.

[6] Rao, R. Velumadhava, and K. Selvamani. "Data security challenges and its solutions in cloud computing." Procedia Computer Science 48 (2015): 204-209.

[7] Rao, B. Thirumala. "A study on data storage security issues in cloud computing." Procedia Computer Science 92 (2016): 128-135.

[8] A. Lawall, D. Reichelt, and T. Schaller, “Resource management and authorization for cloud services,” in Proceedings of the 7th International Conference on Subject-Oriented Business Process Management, ser. S-BPM ONE ’15, New York, NY, USA, 2015, pp. 18:1–18:8.

[9] D. Y. Chang, M. Benantar, J. Y.-c. Chang, and V. Venkataramappa, “Authentication and authorization methods for cloud computing platform security,” Jan. 1 2015, uS Patent 20,150,007,274.

[10] R. Bobba, H. Khurana, and M. Prabhakaran, “Attribute-sets: A practically motivated enhancement to attribute-based encryption,” in Computer Security - ESORICS 2009. Springer Berlin Heidelberg, 2009, vol. 5789, pp. 587–604.

[11] Tiwari, Rajni, and Amit Sinhal. "Block based text data partition with RC4 encryption for text data security." International Journal of Advanced Computer Research 6.24 (2016): 107-13.