International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-3 Issue-11 September-2013

Secured Cloud Data with IA

Prasad N H[1], Lakshmi Narayan B N[2], Pradeep Kumar S[3]

Abstract

Cloud Computing is an emergent technology that provides all the services to the users such as Saas, Paas and Iaas which makes life simpler. Cloud gains its limelight with its effective elastic services. This makes the user to feel convenient but there arise so many security breaches as Cloud's central theme is Outsourcing. The data processed on cloud are usually outsourced and hence the user is worried about the data loss or modification. All other security mechanisms are not suitable for Cloud because of its decentralized and distributed architecture. To address the security issues, a new model named 'Secured Cloud Data with IA' is proposed that is meant to provide integrity and authorization. Experimental results show that this model proves its effectiveness in blocking malicious users.

Keywords

Cloud Computing, Outsourcing, Integrity, Authorization.

1. Introduction

Cloud Computing is an emergent technology that provides all the services to the users such as Saas, Paas and Iaas which makes life simpler. Cloud gains its limelight with its effective elastic services. All the cloud services can be made use of by the users on demand, which is an important principle of Cloud computing. With Cloud computing, users can enjoy the new concept 'Pay as you go', which makes sense that the user is needed to pay only for his/her usage and thus there is no static payment.
This makes the user to feel convenient but there arise so many security breaches as Cloud's central theme is Outsourcing. The data processed on cloud are usually outsourced and hence the user is worried about the data loss or modification. All other security mechanisms are not suitable for Cloud because of its decentralized and distributed architecture and is shown in Fig 1.

Prasad N H, Department of MCA, NITTE Meenakshi Institute of Technology, Bangalore, India.
Lakshmi Narayan B N, Department of MCA, NITTE Meenakshi Institute of Technology, Bangalore, India.
Pradeep Kumar S, Project Manager, MysGenius Software Solutions, Mysore, India.

The data owners have to take certain efforts, to manage their data and also a considerable amount has to be spent for data maintenance.

Also, the data grows with respect to time, so a huge memory space is needed and is not affordable by many, so they go for a good option called outsourcing. With this, the data is outsourced to any commercial public space. Certain amount has to be paid for the public space being used. However, it is more economical to pay rent for the memory in use rather than own excessive memory.
Thus, the economic savings motivate both the individuals and enterprises to outsource their data. In this scenario, many challenges like data security, searching and retrieval of data hit the scene. This is achieved by using a principle called "Coordinate matching", which is a similarity measure that uses the number of query keywords appearing in the document to quantify the relevance of that document to the query.

Importance of Data Outsourcing
In the past, hackers generally targeted larger companies that stored government information or financial data. However, hackers today are becoming increasingly brazen and expanding their sights to information that can lead to more valuable data down the line. According to a magazine named "Information Week", 73 percent of small and medium sized businesses report that they have been the victims of cyber-attacks in the past year and 42 percent have lost confidential and proprietary information [1]. Effective security requires continuous monitoring and management as well as security experts who are able to identify and respond to network threats immediately. Outsourcing data to a loyal public space provides data owners, with a team of experienced security analysts with the ability, to assess the severity of a cyber-attack, to formulate the proper response and implement the optimal defense. Outsourcing allows the data owners to lower costs, save time and increase efficiency. To reduce space complexity, it is advised to outsource the data than to maintain by own. A strong assurance is provided for security.

Benefits of Outsourcing
When the data is outsourced, economic savings and an effective search is experienced. Around 60 percent of the cost is saved, through outsourcing and also a faster and a better service is provided [2].
However, data owners are needed to be cautious while choosing the commercial public space.

Before outsourcing, the security policy of the public space should be checked with an eagle eye. Many data owners may go for data outsourcing; however every piece of data is very sensitive and has to be kept private. Thus, the data owners encrypt their data and index before outsourcing the data.

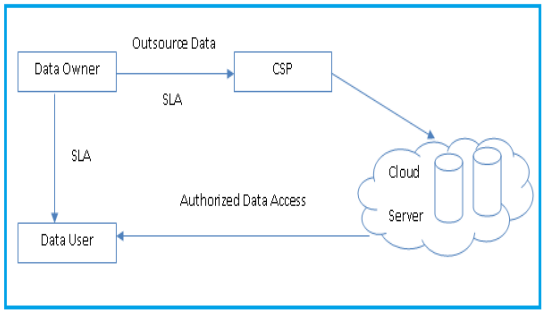

Fig 1: Basic Cloud Architecture

Fig 1 depicts that the data owner outsources his data to a Cloud Service Provider (CSP) based on certain Service Level Agreement (SLA), same way data owners and data users have certain SLA and both parties should not violate the SLAs. To address the security issues, a new model named 'Secured Cloud Data with IA' is proposed that is meant to provide integrity and authorization. This model controls the access, usage pattern by the user.

Our proposed work does the following: firstly, it checks whether the user's access complies with the corresponding user's provision enforced by the data owner, secondly, it keeps track of the user's usage of cloud data continuously, finally, if any data tamper is found an automated trigger is generated that blocks that particular user towards data access.
The first point is accomplished by the way that, every data owner assigns access level to the user which must comply with the user's access.
The second point is achieved by a master point that receives updates about the usage of the cloud data by the user, also all the log information are updated then and there.

Finally, if the user misbehaves, an automated trigger generates which the blocks the user from accessing data and it notifies the data owner. The user can again exploit the resource only after the approval from the data owner. Thus, Authorization and Integrity are provided by this model.

2. Related Work

Cloud computing has raised a range of important privacy and security issues [1], [2], [3]. Such issues

Selection should be done, only on the basis of a strict and a sound security policy.
are due to the fact that, in the cloud, users' data and applications reside at least for a certain amount of time on the cloud cluster which is owned and maintained by a third party. Concerns arise since in the cloud it is not always clear to individuals why their personal information is requested or how it will be used or passed on to other parties. To date, little work has been done in this space, in particular with respect to accountability. Pearson et al. have proposed accountability mechanisms to address privacy concerns of end users [3] and then develop a privacy manager [4].

Their basic idea is that the user's private data are sent to the cloud in an encrypted form, and the processing is done on the encrypted data.
The output of the processing is deobfuscated by the privacy manager to reveal the correct result. However, the privacy manager provides only limited features in that it does not guarantee protection once the data are being disclosed.
In [5], the authors present a layered architecture for addressing the end-to-end trust management and accountability problem in federated systems. The authors' focus is very different from ours, in that they mainly leverage trust relationships for accountability, along with authentication and anomaly detection.
Further, their solution requires third-party services to complete the monitoring and focuses on lower level monitoring of system resources.
Researchers have investigated accountability mostly as a provable property through cryptographic mechanisms, particularly in the context of electronic commerce [6], [7].
A representative work in this area is given by [8]. The authors propose the usage of policies attached to the data and present logic for accountability data in distributed settings. Similarly, Jagadeesan et al. recently proposed a logic for designing accountability-based distributed systems [9].
In [6], Crispo and Ruffo proposed an interesting approach related to accountability in case of delegation.

3. Proposed Work

The user who subscribes himself for a cloud service is expected to register himself with his/her personal information. After the registration process, the user is given provision such as read, write or copy. When the access policy is issued, the user should strictly follow the access policy else the user can be blocked by the data owner all at once.

A log file that describes total number of accesses, location, type of access, date and duration of the user's utilization is sent to the data owner periodically. Also, the log files are needed to be kept secure with some security policy. Our proposed work does allowing the user to get access to the data with the already granted permission, then tracks the usage of the user, blocks the user if the user's activity is malicious and notifies the data owner. Also, a single item can have any number of copies, and all the copies will have a master point in our model. So, if any user needs to download data, it directly communicates the master point and not the replicas. Algorithm for the proposed work is given below.

data upload by data_owner;
service_req from data_user;
data_owner read service_req;
data_owner assigns access level;
data_user login;
generate log_file(ID, LOCN, ACCESS_TYPE, DURATION,DATE);
encrypt log_file;
log_file sent to data_owner;
if(access level!=user_access)
generate trigger to block user;
notify data_owner;
end;

Fig 2: Algorithm

The algorithm is represented via the flow chart as shown below.

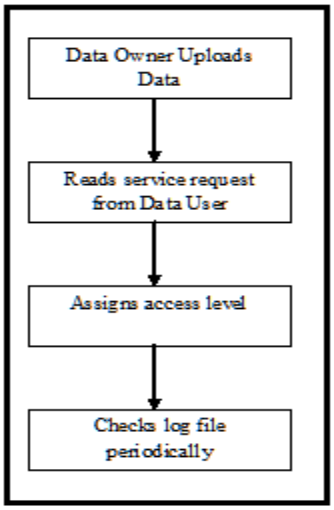

Fig 3: Task Flow of Data Owner

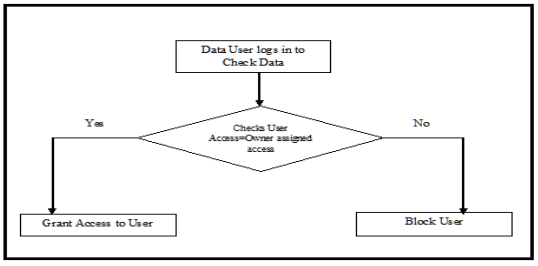

Fig 4: Overall Work Flow

Thus, by the way this work continues and this work strongly provides authorization and integrity. In order to safeguard log file, we encrypt log file with RSA algorithm which is known for its security. Thus, the proposed methodology works.

4. Simulation Results

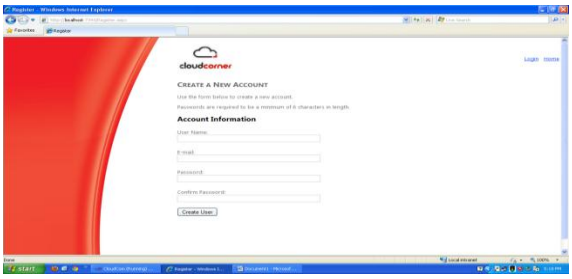

Fig 5: User Registration

Fig 6: Home Page

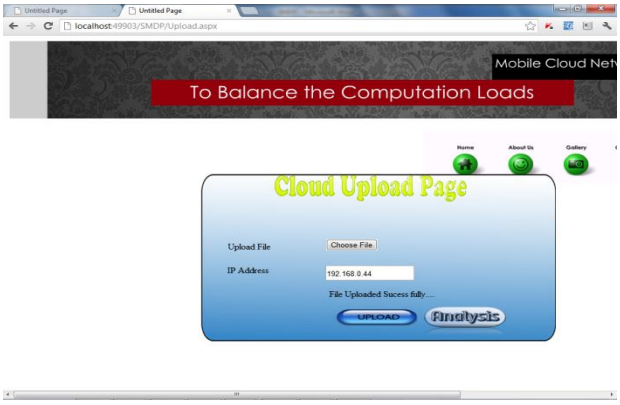

Fig 7: Uploading File

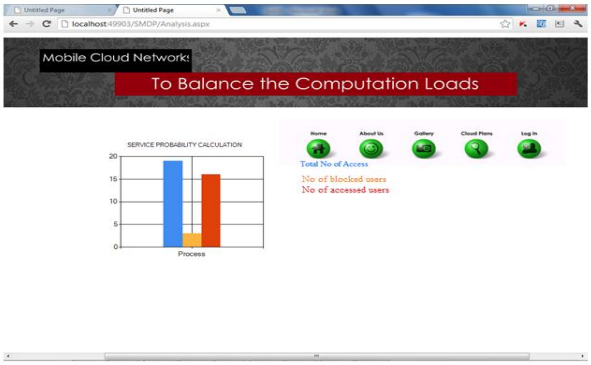

Fig 8: Space Probability Calculation

The above presented dynamic graph shows the total number of accesses made to a particular data with the number of accessed and blocked users. This information is useful for the data owner to check for the malicious and authorized users.

5. Conclusion

This work ensures integrity and authorization, which is a serious issue to take care of. This work blocks the user if the user's access to the data is not found genuine. Hence, there is no chance for tampering data, which in turn affects integrity. This work can further be enhanced to provide authentication.

References

[1] P.T. Jaeger, J. Lin, and J.M. Grimes, "Cloud Computing and Information Policy: Computing in a Policy Cloud?," J. Information Technology and Politics, vol. 5, no. 3, pp. 269-283, 2009.

[2] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice), first ed. O' Reilly, 2009.

[3] S. Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud," Proc. First Int'l Conf. Cloud Computing, 2009.

[4] S. Pearson, Y. Shen, and M. Mowbray, "A Privacy Manager for Cloud Computing," Proc. Int'l Conf. Cloud Computing (CloudCom), pp. 90-106, 2009.

[5] B. Chun and A.C. Bavier, "Decentralized Trust Management and Accountability in Federated Systems," Proc. Ann. Hawaii Int'l Conf. System Sciences (HICSS), 2004.

[6] B. Crispo and G. Ruffo, "Reasoning about Accountability within Delegation," Proc. Third Int'l Conf. Information and Comm. Security (ICICS), pp. 251-260, 2001.

[7] W. Lee, A. Cinzia Squicciarini, and E. Bertino, "The Design and Evaluation of Accountable Grid Computing System," Proc. 29th IEEE Int'l Conf. Distributed Computing Systems (ICDCS '09), pp. 145-154, 2009.

[8] R. Corin, S. Etalle, J.I. den Hartog, G. Lenzini, and I. Staicu, "A Logic for Auditing Accountability in Decentralized Systems," Proc. IIP TC1 WG1.7 Workshop Formal Aspects in Security and Trust, pp. 187-201, 2005.

[9] R. Jagadeesan, A. Jeffrey, C. Pitcher, and J. Riely, "Towards a Theory of Accountability and Audit," Proc. 14th European Conf. Research in Computer Security (ESORICS), pp. 152-167, 2009.

[10] J.H. Lin, R.L. Geiger, R.R. Smith, A.W. Chan, and S. Wanchoo, Method for Authenticating a Java Archive (jar) for Portable Devices, US Patent 6,766,353, July 2004.

[11] F. Martinelli and P. Mori, "On Usage Control for Grid Systems," Future Generation Computer Systems, vol. 26, no. 7, pp. 1032-1042, 2010.

Dr. Prasad N Hamsavath received Master of Technology (M.Tech) in Computer Science & Technology from Jawaharlal Nehru University (JNU), New Delhi, India (2002-04). He has also received Master of Computer Application (MCA) from Nagarjuna University, Guntur, AP, India. He received Ph.D in Computer Science from Jawaharlal Nehru University (JNU), New Delhi, India (2004-2011). Currently he is working as Head of the Department & Professor for the Department of MCA at Nitte Meenakshi Institute of Technology, Bangalore. His area of interest is on AdHoc Networks.

Lakshmi Narayan B N received Master of Computer Application (MCA) from Visvesvaraya Technological University (VTU). He has worked in various IT Industries as Software Engineer. Currently he is working as a Lecturer for the Department of MCA at Nitte Meenakshi Institute of Technology, Bangalore, India. His area of interest is on Cloud Computing. Recently his paper titled "A Fine Methodology for Cervical Image Segmentation" got published in International Conference on "Emerging Research in Computing, Information, Communication and Applications-ERCICA 2013"

Pradeep Kumar S received his Bachelor of Degree in Engineering from Visvesvaraya Technological University (VTU). He has worked as academician in various colleges. Currently he is working as Project Manager in MysGenius Software Solutions, Mysore, Karnataka, India. His area of interest is on Cloud Computing. Recently his paper titled "A Fine Methodology for Cervical Image Segmentation" got published in International Conference on "Emerging Research in Computing, Information, Communication and Applications-ERCICA 2013"