International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 7, Issue 1 (September '2024)

AUDITING MISBEHAVING CLOUD USER DETECTION FOR NETWORKING SERVICES

Dr.K.Vimala,
Assistant Professor,
Department of Computer Science,
SRM Arts and Science College,
Kattankulathur,Tamilnadu,India.

Abstract: *The increasing fashionableness of Cloud computing as an attractive alternative to classic information processing systems has increased the importance of its correct and continuous operation even in the presence of faulty components. We introduce an innovative, system-level, modular perspective on creating and managing service provider in Clouds. We propose a comprehensive high-level approach to shading the implementation details of the fault tolerance service provider techniques to application developers and users by means of a dedicated service layer. In particular, the service layer allows the user to specify and apply the desired level of Service Provider, and does not require knowledge about the fault tolerance service provider techniques that are available in the envisioned Cloud and their implementations.*

Keywords: *Cloud Computing, Network Services, Infrastructure Providers, Fault tolerance service provider, Virtual Machine.*

1. INTRODUCTION

Cloud Computing enabled networking is leveraging cloud services to achieve IT efficiencies not possible with classic network service architectures. It enables enterprises to increase the capacity without having to make capital investments in additional servers, storage, Business goals and networking infrastructure. It provides flexibility and squama, helping enterprise IT boost the utility of their resources, increase their nimbleness to meet business needs, expand their reach, and reliably support users around the world [1].

Outsourcing storage into the cloud service is financially attractive for the cost and complexity of long-term large-scale data storage. At the same time, though, such a service is also eliminating Clients ultimate control over the fate of their data, which clients with high service-level requirements have traditionally anticipated [2] [3]. As clients(User or Owner) no longer physically possess their cloud data, previous cryptographic primitives for the purpose of storage correctness security cannot be adopted, due to their requirement of local data copy for the sincere verification. Besides, the large amount of cloud data and clients constrained computing capabilities further makes the task of data correctness auditing in a cloud environment expensive and even formidable for individual cloud Users. Therefore, enabling public audit ability for cloud storage is of critical importance so that clients(User or Owner) can resort to a specialized Service Provider to audit cloud storage services and maintain strong storage correctness guarantee, while saving their own precious computing resources[4].

In general, a Cloud computing infrastructure provider is built by interconnecting large-scale virtualized data centers, and computing resources are delivered to the user over the Internet in the form of an on-demand service by using Virtual (sincere) machines. While the benefits are innumerable, this computing paradigm has significantly changed the dimension of risks on Clients(user's) applications, specifically because the failures (e.g., server overload, network congestion, hardware faults, Packet Loss) that manifest in the data centers are outside the scope of the user's organization[5]. Nevertheless, these failures impose high recommendation on the applications deployed in virtual machines and, as a result, there is an increasing need to address client' reliability and availability concerns.

II. NETWORK AUDITING SERVICE

Network Auditing Service primarily provides insight into how effective network control and practices are, i.e. its compliance to internal and external network policies and regulations [6] [7]. Network auditing service works through a systematic process where a computer network is analyzed for:

- Security
- Implementation of control
- Availability
- Management
- Performance

The data is assembling, vulnerabilities and threats are identified, and a formal audit report is sent to network administrators. It is generally done by an information system auditor, network system analyst or auditor or any other individual with a network management and/or security background. It uses both manual and automatic techniques to gather data and review network posture. It reviews:

- Each node of an network
- Network control and security processes
- Network monitoring processes
- Other data

Although a network audit service may focus more on network control and security, it is also reviews processes and measures that ensure network availability, performance and quality of service. Activity policies that enable you to set custom alerts to be sent to service provider or actions to

be taken when user activity is detected. For example, if you want to know every time a user tries to log on and fails 100 times in one minute, or if a user downloads 1,000 files or is logged in from India, you can set user activity alerts to be sent to yourself or to the user when these events occur. You can even suspend the user until you have time to investigate what happened. Under Activity match parameters, select whether a policy violation will be triggered when a single activity matches the filters or if a violation is only detected when a user access can specified number of repeated activities are detected[8] [9]. If you choose repeated activity, you can set Group matched activities.

We observe that a Fault tolerance service provider must satisfy the following requirements to effectively realize its functionality and meet its business goals.

1) The service provider must always maintain a consistent view of the resources in the Cloud to efficiently deliver the fault tolerance service provider support to its clients. To this aim, we introduce a resource manager that is maintained by the service provider.
2) The service provider must develop an approach to realize standard fault tolerance algorithms that can extrinsically function on a client's application. A method for evaluating the fault tolerance service provider properties offered by a given mechanism and for matching it with client's requirements, and a delivery scheme that can transparently enforce the desired fault tolerance service provider properties on client applications.
3) The service provider must design a framework that can easily integrate with the existing Cloud infrastructure and meet service provider's goals.

This section provides reference details about Cloud user detection policies, providing explanations for each policy type and the fields that can be configured for each policy.

A User Data policy is an API-based policy that enables you to monitor your Users activities in the cloud, taking into account over 20 file metadata filters (including device type and location). Based on the User data access policy results, notifications can be generated and users can be suspended from the cloud app.
Each policy is composed of the following parts:

- Activity filters – Enable you to create very grainy conditions based on metadata.
- Activity match parameters – Enable you to set a threshold for the clients number of times an activity can repeats to be considered to match the policy.
- Actions – The policy provides a set of regime actions that can be automatically applied when violations are detected.

III. SYSTEM ARCHITECTURE

We introduce an innovative, system-level, modular perspective on creating and managing service provider in Clouds. We propose a comprehensive high-level approach to shading the implementation details of the service provider techniques to application developers and users by means of a dedicated service layer. In particular, the service layer allows the user to specify and apply the desired level of fault tolerance, and does not require knowledge about the service provider techniques that are available in the envisioned Cloud and their implementations

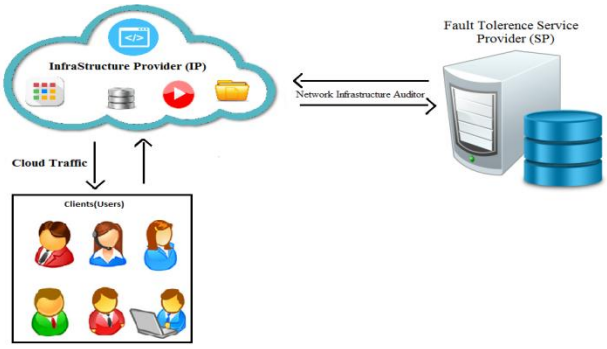

Figure 1: Cloud Network Auditor

We consider two scenarios about cloud service and parallel processing application in the Cloud Computing environment. A cloud service should be available at anytime and should provide the fastest response time regardless of the number of users served. Therefore, a service provider system should scale the service dynamically; extending and shrinking the number of web servers and cloud service components for large requirement and small requirement. Infrastructure provider also allows users to access supercomputer-level computing power by distributing tasks into large amount of cloud computing nodes (virtual machines). Users may not know the exact number of computing nodes should be utilized to efficiently perform their jobs. Thus, the under-provisioning and over-provisioning happen often. A Service provider system should scale the computing nodes according to the workload [10] [11].

The task of offering fault tolerance service provider as a service requires the service provider to realize generic fault tolerance mechanisms such that the client's applications deployed in virtual machine instances can transparently obtain fault tolerance service provider properties. To this aim, we define ft−unit as the fundamental module that applies a coherent fault tolerance mechanism to a recurrent system failure at the granularity of a VM instance. For example, considering plain Rivest, Shanar, and Adleman(RSA) encryption with a public key of plaintext multiplying with the input (plaintext) the one to be encrypted resulting equal to the exponential of the encrypt plaintext function to the power of multiplying with mode of integer number.

Algorithm: Shamir Secret Sharing Scheme

The (x, y)-Shamir Secret Sharing Scheme, where x=2 y−1, enables the division of a secret s into www shares such that the secret can be reconstructed from any subset of y shares, while the knowledge of any subset of y−1shares provides no information about the secret. The core principle of the scheme is that a polynomial of degree y−1 can be uniquely determined by y points.

To share a secret $s \in Z_p$ in , we define the polynomial:

$$f(p)=a_{y-1}p^{y-1}+a_{y-2}p^{y-2}+\cdots+a^1p+a^0$$

Here, $a^0=s$, and the coefficients $a^1,a^2,\ldots,a^{y-1}$ are chosen uniformly at random from Zp. Each share corresponds to a point on this polynomial, represented as $(p_i,f(p_i))$, where p_i is a unique value for each share. The secret s can be reconstructed using Lagrange interpolation with any y points from the polynomial. This scheme is widely used in cryptographic key management and secure multi-party computation due to its ability to ensure both secrecy and recoverability of the shared information.

The Clients(Users) implements the banking service as a multitier application where:

- The data tier uses the storage service offered by the IP to store and retrieve its users data, and
- The Service provider tier uses the IP's compute service to process its operations and respond to client queries. This system architecture allows the banking service to meet its varying business demands with respect to scalability and elasticity of cloud computing resources.

However, a failure in the IP's system can have high implications on the reliability and availability of the banking service. Furthermore, a failure in the storage server may have a remarkably higher impact than a failure in one amongst several compute nodes. This implies that each tier of the banking application requires different fault tolerance service provider properties, and the requirements may change over time based on the business demands. However, using traditional methods, fault tolerance service provider properties of the banking service remain constant throughout its life cycle. Therefore, in the client's perspective, it is easier to engage with the SP, specify its trustworthy and obtainable requirements based on business needs, and apparently obtain desired fault tolerance service provider properties for its applications.

- ***Infrastructure provider (IP):*** the entity that builds a Cloud computing infrastructure and realizes a service oriented computing resources delivery scheme.
- **Client (C):** the entity that uses the infrastructure provider's service to deploy its applications. A client meets its trustworthy and obtainable goals by making use of the service offered by the fault tolerance service provider.
- ***Fault tolerance service provider (SP):*** the entity that provides fault tolerance support to applications based on the client's requirements. We assume that the service provider is trusted by both the infrastructure provider and the client.

III. CONCLUSION

In this paper, we have presented after your Data is protected by Cloud Server Security, all cloud activity is scored according to various pre-defined risk factors. Service provider looks at every user session on your cloud and then takes into consider the risk factors you set here to alert you when something happens that is different from either the baseline of your Data or from the user's regular activity. The anomaly detection policy page allows you to configure and customized which risk factor families will be considered in the risk scoring process. The policies can be enforced by differently for different users, locations, and data sectors. For example, you can create a policy that alerts you when members of your IT team are active from outside your offices.

IV.REFERENCES

[1]. Chandola V., Banerjee A. , Kumar V., Anomaly detection: A survey, ACM Computing Surveys (CSUR); 41(3); 2009;p. 15 .
[2]. Agarwal B., Mittal N., Hybrid Approach for Detection of Anomaly Network Traffic using Data Mining Techniques, Procedia Technology; 6; 2012; p. 996-1003.
[3]. Padhy N., Mishra P. , Panigrahi R., The Survey of Data Mining Applications and Feature Scope; International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), 2(3) ;2012; p. 43-58.
[4]. E. Knorr and G. Gruman, InfoWorld, (2010).
[5]. R. Buyya, Y. S. Chee and V. Srikumar, Dept. Computer Science and Software Engineering, University of Melbourne, Australia, (2008).
[6]. Prodan and S. Ostermann, Proceedings of the 10th IEEE/ACM international conference on Grid Computing, (2009) October 13-15; Banff, Canada.
[7]. Mware Inc., http://www.vmware.com/products/vi/esx/.
[8]. Zen, http//www.xen.org.
[9]. Kernel-based Virtual Machine (KVM), http://www.linux-kvm.org.
[10]. Amazon EC2, http://aws.amazon.com/ec2/.
[11]. T. C. Chieu, A. Mohindra, A. A. Karve and A. Segal, Proceedings of the IEEE international Conference on e-Business Engineering, (2009) October 21-23; Macau, China.