Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

ANALYSIS OF AN EFFECTIVE, SCALABLE AND SECURED DATA SHARING SERVICE IN CLOUD COMPUTING

Ms. P. Sangeetha[1], Mrs. M.M.Kavitha[2]

[1]Research Scholar,M.Sc., [2]M.Phil, Assistant Professor,
Department of Computer Science,
SSM College of Arts & Science, Komarapaliyam, Tamilnadu, India

Abstract- Scalable and flexible privacy-preserving data sharing scheme in the cloud ensures both semantic security and effective availability of user data. To preserve privacy and guarantee data confidentiality against the cloud, the scheme employs a cryptographic primitive, named cipher-text policy attribute-based encryption (CP-ABE) and combines it with an identity-based encryption (IBE) technique; each data file is described by a set of meaningful attributes, allowing each user to be assigned an access structure that defines the scope of data files they can have access to.

To enforce these access structures, this scheme defines a public-private key pair for each attribute. For each user' secret key, there is a combination of user's ID and the attribute's secret key, thereby ensuring that each attribute presents a different key to each user. Data files are encrypted by public key components and access matrices converted from the access structure; user secret keys are defined to reflect their access privileges so that a user can only decrypt a ciphertext if they have the matched attributes to satisfy the ciphertext. To resolve the challenging issues of collusion resistance, this scheme provides users with a public key fitted to their secret keys; This paper use user's ID to "tie" together the attributes belonging to this user so that they cannot be successfully combined with another's user's attributes.

Index Terms: Cloud Computing, Data sharing and security, Access policies and Cryptography

I. INTRODUCTION

The term Cloud refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN. Applications such as e-mail, web conferencing, customer relationship management (CRM), all run in cloud. Cloud Computing refers to manipulating, configuring and accessing the applications online. It offers online data storage, infrastructure and application.

Cloud computing, or the cloud, is a colloquial expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. Cloud computing is a term without a commonly accepted unequivocal scientific or technical definition. In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time.

The phrase is also, more commonly used to refer to network-based services which appear to be provided by real server hardware, which in fact are served up by virtual hardware, simulated by software running on one or more real machines. Such virtual servers do not physically exist and can therefore be moved around and scaled up on the fly without affecting the end user - arguably, rather like a cloud. The popularity of the term can be attributed to its use in marketing to sell hosted services in the sense of application service provisioning that run client server software on a remote location [11]. There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users. Following are the working models for cloud computing:

- Deployment Models
- Service Models

II. RELATED WORK

Three types of pricing options are currently adopted in IaaS clouds. Besides the on-demand and reserved instances, we note that some cloud providers charge dynamic prices that fluctuate over time, e.g., the Spot Instances in Amazon EC2. Some existing works discuss how to leverage these pricing options to reduce instance running costs for an individual user. For example, Chohan et al. [2] investigate the use of Spot Instances as accelerators of the MapReduce process to speed up the overall MapReduce time while significantly reducing monetary costs. Zhao et al. [3] propose resource rental planning with EC2 spot price predictions to reduce the operational cost of cloud applications. Cost savings with a daily billing cycle under the Greedy strategy. instance purchasing strategy to reduce the "margin cost" of over-provisioning. Hong et al. [9] also presents a strategy to combine the use of on-demand and reserved instances, which is essentially a special case of our Heuristic strategy when all demands are given in one reservation period. Chaisiri et al. [10] investigate a similar problem and propose an algorithm by solving a stochastic integer programming problem. Their algorithm limits the reservation decisions to be made at some specific time phases. The recent work proposes optimal online strategies to reserve instances without any a priori knowledge of future demands. Vermeersch [1] implements prototype software that dynamically retrieves instances from Amazon EC2 based on the user workload. All these works offer a consulting service, e.g., [4], that helps an individual user make instance purchasing decisions.

IaaS cloud brokers have recently emerged as intermediators connecting buyers and sellers of computing resources. For example, SpotCloud [5] offers a "clearinghouse" in which companies can buy and sell unused cloud computing capacity. Buyya et al. [2] discuss the engineering aspects of using brokerage to interconnect clouds into a global cloud market. Song et al. [7], propose a broker that predicts EC2 spot price, bids for spot instances and uses them to serve cloud users. Unlike existing brokerage services that accommodate individual user requests separately, our broker serves the aggregated demands by leveraging instance multiplexing gains and instance reservation and is a general framework not limited to a specific cloud.

We note that the idea of resource multiplexing has also been extensively studied, though none of them relates to computing instance provisioning. For example, [8] makes use of bandwidth burstable billing and proposes a cooperative framework in which multiple ISPs jointly purchase IP transit in bulk to reduce individual costs. The anti correlation between the demands of different cloud tenants is exploited to save bandwidth reservation cost in the cloud. Empirically evaluates the idea of statistical multiplexing and resource overbooking in a shared hosting platform. It remains nontrivial to design instance purchasing strategies that can optimally combine different pricing options to reduce cloud usage cost.

III. DATA SHARING WITH SECURITY UNDER CLOUDS

To realize an effective, scalable and privacy-preserving data sharing service in cloud computing, the following challenges need to be met: firstly, data owners should be able to assign other cloud users with different access privileges to their data; secondly, the cloud needs to be able to support dynamic requests so that data owner scan add or revoke access privileges to other users allowing them to create or delete their data; thirdly, the users' privacy must be protected against the cloud so that they can conceal their private information while accessing the cloud; finally, users should be able to access shared data in the cloud through connected technologies with low computing ability, such as Smartphone and tablets. To date, solving these important areas in cloud computing remains elusive. This paper propose an effective, scalable and flexible privacy-preserving data sharing scheme in the cloud, that ensures both semantic security and effective availability of user data. To preserve privacy and guarantee data confidentiality against the cloud, the scheme employs a cryptographic primitive, named cipher-text policy attribute-based encryption (CP-ABE) and combines it with an identity-based encryption (IBE) technique; each data file is described by a set of meaningful attributes, allowing each user to be assigned an access structure that defines the scope of data files they can have access to.

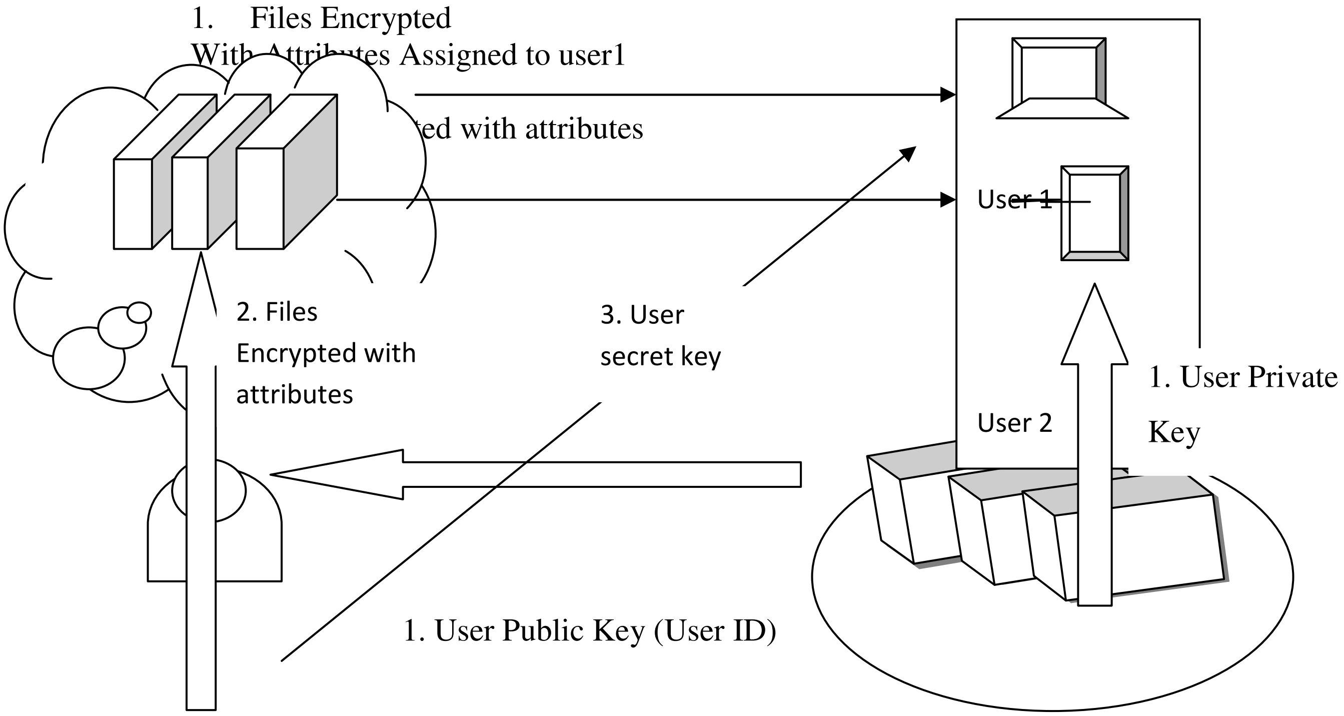

Fig 3.1: Privacy Preserved Cloud Data Services

To enforce these access structures, this scheme defines a public-private key pair for each attribute. For each user' secret key, there is a combination of user's ID and the attribute's secret key, thereby ensuring that each attribute presents a different key to each user. Data files are encrypted by public key components and access matrices converted from the access structure; user secret keys are defined to reflect their access privileges so that a user can only decrypt a ciphertext if they have the matched attributes to satisfy the ciphertext. To resolve the challenging issues of collusion resistance, this scheme provides users with a public key fitted to their secret keys; This paper use user's ID (public key) to "tie" together the attributes belonging to this user so that they cannot be successfully combined with another's user's attributes. To protect user privacy, this scheme does not need to update user secret key so that it prevents cloud access user access structure. To reduce the key management issue, the data owner simply assigns secret keys to users via the cloud. Compared to previous schemes, the proposed scheme provides the benefits of security and efficiency. The cloud can learn nothing about a user's privacy or access structure, as such the scheme is fully collusion resistant. All extended operations, including user revocation, can only affect the current file or user without involving key updates. The proposed scheme elegantly integrates four randomized algorithms: System Initialization, Encryption, Key generation, Decryption to achieve effective, scalable and privacy preserving cloud data sharing service. Fig 3.1 describes a simplified workflow of the proposed scheme.

At the initialization phase, the data owner uses the System initialization algorithm to generate system parameters for all the system entities. The data owner then employs Encryption algorithm to encrypt files with "attributes" and uploads to the cloud. By the key generation algorithm, the data owner generates secret keys for each user and then delivers them to the users via the cloud server. At last, users use Decryption algorithm to decrypt cipher text if their attribute set matches with the file attributes.

IV. PROBLEM DEFINITION

Data owners demand high levels of security and confidentiality when they outsource their data to a cloud; although they usually encrypt their data when storing it in a cloud server, want control over it, for example, if they frequently update it. Direct employment of traditional cryptographic primitives cannot achieve the data security required. Thus, a considerable amount of work has recently been directed towards ensuring the privacy and security of remotely stored shared data using a variety of systems and security models. These have mainly focused on preserving users' privacy while realizing desired security goals, without introducing excessively high levels of complexity to the users at the decryption stage.

To solve these issues, researchers have either utilized key-policy attribute-based encryption (KP-ABE) for secure access control or employed hierarchical identity-based encryption (HIBE) for data security. Yu et al. were the first team to achieve secure data access control with provable security in cloud computing using KP-ABE. By revealing some of the users' attributes to cloud, these systems were unable to fully preserve users' privacy. HIBE-based scheme utilizes hierarchical encryption to ensure data security in a cloud, but this introduces too many private keys for each user to be managed efficiently. In summary, these schemes either have privacy flaws or provide security at the expense of performance; therefore, the challenge of achieving the dual goals of privacy-preserving with effective cloud data sharing remains unresolved. This is the first work that studies and solves the online browsing methods use a representing concept-based user profiles. The weights of the vector elements, which could be positive or negative, represent the interestingness of the user on the concepts.

V. PRIVACY PRESERVED DATA SHARING UNDER CLOUDS

The cloud data security and privacy preservation process is designed with four major modules. They are user interface design, trusted DB provider, user access policy for multi dataset and access key generation using SCPUS.

5.1. User Interface Design

The goal of user interface design is to make the user's interaction as simple and efficient as possible, in terms of accomplishing user goals—what is often called user-centered design. Good user interface design facilitates finishing the task at hand without drawing unnecessary attention to it. Graphic design may be utilized to support its usability.

5.2. Trusted DB Provider

Storage is a model of networked computer data storage where data is stored on multiple virtual servers, generally hosted by third parties, rather than being hosted on dedicated servers. Hosting companies operate large data centers; and people who require their data to be hosted buy or lease storage capacity from them and use it for their storage needs. The data center operators, in the background, virtualizes the resources according to the requirements of the customer and expose them as virtual servers, which the customers can themselves manage. Physically, the resource may span across multiple servers.

5.3. User Access Policy For Multi Dataset

A client sends a query request to the host server through a standard SQL interface. The query is transparently encrypted at the client site using the public key of the SCPU. The host server thus cannot decrypt the query. The host server forwards the encrypted query to the Request Handler inside the SCPU. The Request Handler decrypts the query and forwards it to the Query Parser. The query is parsed generating a set of plans. Each plan is constructed by rewriting the original client query into a set of subqueries and, according to their target data set classification, each subquery in the plan is identified as being either public or private.

The Query Optimizer then estimates the execution costs of each of the plans and selects the best plan for execution forwarding it to the dispatcher. The Query Dispatcher forwards the public queries to the host server and the private queries to the SCPU database engine while handling dependencies. The net result is that the maximum possible work is run on the host server's cheap cycles. The final query result is assembled, encrypted digitally signed by the SCPU Query Dispatcher and sent to the client.

5.4. Access Key Generation Using SCPUS

In this module it creates the fine grained access control key for every user type. The organization admin select the user type and attribute allocation for that user. After select the attributes this module creates the key for access control key. The data access policies should be flexible, i.e., dynamic changes to the predefined policies shall be allowed, especially the organization should be accessible under emergency scenarios. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the database and then decrypt them.

VI. PERFORMANCE ANALYSIS

IBE is a public-key cryptosystem (PKC) in which the public key assigned to each unique user is an arbitrary string similar to a user ID or email address; and a trusted third party, called the private key generator (PKG), calculates the corresponding private key. Compared to a traditional PKC, the IBE scheme eliminates the issue of searching for a recipient's public key, but has a key escrow problem. An attribute-based encryption (ABE) system is essentially a simplified IBE system with only a single attribute. In an ABE scheme, the sender encrypts the message with a set of attributes and specifies a number d; a recipient can only decrypt the encrypted message if they have at least d of the given attributes. Based on these principles, an ABE scheme with fine-grained data access control that supports monotonic access structures, such as AND, OR and other threshold gates. proposed an enhanced scheme that also supports non-monotonic access structures, i.e., NOT gates. In KP-ABE, the access structure is used to encrypt the secret key and the attributes are used to describe the ciphertext. Conversely, CP-ABE uses the access structure to encrypt the ciphertext and the secret key is generated based on an attribute set. The ABE scheme consists of the following four algorithms:

1. System Initialization: the sender chooses the algebraic groups and several secure parameters.
2. Encryption: the sender encrypts the message using the access structure.
3. Key Generation: the sender generates secret keys for the recipients, depending on the set of attributes the recipients possess.
4. Decryption: the recipient decrypts the message with a valid set of attributes.

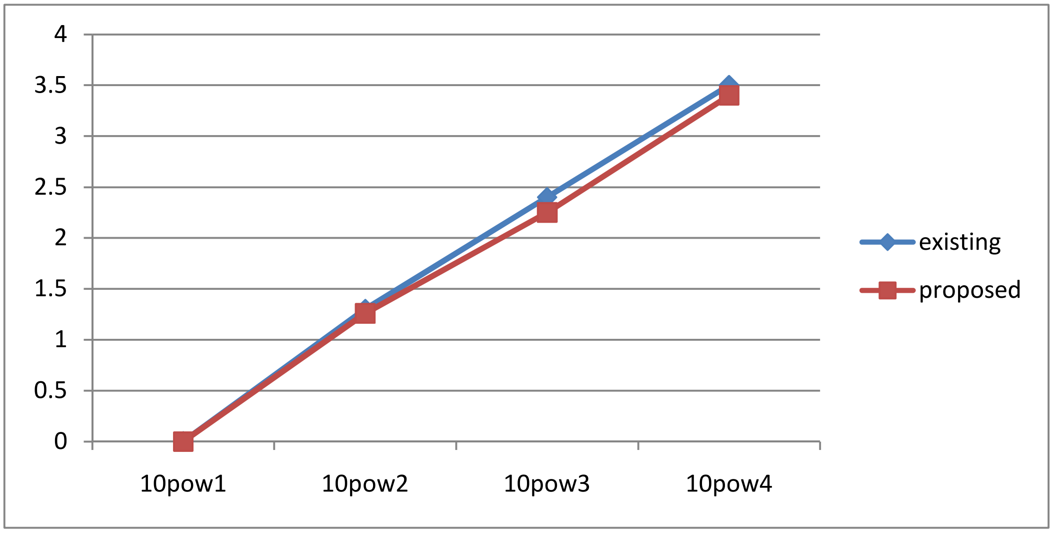

Fig 6.1: The overhead of encryption speed in Global-as-View approach and CP-ABE

In an existing system a distributed attribute-based scheme, based on an efficient construction, that demands a constant number of operations at the decryption stage; the access policy formats have to be expressed as a disjunctive normal form (DNF); therefore, the cipher text size is proportional to the number of conjunctive clauses in the DNF. In a multi-authority ABE scheme in several authorities cooperate to manage the attributes. Each authority manages a domain of attributes and distributes those attributes and secret keys to the users. The main issue affecting this scheme is that it is not practical to have one trusted central authority.

In the existing scheme, the access structure for any given user is only known by the sender; this decentralized mechanism is not suitable for cloud computing. The scheme proposed exploits KP-ABE, by combining it with proxy re-encryption and lazy re-encryption. It simultaneously achieves fine-grainedness, scalability and data confidentiality for data access control. The data owner can delegate most of the computation tasks, such as user revocation, to the cloud server without disclosing any data to the untrusted cloud; by delegating these tasks, some user attributes and secret keys may leak into the cloud. The related ciphertext must be re-encrypted, allowing it to be revealed to non-revoked users. As such, user able to discover the proxy re-encryption techniques applied in CP-ABE.

This paper focuses on providing a dependable and secure data sharing service that allows users dynamic access to their data. In order to achieve this, we propose an effective, scalable and flexible privacy preserving data policy with semantic security, by utilizing cipher text policy attribute based encryption. In addition to ensuring robust data sharing security, this policy succeeds in preserving the privacy of users and supports efficient and secure. Multi-authority ABE scheme to divide users into different domains; however, this scheme is an isolated case and is not generally applied in cloud computing. It presents a formal access control model on outsourced data. In this scheme, each file is encrypted with a symmetric key and each user is assigned a secret key; the complexity of operations of file creation and user grant/revocation is linear to the number of users, which makes this scheme unscalable.

In proposed system data interoperation systems integrate information from different local sources to enable communication and exchange of data between them. A common model for these systems involves a global representation of the local data, which acts as a mediator for translating queries and conveying data to and from these sources using the global-as view (GAV) approach. In addition, global resource employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. This papaer formally prove the security of global resource based on security of the cipher text-policy attribute-based encryption scheme and analyze its performance and computational complexity.

VII. CONCLUSION AND FUTURE WORK

This paper provides secured data sharing in cloud computing. This paper focuses on providing a dependable and secure data sharing service that allows users dynamic access to their data. In order to achieve this, we propose an effective, scalable and flexible privacy preserving data policy with semantic security, by utilizing cipher text policy attribute based encryption. This paper will implement the proposed privacy-preserving and effective cloud data sharing service in a real CSP platform for future work. Future enhancements include building the framework to tap multiple secure processors; memory light, privacy preserving, join methods for inequality joins; pushing down sampling to the data sources by queries and validation in a customer scenario.

A future work would be to take some functionality out of the a secure coprocessor and put it onto the untrusted host. Classic work on database security has examined using a trusted filter in front of an untrusted relational database.16 The aim was to keep the performance advantage of a relational database system and use a minimal filter to enforce access control.

REFERENCES

[1] K. Vermeersch, "A Broker For Cost-Efficient QoS Aware Resource Allocation In EC2," Master's thesis, Dept. Comput. Sci., Univ. Antwerp, Antwerpen, Belgium, 2011.

[2] N. Chohan, C. Castillo, M. Spreitzer, A. Tantawi and C. Krintz, "See Spot Run: Using Spot Instances For Mapreduce Workflows," in Proc. Conf. Hot Topics Cloud Comput., 2010, p. 7.

[3] H. Zhao, M. Pan, X. Liu, X. Li and Y. Fang, "Optimal Resource Rental Planning For Elastic Applications In Cloud Market," in Proc. IEEE 26th Int. Parallel Distrib. Process. Symp., 2012.

[4] Cloud Express. (2014). [Online]. Available: https://www.cloudexpress.com

[5] SpotCloud. (2014). [Online]. Available: http://spotcloud.com/

[6] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg and I. Brandic, "Cloud Computing And Emerging It Platforms: Vision, Hype and Reality For Delivering Computing As The 5th Utility," Future Gener. Comput. Syst., vol. 25, no. 6, pp. 599–619, 2009.

[7] Y. Song, M. Zafer and K.-W. Lee, "Optimal Bidding In Spot Instance Market," in Proc. IEEE Conf. Comput. Commun, 2012, pp.190–198.

[8] R. Stanojevic, I. Castro and S. Gorinsky, "CIPT: Using Tuangou To Reduce IP Transit Costs," in Proc. ACM 7th COnf. Emerging Netw. EXp. Technol., 2011, pp. 1–12.

[9] Y. Hong, M. Thottethodi and J. Xue, "Dynamic Server Provisioning To Minimize Cost In An IaaS cloud," in Proc. ACM SIGMETRICS Joint Int. Conf. Meas. Model. Comput. Syst., 2011.

[10] S. Chaisiri, B.-S. Lee and D. Niyato, "Optimization Of Resource Provisioning Cost In Cloud Computing," IEEE Trans. Serv. Comput., vol. 5, no. 2, pp. 164–177, Apr.–Jun. 2010.

[11] Wei Wang, Di Niu, Ben Liang and Baochun Li, "Dynamic Cloud Instance Acquisition via IaaS Cloud Brokerage", IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 6, June 2015.