ISSN: 2321-7782 (Online)
Volume 4, Issue 3, March 2016
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

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

Reema Swami[1]
Computer Science Department
Sanghvi Institute of Management and Science
SIMS
Indore, India

Narendra Rathor[2]
Computer Science Department
Sanghvi Institute of Management and Science
SIMS
Indore, India

Abstract: ***Cloud computing is the latest trend in computing by which various services, applications and other computing things can be delivered as a service. 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. We have proposed an new security approach in [20] to increase the level of security in cloud storage system. In this paper we trying to evaluate the proposed approach [20] on various parameters of evaluation and its effect on the resource consumption of cloud infrastructure.

Keywords: Genetic Programming, Feature selection, Crossover, Mutation, fitness function, filter approach, wrapper approach, ramped half-and-half method.

I. INTRODUCTION

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 centre 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. 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. 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

II. Related Work

Security and privacy are the major issues in the cloud computing. The content stored in the cloud system can meet the problem of stolen and modified unauthentically. The traditional mechanism is to encrypt the data before it enters to the cloud system but if the size of the data is large then its time complexity for the encryption degrades the performance of the cloud system. Many authors propose symmetric and asymmetric key encryption model in order to achieve confidentiality, authorization, validation, integration and non-repudiation.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

III. 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.

IV. EXPERIMENTAL RESULTS

The aim is towards providing more security and robustness against the traditional breaches which practical implementation of cloud is facing. Proving the data and users security against its confidential and private information concerns the major area of cloud working. These intensions are kept in mind at the time of implementing the suggested concept. Now, it's the time to show how better the approach can work while comparing with their competitors. At the evaluation point of view the approach seems to satisfy all the constraints of data isolation and user access control. Effective access control becomes a core issue in cloud computing because of their accessibility and dependencies of users interactions. If the system provides effective access control but let's open the trapdoors for the malicious user then the confidentiality of the system can be loosed. It has a risk associated with the cloud based outsourced environment.Automatically classifying data with high dimensionality is a difficult task. When we have skewed datasets this becomes more difficult. Different method are used for reducing dimensionality by feature selection are usually biased towards the largest class. Our goal is to maximize classification accuracy in the smallest class.

S. No	User Name	User Type	Tenant ID	IP	Service Selected	Cloud Initialization
1	User1	Moderate User	1777532722	192.168.255.1	File Storage (FTP)	Aneka Demon:12/1/2015 9:43:27 AM INFO- All VMs Initiated
2	User2		1242940967	192.168.255.14		Aneka Demon:12/1/2015 9:48:50 AM INFO- All VMs Initiated
3	User3		735365537	192.168.255.25		Aneka Demon:12/1/2015 9:52:12 AM INFO- All VMs Initiated
4	User4		654994807	192.168.255.7		Aneka Demon:12/1/2015 9:54:27 AM INFO- All VMs Initiated
5	User5		2136048230	192.168.255.46		Aneka Demon:12/1/2015 9:59:36AM INFO- All VMs Initiated

Table-8.1: User Initialization and Tenant Generation.

S. No	Tenant ID	Authentication Token		Verification(TPA)	Service Types
		Time(Mil. Sec.)	Size(bits)	Time(Mil. Sec.)	
1	1777532722	664.235	50	423.147	File Storage (FTP)
2	1242940967	165.245	38	235.21	
3	735365537	119.24	36	354.91	
4	654994807	155.321	40	362.347	
5	2136048230	425.98	45	401.26	

Table-8.2: Features based Analysis of Proposed System

Tenant ID	Processor Pool (%)		Disk Usage (Bits Per Sec)		Memory Pool (% / GB Per Sec)		Network Usage (KB/Sec)	
	Before	After	Read	Write	Physical	Virtual	Sent	Receive
1777532722	16.24	56.23	16.09	86.82	40.34	51.79	15.95	80.05
1242940967	30.26	85.32	36.74	131.36	40.53	51.89	118.36	15.64
735365537	21.22	97.42	08.92	76.25	40.36	51.89	12.37	94.23
654994807	36.15	84.20	17.68	123.45	40.38	51.99	126.32	20.84
2136048230	12.86	38.98	24.21	50.17	40.33	51.88	36.18	124.36

Table-8.3: System Constraints Performance Monitoring

V. CONCLUSION

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.

The proposed work is found satisfactory on the basis of statistics, but there is always a scope of improvement. Our work focuses on the information flow control from user to CSP but not vice versa, that can be new area of research in the future for researchers. In future we can work on the varieties of the tags including more number of rules that can be used to fulfil the requirements of the user. Our work opens a new area of research in access control fro cloud computing moreover any strong encryption policy can also be incorporated to make the system more secure.

ACKNOWLEDGEMENT

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.scose.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. Seny Kamara & Kristin Lauter, "Cryptographic Cloud Storage", in Microsoft Research Article at http://
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. Farzad Sabahi, "Cloud Computing Security Threats and Responses", in IEEE Transaction, ISSN: 978-1-61284-486-2/11, 2011.
16. Wentao Liu, "Research on Cloud Computing Security Problem and Strategy", in IEEE Transaction, ISSN: 978-1-4577-1415-3/12, 2012.
17. Reema Swami, Narendra Rathor"A Parameterized Third Party Auditor Based Access Control & Encryption Security (PTPA-ACE) Model for Cloud Services and Storage " published in International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 9, September 2015 ISSN: 2277 128X.

