

Multi Agent Based Cloud Security Model for Association Rule Mining

Imran Qureshi,

*Associate Professor, Department of Information Technology Guru Nanak Institute of Technology,
Ibrahimpattanam, Telangana, India,*

Shaik Mohammed Imran,

*Asst.Professor, M.E, Computer Science Engineering, Guru Nanak Institute of Technology,
Ibrahimpattanam, Telangana, India*

G.Rama Murthy,

*Professor, International Institute of Information Technology,
Hyderabad, Telangana, India,*

ABSTRACT

In the present day computer era cloud computing is emerging into a huge environment which requires security services incorporated into cloud servers or data centers or even in cloud data storages available in different locations equipped with a very high speed networks. Due to increase in number cloud users and more are showing interest to use the environment, providing security is becoming a major concern because unless the cloud environment is secure no user will show interest and will be keen to invest or migrate from distributed environment to cloud computing environment.

In this paper we designed a security framework which is based on Multi Agent Based System (MABS) architecture that tends to provide security at various levels and providing the authenticated and accurate information to the cloud data seeker, our architecture mainly focuses on dual aspects such as Agent Layer and the Cloud Data Storage Layer and we have implemented the proposed framework in WEKA tool and used JDK 1.5 and generated results pertaining all the agents identified in this paper.

1. INTRODUCTION

In the present day computer era where evolution is considered to be a major achievement in the cloud computing environment where most of the present day commercial and research oriented users are showing enormous interest where each cloud service provider is providing almost everything as a service at the lowest prices when compared with planting a server environment which consists of many disadvantages as per present day requirements of a user.

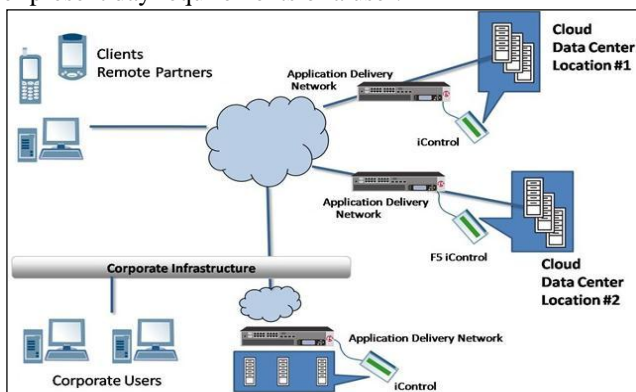


Fig.1. Cloud Computing Architecture

A cloud computing environment is capable of providing with a number of services for users who can connect to the cloud and attain these services as a cloud computing environment is always scalable and adding the concept of agents is an enormous advantage to the present architecture of the clouding computing environment as the agents can be created and destroyed at runtime based on the requirement of a user.

Some of the advantages of a cloud computing environment are:

- **Attaining economies of scale:** as the cloud computing data is increasing day by day in an enormous way the proposed productivity with fewer people can lead to a better utilization or available services in the cloud.
- **Reduce spending on technology infrastructure:** as the cost of maintenance of data is becoming enormous now a days as we need dedicated servers to be mounted and installed and backed up using some paid applications and so but the same can be attained in a cloud environment too.
- **Easy Maintenance:** generally a user will be paying for the maintenance of the application or data usage per annum or so where as in a cloud environment we can pay based on our requirement such as weekly or monthly or quarterly or annually or in any desired plan as per the requirement persists that is on demand.
- **Cheaper Globalization of workforce:** when the application or the desired data is hosted or mounted on the cloud environment using internet, the cost incurred to do it is very cheap comparatively to deploy the same in the distributed or the standalone system as the cloud service providers will provide the same services for multiple users the cost incurred for them intern is also very less or cheap. People worldwide can access the cloud, provided they have an Internet connection.
- **Process Streamlining:** Due to the existence of huge support and availability of many tools and techniques most of the work can be done very easily at very less time as the maintenance and development costs are very less in the desired budget more process can be streamline in the same budget.

Some of the advantages of imposing security in cloud computing environment are:

- **Legal Compliance:** Registering every application or business with Cloud Access Control (CAC) is the first step for ensuring the data available or will be uploaded in the cloud is legally compliant with all the services available and on the same hand will avoid us with unnecessary fines and legal complications.
- **Implementation Fairness:** Cloud computing environment must impose fairness in the implementation of security and while adopting the measures in situations that cannot be handled or when a security breach is identified based on the recovery procedures that are specified to a user at the time of registering to the cloud itself.
- **Dynamic Business Management –** security leads to dynamic business management as the process and procedures will tend to change always for providing better security without overloading a user to perform actions while accessing the data and taking frequent backups as per the requirements placed on your business.
- **Cloud User Security:** when a cloud user gets registered with the CAC it means the cloud service provider has to provide security and all the registered service to the user where a user needs to have complete faith and reliability for uploading the private and confidential data on the cloud computing environment and can access it either directly or through the agents in the system.

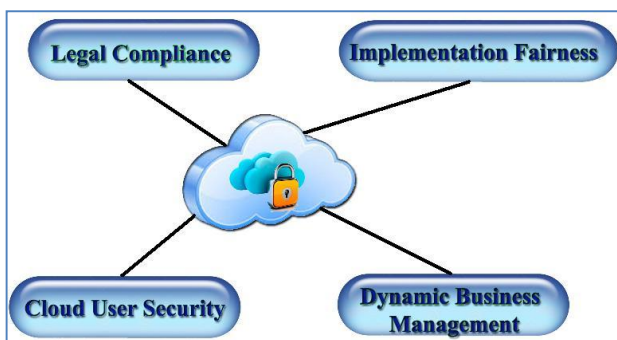


Fig.2. Cloud Security Model

2. RELATED WORK

Most of the researchers have specified that when data is managed internally there won't be any issues as the cloud data will be more secured as no external person is accessing the cloud data which may lead to theft or modification of data and trust can be maintained very easily. Even though the when we host data into a cloud the data will be replicated or distributed over many virtual servers provided by a cloud service provider even though your cloud data repository, most of the malicious code or hackers who tend to steal data can access any server virtually and another aspect is most of the surveys state that most of the data is attained from stolen data devices like smart phones, laptops, etc.,. And some of the researchers

have proposed their researches and some of them are listed below.

In the reference provide by Wang et al, provides a solution for the data security problem while performing the cloud data storage in a distributed storage system as the proposed scheme ensures the authentication and correctness of every data user in a cloud data storage environment that provides an effective and flexible distributed scheme that provides dynamic data support which includes various operations on data that also ensures correcting code for providing redundant file distribution for providing redundancy at imposing parity vectors that guarantee functional dependency while integrating the storage data for implementing the correctness while performing data error localization across the distributed servers implementing the analysis of detailed security and performance [3].

In the reference provide by Takabi et al, provides us with a comprehensive security framework in cloud computing environment while providing the security framework for handling various security challenges as the framework consists of different modules to handle where the main issue is related to key components of various computing environments such as integration of policies with multiple clouds, management of trust among various clouds, integration and implementation of various policies and identity management among distinct computing environments and cloud users for providing semantic heterogeneity among registered policies of distinct cloud users [4].

In the reference provide by Yu et al, provides us with an architecture that consists of two distinct spaces such as kernel space and user space where both of them will connect to network interface card that provides interaction at various levels in the cloud kernel space which is generally used for allocating the cloud user space that will provide processing ability either directly or indirectly [5].

In the reference provide by Du et al, provides the design and implementation of a new service by name RunTest which verifies the integrity of dataflow processing the integrity attestation for the system in a multitenant cloud infrastructures as the proposed system will implement application-level randomization of data attestation while pinpointing the malicious dataflow processing service at large-scale cloud infrastructure using the attestation of the intended graph model for capturing the aggregated data processing based on the attestation graph various results are generated at an extent [6].

In the reference provide by Venkatesan et al, provides us with an efficient multi-agent based static and dynamic data integrity protection model which by occasionally authenticates the hash value of every file that is stored in an enormous data storage by proposing the integrity based multi agent system (MAS) which embeds the agent system with MAS architecture consists of multiple agents for monitoring and maintaining the integrity of architecture [7].

In the reference provide by Taib et al, provides us a technological perspective that consists of MAS and security in CDS framework for facilitating the security of CDS by describing the security framework that formulates detailed security framework that show emphasis on latest technological perspectives [8].

3. METHODOLOGY

In the present computer era there is no specific formal security framework which can be considered to be a benchmark in Agent based Cloud Data Security model due to static and dynamic rules to formulate as a part of framework.

In this paper we try to investigate the problems that attain in the process of agents and then later analyze the formulation of the proposed framework by considering various problems that tend to identify based on the survey being conducted by us for ensuring that the proposed framework meets various objective that are intended and its limitations that can be provided with metrics.

The proposed system deals with conduction of various steps such as: first primarily we need to conduct various surveys by considering the methodology and then analyze it thoroughly, secondly we have to analyze the framework as a whole for attaining the security and finally we intend to represent a security framework which has the potential to uncover all types of errors or bugs.

We have conducted survey in our academic environment by considering various students of our college by forming 10 groups of students where 3 groups represented from information security department and 4 from computer science and engineering department and remaining from Information Technology department and 11 programmers and faculty from the above said three departments and using this set of people we started a pilot study.

We have designed a questioner consisting of 25 questions for gathering the opinion of above said teams and they have responded with the results and analyzed by us and the results are shown in results representing the security framework that is proposed in this paper for theoretical constructs in other technical fields data are still considered to be deficit and the competency evaluation on people or objects are still considered to be critical elements of our research as we tried maximum to keep it valid at a maximum extent.

Our proposed frame work beholds the structured cloud data in a dynamic form where the nature and the implementation will be in the form of electronic documents and it also consists of binary data in the form of cipher text as the text may include data related to multimedia files and other different types of files are also used in the system. In the proposed system both the cloud users and cloud service provider are considered to be main aspects since the cloud service provider will tend to facilitate various services that are registered by the cloud user. And all the participating agents will be responsible for providing the security policies as most of the communication process will be held between the cloud user and cloud service provider is through agents itself.

➤ **Cloud Data Validity Agent (CDVA)** will facilitate various security policies for assuring the validity of data that is uploaded by a cloud user through verification process at the cloud service provider. The main reliability of the agent lies in various block level operations that are performed to generate the correctness as the cloud user performs various modification operations and even informs to the cloud service provider upon failure of any technique

or service by sending a security notification or a specific security report of the exception cause.

➤ **Cloud Data Privacy Agent (CDPA)** facilitates the cloud user and the cloud service provider with the security policy of privacy where the responsibility lies with the agent is to provide novel access control policies rather than the conventional access control lists for providing authorization and authentication upon identification of each and every agent who tends to provide the privacy for enforcing the communicative and flexible access structure for each and every cloud user which is defined as a logical formula over various cloud data file properties and tends to represent any targeted cloud data documents and their policies.

➤ **Cloud Data Service Provider Agent (CDSPA)** is one of the most intelligent agents that consists of a interface for allowing the cloud users to register various services based on the policies that are abide by the cloud user. CDSPA provides a graphical interface where the user can request for services, register those services and can make user of those services either in a public cloud or in a private cloud and the CDSPA will be interfacing between Cloud and the Cloud Service Provider.

➤ **Cloud Data Accessibility Agent (CDAA)** is the agent that facilitates various security policies for accessing the cloud data only when it is available in the system where the main responsibility of this agent lies with the imposing of security measures at various levels and provides with notifications and reports to the cloud service provider and the registered or specified cloud user are to be informed upon violating of the security policies. CDAA is also responsible for the services in the cloud such as file distribution and its retrieval upon request by implementing its own data structures without allowing any malicious action by any cloud user or agent.

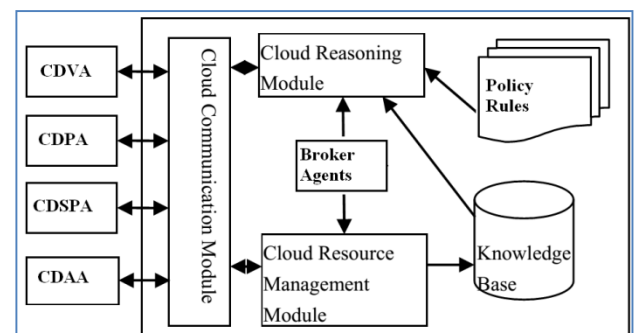


Fig.3. Proposed Framework Architecture

The above figure 3 represents the proposed system architecture and it comprises of various agents such as:

4. RESULTS

We have implemented our proposed system in java and executed in the academic environment by 15 students of M.Tech final year and some of the screens are:

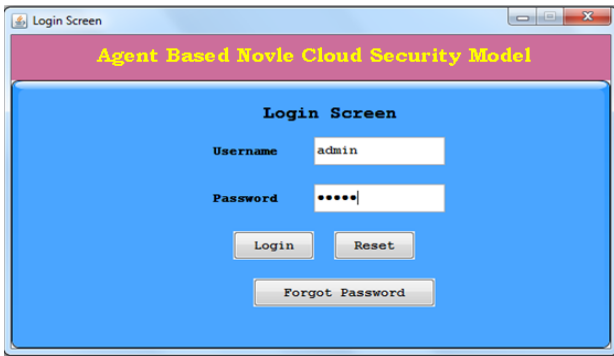


Fig.4. Login Screen of Implemented System

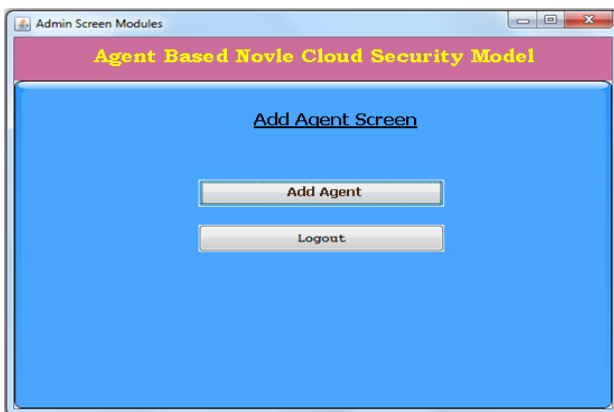


Fig.5. Add Agent Screen



Fig.6. User Screen

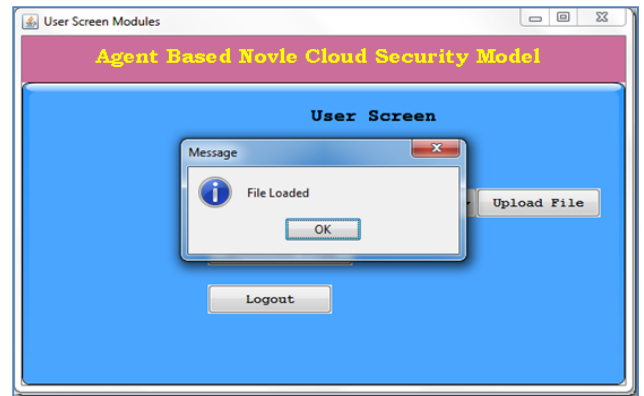


Fig.7. File Upload Screen

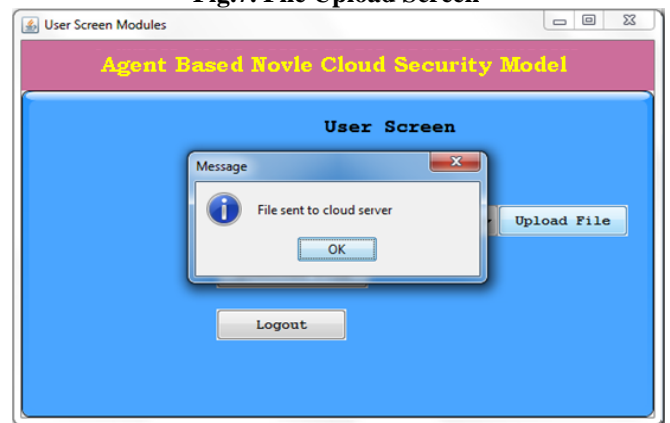


Fig.7. File Sent Information Screen

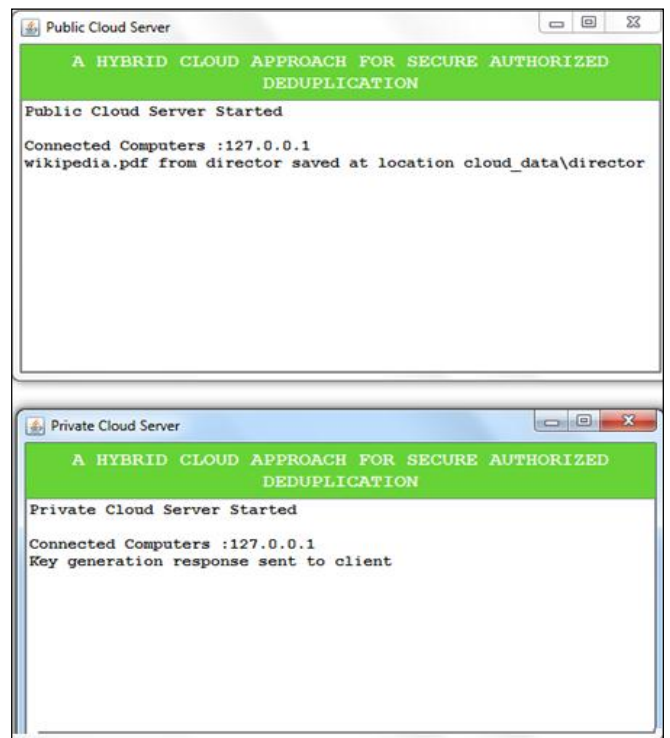


Fig.8. Public and Private Cloud Implementation Screen



Fig.9. Agents Creation Screen

5. CONCLUSION

In this paper we have proposed agent based novel cloud security model incorporated into cloud servers or data centers using very high speed networks for providing security by implementing a security framework which is based on Multi Agent Based System (MABS) architecture that tends to provide security at various levels and providing the authenticated and accurate information to the cloud data seeker, our architecture mainly focuses on dual aspects such as Agent Layer and the Cloud Data Storage Layer and we have implemented the proposed framework in WEKA tool and used JDK 1.5 and generated results pertaining all the agents identified in this paper.

REFERENCES

- [1] M. Zhou, R. Zhang, W. Xie, W. Qian and A. Zhou, "Security and Privacy in Cloud Computing: A Survey," Proceedings of the Sixth International Conference on Semantics Knowledge and Grid (SKG), Beijing, 2010, pp. 105-112.
- [2] A. M. Talib, R. Atan, R. Abdullah and M. A. A. Murad, "Formulating a Security Layer of Cloud Data Storage Framework Based on Multi-Agent System Architecture," TGSTF International Journal on Computing, Vol. 1, No. 1, 2010, pp. 120-124.
- [3] C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring Data Storage Security in Cloud Computing," IEEE, Vol. 186, No. 978, 2009, pp. 1-9.
- [4] A. M. Talib, R. Atan, R. Abdullah and M. A. A. Murad, "Towards New Access Data Control Technique Based on Multi Agent System Architecture for Cloud Computing in Software Engineering and Computer Systems Part II," In: V. Snasel, J. Platos and E. El-Qawasmeh, Eds., Springer Series: Communications in Computer and Information Science 189, Springer-Verlag, pp. 268-279.
- [5] H. Yu, N. Powell, D. Stembridge and X. Yuan. "Cloud Computing and Security Challenges," ACM, 2012, pp. 298-302.

- [6] J. Du, W. Wei, X. Gu and T. Yu, "RunTest: Assuring Integrity of Dataflow Processing in Cloud Computing Infrastructures," ASIACCS'10, Beijing, 13-16 April 2010, pp. 293-304.
- [7] S. Venkatesan and A. Vaish, "Multi-Agent Based Dynamic Data Integrity Protection in Cloud Computing," 2011, pp. 76-82.