ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

Design and Implementation of Data Protection as a Service (DPaaS) for Cloud Computing

Meena.S[1], Ashok.J[2], Swarajyam[3]

Student, CSE, Gurunanak Institute of Technology, Hyderabad, India [1]

Associate Professor, CSE, Gurunanak Institute of Technology, Hyderabad, India [2]

Student, SE, SNIST, Hyderabad, India [3]

Abstract--Cloud computing technology has emerged to a great extent and people have realized the benefits of it. The commoditization of computing resources has become popular and there are many service providers available. As a new computing model, the cloud computing technology bestows plethora of benefits including the cost effective outsourcing of data. Cloud provides unlimited storage space without the need for capital investment in pay per use fashion. However, the data is stored in cloud servers that are treated as "untrusted". This is because the cloud servers are accessed through Internet and they are remote in nature. There are many security concerns expressed by cloud users with respect to the protection of data. If every cloud user has to take responsibility of security of his data, it is not an easy job. At the same time if every cloud service provider has different security mechanisms for protecting data, it also implies reinventing the wheel. A common protection service can help masses (cloud users in abundance) to have protection as a service which is part of cloud computing. In this paper we attempt to realize such service which is based on the idea provided by Song et al. We built a prototype application that demonstrates the proof of concept. The empirical results revealed that the data protection as a service can dramatically reduce the pre-application deployment effort required in order to ensure the data of cloud users is protected.

Index Terms – Cloud computing, data protection as a service, outsourcing

I. INTRODUCTION

There are many security and privacy challenges in cloud computing. Cloud users outsource their data to cloud server. The cloud service providers provide security to data when it is in cloud. However, the complete security solution is not provided by them. Many researches came into existence to secure cloud data storage. These solutions were needed as there are many security and privacy challenges in cloud computing. The cloud environment is described here.

- Services are provided to huge number of cloud users concurrently.
- Data model used contains shareable data units with provided access control lists.
- Developers can write programs that can interact with cloud and use all the facilities provided by cloud.

In these complex scenarios in a distributed environment there are many security risks including insider thefts, data inconsistencies, and illegal accessing of data, security attacks and so on. To overcome these drawbacks, cloud service providers can't make some pre-deployment security arrangements separate for each user. They need a common service for data protection. Towards this Song et al. proposed a new service model by name Data Protection as a Service (DPaaS). The cloud computing has already other service models such as platform as a service, infrastructure as a service, and software as a service. Therefore it becomes the new and fourth service model available for cloud computing. In this paper we implement the DPaaS architecture that helps cloud service providers to reduce the pre-application deployment activities with respect to data protection dramatically.

The remainder of the paper is structured as follows. Section II provides review of literature. Section III provides information about the proposed architecture for DPaaS. Section IV presents the prototype application. Section V presents experimental results while section VI concludes the paper.

II. RELATED WORKS

Cloud computing has many security issues as explored in [1], [2] and [3]. Most of the issues are related to cloud data storage. As the data storage and retrieval and other data dynamics are the usual operations done by cloud users. They are to be protected. Moreover cloud users trust the cloud service providers and outsource data. Since the cloud servers

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

are treated as "untrusted" many security mechanisms came into existence to protect data. The accountability to the outsourced data is the active research in cloud computing. Provable data possession is the security concept introduced in [4], [5] and [6]. The notion of accountability to cloud data was introduced in [7]. In [8] self-defending objects (SDO) is used to protect data. Prevention of privacy leakage from the concept of indexing is explored in [9]. A technique known as Proof – Carrying Authentication (PCA) was employed in [10] using high order logic language. Identity Based Encryption (IBE) [11] was introduced by Mont et al. for storage security. Secure data 14provenance is another concept proposed in [12], [13] and [6] for storage security. Security at various levels of granularity was explored in [15] and [16]. Secure outsourcing techniques were provided in [17] and [18].

III. PROPOSED DPaaS ARCHITECTURE

The proposed architecture is the new service model for cloud computing. This service model is meant for data protection. It is named as DPaaS (Data Protection as a Service). This kind of service model built into cloud computing environment can reduce the effort required by cloud service providers to have mechanisms to protect data of cloud users. This will help increase the efficiency of cloud in terms of data protection. This will automatically encourage other people to become cloud users and thus cloud computing becomes much more reliable and popular. The architecture is built keeping many issues in mind such as trust and key management, sharing, aggregation, performance, ease of deployment and maintenance. This approach actually moves access control polices and key management into middle tier which is nothing but the computing platform that provides a common platform for masses (all users of cloud computing alike). The proposed cloud service model "DPaaS" is as shown in figure 2.

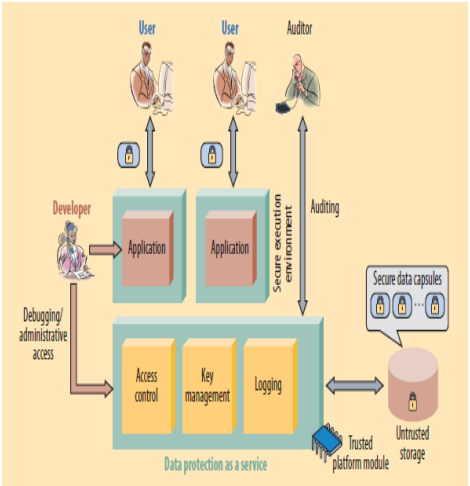

Fig. 2 – Architecture of DPaaS [19]

As can be seen in figure 2, it is evident that the proposed data protection architecture allows developers to incorporate access control, logging and key management into their applications. It also supports auditing of data protection. It makes a secure execution environment where cloud applications can run with built in DPaaS service. There is no re-invention of wheel because the application developers have access to build in security module known as trusted platform module. This enables developers of cloud applications to have provisions for access control list, key management and logging in built.

The proposed architecture is fully aware of user authentication, running binaries, based on the users and application requirements. It has auditing mechanism that ensures that the cloud data protection is in place and no discrepancies occurred in cloud computing paradigm. To realize this architecture we built a prototype application that demonstrates the usefulness of the architecture.

IV. PROTOTYPE APPLICATION

The application is built using Java platform. The prototype simulates the cloud environment where the cloud service model proposed in this paper i.e., "DPaaS" automatically protects privacy and security of data. The environment used to build the application includes a PC with 4GB RAM, core 2 dual processing running Windows 7 operating system. The application is based on the following flow of data. There are two users who can operate the proposed application. They are administrator which high privileges and user with low privileges. Auditor is another user involved in the application with auditing privileges.

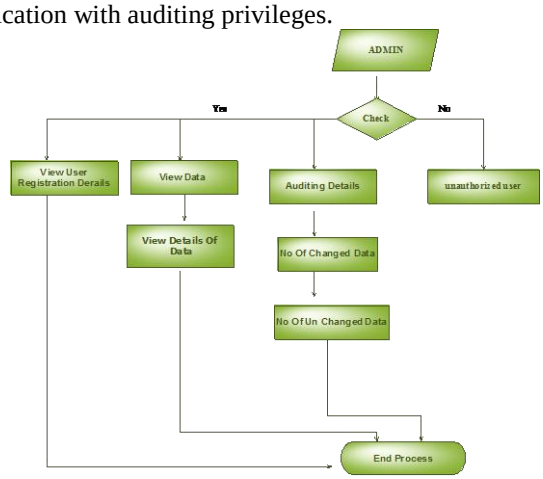

Fig. 3 – Activities of Admin user

As can be seen in figure 3, the administrator user can view auditing details, data inconsistencies, authentication of users, data and other details. The normal user has less number of

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

privileges. The privileges of normal user are presented in figure 4.

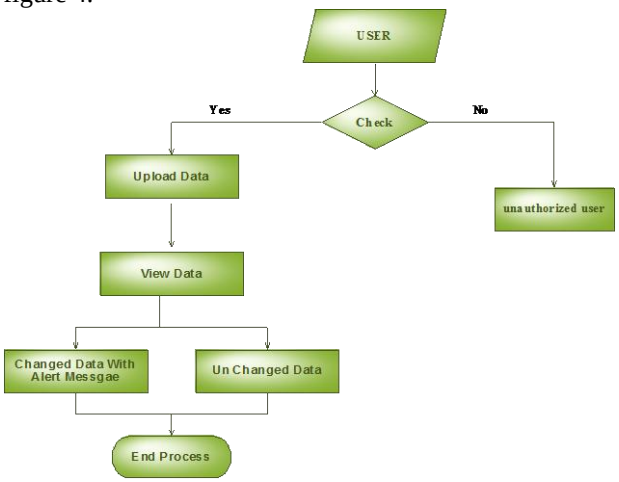

Fig. 4 – Activities of user

As seen be seen in figure 4, it is evident that the users can perform usual operations like sending and receiving data securely. They can view inconsistencies of the data that arise due to many reasons. The DPaaA service takes care of protection.

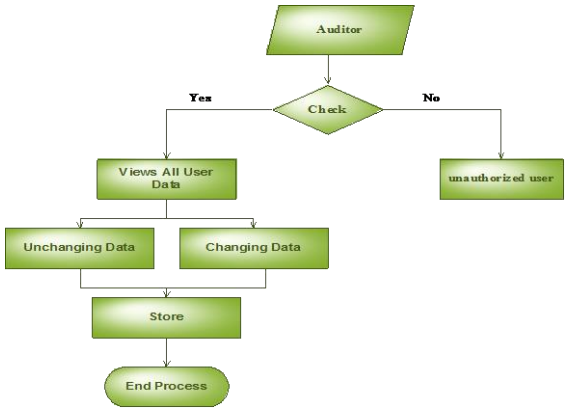

Fig. 5 - Activities of auditor

As seen be seen in figure 4, it is evident that the auditor can perform usual operations like auditing the data. This user can find the application to see whether it is functioning according to the expectations. The auditor is able to login and perform operations like checking authenticity of data and view data discrepancies if any.

V. EXPERIMENTAL RESULTS

We made experimental in terms of checking the attributes of data protection as a service which is one of the service models of cloud computing according to this paper. The security mechanisms are applied to all cloud users alike. The service model implemented in this paper is not user specific. Instead it treats every user alike and provides security to data automatically as a service. The results are presented here.

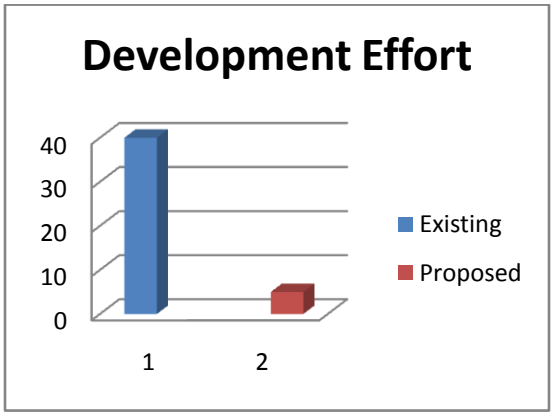

Fig 6. Development effort

As shown in the above figure represents the development effort.

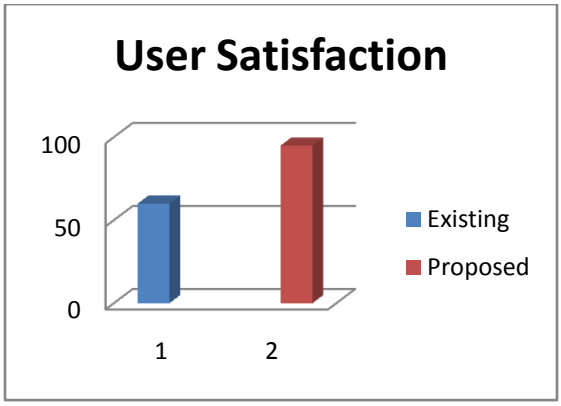

Fig 6. User Satisfaction

As shown in the above figure represents the user satisfaction.

VI. CONCLUSION

In this paper we attempt to realize a cloud service model known as “data protection as a service”. This is the service which can protect the data of cloud users and is part of cloud computing. This will help all cloud service providers to support the cloud data protection for masses. The

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

architecture was initially conceived by Song et al. [19]. In this paper we implement that architecture in order to make the said service a reality. The architecture provides complete security with the help of access control, logging, and key management mechanisms proposed in this paper. We also built a prototype application that demonstrates the proof of concept. The empirical results are encouraging and the service can be used in the real world cloud servers.

REFERENCES

[1] S. Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud," Proc. First Int'l Conf. Cloud Computing, 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] 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.
[4] R. Kailar, "Accountability in Electronic Commerce Protocols," IEEE Trans. Software Eng., vol. 22, no. 5, pp. 313-328, May 1996.
[5] R. Corin, S. Etalle, J.I. den Hartog, G. Lenzini, and I. Staicu, "A Logic for Auditing Accountability in Decentralized Systems," Proc. IFIP TC1 WG1.7 Workshop Formal Aspects in Security and Trust, pp. 187-201, 2005.
[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] J.W. Holford, W.J. Caelli, and A.W. Rhodes, "Using Self- Defending Objects to Develop Security Aware Applications in Java," Proc. 27th Australasian Conf. Computer Science, vol. 26,
pp. 341-349, 2004.
[9] A. Squicciarini, S. Sundareswaran, and D. Lin, "Preventing Information Leakage from Indexing in the Cloud," Proc. IEEE Int'l Conf. Cloud Computing, 2010.
[10] X. Feng, Z. Ni, Z. Shao, and Y. Guo, "An Open Framework for Foundational Proof-Carrying Code," Proc. ACM SIGPLAN Int'l Workshop Types in Languages Design and Implementation, pp. 67-78, 2007.
[11] M.C. Mont, S. Pearson, and P. Bramhall, "Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services," Proc. Int'l Workshop Database and Expert Systems Applications (DEXA), pp. 377-382, 2003.
[12] R. Bose and J. Frew, "Lineage Retrieval for Scientific Data Processing: A Survey," ACM Computing Surveys, vol. 37, pp. 1-28, Mar. 2005.
[13] R. Hasan, R. Sion, and M. Winslett, "The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance," Proc. Seventh Conf. File and Storage Technologies, pp. 1-14, 2009.
[14] P. Buneman, A. Chapman, and J. Cheney, "Provenance Management in Curated Databases," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD '06), pp. 539-550, 2006.
[15] A. Pretschner, M. Hilty, and D. Basin, "Distributed Usage Control," Comm. ACM, vol. 49, no. 9, pp. 39-44, Sept. 2006.
[16] A. Pretschner, F. Schuo¨ tz, C. Schaefer, and T. Walter, "Policy Evolution in Distributed Usage Control," Electronic Notes Theoretical Computer Science, vol. 244, pp. 109-123, 2009.
[17] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.
[18] T.J.E. Schwarz and E.L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc. IEEE Int'l Conf. Distributed Systems, p. 12, 2006.
[19] Dawn Song, Elaine Shi, and Ian Fischer, "Cloud Data Protection for the Masses". JANUARY 2012.