Integrated Resource Management Platform for Collaborative Cloud Computing

Maniraj S.P. [1], Anshumaan Chandrakar [2], Abhishek Kumar [3], Rishabh Iyer [4], Shubham Jha [5]
[1] Assistant Professor, Dept of CSE, SRMIST, Ramapuram, Chennai, Tamil Nadu, India.
[2, 3, 4, 5] UG Scholar, CSE Department, SRMIST, Ramapuram, Chennai, Tamil Nadu, India.

Abstract – Collaborative cloud computing (CCC) is a system in which globally distributed cloud resources which belongs to different organizations or people is collectively used to give services. Attributable to the autonomous features of entities in CCC, the problem of resource management and reputation management ought to be collectively self-addressed so as to make sure the successful deployment of Collaborative cloud computing. However, these issues have typically been addressed separately in previous research efforts, and simply combining the two systems generates double overhead. Also, the previous resource and reputation management methods are not efficient or effective. By providing one name price to every node, the strategies cannot mirror the name of node in providing differing types of resources. By perpetually choosing the highest reputed node, the strategy fails to take advantage of node name in resource choice to totally and fairly utilize the resources in system and to fulfill users' various QoS demands. We propose a Collaborative cloud computing platform which combines resource and reputation management in an accord. This platform incorporates five key innovations: reputation control, integrated multifaceted resource, reputation management, multi-QoSoriented resource selection, and price-assisted resource,. The data collected from an online trading platform implies the importance of multi-faceted reputation and the drawbacks of highest-reputed node choice. Simulations and trace-driven experiments on the real-world Planet Research Lab bed show that this platform outperforms existing resource management and reputation management systems in terms of QoS, potency and effectiveness.

Index Terms – Cloud Computing; Security; Privacy; User Revocation; Encryption; Policy Management.

1. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort. Proponents claim that cloud computing allows companies to avoid upfront infrastructure costs, and focus on projects that differentiate their businesses instead of on infrastructure. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud providers typically use a "pay as you go" model. This can lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model. The present availability of high-capacity networks, low cost computers and storage devices as well as the widespread adoption of hardware virtualization, service oriented architecture, and autonomic and utility computing have led to a growth in cloud computing. Companies can scale up as computing needs increase and then scale down again as demands decrease.

Cloud computing has now become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability. Cloud vendors are experiencing growth rates of 50% per annum. But due to being in a stage of infancy, it still has some pitfalls which need to be given proper attention to make cloud computing services more reliable and user friendly.

Cloud computing is the result of the evolution and adoption of existing technologies and paradigms. The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs, and helps the users focus on their core business instead of being impeded by IT obstacles. The main enabling technology for cloud computing is virtualization. Virtualization software separates a physical computing device into one or more

"virtual" devices, each of which can be easily used and managed to perform computing tasks. With operating system–level virtualization essentially creating a scalable system of multiple independent computing devices, idle computing resources can be allocated and used more efficiently. Virtualization provides the agility required to speed up IT operations, and reduces cost by increasing infrastructure utilization. Autonomic computing automates the process through which the user can provision resources on-demand. By minimizing user involvement, automation speeds up the process, reduces labor costs and reduces the possibility of human errors. Users routinely face difficult business problems.

Cloud computing adopts concepts from Service-oriented Architecture (SOA) that can help the user break these problems into services that can be integrated to provide a solution. Cloud computing provides all of its resources as services, and makes use of the well-established standards and best practices gained in the domain of SOA to allow global and easy access to cloud services in a standardized way. Such metrics are at the core of the public cloud pay-per-use models. In addition, measured services are an essential part of the feedback loops in autonomic computing, allowing services to scale on demand and to perform automatic failure recovery. Cloud computing is a kind of grid computing; it has evolved by addressing the QoS (quality of service) and reliability problems. Cloud computing provides the tools and technologies to build data/compute intensive parallel applications with much more affordable prices compared to traditional parallel computing techniques.

2. RELATED WORK

Cloud resource orchestration (i.e., resource provision, configuration, utilization and decommission across a distributed set of physical resources in clouds) has been studied in recent years, these two issues have typically been addressed separately. Simply building and combining individual resMgt and repMgt systems in CCC will generate doubled, prohibitively high overhead. Moreover, most previous resMgt and repMgt approaches are not sufficiently efficient or effective in the large-scale and dynamic environment of CCC. Previous repMgt systems neglect resource heterogeneity by assigning each node one reputation value for providing all of its resources. In existing system claim that node reputation is multi-faceted and should be differentiated across multiple resources (e.g., CPU, bandwidth, and memory). For example, a person trusts a doctor for giving advice on medical issues but not on financial issues. Similarly, a node that performs well for computing services does not necessarily perform well for storage services. Thus, previous repMgt systems are not effective enough to provide correct guidance for trustworthy individual resource selection. However there are some limitations.

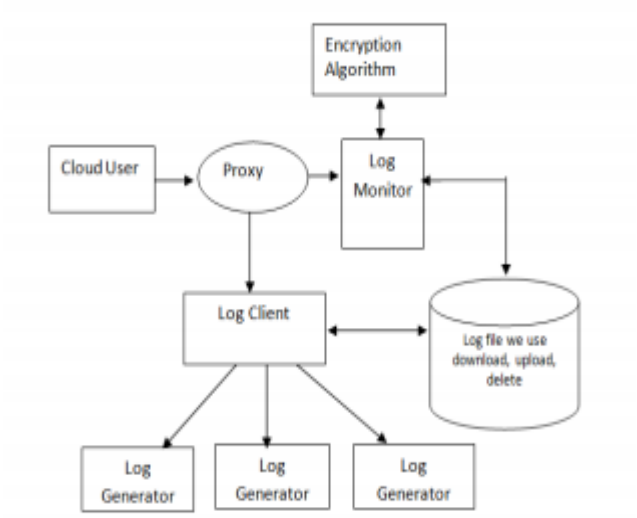
- Limitations

2.1. Limitations

- Due to the issues of resMgt and repMgt, this is not efficient and trustworthy.
- Single-QoS-demand assumption.

3. PORPOSED MODELLING

In this paper, we propose an integrated resource/reputation management platform, for collaborative cloud computing (CCC). We introduce a CCC platform with harmoniously integrated resource management and reputation management. It can achieve enhanced and joint management of resources and reputation across distributed resources in CCC. We propose a comprehensive solution for storing and maintaining log records in a server operating in a cloud based environment.



We address security and integrity issues not only just during the log generation phase, but also during other stages in the log management process, including log collection, transmission, storage, and retrieval. The major contributions of this paper are as follows. We propose architecture for the various components of the system and develop cryptographic protocols to address integrity and confidentiality issues with storing, maintaining, and querying log records at the honest but curious cloud provider and in transit.

4. RESULTS AND DISCUSSIONS

According to the importance of privacy in cloud-based environments and due to the lack of efficient user revocation process in clouds, a policy-based user revocation model was presented in this paper to ensure the security of associated cloud nodes after a user is revoked from a part of whole system. According four main components are defined to

define and manage security policies, to separate access and revocation management processes, and to apply encryption and reencryption policies after user revocation. This model was evaluated with performance, security and competitive analysis. According to the results, the reliability and efficiency of the suggested schema was assured for managing user revocation requests in cloud-based environments.

TABLE I. SECURITY ANALYSIS OF PROPOSED MODEL

Security Concern	Classification	Solution Method
Access Requests after Revocation	Access	Using **Temporary Suspension Flag** to transfer access requests of affected users from *Access Engine* to *Revocation Engine*.
Requests on the Run-Time	Access	Using **Time-Stamps** in both sides for checking the access requests.
Security of Time-Stamps	Access	Using **Hash-Function** in both Time Stamps.
Security of Associated Nodes	Policy	Calling **Policies** for each associated node of a user revocation request from *Policy Engine*.
Security and Reliability of Policies	Policy	**Classification of Policies** to three main parts based on Priority and Type by Revocation Engine.
Integrity of All Defined Policies	Application	Using **Revocation Flag** to check all policies are applied or not.
Encryption and Re-Encryption	Application	Using *Check Point* to schedule re-encryption methods based on defined policies and to check whether all encryption policies are applied or not.
Reliable Policy Update	Application	Checking *Policy Engine* **Database** to ensure are necessary policies are updated according to the user revocation request.
Security of Nodes	Application	Using **Revocation Flag** to check all policies are applied or not. Also, sending **Revocation Confirmation** Flag to associated cloud nodes after successful Policy Application.

TABLE II. COMPETITIVE ANALYSIS OF PROPOSED MODEL

Objectives	ABS	E-ABS	AGBS	Panda	Proposed Model
Policy-Based	No	No	No	No	Yes
Encryption & Re-Encryption	Yes	Yes	Yes	Yes	Yes
Separate Access Management	No	No	No	Yes	Yes
Group Access Management	No	No	Yes	No	Yes
Temporary Suspension	No	No	No	No	Yes
Revocation Flag	No	Yes	No	Yes	Yes
Policy Classification	No	No	No	No	Yes
3 Level Revocation	No	No	No	No	Yes
Cloud-Based	Yes	Yes	Yes	Yes	Yes

5. CONCLUSION

We proposed a complete system to securely outsource log records to a cloud provider. We reviewed existing solutions and identified problems in the current operating system based logging services such as syslog and practical difficulties in some of the existing secure logging techniques. . In this work, find out the challenges for a secure cloud based log management service. The attackers use below three steps to hack. First, the attacker can intercept any message sent over the Internet. Second, the attacker can synthesize, replicate, and replay messages in his possession. And Last The attacker can be a legitimate participant of the network or can try to impersonate legitimate hosts. We implement how to store secure log file in cloud and that file we can change read, write, delete, upload and download. We can implement AES algorithm that uses for log monitor and log generator. We then proposed a comprehensive scheme that addresses security and integrity issues not just during the log generation phase, but also during other stages in the log management process, including log collection, transmission, storage and retrieval. One of the unique challenges is the problem of log privacy that arises when we outsourced log management to the cloud. Log information in this case should not be casually linkable or traceable to their sources during storage, retrieval and deletion. We provided anonymous upload, retrieve and delete protocols on log records in the cloud using the Tor network. The protocols that we developed for this purpose have potential for usage in many different areas including anonymous publish-subscribe.

REFERENCES

[1] S.Azodolmolky, P. Wieder, and R.Yahyapour, "Cloud Computing Networking: Challenges and Opportunities for Innovations," IEEE Commun. Mag., vol. 51, no. 7, pp. 54– 62, 2013.

[2] F. Fatemi Moghaddam, M. Ahmadi, S. Sarvari, M. Eslami, and A. Golkar, "Cloud Computing Challenges and Opportunities: A Survey," in 1st International Conference on Telematics and Future Generation Networks (TAFGEN), 2015, pp. 34–38.

[3] D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Futur. Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, 2012.

[4] D. S. Kasunde and A. A. Manjrekar, "Verification of MultiOwner Shared Data with Collusion Resistant User Revocation in Cloud," in 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 2016, pp. 182– 185.

[5] M. B. Chhetri, B. Q. Vo, and R. Kowalczyk, "Policy-Based Management of QoS in Service Aggregations," in 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing, 2010, pp. 593–595.

[6] G. Di Modica and O. Tomarchio, "Semantic Security Policy Matching in Service Oriented Architectures," in 2011 IEEE World Congress on Services, 2011, pp. 399–405.