Volume 5, Issue 9, September 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Parameterized Third Party Auditor Based Access Control & Encryption Security (PTPA-ACE) Model for Cloud Services and Storage

[1]Reema Swami*, [2]Narendra Rathor
[1]M.Tech Scholar, CSE Department, Sanghvi Institute of Management and Science, Indore, Madhya Pradesh, India
[2]Assistant Professor, CSE Department, Sanghvi Institute of Management and Science, Indore, Madhya Pradesh, India

Abstract— Cloud computing is a new flexible approach for providing higher computational power in shared medium. It provides the distributed model based on self evaluating techniques to improve the processing capabilities of the system with lesser managerial concerns. It is made up of client, application, platform, servers and infrastructures. This computing model delivers computation capabilities as a calculated service from above components to end users. Though a wide variety of devices and their integration are concerned, priority of handling security will go down. As the users of cloud is increasing day by day, one need to handle the data, system and confidentiality issues carefully.

So a new security model must be added along with existing system to provide authenticated access of authorized data in a cloud environment. Also the type of users & their accessing medium is an outside world and due to that the unauthorized changes in the system may occur. The most damaging aspect is the loss of data and software through virus, attackers and hackers. This some secure mechanism is required to provide such improved level of security through cloud.

Keywords— Cloud computing, Third Part Auditor (TPA), Cloud Service Provider(CSP), Data Storage, Security, Access control, Authorization parameters, Encryption.

I. INTRODUCTION

Cloud in a service which perform on real time network and give a computation, unite more than two computing resource in type of bunch in another word cloud additionally called Distributed Computing. Most cloud three sort service gives us, PAAS and SAAS Together with virtualization, clouds could be characterized as computers that are networked anywhere on the planet with the availability of paying the used clouds in a pay-per-use way, implying that simply the resources that are, used will be paid.

Cloud computing methodology is a conceptual framework for providing effective and low cost computation as a service to the users. It is a network based computing paradigm, where resources are used in a shared manner like to share software‘s, and infrastructure and development platform. It provides all the above features as utility measured services.

Storing the data at remote locations through cloud offers great convenience. In a cloud storage system, a third party data center known as a cloud service provider (CSP) plays an important role in data management and storage policy settings. Since the CSP is the authority that controls the data items stored in the system, the CSP can look into data items stored in cloud storage without the data owners‘ permission. Thus to make the system more reliable client needs to make some security trusted deals with its data. The actual deployment of cloud computing services is not reliable as they claim because the existing security model doesn‘t work after migration of services to clouds.

This migration follows multitenant model and cloud computing is bringing remarkable impact on information security fields. Such issues generated because of dynamic scalability, service abstraction and location transparency. Unfortunately, to the best of the known methodologies, most commercial cloud STORAGE systems provide simple storage services in which the data content is stored in plaintext form. Therefore, there is concern about privacy issues of the outsourced data, due to either the CSP‘s malfunction or abuse for illicit profit, even if the data owners do not want to reveal any information.

While these internet-based online services do provide massive amounts of storage space and customizable computing resources, the user loses control of the data. While mentioning these security and privacy issues, trusted mechanism needs to be developed.

There are a number of security issues/concerns associated with cloud computing, but these issues fall into two broad categories: Security issues faced by cloud providers and security issues faced by the end users of the service in which the interaction depends. In traditional systems the service provider must ensure the user about the services and infrastructure related to the security of their clients‘ data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect the user‘s data. The increased user of virtualization in cloud computing platform brings unique security concerns for customers or tenants of a public cloud service.

Cloud computing systems provide various Internet-based data storage and services. Due to its many benefits, including cost effectiveness, high scalability, fault tolerance and flexibility, cloud computing are gaining pace through its user‘s quantity increased for distributed computing for various applications, especially for intelligent business solutions.

Internet application is getting denser due to their heavy infrastructure and users through its services and hypervisor virtualization technologies. It provides the solutions to users problem as a service model in which each computation paradigm can be used based on a tenancy model. But the concern is that how such security services is delivered to end user in utility manner and hence the solution proposed in [7]. But as the popularity of cloud increasing user expectation is also increasing like it cannot protect the confidentiality of users' data from service providers One of the other aspects of data security is the need to assess before embarking on creating a security model for data in the cloud is the levels of need; that is, how secure do you want that data to be? The levels of security of any data object should be thought of as concentric layers of increasingly pervasive security, which I have broken down here into their component parts to ***show the increasing granularity of this pervasiveness:***

Level 1: Transmission of the file using encrypted protocols

Level 2: Access control of the file itself, but without encryption of the content

Level 3: Access control (including encryption of the content of a data object)

Level 4: Access control (including encryption of the content of a data object) also including rights management options (for example, no copying content, no printing content, date restrictions, etc.)

Cloud computing security is the sub domain of network security in which the data handling and storage goes through the life cycle process of generation, transfer, user, share, store, archive and destruct [4].

Thus, it needs to be taken as more secure data and when it is handled by providers, there is an always way to do is open. Thus to make the system more reliable client needs to make some security trusted deals with its data.

II. LITERATURE REVIEW

Various cloud based security model is being proposed to resolve the issues related to the security. Among all of them trusted security is gaining popularity due to its effectiveness.

The paper [8], have analyzed the trusted computing in the cloud environment. The paper proposes an approach Trusted Computing Group (TCG) and related open specifications and development efforts for servers, clients, and pervasive devices to provide a hardware-root of trust‖ that can leverage up the stack. It enables integrity, reporting and provides several capabilities for the trust framework to enable trust in the infrastructure.

At the initial level of research, the approach provides a great guiding rule for trust based security. During the last few years, many of the researchers had focused their intentions towards the better cloud storage model with a higher degree of security. Taking security as a prime vision of cloud and can be achieved through cryptographic functions.

In the paper [9], the author gives the survey on benefits of architecture provided by these cryptographic mechanisms. The paper also describes a high level architecture for a cryptographic storage service. It consists of three components: a data processor (DP), which processes data before it is sent to the cloud; a data verifier (DV), that checks whether the data in the cloud has been tampered with; and a token generator (TG) that generates tokens that enable the cloud storage provider to retrieve segments of customer data. The work also uses a credential generator that implements an access control policy by issuing credentials to the various parties in the system (these credentials will enable the parties to decrypt encrypted files according to the policy).

The paper also gives the design for both commercial & non benefited users. Now a day the user trends shows that connectivity and external storage are getting denser through the sharing request and data flows complexities. These are handled by the provider‘s solution, but the client is not sure about the security mechanism of such an outsider. To overcome this limitation, [10] presents an approach for enabling users to regulate access to resources they wish to share in a selective way with other users in a community. The approach also exploits encryption to attach the access control restrictions to the resources and relies on key agreement and key derivation techniques to ensure manageability and scalability of key management.

The proposed approach provides the users with the functionality for publishing and accessing resources. The publish functionality allows data owners to compute the digest, sign, and correctly encrypt their resources and to deliver the encrypted resources to the service for their management. TAAC (Temporal Attribute based Access Control) a user access control is given in [11].

It is an efficient data access control scheme for multi-authority cloud storage service systems in which each authority will work as a different entity and no centralized authority is required. The proposed scheme can efficiently achieve temporal access control of behavior attributes level rather than on the user parameter level. Moreover, different from the existing schemes with characteristic revocation functionality, It does not require re-encryption of any cipher texts when the attribute revocation happens, which means great enhancement of the efficiency of attribute revocation. TAAC is highly scalable in nature.

Similar to that [12] present a temporal attribute based encryption (TABE) scheme to implement temporal constraints for data access control in clouds. This scheme has a constant size for cipher texts, private-key, and a nearly linear-time complexity. It has four algorithms named as setup, generate key, encrypt & decrypt. At the initial level its security model seems to be good & effective.

Similarly DAAC is proposed in [13] which distribute access control in clouds, where one or more KDCs distribute keys to data container and users. The key distribution center may provide access to particular fields in all records. Thus, a particular key replaces separate keys from the owner. The owner and user are allocated a certain set of attributes. Owner encrypts the data with the attributes it has and stores them in the cloud.

The users with matching set of attributes can retrieve the data from the cloud. Thus, various approaches are suggested based on the runtime environment to improve the user attribute based encryption performance. Another way to

make the data protected is using encryption standards such as RC5, DES, AES, and Blowfish. Using such techniques makes the data transfer in a secure manner. But there are always some constraints related to those algorithms.

So before selecting them some needs to make better comparisons between those as given by [14]. The paper provides a fair comparison between four most common and used symmetric key algorithms: AES, DES, 3DES and Blowfish. A comparison has been made on the basis of these parameters: rounds block size, key size, and encryption/decryption time, CPU processing time in the form of throughput and power consumption. These results show that blowfish is more suitable than AES. But while taking the encryption for security always raises the decryption issues & time drops. Some approach is required which gives the security of encryption without decrypting the data to be read. This feature is given by homomorphic encryption. The further usage & modification of fully homomorphic encryption (FHE) is explained in [15] also.

Here the fully homomorphic encryption scheme means that it keeps data private, but that allows a worker that does not have the secret decryption key to compute any (still encrypted) result of the data, even when the function of the data is very complex.

In the paper [16], the usage & behavior of homomorphic encryption are thoroughly defined. It also proposes an efficient and Secure Data Sharing (SDS) framework using homomorphic encryption and proxy re-encryption schemes that prevent the leakage of unauthorized data when a revoked user rejoins the scheme. The proposed construction is secure under the security descriptor of Secure Multi Party Computation (SMC).

Also a generic approach of any additive homomorphic encryption and proxy re-encryption schemes can be used as the fundamental sub-routines. In addition, it also modifies the underlying Secure Data Sharing (SDS) framework and present a new solution based on the data distribution technique to prevent the information leakage in the case of collusion between a user and the Cloud Service Provider.

III. PROBLEM IDENTIFICATION

Also a generic approach of any additive homomorphic encryption and proxy re-encryption schemes can be used as the fundamental sub-routines. In addition, it also modifies the underlying Secure Data Sharing (SDS) framework and present a new solution based on the data distribution technique to prevent the information leakage in the case of collusion between a user and the Cloud Service Provider.

***Problem-I*:** In traditional security mechanism encryption standards are used which cannot be directly adopted by normal users. There is also a loss of control occurs over data for users as it is moving towards cloud providers. Thus a new verification mechanism had to be used without measuring the concerned issues for whole data. Taking a different kind of data values for each user, stored in the cloud and the demand of long term data security for them is getting typical because of heavy exchanges [17].

Here multiple users accessing the data in the same location simultaneously. So in some case condition may arise when incorrect data are displayed to users due to congestion & load. Thus, for better securing the property of data isolation has to be fully satisfied.

Problem-II: As the cloud faces continuous exchanges of data by users through various commands like insertion, deletion, reordering, appending, modification, etc. Thus the user needs to be authenticated for performing the operations on the data. It will also make sure that users may access its data through authorized cloud services. Thus, both cloud & user had to be verified for such operations. New mechanism had to be developed through a third party to solve such issues [18].

***Problem-III*:** Since all the existing security mechanism focuses on the single server interaction environment. But as the type of interaction is increasing in case of cloud integration like cloud, cloud-user, user-user providing security is getting difficult & complex. Thus a new mechanism had to be developed which reduces the user efforts for encryption &decryption & increases the security & isolation of data stored on third party cloud [19].

IV. PROPOSED WORK

The proposed work is providing a novel method which gives priority to client systems and make their data secure by taking their behaviour elements as a key for encryption. This can be achieved by a known key cryptography method named as public key infrastructure with attribute values of user and data working as a key. It also added an additional padding bit with modified hash function to make the cloud more secure & reliable.

The approach works on a trust model of the user. Each user is having different types attribute elements of their own and the type of data used is also different. This area is described as its access area. During this mechanism a user is able to store and retrieve the data from cloud in an encrypted form. The proposed architecture is a 6 step trust model based fine grained access control mechanism for improving the security of storage for cloud.

The proposed architecture is shown in the figure below. It shows that when a user wants to access his data area, he had to give request to any third party server, which verifies its integrity from its databases & having a specified trust value in case of each user with given authorization parameters like credentials, Role, Network properties etc.. Then the third party auditor replies the user with its tenant ID having a unique kind of token to access the data. Same token is also being provided to the cloud service provider. When a user demands an access to cloud this token gets verified and the permission is granted.

The request for data storage from user to cloud had to go through an encryption service in which the user‘s behavior element works as a key. This key is a combination of various other elements like session information, UIDs, password, timestamp, existing history of content type and service used, etc. The above element will automatically do the encryption without the user's knowledge.

After this step even cloud doesn‘t know the type of data which the user had stored in the storage. After this the cloud provides the user an access ID for a data storage session to the users so as to interact directly with the storage. When the client demanded for its stored data same behavioral element works as a decryption key. After applying such mechanism the problem related to data isolation & incorrect data display to the user is also solved.

The approach PTPA-ACE (as shown in Fig 1.0) works on a trust model of the user. Each user is having different types attribute elements of their own and the type of data used is also different. This area is described as its access area. The purpose of this proposed work is to identify various issues related to cloud storage with customized client end security services. It provides the virtual security mechanism as a service.

It solves the problem arises due to remote data locations. The study also develops an approach to implement above mentioned service on real cloud platform. It meets all the security requirements of deploying configuration of security as a service. The proposed parameterized third party auditor based access control & encryption security model for cloud services and storage.

This trust model PTPA-ACE (as shown in Fig 1.0) in combination of behaviour based encryption satisfies all the constraints. Various other existing encryption algorithms are studied, but can‘t be able to solve the client level security problem..

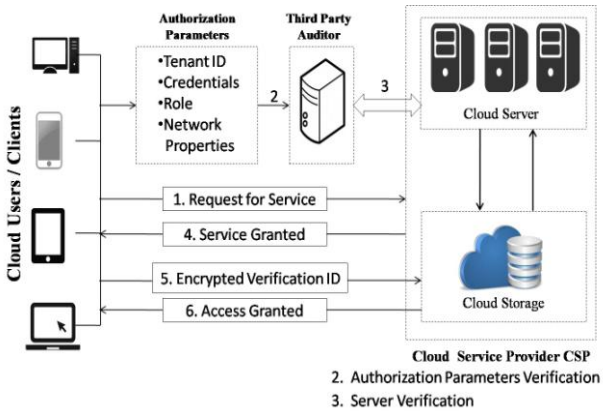

Fig 1 proposed architecture of parameterized third party auditor based access control & encryption(ptpa-ace) security model for cloud services and storage.

Steps Involved in Designing above Architecture of PTPA-ACE (as shown in Fig 1.0):

Step 1 Client Application: This step processed all the elements on behalf of which the client can access the data. It includes various details of users' behavior such as its session details, failed login attempts, timestamps, historical data, type of files, its size etc. This model will also request for service of storage to third party auditors, cloud server and storage locations. It user various policy setting elements such as key policy of these various behavioral elements work as a key for data encryption and decryption.

Step 2 Third Part Auditor (TPA): A TPA has the expertise and capabilities that users may not have, are trusted to assess and expose the risk of cloud storage services on behalf of the users upon request. It is a verification entity where both client and cloud can verify themselves before accessing the service. At the start the TPA assigns each user a unique Tenant ID and other parameters like credentials, roles and network properties, same is the case with cloud also. It also assigns a unique ID to cloud provider so as to recognize the type of service and its authenticity.

Step 3 CSP and its Servers: A CSP, who has considerable resources and proficiency in building and managing distributed cloud storage servers, owns and operates live cloud computing systems,. When the client needs to connect the cloud, it is the responsibility of CSP to look over all the configurations requires delivering those services to end user. It also handles the various virtual machines created to work as isolation modules. It considers that the user came with the token provided by TPA is authentic and starts giving the service to it. It also deals with the various types of interaction scenarios of user with TPA, CSP and storage servers.

Step 4 Cloud Data Storage: It is the storage module which contains the data of different users with their behavioural elements. The user can access its storage area after a verification certificate is provided to it by the CSP. It performs the block level operation of security through various encryption standards available to it. It is a distributed storage server in which multiple fragments of the same data are stored at different locations & whose combination information is stored in them as a pointer to next location other part of the data. Storage also desire to move data that have not been or is rarely accessed to a lower tier of storage than agreed for monetary reasons, but it may also attempt to hide a data loss incident due to management errors, Byzantine failures and so on.

Step 5 In this step Verification ID provided by third party auditor is passed to the storage systems of the CSP and request for granting access.

Step 6 This step involves verification of the ID provided in the previous step, if the ID passes the thorough verification, access is granted to the consumer now client can start accessing the data from the storage systems.

Thus, by applying all the above mentioned settings will make the system secure in an effective ways. It will also increase user capabilities to work on cloud services. The proposed model will be implemented on Cloud swim platform and will configure to provide the behavior based encryption with improved access mechanism through security as a service deployment.

V. CONCLUSIONS

In order to measure and compare the performances of the proposed scheme, the work continues to adopt the various comparison metrics, First is key size & generation is very effective and very less in case of existing encryption standard. Second is secure, data access mechanism. The work makes the following observations about the proposed work.

1. Improved security and data access can be implemented in an efficient manner. It will also ensure the successful satisfaction of various integrity rules for correctness of data.
2. Data isolation and access control can be guaranteed by using access and key policies for various types of user. Policies are used here to define finer grained access control.
3. Dynamic operations on data block are supported like an update, delete and append. This mechanism will improve the efficiency of the system due to parallel processing of data updating and its encryption.
4. The new key combination approach is developed to further increasing security through key policy using attribute based encryption. Multiple attributes of user are combined together to generate a new key in this.
5. User behavioural elements can be easily calculated which decrease the user effort. It causes a reduction of efforts because user doesn‘t know about its security process, key calculation and data transfer.
6. The effective trust model is used for continuous monitoring the user behaviour. This trust model regularly measuring the user behaviour & recognizes any changes in it very soon to prevent any data loss.

VI. EXPECTED BENEFITS

The security and sustainable computing are the latest area of work for cloud computing. In traditional storage environment the control of access and data modifications is totally handled by the cloud provider. User had nothing to do with that causes a un- satisfaction of security. It can be removed by using the client level security approaches, but this will generate an extra load on the user. So some mechanism had to be developed which improves the security of data without the effort increase at the user‘s level. This work proposes a novel model PTPA-ACE (as shown in Fig 1.0) for the security of the cloud using parameterized third party auditor based access control & encryption security model for cloud services and storage.

It manages each interaction scenario of user, cloud and storage through a token system. The work also uses a user attribute based encryption method for security of data. This attribute will work as parameters of key generation and will improve the data isolation issues. The work extends the trusted computing technology into the cloud computing environment to achieve the security, computing requirements with efficiency and then fulfil consumer requirements and gains the higher trust values.

ACKNOWLEDGMENT

The authors express their thanks to Assistant Prof. Narendra Rathor, SIMS, Indore, who has helped in different ways to complete this work. Thanks are also due to the anonymous reviewers and our colleagues for their suggestions to improve the manuscript.

REFERENCES

[1] Dongyoung Koo, Junbeom Hur & Hyunsoo Yoon, “Secure and efficient data retrieval over encrypted data using Attribute-based encryption in cloud storage”, in Computers and Electrical Engineering Journal of Elsevier, ISSN: 0045-7906, doi:10.1016/j.compeleceng.2012.11.002, Vol. No 39, Jan 2013. pp 34–46

[2] Guojun Wang, Qin Liu, Jie Wu & Minyi Guo, “Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers”, in Computer & Security Journal of Elsevier, ISSN: 0167-4048, doi: 10.1016/j.cose.2011.05.006, Vol. No. 30, July 2011. pp 320-331

[3] Shucheng Yu, Cong Wang, Kui Ren & Wenjing Lou, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing”, in Proceedings of IEEE Infocomm., ISSN: 978-1-4244-5837-0/10, 2010.

[4] Deyan Chen & Hong Zhao, “Data Security and Privacy Protection Issues in Cloud Computing”, in International Conference on Computer Science and Electronics Engineering, IEEE Computer Society, ISSN: 978-0-7695-4647-6/12, doi: 10.1109/ICCSEE.2012.193, 2012.

[5] Stephen S. Yau & Ho G. An, “Confidentiality Protection in Cloud Computing Systems”, in International Journal of Software Informatics, ISSN 1673-7288, Vol.4, No.4, December 2010, pp. 351-365

[6] Mohemed Almorsy, John Grundy & Amani S. Ibrahim, “Collaboration-Based Cloud Computing Security Management Framework”, in 4th International Conference on Cloud Computing, IEEE Computer Society, ISSN: 978-0-7695-4460-1/11, doi:10.1109/Cloud.2011.9, 2011.

[7] Daryl C. Plummer, Thomas J. Bittman, Tom Austin, David W. Cearley & David Mitchell Smith, “Cloud Computing: Defining and Describing an Emerging Phenomenon”, in Gartner Research Publication, ID Number: G00156220, June 2008.

[8] Pardeep Kumar, Vivek Kumar Sehgal , Durg Singh Chauhan, P. K. Gupta & Manoj Diwakar, “Effective Ways of Secure, Private and Trusted Cloud Computing”, in International Journal of Computer Science Issues, ISSN (Online): 1694-0814, Vol. 8, Issue 3, No. 2, May 2011.

[9] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, G. Pelosi & P. Samarati, “Encryption-based Policy Enforcement for Cloud Storage”, in IEEE Transaction, at Universita degli Studi, di Milano, 2010.

[10] Kan Yang, Zhen Liu, Zhenfu Cao, Xiaohua Jia, Duncan S. Wong & Kui Ren, “TAAC: Temporal Attribute-based Access Control for Multi-Authority Cloud Storage Systems”, in IEEE Transaction, 2011.

[11] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Xiaorui Gong & Shimin Chen, "POSTER: Temporal Attribute-Based Encryption in Clouds", in ACM Journal, ISSN:978-1-4503-0948-6/11/10, Oct 2011.

[12] Sushmita Ruj, Amiya Nayak and Ivan Stojmenovic, "DACC: Distributed Access Control in Clouds", in International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-1, ISSN: 978-0-7695-4600-1/11, doi:10.1109/TrustCom.2011.15, 2011.

[13] Pratap Chandra Mandal, "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish", Journal of Global Research in Computer Science, ISSN: 2229-371X, Volume 3, No. 8, August 2012.

[14] Craig Gentry, "Computing Arbitrary Functions of Encrypted Data", in ACM Journal, ISSN: 0001-0782/08/0X00, 2008.

[15] Bharath K. Samanthula, Gerry Howser, Yousef Elmehdwi, and Sanjay Madria, "An Efficient and Secure Data Sharing Framework using Homomorphic Encryption in the Cloud", in ACM Journal, ISSN: 978-1-4503-1596-8/12/08., 2012.

[16] Farhan Bashir Shaikh & Sajjad Haider, "Security Threats in Cloud Computing", in 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirates Dec 2011.

[17] Farzad Sabahi, "Cloud Computing Security Threats and Responses", in IEEE Transaction, ISSN: 978-1-61284-486-2/11, 2011.

