I J C T A, 9(5), 2016, pp. 2227-2233

An Efficient Data Security Mechanism in Cloud Computing Using Anonymous ID Algorithm

A. Manimaran* and K. Somasundaram**

ABSTRACT

Cloud computing has evolved from a risky and confusing concept to a strategy that organization large and small are beginning to adopt as part of their to overall computing strategy. Cloud computing is a method of providing a set of shared computing resources that includes application, computing, storage, netorking, development and deployment platforms as well as business processes.. Research on the topic of trust in this field has largely focused on privacy-preserving access authority sharing. In this paper, we propose a efficient data security based on privacy-preserving authentication protocol for cloud storage. The users may want to access and share each other's authorized data fields to achieve dynamic benefits from the cloud environment, which brings new privacy and security challenges in the cloud storage. Shared access authority is achieved by unknown access request matching mechanism with privacy and security consideration (e.g., authentication, data anonymity, user privacy and forward security). An Efficient attribute based access control is adopted to understand that the user can only access their own data field in cloud storage. The Proxy re-encryption will be functional by the server in cloud to provide data sharing among different user. To ability model is established to prove that the Shared an Efficient authority Based Privacy Preserving authentication Protocol has the design correctness and it indicates that the proposed protocol realizing privacy-preserving data access authority sharing is attractive for multiple users in favor of sharing data in cloud application.

Keywords: Cloud computing, cloud model, Security challenges

1. INTRODUCTION

Cloud computing has transformed the way organizations approach IT, enabling them to become more agile, introduce new business models, provide more services, and reduce IT costs. Cloud computing technologies can be implemented in a wide variety of architectures, under different service and deployment models, and can coexist with other technologies and software design approaches. A cloud typically contains a virtualized significant pool of computing resources, which could be reallocated to different purposes within short time frames. The entire process of requesting and receiving resources is typically automated and is completed in minutes. The cloud in cloud computing is the set of hardware, software, networks, storage, services and interfaces that combines to deliver aspects of computing as a service. Share resources, software and information are provided to computers and other devices on demand. It allows people to do things they want to do on a computer without the need for them to buy and build an IT infrastructure or to understand the underlying technology. Through cloud computing clients can access standardized IT resources to deploy new applications, services or computing resources quickly without reengineering their entire infrastructure, hence making it dynamic. The core concept of cloud computing is reducing the processing burden on the users terminal by constantly improving the handling ability of the cloud. All of this is available through a simple internet connection using a using a standard browser.

In this paper, we address the data security mechanism to propose a shared Efficient authority based privacy preserving authentication protocol (EAPA) for the cloud data storage, which realizes

authentication without compromising a user's private information. The main contributions are as follows.

1. Identify a new security and privacy challenge in cloud computing, and address a privacy issue during a new user challenging the cloud server for data sharing.
2. Propose thean efficient authentication protocol to enhance a user's access request related security and privacy, and shared access authority is achieved by anonymous access request mechanism.
3. Apply attribute based access control to realize that the user can reliably access its own data field.

2. DATA SECURITY ISSUES IN THE CLOUD

Privacy and Confidentiality: The client host data should be some guarantee that access to that data will only be limited to the efficient authorized access. In efficient authorized access to customer data by cloud personnel is another risk that can potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and methods should be in place to assure the cloud users of the data safety. The cloud seeker should be assured that data hosted on the cloud will be confidential.

Data integrity: To providing the efficient security of data, cloud service providers should be implement security mechanisms to ensure data integrity and be able to tell what happened to a certain dataset. The cloud provider should be make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place. In this paper purposes, it may be necessary to have exact records as to what data was placed in a public cloud, when it occurred, what is a virtual memories (VMs) and storage it reside done, and where it was processed. When such as data integrity requirements exists, that the origin and information must be maintained in order to prevent tampering or to prevent the exposure of data beyond the agreed territories (either between different servers or different networks).

Data location and Relocation: Cloud computing offers a high degree of data mobility.Consumers does not always know the location of their data. However, when an enterprise has some efficient data that is kept on a storage device in the Cloud, they may want to know the location of it. They may also wish to specify a preferred location (e.g. data to be kept in Tamilnadu). This, then, requires a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server.. Also, cloud providers should take responsibility to ensure the security of systems (including data) and provide robust authentication to safe guard customers 'information .Another issue is the movement of data from one location to another location. Data is initially stored at an appropriate location decide by the Cloud provider. However, it is often moved from one place to another. Cloud providers have contracts with each other and they use each others' resources

Data Availability: Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.

Storage, Backup and Recovery: When you decide to move your data to the cloud the cloud provider should ensure adequate data resilience storage systems. At a minimum they should be able to provide RAID(Redundant Array of Independent Disks) storage systems although most cloud providers will store the data in multiple copies across many independent servers. In addition to that, most cloud providers should be able to provide options on backup services which are certainly important for those businesses that run cloud based applications so that in the event of a serious hardware failure they can roll back to an earlier state.

3. DEPLOYMENT CLOUD MODELS

Public cloud: The cloud infrastructure is made available to the public people or a large industry group and provided by single service provider selling cloud services.

Private cloud: The cloud infrastructure is operated solely for an organization. The main advantage of this model is the security, compliance and QoS.

Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns like security requirements, policy, and compliance considerations.

Hybrid cloud: The cloud infrastructure is a combination of two or more clouds. It enables data application portability through load balancing between clouds.

4. CLOUD CHARACTERISTICS

On demand service: Cloud is large resource and service pool that you can get service or resource whenever you need by paying amount that you used.

Ubiquitous network access: Cloud provides services everywhere though standard terminal like mobile phones, laptops and personal digital assistants.

Easy use: The most cloud provider's offers internet based interfaces which are simpler than application program interfaces so user can easily use cloud services.

Business model: Cloud is a business model because it is pay per use of service or resource.

Location independent resource poling: The providers computing resources are pooled to serve multiple customers using multitenant model with different physical and virtual resources dynamically assigned and reassigned according to demand

5. RELATED WORK

In this paper proposed that IT has moved into next generation with cloud computing being realized. This paper focuses on the efficient security and integrity of data stored in cloud data servers. The data integrity verification is done by using a third party auditor who is authorized to check integrity of data. Hash Tree is used to improve block level authentication. In order to handle auditing tasks simultaneously, bilinear aggregate signature is used and it enables to perform auditing concurrently for multiple clients. The experiments reveal that the proposed system is very efficient and also secure.

While data outsourcing relieves the owners of the burden of local data storage and maintenance, it also eliminates their physical control of storage dependability and security. In this article we propose that publicly auditable cloud data storage is able to help this emerging cloud economy become fully established. We describe approaches and system requirements that should be brought into consideration, and outline challenges that need to be resolved for such a publicly auditable secure cloud storage service to become a reality.

Provable data possession (PDP) is a technique which used for integrity of data in storage outsourcing. In this paper, we present a schema for the construction of an efficient PDP scheme for distributed cloud storage to support the scalability of service and data migration. We present a Efficient PDP (EPDP) scheme based on verifiable response using cryptographic and hash index hierarchy. We are using Attribute set methods for cryptographic. Our experiments show that our solution introduces lower computation and communication overheads in comparison with non-efficient approaches. Cloud Service Provider (CSP) who offers high storage space with low cost. In this paper, we propose an efficient and secure protocol to address these issues. It allows third party auditor to periodically verify the data integrity and security. We prove that our method is secure and through performance and experimental results, we also will be proving that our method is efficient. To compare with existing schemes, our scheme is more secure and efficient.

Cloud computing environment have various advantages as well as disadvantages on the data security of service consumers. This paper aims to emphasize the main security issues existing in cloud computing

environments. This paper focuses on the usage of Cloud services and security issues to build these cross-domain Internet-connected collaborations.

The main objective of this paper is to design secure auditing protocol, during the data uploading to the server (Regular server/Cloud) through the data owner. We introduced a secure and efficient dynamic distribution and verification algorithms. Our proposed approach is efficient than the traditional protocols. The unique paradigm brings about many new security challenges, which have not been well understood.

This work studies the problem of ensuring the integrity of data storage in Cloud Computing. We improve the existing proof of storage models by manipulating the Hash Tree construction for block tag authentication. Extensive efficient data security and performance analysis will be show that the proposed schemes are highly efficient and provably secure.

In this paper, we address the construction of an efficient PDP scheme for distributed cloud storage to support the scalability of service and data migration. We present a *efficien PDP* (EPDP) scheme based on homomorphism verifiable response and hash index hierarchy. Our experiments show that our solution introduces lower computation and communication overheads in comparison with non-cooperative approaches.

6. PROPOSED SYSTEM

During data accessing in the cloud computing to achieve Privacy-preserving access authority sharing. Authentication is established to guarantee data confidentiality and data integrity. Data anonymity is achieved where any irrelevant entity cannot recognize the exchanged data and communication state even it intercepts the exchanged messages via an open channel. Forward data security is realized any adversary cannot correlate two communication sessions to derive the prior interrogations according to the currently captured messages.

System Shared access authority is achieved by anonymous access request matching mechanism with efficient security and privacy considerations (e.g., authentication, data anonymity, user privacy, and forward security). Attribute Set based access control is adopted to realize that the user can only access its own data fields. Proxy re-encryption is applied by the cloud server to provide data sharing among the multiple clients. This model is established to prove that the ASBA (Attribute Set Based Access) theoretically has the design

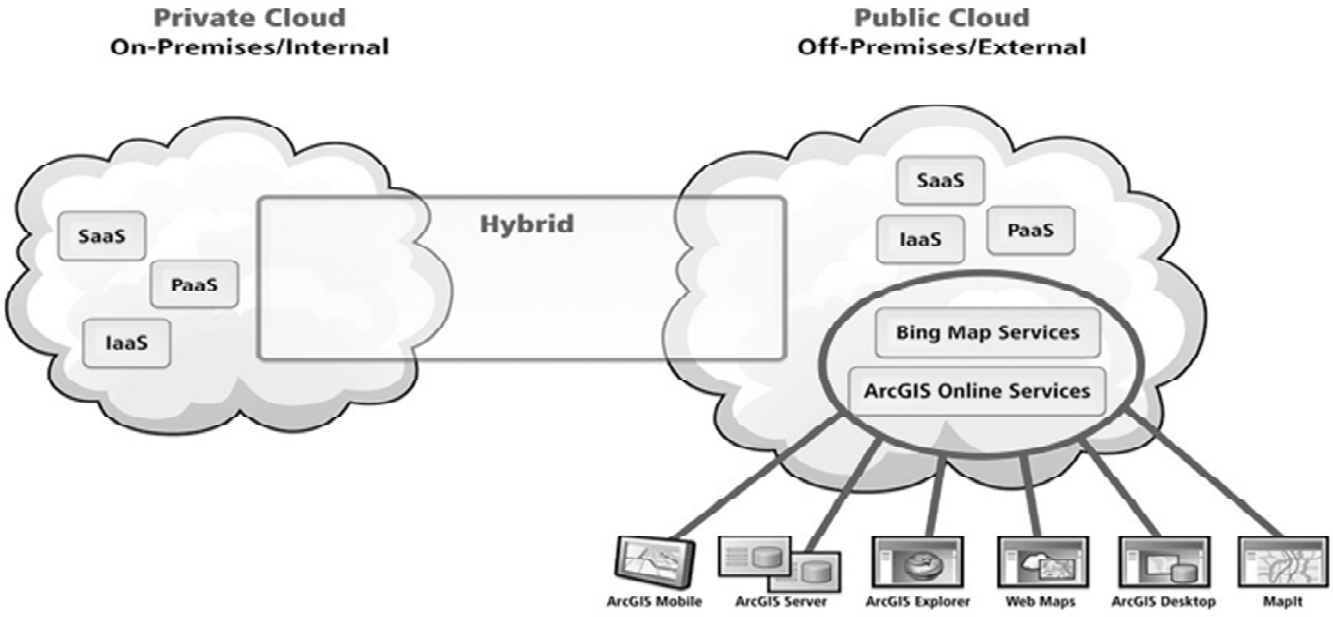

Figure 1: System Architecture

correctness. It indicates that the proposed protocol realizing efficient security and privacy-preserving data access authority sharing, is attractive for multi-client collaborative cloud applications areas.

7. ANONYMOUS ID ASSIGNMENT BASED DATA SHARING ALGORITHM

Suppose each node is had a unique, anonymous identification. Upon choosing to opt-out, a node could simply turn in their ticket to declare opt-out and then concurrently clobber the global sum with a large random number to make it non-viable. If the anonymous identification were turned in anonymously and if the identification could not be traced to the node turning it in, then the opt-out would be truly anonymous. Moreover, since the opt-out method is separated from making the global sum non-viable, one would never mistakenly accept illegitimate data as useful. Therefore, the first step in developing an anonymous opt-out feature is to show how to anonymously assign this identification to each node. We describe just such a method in Algorithm which anonymously identification assigns each node a unique identification using an array version, that is, an array of sums or slots (slot array S of length N) is passed around the circuit rather than a single scalar value.

AIDA Algorithm Implementation

Given nodes $n1, ..., nN$, use distributed computation (without central authority) to find an anonymous indexing permutation s: {1, ..., N}

1) Set the number of assigned nodes $A = 0$.
2) Each unassigned node chooses a random number in the range 1 to S. A node assigned in a previous round chooses $r1 = 0$.
3) The random numbers are shared anonymously. Denote the shared values by $q1, ..., qN$.
4) Let $q1, qk$ denote a revised list of shared values with duplicated and zero values entire l removed where k is the number of unique random values. The nodes in which drew unique random numbers then determine their index is from the position of their random number in the revised list as it would appear after being sorted:

$$Si = A + \text{Card } \{qj: qj \Leftarrow ri\}$$

5) Update the number of nodes assigned:

7.1. Key Generation

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

Steps:

1. Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.
2. Compute $n = a * b$.
3. Compute Euler's to function,

$$Ø(n) = (a - 1) * (b - 1).$$

4. Chose an integer e, such that $1 < e < Ø(n)$ and greatest common divisor of e, $Ø(n)$ is 1. Now e is released as Public-Key exponent.
5. Now determine d as follows:

$$d = e - 1(\text{mod } Ø(n))$$

i.e., d is multiplication inverse of

e mod $Ø(n)$.

6. d is kept as Private-Key component, so that $d * e = 1$ mod $Ø(n)$.
7. The Public-Key consists of modulus n and the public exponent e i.e, (e, n).
8. The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e, (d, n).

   $A < N$ then return to step (2).

7.2. Encryption

Encryption is the process of converting original plain text (data) into cipher text (data).

Steps:

1. Cloud service provider should give or transmit the Public-Key (n, e) to the user who wants to store the data with him o rher.
2. User data is now mapped to an integer by using an agreed upon reversible protocol, known as adding scheme.
3. Data is encrypted and the resultant cipher text(data) C is C = me (mod n).
4. This cipher text or encrypted data is now stored with the Cloud service provider.

7.3. Decryption

Decryption is the process of converting the cipher text(data) to the original plain text(data).

Steps:

1. The cloud user requests the Cloud service provider for the data.
2. Cloud service provider verifies the authenticity of the user and gives the encrypted data i.e, C.
3. The Cloud user then decrypts the data by computing, m = Cd (mod n).
4. Once m is obtained, the user can get back the original data by reversing the padding scheme.

8. CONCLUSION

A new efficient data security mechanism to data accessing in the cloud computing to achieve privacy-preserving access authority sharing. Authentication is established to guarantee efficient data confidentiality and data integrity. Data anonymity is achieved since the wrapped values are exchanged during transmission. User privacy is enhanced by anonymous access requests to privately inform the cloud server about the users' access desires.

9. FUTURE WORK

In future work the detailed design scheme to support efficient third-party auditing, where users can safely delegate the integrity checking tasks to third-party auditors and be worry-free to use the cloud storage services. Through detailed efficient security mechanism and extensive experiment results. So, in our project we are going to do cloud data security, the purpose of data security is who is the cloud users shared the files among the cloud server. The server investigates how many clients are going to share the data's into the

cloud server and how much space allocates for every clients. So, we were auditing the all authenticated users among cloud server. The cloud users when the time of upload the files within the key only possible to upload the among cloud server, that same key possible to give that the time of download is possible. So the download users how to know the symmetric key by the way of accessing mail concepts only we can access the all files data.

REFERENCE

[1] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," National Institute of Standards and Technology, USA, 2009.

[2] A. Mishra, R. Jain, and A. Durresi, "Cloud Computing: Networking and Communication Challenges," IEEE Communications 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,[online] ieee.org/stamp, 2012.

[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 rovable Data Possession for Integrity Verification in Multi-cloud Storage*," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no, 12, pp. 2231-2244, 2012.

[7] H. Wang, "*Proxy Provable Data Possession in Public Clouds*," IEEE Transactions on Services Computing, 2012.

[8] K. Yang and X. Jia, "*An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing*," IEEE Transactions on Parallel and Distributed Systems,[online], 6311398, 2012.

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