ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Preserving Privacy by Enhancing Security in Cloud

N.Vaitheeka[1], V.Rajeswari[2], D.Mahendran[3]

Assistant Professor, Department of IT, Karpagam College of Engineering, Coimbatore, India[1,3].

Associate Professor, Karpagam College of Engineering, Coimbatore, India[2].

ABSTRACT: Cloud computing is emerging as a prevalent data interactive paradigm to realize users' data remotely stored in an online cloud server. Cloud services provide more benefits for the users to enjoy the on-demand cloud applications without considering the local limitations. When accessing the data, many users may be in a collaborative relationship, and thus sharing of is significant to achieve productive benefits. The present solutions for security focuses on the authentication to realize that a user's privative data cannot be accessed if it is found to be unauthorized, but it eliminates a subtle privacy issue during a user challenging the cloud server to request other users when the data being shared. The challenge is the request for accessing reveals the user's privacy no matter whether it has got the data access permissions. The distributed privacy-preserving authentication protocol (SAPA) which is authority based to address above privacy issue for cloud storage. shared authority based privacy-preserving authentication protocol (SAPA) to address above privacy issue for cloud storage. In the SAPA, 1) shared access is achieved by anonymous access request matching mechanism with security and privacy considerations 2) attribute based access control is adopted to realize that the user can only access its own data fields; 3) proxy re-encryption is applied by the cloud server to provide data sharing among the many users. Meanwhile, universal compos ability (UC) model is established to prove that the SAPA theoretically has the correct design. This clearly shows that the proposed protocol realizing privacy-preserving data access authority sharing is impressive for multiple users collaborative cloud applications.

I. INTRODUCTION

Cloud computing enables highly scalable services to be easily consumed over the Internet on an as-needed basis. An important benefit of the cloud services is that users' data are usually processed remotely in unknown machines that users do not possess or use. While enjoying the convenience brought by this technology, users' get scared of missing their data. It can become a significant barrier to the wide adoption of cloud services. A novel highly distributed information accountability framework to keep track of the actual usage of the users' data in the cloud. We introduce an object-centered approach that enables enclosing our logging mechanism together with users' data and policies. We influence the JAR coding capabilities to both create a dynamic and moving object, and to make sure that any access to users' data will trigger authentication and automated logging local to the JARs. To make the user's control stronger, we provide distributed mechanisms for auditing. We provide widespread experimental studies that demonstrate the efficiency and effectiveness of the proposed approaches. It is typically a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications.

In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services — such as servers, storage and applications —are delivered to an organization's computers and devices through the Internet.
When compared to grid computing, a computing type where processing cycles that are unused for all computers in a network are harnesses to solve problems too intensive for any stand-alone machine. The applications are Big Data Analytics. Cloud computing is a type of computing where unused processing cycles of all computers in a network are harnesses to solve problems too intensive for any stand-alone machine.
The advantages are

- Scalability and Storage
- Cost Efficient
- Backup and disaster recovery

- Enable IT Innovation
- Unlimited storage
- Easy access of information
- Quick deployment

A Applications

- Big Data Analytics - From fraud detection to statistical research, big data is everywhere. Explore how Hadoop and high performance computing clusters can be best deployed in public and private clouds.
- Development and Test - Develop and test applications in on-demand environment using consistently configured resources, lowering costs and shortening release cycles.
- Disaster Recovery – Public and private cloud enable cost-effective solutions to maintain highly available applications with resilient multi-datacenter and multi-provider architectures, minimizing down time and data loss. Infrastructure -as-a-Service provides the customer with virtual server instances, storage, as well as application program interfaces allows the customer to start, stop, access and configure the virtual servers and storage. Platform-as-a-service in the cloud is defined as a set of software development tools hosted on the provider's network. Developers begin applications on the provider's platform over the Internet. In the software-as-a-service cloud model, the sellers supplies the hardware infrastructure, the software product and communicates with the user through a front-end portal.

II. LITERATURE SURVEY

A Multi-Keyword Ranked Search Over Encrypted Cloud Ns2 Project

Consumer-centric cloud computing paradigm has emerged as the development of smart electronic devices combined with the emerging cloud computing technologies. Many cloud services has been delivered to the consumers with the premise that an effective and efficient cloud search is done. For consumers, the most related products or data that is highly desirable in the “pay-as-you use” cloud computing paradigm? Sensitive data are encrypted before outsourcing to cloud. The existing search is encrypted cloud data support only exact or fuzzy keyword search.

Therefore to enable an effective searchable system with support of ranked search remains a problem. This provides an effective approach to solve the problem of multi-keyword ranked search over encrypted cloud data supporting synonym queries. The main content of this paper is elaborated in two aspects multi-keyword ranked search to achieve more accurate search results and synonym-based search to support synonym queries.

B A Novel Privacy Preserving Location-Based Service Protocol With Secret Circular Shift For K-Nn Search

Location-based service (LBS) is booming up in recent years with the rapid growth of mobile devices and the emerging of cloud computing paradigm. The user privacy issue is the important problem. For privacy-preserving LBS to be successful it must be secure and provide accurate query [e.g., -nearest neighbor (NN)] results. Here we use a protected circular query protocol (PCQP) to deal with the privacy and the accuracy issues of privacy-preserving LBS. Initially, we connect the points of interest (POIs) on a map to form a circular structure.Since the POI-info after shifting and the amount of shifts are encrypted, LBS providers (e.g., servers) have no knowledge about the user's location during the query process. The protocol resists correlation attack and support a multiuser scenario as long as the predescribed secret circular shift is performed before each query; Finally the security level of the proposed protocol is close to perfect secrecy without the aid of a trusted third party and simulation results show that the k-NN query accuracy rate of the proposed protocol is higher than 90% even when is large.

III. EXISTING SYSTEM

Cloud computing provides a new scheme to supplement the current usage. The users may not know the machines which process and publish their data. During their convenience brought by this new technology, users are worried about losing control of their own data.

The data processed on clouds are often utilized, leading to a number of issues related to accountability, which includes the handling of information. Such drawbacks are becoming a hurdle to the wide adoption of cloud services.

Cloud computing enables highly scalable services to be easily consumed over the Internet on an as-needed basis. An important characteristic of the cloud services is that users' data are usually processed remotely in unknown machines that users do not own or operate

A Disadvantage

The existing system does not have the option of granting/revoking data access. It has very less security where hacking plays a great role.

IV. PROPOSED SYSTEM

We innovate a novel highly distributed information accountability framework to keep track of the actual usage of the users' data. An object-centered approach provides enclosing our signing in mechanism together with users' data and policies. The JAR programmable capabilities creates a dynamic and moving object, and to ensure that any access to users' data will trigger authentication and automated logging local to the JARs. To strengthen user's control, we provide many auditing mechanisms. We provide large experimental studies that demonstrate the efficiency and effectiveness of the proposed approaches.

The automatic and enforce enable logging mechanism in the cloud. This approach to data accountability through the novel usage of JAR files is proposed is used for the first time.

We conduct experiments on a real cloud tested. The results demonstrate the efficient scalable, and granular. Analysis is made to make it reliable and to strengthen of our architecture.

A Advantages

The security of the data to be uploaded in the website is enhanced using the concept of One Time Password (OTP). This technique will ensure that only authorized users can access the data. It will be a great task for the hackers to hack the system and steel the data.

V. CONCLUSION

Here a new privacy challenges during data accessing in the cloud computing to achieve privacy-preserving access authority sharing. Authorization establishes guaranteed data confidentiality and data integrity. Data incorruptibility is achieved since the enclosed values are exchanged during transmission. User confidentiality is enhanced by unidentified access requests to privately inform the cloud server about the users' access. Forward security is achieved by the session identifiers to prevent the session interrelationship. The scheme that is proposed is possibly applied for enhanced privacy preservation in cloud applications.

VI. FUTURE ENHANCEMENT

Random number is generated and used for enhancing security. This random number is given to the end users in the form of One Time Password (OTP). This will ensure that the files of the user are safe. So in future time to receive the

OTP can be increased with more upcoming technologies. Random number can be generated by using homo-generic algorithm and calculations which will enhance more security.

REFERENCES

[1] "P. Mell and T. Grance, Draft NIST Working Definition of Cloud Computing,¿¿¿ Nat¿¿¿l Inst. of Standards and Technology, 2009",

[2] A. Mishra , R. Jain and A. Durresi "Cloud Computing: Networking and Communication Challenges", *IEEE Comm. Magazine*, vol. 50, no. 9, pp.24 -25 2012

[3] R. Moreno-Vozmediano , R.S. Montero and I.M. Llorente "Key Challenges in Cloud Computing to Enable the Future Internet of Services", *IEEE Internet Computing*, vol. 17, no. 4, pp.18 -25 2013 [online] Available:

[4] K. Hwang and D. Li "Trusted Cloud Computing with Secure Resources and Data Coloring", *IEEE Internet Computing*, vol. 14, no. 5, pp.14 -22 2010

[5] J. Chen , Y. Wang and X. Wang "On-Demand Security Architecture for Cloud Computing", *Computer*, vol. 45, no. 7, pp.73 -78 2012

[6] Y. Zhu , H. Hu , G. Ahn and M. Yu "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage", *IEEE Trans. Parallel and Distributed Systems*, vol. 23, no. 12, pp.2231 -2244 2012

[7] H. Wang "Proxy Provable Data Possession in Public Clouds", IEEE *Trans. Services Computing*, vol. 6, no. 4, pp.551 -559 2012 [online] Available:

[8] K. Yang and X. Jia "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", *IEEE Trans. Parallel and Distributed Systems*, vol. 24, no. 9, pp.1717 -1726 2013 [online] Available:

[9] Q. Wang , C. Wang , K. Ren , W. Lou and J. Li "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", *IEEE Trans. Parallel and Distributed Systems*, vol. 22, no. 5, pp.847-859 -25 2011

[10] C. Wang , K. Ren , W. Lou and J. Li "Toward Publicly Auditable Secure Cloud Data Storage Services", *IEEE Network*, vol. 24, no. 4, pp.19 -24 2010

[11] L.A. Dunning and R. Kresman "Privacy Preserving Data Sharing with Anonymous ID Assignment", *IEEE Trans. Information Forensics and Security*, vol. 8, no. 2, pp.402 -413 2013

[12] X. Liu , Y. Zhang , B. Wang and J. Yan "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", *IEEE Trans. Parallel and Distributed Systems*, vol. 24, no. 6, pp.1182 -1191 2013 [online] Available:

[13] S. Grzonkowski and P.M. Corcoran "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking", *IEEE Trans. Consumer Electronics*, vol. 57, no. 3, pp.1424 -1432 2011

[14] M. Nabeel , N. Shang and E. Bertino "Privacy Preserving Policy Based Content Sharing in Public Clouds", *IEEE Trans. Knowledge and Data Eng.*, vol. 25, no. 11, pp.2602 -2614 2013 [online] Available:

[15] C. Wang , Q. Wang , K. Ren , N. Cao and W. Lou "Toward Secure and Dependable Storage Services in Cloud Computing", *IEEE Trans. Services Computing*, vol. 5, no. 2, pp.220 -232 2012

[16] S. Sundareswaran , A.C. Squicciarini and D. Lin "Ensuring Distributed Accountability for Data Sharing in the Cloud", *IEEE Trans. Dependable and Secure Computing*, vol. 9, no. 4, pp.556 -568 2012

[17] Y. Tang , P.C. Lee , J.C.S. Lui and R. Perlman "Secure Overlay Cloud Storage with Access Control and Assured Deletion", *IEEE Trans. Dependable and Secure Computing*, vol. 9, no. 6, pp.903 -916 2012

[18] Y. Zhu , H. Hu , G. Ahn , D. Huang and S. Wang "Towards Temporal Access Control in Cloud Computing", *Proc. IEEE INFOCOM*, pp.2576 -2580 2012

[19] S. Ruj , M. Stojmenovic and A. Nayak "Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds", *IEEE Trans. Parallel and Distributed Systems*, vol. 25, no. 2, pp.384 -394 2014 [online] Available:

[20] R. Snchez , F. Almenares , P. Arias , D. Daz-Snchez and A. Mar¿¿n "Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing", *IEEE Trans. Consumer Electronics*, vol. 58, no. 1, pp.95 -103 2012