Journal Homepage: -www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI:10.21474/IJAR01/8089
DOI URL: http://dx.doi.org/10.21474/IJAR01/8089

RESEARCH ARTICLE

CLOUD DATA STORAGE SECURITY STRUCTURE WITH MULTI AGENT SYSTEM ARCHITECTURE.

Geetha radhakrishnan[1] and Shunmuganthankl[2].

1. Research Scholar, Bharathiar University, Coimbatore.
2. Principal, Dhanalakshmi College of Engineering, Chennai.

Manuscript Info

Manuscript History
Received: 12 September 2018
Final Accepted: 14 October 2018
Published: November 2018

Keywords:-
Architecture; Cloud; Data Storage; Multi-Agent System.

Abstract

The purpose of this paper is to demonstrate the usage of Multi-Agent System techniques that can be used in Cloud platform for instilling security features in the same. Agents have proactive and reactive features which are beneficial for cloud data storage security. The architecture of the system is formed from a set of agent groups. This paper illustrates the usage of JADE collaborative environment. In order to vastly enhance security features, our architecture provides many security attributes originating from the essential security norms of precision, reliability, and accessibility of users' data in the cloud. This also describes the approach for designing a cloud security platform using Multi-Agent System architecture. The usage of dedicated self-directed agents for certain safety services permits agents to work together with Cloud Data Storage.

Introduction:-

Security is even now recognized as one of the most baffling issues. Many experiments have been conducted for this purpose by employing software agents. Verification and approval were considered as the most important criteria in this method.

Data storage systems need to adhere to stringent norms for monitoring and managing users' data but due to the contradictory features of these norms, a single system cannot manage this task. For example, availability, scalability and data consistency can be considered to be three contradictory tasks. The Multi-Agent System Architecture is initiated to manage the accuracy, confidentiality**,** and reliability of users' Cloud Data Storage.

Cloud computing has to meet the challenges posed by data-level security; sensitive data is the field of the enterprise, and not the CSP. Safety features have to shift towards the data level for the sake of protecting the enterprise wherever it may be. For instance, with data-level security, the enterprise can ascertain whether a particular set of data can be permitted to leave a particular cloud server. It can bring about encryption of specific data types, and allow only authorized users to gain entry to the data. CDSS is a difficult and contemporary issue for the local data centers because shifting of data to the cloud poses formidable security concerns. Many CSPs offer basic security for data but none have inbuilt authentication and encryption that can supply real CDSS.

Corresponding Author:-Geetha radhakrishnan.
Address:-Research Scholar, Bharathiar University, Coimbatore.

This security structure comprises two levels: agent level and cloud data storage level. The MAS architecture possesses five agents namely, User Interface Agent, User Agent, DER Agent, Data Retrieval Agent and Data Distribution Preparation Agent.

Information has been gleaned from a range of sources and is not confined to academic growth over the past few years. This paper presents an outline of the main features found in relevant literature.

CDS, CDSS and cloud implementation have been described and Cloud platforms devices have been differentiated. MAS and its various methods, along with the execution by Java Agent Development (JADE) are given here. CDS policies and its features in a cloud computing context are also highlighted. Global standards however have still not come into being for authenticating CDSS. It outlines the requirements of CDSS as necessitated by the structural design.

Cloud Computing

Cloud computing is both a platform as well as an application. A cloud computing platform provides, configures, servers when required. Cloud servers can be physical entities or virtual devices. Sophisticated cloud versions contain other computing resources like storage area networks (SANs), network equipment, firewall and other security devices. Cloud computing applications can also be accessed via the Internet. They use large data centers and strong servers that host Web applications and Web services. Internet users can easily access cloud applications.

Multi-Agent System

Multi-Agent systems are techniques in AI where numerous agents interact. MAS is a slackly joined system of problem-solving units that tries to find answers to complex problems that are impossible to solve on an independent basis.

Cloud Data Storage

CDS possesses thousands of cloud storage machines held together by networking, distributed filing and other storage middleware for providing cloud storage. The usual structure of CDS includes storage resource pool, distributed file system, service level agreements (SLAs), and service interfaces. On a global scale, they can be categorized by physical and logical functions and relationships to supply more compatibility. CDS tends to combine with CDSS, which will ensure enhanced security. CDS can offer cloud storage resources for all clients, and the fee can be decide on the basis of CDS capacity or CDS bandwidth from time to time. The data life cycle management in CDS depends upon on server configuration or on the contracts between servers and clients when CDS services commence. CDS can also enable new application types via SOA, Web services, APIs and unified service over a network at an affordable cost; it can be provided anytime and anywhere. CDSS can also be extended to the entire gamut of storage services, hardware, software, network security and customers' privacy.

Security Framework

This section describes the security framework to facilitate CDSS upload by users in cloud computing and how we intend to apply it jointly with data sources. The framework has been built by using two layers.

The functional features of those layers are as follows:

1. Agent layer: This layer has one agent: the User Interface Agent. User Interface Agent functions as an powerful link between the user and the other agents.
2. CDS layer: CDS has two varied system entities which are given below:
3. Cloud User: Cloud data users, who store data in the Cloud, comprise independent consumers and organizations.
4. CSP: a CSP, is an entity who possesses considerable resources and expertise in constructing and monitoring distributed CDS servers; the CSP also owns and operates live Cloud Computing networks.

Multi Agent System Architecture

In MAS architecture, five types of agents have been employed: User Interface Agent (UIA), User Agent (UA), DER Agent (DERA), Data Retrieval Agent (DRA) and Data Distribution Preparation Agent (DDPA).

The architecture of the MAS is described as follows:

1. UIA Architecture*:* As the leader agent, this acts as an effective link between the user and the rest of the agents. These agents help cloud users to operate an interactive border by recording the messages and data shared amongst agents and also acts as a data access node for other agents, which includes cloud users as well.
2. DDPA Architecture*:* In CDS, this agent disperses the data file across a set of distributed servers. The main task of this agent is to create an accurate security policy to protect the CDS.
3. DRA Architecture*:* This aids the cloud user for reconstructing the original data by downloading the data vectors from the servers. The chief task of this agent is to create robust security policies for securing the CDS.
4. UA Architecture: This functions as a client entry that makes MAS features available to cloud users. It includes the responsibility of providing cloud users with actual information of entities present in the MAS.
5. User Agent also permits cloud users to monitor the condition of loads on a priority basis that has already been defined by the cloud user. The main goal of this agent is to generate safe security policies for protecting the CDS.
6. DERA Architecture*:* This agent stores DER information. DER information can include identification number, type, local fuel access, selling price of cloud users and the DER availability. The main goal of this agent is to generate suitable security policies for securing the CDS.

Findings

In spite of work carried out on related topics, security research for CDS is still in its nascent stage. Two perspectives have been examined here: Secure Statistic CDS and Secure Dynamic CDS, on which the proposed security framework is built. We have attempted to deliver a comprehensive security service method to secure the CDS. To satisfy our goal, we projected MAS architecture as 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 a robust link between the cloud user and the rest of the agents. Such agents can greatly help a user in operating an interactive interface by recording the messages and data distributed among agents and also doubles as a data access point for other agents and cloud users.

DDPA is used for withstanding multiple failures in distributed storage networks. In CDS, we rely on this agent to diffuse the cloud data file redundantly across a set of distributed servers. DRA is employed to enable the cloud user for rebuilding the original data by downloading the cloud data vectors from the servers. UA acts as a client entry point that makes features of MAS available to cloud consumers. It includes the responsibility of providing cloud users with actual information of entities in the MAS. UA also permits cloud users to monitor and manage the load status based on the priority predefined by a cloud user. DERA stores the related DER information.

Cisco's Secure Cloud Data Center Framework shows the threat model of a cloud data nodal centre and the steps that that can be taken to lessen security concerns. In addition to this, the framework shows the controls, conformity, and SLA components. The most important aspect in cloud data centre security is that security has to be applied across all levels of architecture.

The challenge in cryptography is to apply cryptographic principles in a cloud computing ambience. Replication, which is the core of cloud computing, is mainly used for encryption and decryption keys.

MAS Design, Implementation and Simulation in CDSS

At present, MAS platforms and standards offer security components at a low level. Security related parameters can be fixed in an agent message cover, indicating its requirement for security service, according to the FIPA ACL message standards. The agent platform security manager and the agent management system can then be used in agent platforms to monitor and maintain security through public and private key verification or public key network. However, this makes available secure agent communication within the transportation level limited in scope.

Its use of policy files is intended only for general-purpose access control to local resources such as system files, network, and so on. Permissions are defined on the basis of system-oriented actions such as: passing messages, moving among containers, and creating/killing agents.

Therefore, the responsibility of enforcing security in MAS goes to the agent designers and developers who have to meet particular business-specific needs. Usually distributed over their runtime environment, agents behave and interact with each other dynamically, if not in a completely independent manner. Access control in such a highly dynamic environment is very difficult due to the large number of agent interactions, unforeseen agent behavior, and agent interaction process that could emerge at runtime. The agent research community and developers largely ignore the security issue in the context of the complexity of MAS-specific security implementation. Ignorance of security constraints will lead to unprecedented behaviour. By enforcing the right control upon agent behavior, can provide authorized system access. On the whole, the dynamic feature of agents is not always connected with a fixed set of data. This necessitates a radically new way of security modeling.

Security models such as the RBAC model are often concerned about permission control for human users. In MAS, some agents operate on behalf of users and others perform business functions as a result of system design. The concepts of agent rights and agent roles, resembling those of user rights and user roles are absent in the context of system resource access.

This imposes difficulty on general modeling of all access subjects when access control is concerned. Both human actors and system agents should be restricted in their behavior in MAS as a result of security needs.

Apart from the access subjects, the access objects need matching notions in the design of a unique MAS security model. The agent concept in the resource access pattern raises the level of abstraction of access subjects. The usual access objects of types of files, objects, and class methods in the OO paradigm, however, do not fit well in the pattern. We can consider agents as the agents of services through which they are accessed and utilized. But work in the area of secure service access management via agents is a rarity. Since simply borrowing OO security mechanisms is dysfunctional and negligible work has been done in security modeling of the MAS, there is a need to investigate the mainstream security access control models for finding a useful one and modify it as required to blend into the MAS context. The concept of creating a brand new security model in the MAS domain could pose obstacles to the existing security arrangements.

Even if the above-mentioned toolkits are apt for modeling and simulating the Grid application behaviors, none can support the infrastructure and application-level requirements in Cloud computing. Specifically, there is very little support in existing Grid simulation toolkits for modeling of on-demand virtualization enabled resource and application management. Furthermore, Clouds deliver services on subscription-basis in a moment-by-moment payment to Cloud customers. Hence, Cloud infrastructure modeling and simulation toolkits must provide support for economic entities such as Cloud brokers and Cloud exchange for enabling actual trading of services between clients and sellers. Among the available simulators discussed here, only GridSim is suitable for economic-driven resource management and application scheduling simulation.

Cloud developers are interested in economic strategies for the provision of virtualized resources to the incoming user's requests, scheduling of applications, resources discovery, inter-cloud negotiations, and federation of clouds. To augment and accelerate the Cloud computing research, applications and services, it is imperative that the requisite software instruments are designed and developed.

Due to the tightly-knit nature of HLA federations, the approaches to HLA security need to rely on the runtime network or secure gateways to put into practice access control and prevent counterfeit federates from obtaining information. The security concerns in ABELS are influenced by the fact that ABELS is a loosely-knit system in which most information swaps occur directly between individual GLAs instead of employing brokering systems. In ABELS, each GLA and its user entities are considered as being independent from the ABELS cloud, making it suitable to assign most of the responsibilities of entity security in the cloud to the concerned GLAs. This is the leading principle in the design of the ABELS security architecture.
Security characterization has omitted the quantitative part and dwelt mainly on the qualitative security of computing and information systems.

Conclusion:-

At the end of this review, we now believe that, the facilitation of CDS security on MAS architecture, is a very complicated phenomenon that occurs at multiple levels.

References:-

1. Cachin, C., Keider, I., Shraer, A. (2009). "Trusting the Cloud". IBM Research, Zurich Research laboratory.
2. Curtmola. R, Khan. O, Burns. R,&Ateniese. G. (2008). "MR-PDP: Multiple- Replica Provable Data Possession," Proc. of ICDCS '08, pp. 411–420.
3. Dahmann, J. S. Fujimoto, R. M and Weatherly. R. M. (1998). "The DoD High Level Architecture: An update". In Proceedingsofthe1998WinterSimulationConference,pp0.