Formulating a Security Layer of Cloud Data Storage Framework Based on Multi Agent System Architecture

Amir Mohamed Talib[#1], Rodziah Atan[#2], Rusli Abdullah[#3] and Masrah Azrifah Azmi Murad[#4]

Faculty of Computer Science & IT, Information System Department,
University Putra Malaysia
43400 UPM, Serdang, Selangor, Malaysia
Email: ganawa53@yahoo.com & (rodziah, rusli & masrah)@fsktm.upm.edu.my

***Abstract*—The tremendous growth of the cloud computing environments requires new architecture for security services. In addition, these computing environments are open, and users may be connected or disconnected at any time. Cloud Data Storage, like any other emerging technology, is experiencing growing pains. It is immature, it is fragmented and it lacks standardization. To verify the correctness, integrity, confidentially and availability of users' data in the cloud, we propose a security framework. This security framework consists of two main layers as agent layer and cloud data storage layer. The propose MAS architecture includes five types of agents: User Interface Agent (UIA), User Agent (UA), DER Agent (DERA), Data Retrieval Agent (DRA) and Data Distribution Preparation Agent (DDPA). The main goal of this paper is to formulate our secure framework and its architecture.**

***Keywords*—Cloud Computing, Multi-Agent System, Cloud Data Storage, Security Framework and Cloud Service Provider**

1. INTRODUCTION

Cloud storage is composed of thousands of storage devices clustered by network, distributed file systems and other storage middleware to provide cloud storage service for users. The typical structure of cloud storage includes storage resource pool, distributed file system, service level agreements (SLA), and service interfaces, etc. Globally, they can be divided by physical and logical functions, boundaries and relationships to provide more compatibilities and interactions. Cloud storage is tending to combine with cloud security, which will provide more robust security [1].

Storage security involves storage media physical security and data security. As general network storage, the security of cloud storage includes certification, authority, audit and encryption, etc. Through automatic redundant replications the data will be easy recovered once failover. The cloud storage security can also expand to the whole procedure of storage service, including hardware, software, data, information, network security and clients' privacy security, etc [1].

The study of MAS focuses on systems in which many intelligent agents interact with each other. The agents are considered to be autonomous entities, such as software programs or robots. Their interactions can be either cooperative or selfish. That is, the agents can share a common goal, or they can pursue their own interests. Security plays an important role in the development of MASs and is considered as one of the main issues to be dealt for agent technology to be widely used outside the research community [2].

Determining data security is harder today, so data security functions have become more critical than they have been in the past [3]. The problem of verifying correctness, confidentially, integrity and availability of cloud data storage becomes even more challenging [4]. Cloud computing inevitably poses new challenging security threats for a number of reasons:

- Firstly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users.
- Secondly, the deployment of Cloud Computing is powered by data centers running in a simultaneous, cooperated and distributed manner. Individual user's data is redundantly stored in multiple physical locations to further reduce the data integrity threats.

Our security framework has been built by using two layers: agent layer and cloud data storage layer. The MAS architecture has five agents UIA, UA, DERA, DRA and DDPA, more details in [5].

The main goals of this paper are to formulate our cloud data storage framework and its architecture to facilitate the security issues that are offered by MAS of cloud data storage. As well as described the way of how our MAS works simultaneously and highlighted the any of the security attribute offered by any agent separately and combines all those attributes by MAS to come out with the new MAS security issue to protect the cloud data storage.

The contributions of the paper are two-fold. First, this research shall contribute to the new proposed cloud data storage security framework and would be documented for future use in facilitating cloud data security. Second, formulate cloud data storage security framework and its architecture to

DOI: 10.5176_2010-2283_1.1.20

facilitate the security issues that are offered by MAS of cloud data storage.

The remainder of this paper is organized as follows. Section 2 presents an overview of related work. Section 3 describes the cloud data security issues and its attributes. The proposed security framework is discussed in Section 4, followed by our proposed secure MAS architecture in Section 5. Conclusion is discussed in Section 6.

2. RELATED WORK

Although many research papers have been published on related topics, security research for cloud computing is still in its early stage. Here, we will discuss the achievements of two research directions: secure statistic cloud data storage and secure dynamic cloud data storage, from which our proposed security framework benefits. In our work, we attempted to provide a complete security service solution to secure the cloud data storage. To achieve our goal, we proposed MAS architecture for a security service system that consists of five types of agents: User Interface Agent (UIA), User Agent (UA), DER Agent (DERA), Data Retrieval Agent (DRA) and Data Distribution Preparation Agent (DDPA). UIA acts as an effective bridge between the user and the rest of the agents. Such agents actively assist a user in operating an interactive interface, recording the messages and data shared among agents and also serves as a data access point for other agents, as well as users. DDPA is used to tolerate multiple failures in distributed storage systems. In cloud data storage, we rely on this agent to disperse the data file redundantly across a set of distributed servers. DRA is used to enable the user to reconstruct the original data by downloading the data vectors from the servers. UA acts as a customer gateway that makes features of MAS accessible to users. It includes responsibility of providing users with real-time information of entities residing in the MAS. UA also allows users to control the status of loads based on priority predefined by a user. DERA is responsible for storing associated DER information. DER information to be stored may include DER identification number, type, local fuel availability, cost function or price at which users agree to sell, as well as DER availability, more details in [5].

In data integrity work, [6] proposed to verify data integrity using RSA-based hash to demonstrate uncheatable data possession in peer-to-peer file sharing networks. However, their proposal requires exponentiation over the entire data file, which is clearly impractical for the server whenever the file is large. In the same work, [7] proposed to ensure file integrity across multiple distributed servers using erasure-coding and block-level file integrity checks. However, their scheme only considers static data files and does not explicitly studies the problem of data error localization.

In a distributed servers work, [8] built on this model and constructed a random linear function based homomorphic authenticator which enables unlimited number of queries and requires less communication overhead. [9] Proposed an improved framework for POR protocols that generalizes both [8, 9]. Our Data Distribution Preparation Agent will do the same job of [7, 8, 9].

In a data possession work, [10] defined the "provable data possession" (PDP) model for ensuring possession of file on untrusted storages. Their scheme utilized public key based homomorphic tags for auditing the data file, thus providing public verifiability. However, their scheme requires sufficient computation overhead that can be expensive for an entire file. In their subsequent work [11] described a PDP scheme that uses only symmetric key cryptography. This method has lower-overhead than their previous scheme and allows for block updates, deletions and appends to the stored file, which has also been supported in our work. However, their scheme focuses on single server scenario and does not address small data corruptions, leaving both the distributed scenario and data error recovery issue unexplored. Our User Agent will do the same job of [10, 11].

In another data possession work, [12] aimed to ensure data possession of multiple replicas across the distributed storage system. They extended the PDP scheme to cover multiple replicas without encoding each replica separately, providing guarantees that multiple copies of data are actually maintained. Our DER Agent will do the same job of [12].

3. CLOUD DATA SECURITY ISSUES AND ATTRIBUTES

The following section describes several specific security policies that fall under these four security goals in our MAS architecture.

3.1 **Cloud Data Correctness**: Ensuring that the cloud data is stored and secured properly. Cloud data correctness has many attributes offered by our MAS architecture such as: Num of correctness insurances (NoCIs), Num of cloud data error localization (NoCDEL), Num of cloud data blocks (NoCDBs) and Num of cloud data dynamic (NoCDD).

3.2 **Cloud Data Confidentially**: Ensuring that the cloud data is not disclosed to unauthorized persons. Cloud data confidentially has many attributes offered by our MAS architecture such as: Num of trusted non-repudiation mechanism (NoTNRM) and Num of access control lists (NoACLs) offered by MAS architecture.

3.3 **Cloud Data Integrity**: Ensuring that the cloud data held in a system is a prior representation of the cloud data and that it has not been modified by an unauthorized person. Cloud data integrity has many attributes offered by our MAS architecture such as: Num of an authorized change (NoAACh), Num of access cloud users (NoACU) and Num of cloud datacenter (NoCDc).

3.4 **Cloud Data Availability**: Ensuring that the cloud data processing resources are not made unavailable by malicious action. The availability of cloud storage includes persistent runtime and recovery. High availability is needed to ensure application QoS. Cloud data availability has

many attributes offered by our MAS architecture such as: Num of the cloud resources (NoCRs) and Num of cloud servers (NoCSs).

4. CLOUD DATA STORAGE SECURITY FRAMEWORK

This section describes the security framework to facilitate cloud data security upload by users in cloud computing and how we intend to apply it jointly with data sources. Fig 2 shows a schematic representation of security framework. The framework has been built by using two layers, more details in [5].

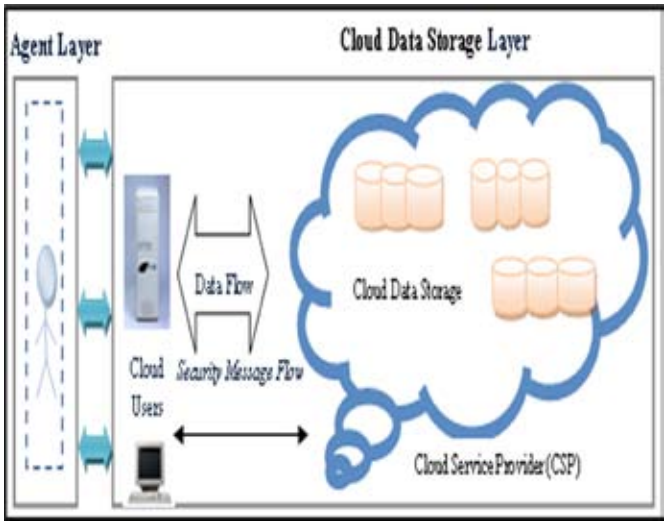

Fig. 2. Security Framework

The functionality of those layers can be summarized as follows [5]:

- Agent layer: This layer has one agent: the User Interface Agent. User Interface Agent acts as an effective bridge between the user and the rest of the agents.
- Cloud Data Storage layer: Cloud data storage has two different network entities and can be identified as::
  - Cloud User: Cloud users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.
  - Cloud Service Provider (CSP): a CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.

In cloud data storage layer, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, cooperated and distributed manner. Data redundancy can be employed with technique of erasure-correcting code to further tolerate faults or server crash as user's data grows in size and importance. Thereafter, for application purposes, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data. The most general forms of these operations we are considering are block update, delete, insert and append [5].

5. SECURE MAS ARCHITECTURE

In our MAS architecture, we proposed five types of agents: User Interface Agent (UIA), User Agent (UA), DER Agent (DERA), Data Retrieval Agent (DRA) and Data Distribution Preparation Agent (DDPA). The architecture of MAS presented in Fig 3, more details in [5].

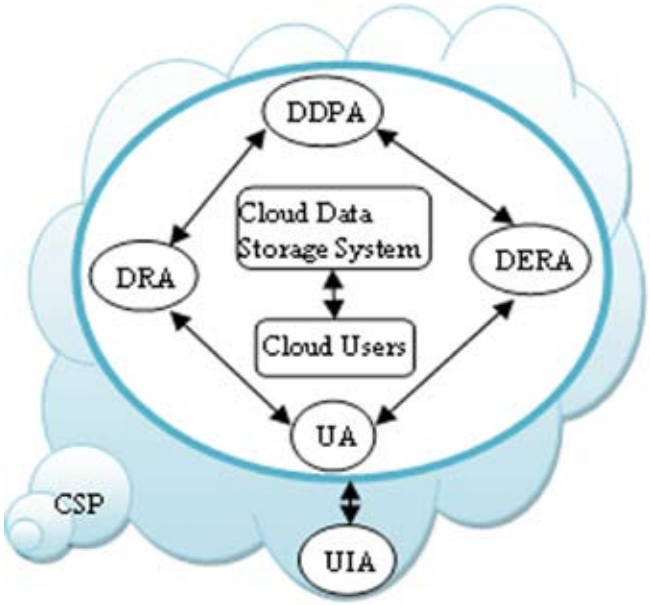

Fig. 3. Secure MAS Architecture

The rest of architecture of our secure MAS is described as follows [5]:

5.1 **UIA Architecture**: is considered as the main and leader agent, this agent acts as an effective bridge between the user and the rest of the agents. Such agents actively assist a user in operating an interactive interface, recording the messages and data shared among agents and also serves as a data access point for other agents, as well as users. The architecture of UIA is shown in Fig. 4.

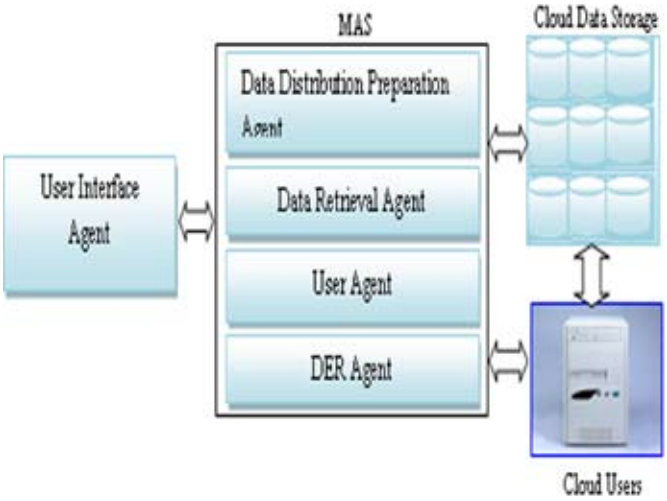

Fig. 4. UIA Architecture

5.2 **DDPA Architecture**: is used to tolerate multiple failures in distributed storage systems. In cloud data storage, we rely on this agent to disperse the data file redundantly across a set of distributed servers. The main goal of this agent is to generate a correctness security policy to protect the cloud data storage security. The correctness security policy has four attributes as shown in Fig 5.

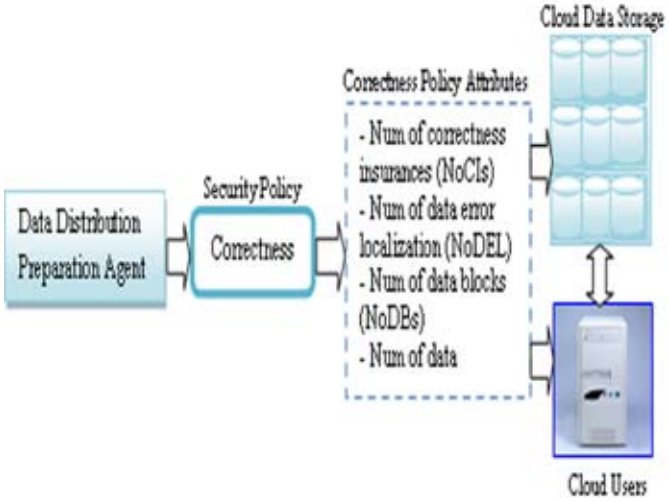

Fig. 5. DDPA Architecture

5.3 **DRA Architecture**: is used to enable the user to reconstruct the original data by downloading the data vectors from the servers. The main goal of this agent is to generate integrity security policy to protect the cloud data storage security. The integrity security policy has three attributes as shown in Fig 6.

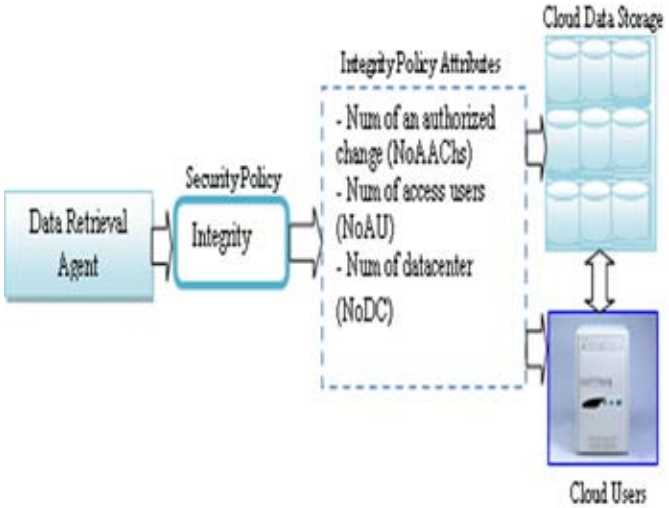

Fig. 6. DRA Architecture

5.4 **UA Architecture**: acts as a customer gateway that makes features of MAS accessible to users. It includes responsibility of providing users with real-time information of entities residing in the MAS system. A user agent also allows users to control the status of loads based on priority predefined by a user. The main goal of this agent is to generate both confidentially and integrity security policy to protect the cloud data storage security. The confidentially security policy has two attributes and integrity security policy has three attributes as shown in Fig 7.

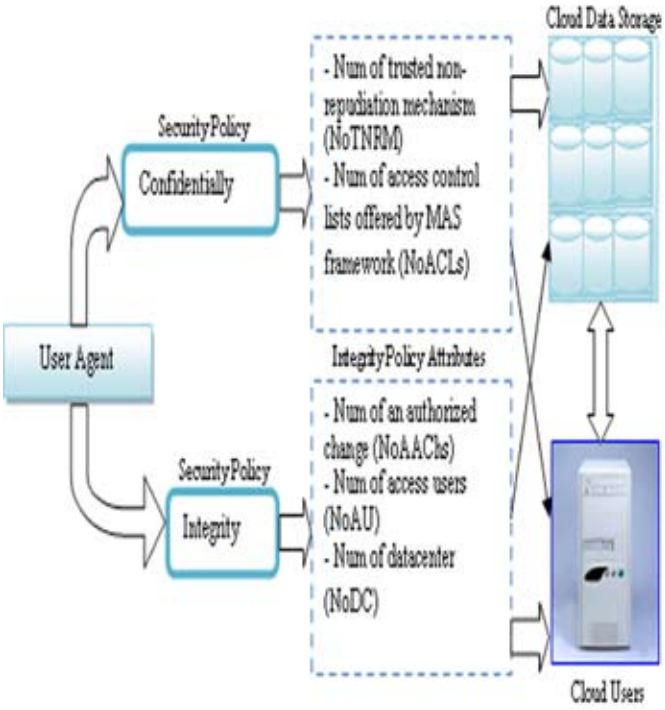

Fig. 7. UA Architecture

5.5 **DERA Architecture**: is responsible for storing associated DER information, DER information stored may include DER identification number, type, local fuel availability, cost function or price at which users agree to sell, as well as DER availability. The main goal of this agent is to generate availability security policy to protect the cloud data storage security. The availability security policy has two attributes as shown in Fig 8.

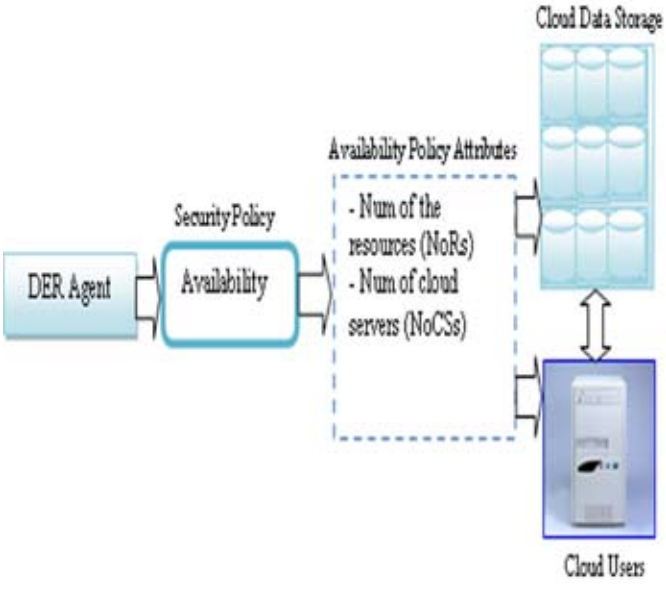

Fig. 8. DERA Architecture

6. CONCLUSION

In this paper, we investigated the problem of data security in cloud data storage, to ensure the correctness of users' data in cloud data storage; we proposed a security framework and MAS architecture to facilitate security of cloud data storage. This security framework consists of two main layers as agent layer and cloud data storage layer. The propose MAS architecture includes five types of agents: UIA, UA, DERA, DRA and DDPA. In order to facilitate the huge amount of security, our MAS architecture offered eleven security attributes generated from four main security policies of correctness, integrity, confidentially and availability of users' data in the cloud.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable remarks and comments.

REFERENCES

[1] W. Zeng, Y. Zhao, K. Ou, and W. Song, "Research on cloud storage architecture and key technologies," ACM, 2009, pp. 1044-1048.

[2] H. Mouratidis, P. Giorgini, and G. Manson, "Modelling secure multiagent systems," ACM, 2003, pp. 866.

[3] J. Rittinghouse, Cloud Computing: Implementation, Management, and Security, CRC, 2009.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," 2009.

[5] A.M. Talib, R. Atan, R. Abdullah, and M.A.A. Murad, "A Framework of Multi-Agent System to Facilitate Security of Cloud Data Storage" Proc. Annual International Conference on Cloud Computing and Virtualization CCV, Global Science & Technology Forum GSTF, 2010, pp. 241.

[6] B. Dlg Filho, "PSLM: Demonstrating data possession and uncheatable data transfer," Book PSLM: Demonstrating data possession and uncheatable data transfer, Series PSLM: Demonstrating data possession and uncheatable data transfer, ed., Editor ed.^eds., Cryptology ePrint Archive, Report 2006/150, 2006, pp.

[7] T.S.J. Schwarz, and E.L. Miller, "Store, forget, and check: Using algebraic signatures to check remotely administered storage," 2006, pp. 12-12.

[8] H. Shacham, and B. Waters, "Compact proofs of retrievability," Advances in Cryptology-ASIACRYPT 20082010, pp. 90-107.

[9] K. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: Theory and implementation," Available from ePrint, report2008.

[10] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," ACM, 2007, pp. 609.

[11] G. Ateniese, R. Di Pietro, L.V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," ACM, 2008, pp. 9.

[12] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-replica provable data possession," 2008, pp. 411-420.

Rodziah Atan received her B.Sc. degree in Computer Science in 1996 from Agricultural University of Malaysia and M.Sc. in 1998 from University Putra Malaysia. She completed her Ph.D. from the same university in 2005. She has been supported by the government of Malaysia and the University's Young Lecturer Scheme (SLAB). Her field of interest is software process and business process modeling and pursuing for new knowledge in bioinformatics visualization tools.

Masrah Azrifah Azmi Murad is a Senior Lecturer at the Department of Information System, University Putra Malaysia. She received her Bachelor in Management Information System (1997) from Drexel University, Philadelphia, USA; Masters of Computer Science (1999) from University Kebangsaan Malaysia and her Ph.D. (2005) from University of Bristol, UK. She worked as a tutor in University Putra Malaysia from 2000 to 2005 and became a lecturer in 2005 until present. Her areas of specialization are text mining, information retrieval and artificial intelligence. She is a committee member of IADIS International E-Commerce Conference (2007), Second International Conference on Informatics (2007) and Malaysian Software Engineering Conference (2007).

Amir Mohamed Talib received his B.Sc. degree in Computer Engineering (Electrical & Electronics Engineering), from Technological & Science University, Sudan in 2006. He received his master degree from the Faculty of Computer Science & IT, University Putra Malaysia in 2009. He is currently pursuing his Ph.D. at the Faculty of Computer Science & IT, University Putra Malaysia. His areas of interest include software engineering and artificial intelligence.

Rusli Abdullah received his B.Sc. and M.Sc. degrees in Computer Science from University Putra Malaysia in 1988 and 1996 respectively, and Ph.D. in Software Engineering from Technological University of Malaysia in 2005. His research interests include information system, knowledge management and software engineering. He is now with the Faculty of Computer Science and Information Technology in University Putra Malaysia as a full-time lecturer.