Secure Access Control on Encrypted DATA in Cloud Storage

C.T.R. Saranya Raj[1#] Dr.S. Maria Celestin Vigila[2#]

[#1]PG Scholar, ME Cyber Security, Noorul Islam University, Kumaracoil-629180, Tamil Nadu, India

[#2]Associate Professor, Department of Information Technology, Noorul Islam Center for Higher Education, Kumaracoil-629180, Tamil Nadu, India

Abstract- Cloud computing gives much more services to users on demand. In the public cloud, cloud is made up of various data centres and they are located in distributed manner. Therefore, unauthorized access can be made by many hackers who want to hack particular data. So that, to provide security in terms of data access, various access control mechanism is developed, that can be helpful in reducing unauthorized access. In this paper, the concept of public cloud infrastructure is used with cryptographic approach in order to provide a secure solution for securing the files on cloud yet maintains the confidentiality of data. Confidential files can be encrypted using randomized encryption and uploaded on cloud. Access Control methods ensure that authorized user's access the data and the system. This system proposed a new extended architecture of constant size cipher text policy attribute-based encryption which can resolve the security issues and data loss issues by using restriction policy. The implemented scheme shows that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing with comprehensive experiments.

***Keywords*—Access control, cloud computing, data security.**

I. INTRODUCTION

Cloud computing is a new computing prototype that is constructed on virtualization, parallel and distributed computing, value computing, and service-oriented architecture. In the last numerous years, cloud computing has appeared as one of the most powerful standards in the IT industry, and has involved wide courtesy from both academia and industry. Cloud computing grips the capacity of providing computing as the fifth utility [1] after the other four utilities. The paybacks of cloud computing include cheap costs and capital expenditures, increased operational efficiencies, scalability, flexibility, immediate time to market, and so on. Different service-oriented cloud computing models have been proposed [2], including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Although the great benefits brought by cloud computing paradigm are exciting for IT companies, academic researchers, and potential cloud users, security problems in cloud computing become serious obstacles which, without being appropriately addressed, will prevent cloud computing extensive applications and usage in the future [3,4]. One of the prominent security concerns is data security and privacy in cloud computing due to its Internet-based data storage and management. In cloud computing, users have to give up their data to the cloud service provider for storage and business operations, while the cloud service provider is usually a commercial enterprise which cannot be totally trusted [5]. Data represents an extremely important asset for any organization, and enterprise users will face serious consequences if its confidential data is disclosed to their business competitors or the public. Thus, cloud users in the first place want to make sure that their data are kept

confidential to outsiders, including the cloud provider and their potential competitors [6, 7].

At present, in the area of cloud computing different security models and algorithms are applied. But, these models have failed to solve all most all the security threats. Moreover for E-commerce [8] and different types of online business, we need to imply high capacity security models in cloud computing fields. Security models that are developed and currently used in the cloud computing environments are mainly used for providing security for a file and not for the communication system [9]. Moreover present security models are sometimes uses secured channel for communication [10]. But, this is not cost effective process. Again, it is rare to find a combined work of main server security, transaction between them and so on. Some models attempt on discussing about all of these, but are completely dependent on user approach. The models usually fail to use machine intelligence for generating key and newer proposed model. Some models have proposed about hardware encryption system for secured communication system [11]. The idea is usually straightforward, but the implementation is relatively difficult. Besides, hardware encryption is helpful only for the database system, not for other security issues. Authenticated user detection technique is currently very important thing. But, this technique is rarely discussed in the recently used models for ensuring security in cloud computing.

To overcome the drawbacks of traditional methods for security in cloud computing, hybrid encryption and access control techniques has been proposed in this system [12]. For data encryption process an optimized encryption technique using an arbitrary matrix with probabilistic encryption is used. For access control the proposed CP-ASBE algorithm arranges user attributes into a recursive set based structure [13]. It allows users to force dynamic constraints on how those attributes may be combined to satisfy a policy. The CP-ASBE consists of recursive set of attributes.

This paper is formatted in the following way: - section 2 describes related work of this paper work, section 3 describes proposed architecture and its working steps, section 4 describes the experimental environment, results in different aspects and advantages of the proposed model, and section 5 describes the conclusion and future aspects.

II. RELATED WORK

In the literature, several encryption schemes have been proposed with arbitrary based encryption techniques. There exist many access control schemes which have been constructed based on encryption schemes, and approaches using access control schemes to enforce AC policies for data storage are discussed in these solutions have several limitations. For instance, if there is a large number of data owners and users involved, the overhead involved in setting up the key infrastructure can be very high indeed. Furthermore, when a user's access permission is revoked, all the keys known to this user as well as all the public values related to these keys need to changed, which makes these schemes impractical.

Yang Xiao and Haizhon [14] proposed a global data parameter control scheme integrated with a measurement-based admission control scheme for the IEEE 802.11e enhanced distributed channel access. In the global data control scheme, the access point dynamically controls best-effort data parameters of stations globally based on traffic condition [15]. Such a global/centralized data parameter control mechanism provides the best fairness for data transmissions among stations. The centrally-assisted distributed admission control scheme for voice and video transmissions, stations listen to available budgets from the access point to make decisions on acceptance or rejection of a voice or video stream. Such a scheme provides good differentiation among different access categories and provides good fairness among real-time streams within the same access category. This mechanism evaluated via extensive

simulations. Studies show that, with the proposed global data control scheme and the admission control scheme, quality of service can be greatly improved while maintaining a good utilization.

Amit Sahai and Waters [16] introduced fuzzy identity based encryption. Identity-based encryption allows for a sender to encrypt a message to an identity without access to a public key certificate. The ability to do public key encryption without certificates has many practical applications. For example, a user can send an encrypted mail to a recipient, without the requiring either the existence of a public-key infrastructure or that the recipient be on-line at the time of creation. One common feature of all previous identity-based encryption systems is that they view identities as a string of characters. Here, a new type of identity-based encryption that calls fuzzy identity-based encryption in which view identities as a set of descriptive attributes [17]. In a fuzzy identity-based encryption scheme, a user with the secret key for the identity is able to decrypt a cipher text encrypted with the public key if and only if and 0 are within a certain distance of each other as judged by some metric. Therefore, the system allows for a certain amount of error-tolerance in the identities.

Punithasurya and JebaPriya[18,19] proposed analysis of different access control mechanism in cloud. In the mandatory access control mode, users are given permissions to resources by an administrator. Only an administrator can grant permissions or right to objects and resources. Access to resources is based on an object's security level, while users are granted security clearance. Only administrators can modify an object's security label or a user's security Clearance.

Dongyoung Koo et al [20]presented about secure data retrieval over encrypted data in cloud services, most of them focus on providing the strict security for the data stored in a third party domain. However, those approaches require stupendous costs centralized on the cloud service provider, which could be a principal impediment to achieve efficient data retrieval in cloud storage [21]. This scheme is best suited for cloud storage systems with massive amount of data. It provides rich expressiveness as regards access control and fast searches with simple comparisons of searching entities. It also guarantees data security and user privacy during the data retrieval process.

Hadia M.S. et.al [22] introduced link encryption algorithm proposed stream cipher algorithm. The idea of this algorithm is building up the key character sequence of combination of two different sequences, where the first one has probable long period and the second one is high complexity by using nonlinear functions. Moreover, both of these sequences are statistically flat. The good statistical properties of the first sequence are in principle that of Liner Feedback Shift Registers (LFSRs) with primitive characteristic polynomials to achieve maximal-length period [23]. Also, those of the second part are achieved by using well distributed generated substitution boxes, confusion, and diffusion. The encryption algorithm can be divided into a driving part and a combining part. The driving part consists of a set of maximum length LFSRs. It mainly governs the state sequence of the generator and is responsible for providing sequences of large periods and good statistics. The combining part is essentially nonlinear. It has the task to make the cipher stream generation to be mathematically complex.

Although these models ensures secured communication between users and servers, but they do not encrypt the loaded information. For best security ensuring process, the uploaded information needs to be encrypted so that none can know about the information and its location. Recently some other secured models for cloud computing environment are also being researched [24, 25]. But, these models also fail to ensure all criteria of cloud computing security issues [26].

III. PROPOSED SYSTEM

The cloud service provider manages a cloud to provide data storage service. 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 cloud and then decrypt them. Each data owner/consumer is administrated by a domain authority. A domain authority is managed by its parent domain authority or the trusted authority.

A cloud computing system under concern consists of five types of parties: cloud service provider, data owners, data consumers, domain authorities, and trusted authority. The cloud service supplier administers a cloud to provide data storage service. Data proprietors encrypt their data records and store them in the cloud for sharing with data consumers. To entrance the joint data files, data consumers download encrypted data files of their attention from the cloud and then decrypt them. Each data owner/consumer is monitored by a domain authority. By the parent domain authority or the trusted authority, a domain authority is managed. Domain authorities, data owners, data consumers, and the trusted authority are organized in a hierarchical way. The conditioned authority is the origin authority and in charge for managing top-level domain authorities.

Each top-level domain authority matches to a top-level association, such as an amalgamated enterprise, whereas each lower-level domain authority communicates to a lower-level organization, such as an associated company in a federated organization. Data owners/consumers may correspond to employees in an organization. Every domain authority is responsible for managing the domain authorities at the next level or the data owners/consumers in its domain. In this system, neither data owners nor data consumers will be always online.

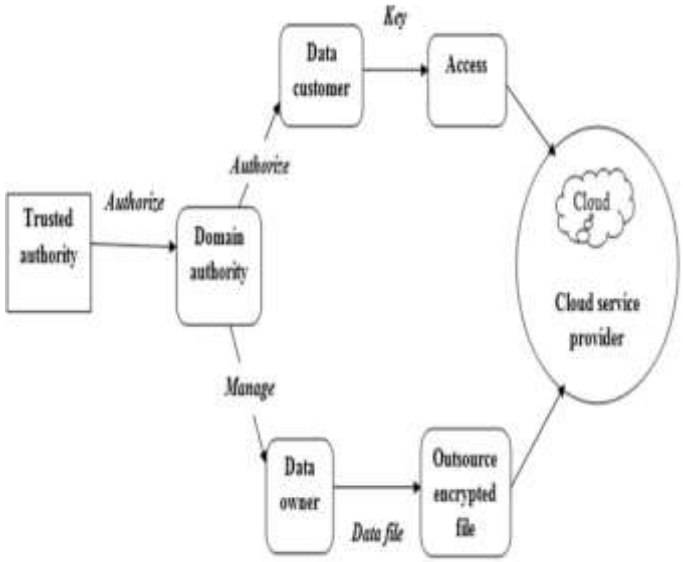


Figure: 1 Proposed System Architecture

They come online only when essential, while the cloud service provider, the trusted authority, and domain authority are always online. The cloud is unspecified to have abundant storage capacity and computation power. In addition, we take for granted that data consumers can access data files for interpretation only. Data owners, data consumers, domain authorities, and the trusted authority are organized in a hierarchical manner as Fig.1 represents the system architecture. The modules used in the proposed system are Data Owner Module, Data Consumer Module, Cloud Server Module and Access Control Module.

A. Probabilistic Encryption

Historically, encryption schemes were the first central area of interest in cryptography. They deal with providing means to enable private communication over an insecure channel. A sender wishes to transmit information to a receiver over an insecure channel, which is a channel which may be tapped by an adversary.

Thus, the information to be communicated, which we call the plaintext, must be transformed (encrypted) to a cipher text, a form not legible by anybody other than the intended receiver [27]. The latter must be given some

way to decrypt the cipher text, i.e. retrieve the original message, while this must not be possible for an adversary. This is where keys come into play; the receiver is considered to have a key at his disposal, enabling him to recover the actual message, a fact that distinguishes him from any adversary.

An encryption scheme consists of three algorithms: The encryption algorithm transforms plaintexts into cipher texts while the decryption algorithm converts cipher texts back into plaintexts. A third algorithm, called the key generator, creates pairs of keys: an encryption key, input to the encryption algorithm, and a related decryption key needed to decrypt. The encryption key relates encryptions to the decryption key. The key generator is considered to be a probabilistic algorithm, which prevents an adversary from simply running the key generator to get the decryption key for an intercepted message.

(a) *Key generation*

- Consider the sequence for 0 to n-1 values for a source text of size n = pow (p, p) characters.
- Convert each element of the sequence into a form with base p.
- Represent the values of step 2 in a matrix form A of order n x p.
- Subtract 1 from each element of A.
- Consider a random matrix B of size p x p.
- Multiply the matrix A with B to generate a result matrix R.
- Substitute all positive integers of R with +1, negative integers to -1 and zero by 0 using a substitute function.
- Increment each element of R by 1.
- Convert each row of R, from the base p to decimal to generate the key sequence set.

(b) *Encryption Algorithm*

- Let C_i be the plain text for i = 0 to n-1.
- Let the numerical equivalent NE_i of a character C_i, Where, N_i = ASCII value of C_i, for each i from 0 to n-1.
- Find the sum index $S_i = NE_i + K_i$, for each i from 0 to n-1, where K_i is the i^{th} key generated in the sequence.
- Find the remainder index $R_i = S_i \% 36$, for each i from 0 to n-1.
- Find the cipher text for each input character as CT_i, where CT_i is the character equivalent of each R_i, where i varies from 0 to n-1.

(c) *Decryption Algorithm*

- Let CT_i be the cipher text.
- Find the Alpha numeric equivalent NE_i for each CT_i, Where, N_i = ASCII value of C_i, for each i from 0 to n-1.
- Find the sum index S_i, where $S_i = NE_i + 36$, if $0 \leq NE_i \leq 9$ else $Si = NE_i$.
- Find the Difference index $D_i = S_i - {}_i i$, for i= 0 to n-1, where K_i is the ith key generated in the sequence.
- Find C_i, where C_i is the character equivalent of D_i, for i = 0 to n-1.

B. Access Control

As compared to CP-ABE scheme in which the decryption keys only support user attributes that are organized logically as a single set, so users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies.

To solve this problem, cipher text-policy attribute-set based encryption (CP-ASBE or ASBE for short) is introduced by Bobba, Waters et al. ASBE is an extended form of CPABE which organizes user attributes into a recursive set structure. Cipher text Policy Attribute Set Based Encryption (CP-ASBE) is a modified form of CP-ABE. It differs from existing CP-ABE schemes that represent user attributes as a monolithic set in keys. It organizes user attributes into are cursive set based structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a

policy. The CP-ASBE consists of recursive set of attributes.

Algorithm 1: CP-ASBE Algorithm
Setup: – Here is the depth of key structure. Take as input a depth parameter'd'. It outputs a public key *PK* and master secret key *MK*. *Key-gen*: – Takes as input the master secret key *MK*, the identity of user u, and a key structure *A*. It outputs a secret key *SK* for user u. *Encrypt*: – Takes as input the public key *PK*, a message *M*, and an access tree *T*. It outputs a cipher text *CT*. *Decrypt*: – Take as input a cipher text *CT* and a secret key *SK* for user u. It outputs a message *M*. If the key structure *A* associated with the secret key *SK*, satisfies the access tree *T*, associated with the cipher text *CT*, then m is the original correct message *M*. Otherwise, *M* is null.

User attributes are organized into a recursive family of sets and Allowing attributes to combine from multiple sets. Thus, by grouping user attributes into sets and no restriction on how they can be combined, CP-ASBE can support compound attributes. More flexibility and fine grained access is provided by CP-ASBE. Similarly, multiple numerical assignments for a given attribute can be supported by placing each assignment in a separate set as well as placing it into a single set.

IV. EXPERIMENTAL RESULTS AND COMPARISION

In this section the experimental results of the proposed system are given for various environments and the results of proposed system are compared with existing methods. The important parameters of execution time and security level are taking for comparison.

A. Experimental Setup

The proposed system implemented in java platform, the hardware configurations are Intel i7 processor with 4 GB RAM and hard disk size of 500 GB.

B. Execution Time

The execution time for the proposed system for uploading a file with various file sizes are given in the following table.

Table 1 Execution Time for uploading a file with Various Sizes

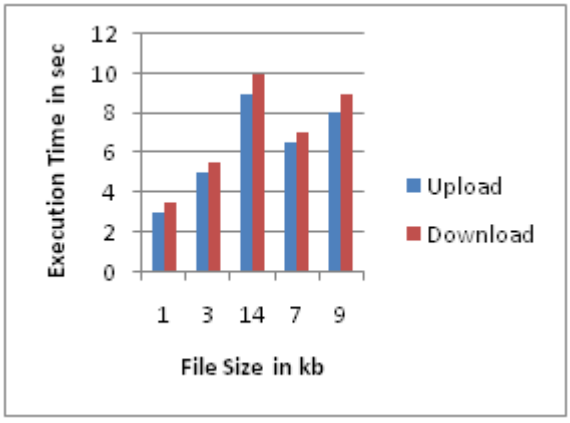
S.No	File Size	Time
1	1 kb	3 sec
2	3 kb	5 sec
3	14 kb	9 sec
4	7 kb	6.5 sec
5	9 kb	8 sec

Downloading a file with various sizes from the cloud was given in the Table 2. This time is considered as the execution time for the downloading process.

Table 2 Execution Time for downloading a file with Various Sizes

S.No	File Size	Time
1	1 kb	3.5 sec
2	3 kb	5.5 sec
3	14 kb	10 sec
4	7 kb	7 sec
5	9 kb	9 sec

The comparison of execution time of uploading and downloading a file in cloud was shown in the following bar chart.



From table 1 and table 2 we can see that the proposed model takes quite same time for execution like other present models. But it ensures higher security. Information is stored in main server about the databases where the encrypted files are kept. Thus, database

encryption only in main server is enough so that no information is leaked. This makes the model cost effective and less time required for execution of the whole process. Secured information exchanging between the users and system gives protection of hiding information from the unauthorized users and intruders.

V. Conclusion

Cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; Security of the data stored in the cloud is the main problem in cloud computing technique. To provide efficient data security and access control for users this paper used probabilistic encryption method and cipher policy ABE algorithms. The implementation results show that the proposed technique take the security and access control in next level.

References

[1] Amazon Web Services (AWS) [Online]. Available: https://s3.amazonaws.com

[2] Ameni Ben Fadhela, Domenico Biancullib and Lionel Briand (2015), "A comprehensive modeling framework for role-based access control policies", The Journal of Systems and Software No.107, pp.110–126.

[3] Amit Sahai and B. Waters, (2005) "Fuzzy identity based encryption", International Association for Cryptologic, Vol. 3494, pp. 457–473.

[4] Amit Sahai, Brent Waters, Vipul Goyal and Omkant Pandey (2006), "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", International Journal of Computer Applications.

[5] Bethencourt.J, A. Sahai, and B. Waters (2007), "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp.Security and Privacy, Oakland, CA.

[6] Dongyoung Koo, JunbeomHur and Hyunsoo Yoon (2013), "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage", Elsevier Ltd, Computers and Electrical Engineering, No.39, pp.34–46,

[7] Gitanjali ,Sukhjit Singh Sehra and Jaiteg Singh (2013), "Policy Specification in Role based Access Control on Clouds", International Journal of Computer Applications (0975 – 8887) Volume 75, No.1.

[8] Gokuldev.S and S.Leelavathi (2013), "A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control by Separate Encryption/Decryption in Cloud Computing", International Journal of Engineering Science and Innovative Technology, Volume 2, Issue 3.

[9] Google App Engine [Online], Available: http://code.google.com/appengine

[10] Goya.V, O. Pandey, A. Sahai, and B.Waters (2006), "Attibute-based encryption for fine-grained access control of encrypted data", Address Complete MessageConferance on Computer and Communications Security, Alexandria.

[11] Hadia M.S El Hennawy, Alaa E.A. Omar and Salah M.A. Kholaif (2015), "Link Encryption Algorithm Proposed Stream Cipher Algorithm", Ain Shams Engineering Journal, No.6, pp.57- 65.

[12] Kan Yang and XiaohuaJia (2014), "Expressive, Efficient, And Revocable Data Access Control for Multi-Authority Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 7, pp.1735-1744.

[13] Kan Yang XiaohuaJia, KuiRen,Bo Zhang and RuitaoXie (2013)," Effective Data Access Control for Multiauthority Cloud Storage Systems", IEEE Transactions On Information Forensics And Security, Vol. 8, No. 11, pp.1790-1802.

[14] Lan Zhou and J. Biskup (2013), "Secure Administration of Cryptographic Role Based Access Control for Large Scale Cloud Storage Systems", Journal of Computer and System Sciences No.80, pp.1518–1533.

[15] Lan Zhou, Vijay Varadharajan and Michael Hitchens (2013), "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage", IEEE transaction on information forensics and security, Vol.8, No.12.

[16] Manpreet Kaur and Rajbir Singh (2013), "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 70– No.18.

[17] Minu George, Dr. C.SureshGnanadhas and Saranya.K (2013),"A Survey on Attribute Based Encryption Scheme in Cloud Computing", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 11.

[18] Parminder Singh and Sarpreet Singh (2013)," A New Advance Efficient RBAC to Enhance the Security in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, ISSN: 2277,pp.1136-1142.

[19] ParsiKalpana and SudhaSingaraju (2012), "Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in Computer and Communication technology, ISSN 2278-5841, Vol.1, Issue 4.

[20] Punithasurya K and JebaPriya S (2012), "Analysis of Different Access Control Mechanism in Cloud", International Journal of Applied Information Systems, Volume 4, No.2, pp.34-39.

[21] Qi Li, Xinwen Zhang, Qingji Zheng, Ravi Sandhu, and Xiaoming Fu (2015), "Lightweight Integrity Verification and Content Access Control for Named Data Networking", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 2, pp. 308-321.

[22] Sahai.A and Waters.B (2015), "Fuzzy identity based encryption," in Proc.Acvances in Cryptology—Eurocrypt, vol. 3494, LNCS, pp. 457–473.

[23] Waleed W. Smari, Patrice Clementeb and Jean-Francois Lalande (2014), "An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system", Future Generation Computer Systems, Elsevier, No.31, pp.147-168.

[24] Wan Zhiguo, Jun'e Liu, and Robert H. Deng (2012), "HASBE: A Hierarchical Attribute-Base Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE transactions on information forensics and security, Vol. 7, No. 2.

[25] Wang G, Q. Liu, and J.Wu (2010), "Hierachical attribute-based encryption for fine-grained access control in cloud storage services," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago.

[26] Xu Zhongyuan and Scott D. Stoller (2015), "Mining Attribute-Based Access Control Policies", IEEE Transactions on Dependable and Secure Computing, Vol. 12, No. 5.

[27] Yang Xiao and Haizhon Li (2004)," Voice and Video Transmissions with Global Data Parameter Control for the IEEE 802.11e Enhance Distributed Channel Access", IEEE Transactions on Parallel and Distributed Systems, Vol. 15, No. 11, pp.1041-1053.

[28] Yuanchao Shu and Jiming Chen (2014)," Dynamic Authentication with Sensory Information for the Access Control Systems", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 2, pp.427-436.