An Efficient Framework for Secured Proxy-based Multi-cloud Computing Composition

Dr. Shanmugam Kannan[1], Goski Sathish[2]

[1]*Associate Professor,* [2]*Assistant Professor, Department of IT*
[1,2]*Malla Reddy Engineering College (A), Hyderabad, Telangana, India.*

Abstract

Today expanding cloud computing services take great opportunities for consumers to take better service and security conveniently new challenges to select the best service reporter out of the huge pool. In the proposed system the trust value is finding with the interaction between the users and the reporter. With the help of the ratings reporter to the cloud service providers by the users trust worthiness is estimated at different level, which is determined by the present interaction and the interaction. Oriented by requirement of trust management in number of cloud environment this paper presents T-broker a trust total service brokering method for efficient matching cloud services to satisfy different user requests. Trustworthiness is computed from personal work gained in direct interactions. Competence is assessed based on transparency in provider's SLA guarantees. We proposed secured proxy-based multi-cloud computing composition take dynamic, on the- fly collaborations and resource sharing many cloud-based services, addressing trust, policy, and security models. We integrate cloud with data confidentiality and the possibility of executing concurrent operations on encrypted data The prototype is implements the proposed cloud scheduler. The trusted Scheduler component it is important to analysis clouds is managed. The Scheduler trusted input trust status of the cloud infrastructure and provides cover new properties the foundation for planned future work. Cloud Trust Management, which provides the scheduler entry in the trust status of the cloud infrastructure

Index Terms*: Scheduling, Trust Management, Resource Allocation, Trusted Computing, - Cloud Computing, Cloud Service Provider (CSP), File Upload, File Download, service level agreement, control, Transparency.*

1. Introduction

Many of today's Information Technology (IT) applications rely on access to state-of-the-art computing facilities. In response to the resulting demand for flexible computing resources, cloud computing has taken the IT industry by storm over the past few years [2]. Cloud computing emerges as a paradigm to deliver on-demand service to customers, much akin to electricity or cable television [3], [4]. The paradigm shift from IT as a product to IT as a service and the accompanying flexibility proliferate the cloud applications [5], [6]. According to [7], [8], the public cloud services market is expected to expand from $109 billion in 2012 to $207 billion by 2016. The same physical resource among several tenants Customer does not have to manage and maintain servers, and in turn, uses the resources of cloud provider as services, and is charged according to pay-as-

you-use model. Similar to other on-line distributed systems, like e-commerce, p2p networks, product reviews, and discussion forums, a cloud provides its services over the Internet [1]. Cloud service provider provides [9] users the immediate access of a large range of resources. Cloud consumers have a wide range of choice of cloud service providers. Cloud Service Level Agreements (Cloud SLAs) are an important one for the relationship between a cloud service, customer and a cloud service provider [10] of a cloud service. The service provider must have the property like availability, response time and performance. The services and the storage space specified in the SLA are not satisfied and the trust and transparency are not maintained.

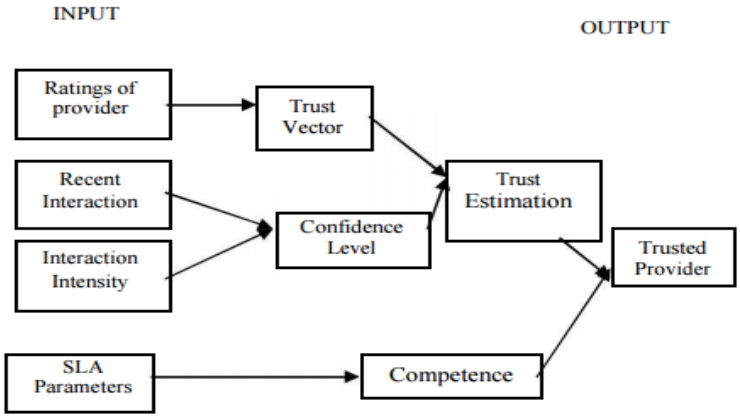

Figure 1. Trust Based System Architecture

Topical progressions in reckoning, storage service-oriented architecture, and network admission have simplified rapid growth in cloud marketplace. For any service a cloud customer may have many service providers to choose from. Major challenge lies in choosing an "ideal" service provider among them. By the term ideal, we suggest that a service provider is trustworthy as well as competent. Range of an ideal service provider is non-trivial because a customer practices third-party cloud services to serve its clients in cost-effective and efficient manner. In this situation from the cloud customer's perspective, persevering to a guaranteed level of service, as negotiated through starting service level agreement (SLA), is crucial Data loss owing to provider's incompetence or malicious intent can never be replaced by service credits.

- Support for customer-driven service management based on customer profiles and QoS requirements.
- Definition of computational risk management tactics to identify, assess and manage risks involved in the execution of applications with regards to service requirements and customer needs.
- Derivation of appropriate market-based resource management strategies that encompass both customer-driven service management and computational risk management to sustain SLA-oriented resource allocation;

2. Related Work

Decision trust is the extent to which one party is willing to depend on another even though negative consequences are possible. In cloud scenario, both notions are prevalent as customer depends on third-party provider, believing that it is reliable enough to

produce positive utility. Some works [11], [12] have proposed computation models for trust by incorporating the concept of risk. Like trust, reputation has also been studied extensively. From the perspective of social network researchers [13], reputation is perceived as an entity which is globally visible to all members of a social network community. Trust in cloud systems is often subjective and may be calculated using a centralized or distributed approach. When using a centralized approach, a single authority or trust broker collects all ratings from consumers, computes a reputation score for every participant, and makes all scores publicly available. When using a distributed approach, there can be distributed storages where ratings can be submitted, requiring interaction between storages to compute a single trust value for a given provider. A broker-based trust model was proposed in [1] based on SLA violation and user experience where the authors exploited SLA and cloud characteristic parameters such as CPU, number of virtual machines (VMs), and service down time, for evaluating the trustworthiness of providers. This approach is also robust against malicious group of entities performing reputation-based attacks. Recently, Ghosh [14] proposed SelCSP, a risk model which enables clients to select the most reliable CSP by using trustworthiness and competence of each CSP to estimate the provider reliability. SelCSP focuses on metrics such as number of CPUs and VMs, down time and interaction. This is a review paper based on the research work done by the researcher in the field of a new environment in cloud computing i.e. the collaboration of multi-cloud. This will give an overview of the techniques which will be helpful for shifting from the single cloud architecture to multi-cloud architecture, a security model and cost effectiveness of multi-cloud compared to a cloud. This section reviews literature that has been available on cloud computing security issues and other related topics. There were many researches that focused on cloud computing security issues. For instance, in [15] multi-shares were proposed that makes use of secret sharing algorithm Single cloud environment issued in [16] to solve service availability problem. The main issue in implementing multi-cloud is its working in a distributed environment as the services are to be collaborated with different cloud service providers to make it possible a framework is laid in the research work of “Collaboration Framework for Multi-cloud Systems” which specify the use of proxies at different level of collaboration. Trust plays an important role in all commercial grid and cloud environments. It is the estimation of competence of a resource provider in completing a task based on reliability, security, capability and availability in the context of distributed environment. It enables users to select the best resources in the heterogeneous grid and cloud infrastructure. This paper introduces. A novel trust model to evaluate the grid and cloud resources by means of resource broker. The resource broker chooses appropriate grid/cloud resource in heterogeneous environment based on the requirements of user. Our proposed trust management system is implemented with Kerberos authentication and PERMIS authorization to enhance the trust of the broker itself. The proposed trust enhanced resource broker evaluates the trust value of the resources based on the identity as well as behavioral trust. The proposed model considers metrics suitable for both grid and cloud resources. The results of the experiments show that the proposed model selects the dependable and reliable resources in grid and cloud environment.

3. System Design

User requirements are both hardware and software requirement. Infrastructure properties are availability, reliability, security, privacy concern. Users enter the cloud environment a chain of trust made consisting of username, password and provide some unique ID to enter the cloud. Scheduling perform as committing resource between possible task. Trust management implemented information security, in particular access control policies. Resource allocation are the virtual machine managed by the cloudlet length of resource management. This middleware uses a confidence conscious brokering architecture, in which the broker itself as the TTP acts for the trust management and resource planning. Cloud dispatchers do not consider the entire cloud infrastructure not look at them the entire user and infrastructure characteristics. Virtual resources are hosted using physical resources that meet their needs without getting users to understand the details of the cloud infrastructure involved. The prototype made available implements the proposed cloud scheduler. The trusted Scheduler component, it is important to understand how to have clouds, are managed. The Scheduler trusted input via the trust status of the cloud infrastructure and provides cover other properties the foundation for planned future work. Cloud Trust Management which provides the scheduler entry via the trust status of the cloud infrastructure

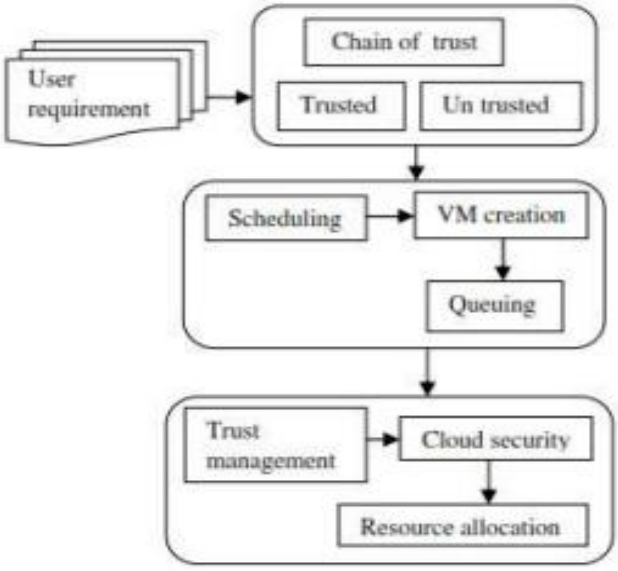

Figure 2.System Design

4. Proposed System

Independent systems dynamically come together to share information for a period of time. No global policy is maintained as interoperation requests are “on-demand” to facilitate dynamic data sharing. In a cloud environment, both tight and loose coupling may take place depending on the nature of collaboration. For example, if different departments of an organization collaborate using cloud services, it is an instance of tightly coupled collaboration. However, if autonomous domains mash-up “on demand” for a limited period of time, it is an example of loosely coupled collaboration. For both collaborations, if multiple collaboration requests are generated within the same period of time or particular session. propose a trust-aware framework to verify the security controls

considering consumers' requirements [15]. The authors model the security controls in the form of trust properties. Then, they introduce taxonomy of these properties based on their semantics and identify the authorities who can validate the properties. The taxonomy of these properties is the basis of trust formalization in their proposed framework. Furthermore, a decision model is proposed as an integral part of the framework in order to empower consumers to determine trustworthiness of cloud providers. A trust enhanced secure model for trusted computing platforms [11]. The authors argue that given the nature of both binary and property-based attestation mechanisms, an attestation requester cannot be absolutely certain if an attesting platform will behave as it is expected to behave.

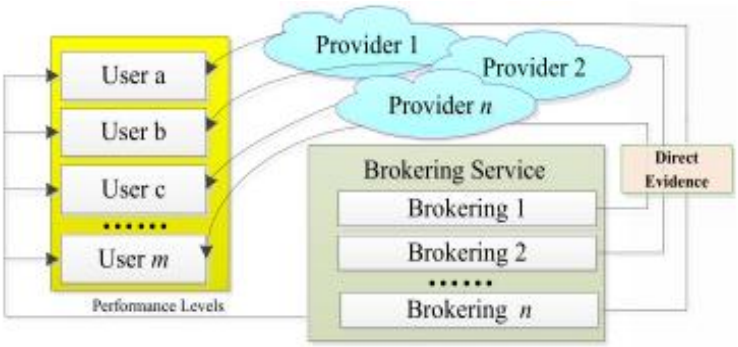

Figure 3. Scenario without user feedback

4.1. Sensor-Based Service Monitoring (SSM)

This module is used to monitor the real-time service data of allocated resources in order to guarantee the SLA (Service Level Agreement) with the users. In the interactive process, this module dynamically monitors the service parameters and is responsible for getting run-time service data. The monitored data is stored in the evidence base, which is maintained by the broker. To calculating QoS-based trustworthiness of a resource [7], [10], we mainly focus on five kinds of trusted attributes of cloud services, which consists of node spec profile, average resource usage information, average response time, average task success ratio, and the number of malicious access. The node spec profile includes four trusted evidences: CPU frequency, memory size, hard disk capacity and network bandwidth. The average resource usage information consists of the current CPU utilization rate, current memory utilization rate, current hard disk utilization rate and current bandwidth utilization rate. The number of malicious access includes the number of illegal connections and the times of scanning sensitive ports.

4.2. Virtual Infrastructure Manager (VIM)

Each cloud provider offers several VM configurations, often referred to as instance types. An instance type is defined in terms of hardware metrics such as CPU frequency, memory size, hard disk capacity, etc. In this work, the VIM component is based on the OpenNebula virtual infrastructure manager [12], [13], this module is used to collect and index all these resources information from multiple cloud providers.

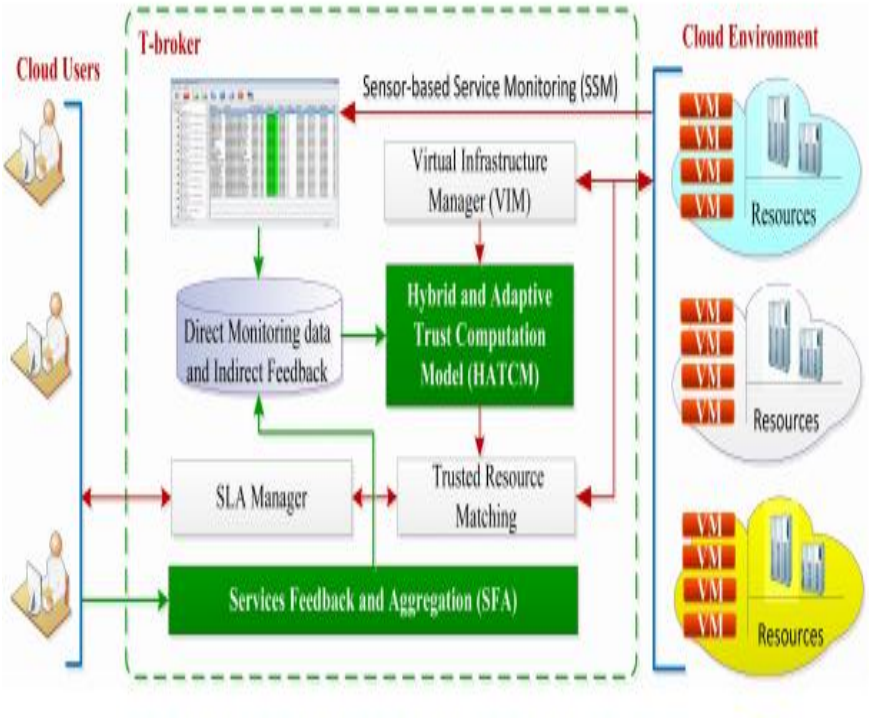

Figure 4. T-broker's Architecture and main function modules

It obtains the information from each cloud provider and acts as a resource management interface for monitoring system. Cloud providers register their resource information through the VIM module to be able to act as sellers in a multi-cloud marketplace. This component is also responsible for the deployment of each VM in the selected cloud as specified by the VM template, as well as for the management of the VM lifecycle. The VIM caters for user interaction with the virtual infrastructure by making the respective IP addresses of the infrastructure components available to the user once it has deployed all VMs.

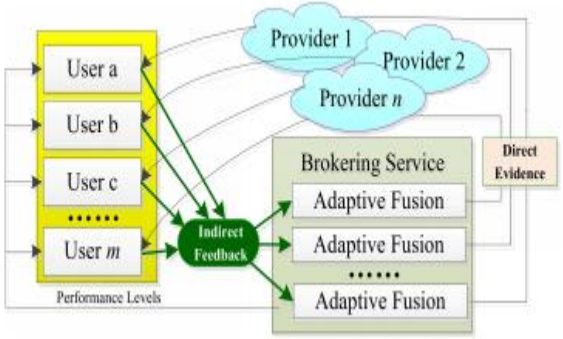

Figure 5. Scenario with adaptive fusion mechanism

4.3. Methods

1) Create Cloud Environment: We provide cloud users and cloud data centers and virtual machines as per our requirement. Job Manager, Cloud Controller also created. The Job Manager is replaced by the customer's orders, which is responsible for planning them responsible and coordinates their execution. It is capable of the cloud server provides the

interface communicates the instantiation of VMs to control. We call this interface, the Cloud Controller. Using the Cloud Controller Job Manager can configure or deallocate VMs after the current job execution phase.

2) Chain of Trust: A chain of trust is designed to allow multiple users and use the system to create software that would be more difficult if all the keys were stored directly in the hardware. The signing authority will sign only boot programs to enforce the security as they run only programs that are registered, or only allow signed code access to certain features of the machine to have. The final software can be trusted to have certain characteristics, because if it has been changed illegally his signature would be invalid and the previous software would not run it.

3) Scheduling: It is the process of deciding how to commit the resources between the varieties of possible tasks. Shared resources are available at certain times and events are planned at this time. The schedule keeps separation between the users of the resources. Scheduler, often as workload automation, usually offers a single point of control for the definition and monitoring. Scheduling is the method given by the threads, processes or data streams access to system resources. This is done to load normally, a system balance effectively or reach a target quality of service. The need for a scheduling algorithm results from the requirement for most modern systems multitasking and performs multiplexing. Job Scheduling is the most important task in cloud computing environment because the user used to pay for resources, based on time. Thus, an efficient use of resources must be important, and because of this scheduling plays an important role maximum advantage of the resource base.

4) Trust Management: The trust management is an abstract system that processes symbolic representations of social trust, usually automated decision-making support. The automated verification of measures against security policies In this concept, actions are allowed if they show sufficient credentials, regardless of their actual identity, to separate symbolic representation of the confidence of the actual person. Trust management can be used as an icon-based automation of social decisions be seen in connection with trust, where social actors instruct their technical presentations on how to act to make technical presentations while other agents. Further automation of this process can lead to automated trust negotiation in which technical devices negotiate confidence by selective disclosure Credential, defined according to the rules of social agents that represent them.

5) Resource Allocation: Resource allocation is used to allocate the available resources in an economical manner. Resource allocation is the planning of activities and the necessary resources from these activities, while taking into account both the availability of resources. could Resource access to a section of the store computer data in a device interface buffers, one or more files or the required amount of processing power. A single processor can perform only one process at a time, charged regardless of the number of programs by the user.

5. Experimental Results

The Trust Based Cloud Service Provider Selection involves the procedure of finding the cloud service provider for the effective use of their resources by the cloud consumers. The trustworthiness and the competence are said to be determined with the interaction of providers with consumers that are provided as in the form of ratings. The Extended

Opinion dataset is used in order to find the trust, it contains 5000 user feedbacks in it. The dataset file contains the item id, rating, user ID, date. Trust Based Cloud Service Provider helps to efficiently find the cloud service provider it uses trustworthiness and competence estimating technique in finding the effective cloud service provider. The trustworthiness and competence are said to be determined, calculating the evaluation of the ratings that are provided by the users to the cloud service providers by the interaction with the providers. The trust estimation is determined by calculating the various parameters. The competence is determined by the interaction with the providers and SLA parameters. By comparing the value of the trustworthiness, the trust estimation is said to be calculated. This experimental result shows efficient results by using this trustworthiness and competence estimation.

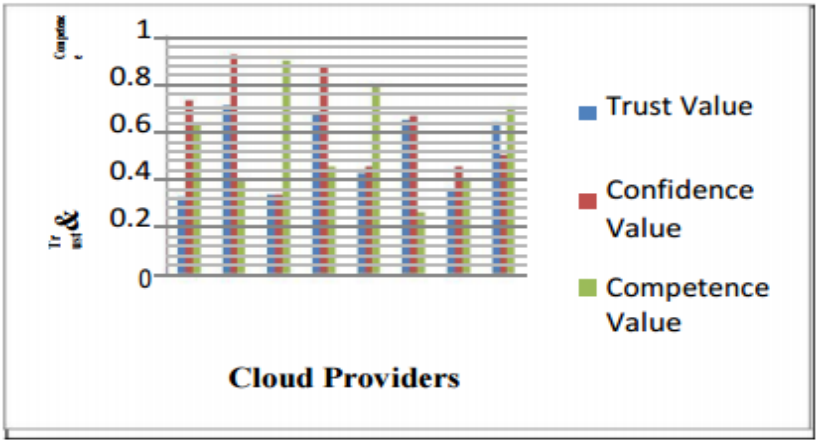

Figure 6. Comparison between Trust and Competence

6. Conclusion

We propose a risk model to characterize data breach for cloud service providers, enabling users to identify parameters of most concern to them and provide a weighting function to priorities them. Multi-attribute utility theory is used to aggregate risk probabilities across the measured parameter. The cloud service providers are determined based on the interaction of the providers and the users. It also considers various parameters like security and availability. The trustworthiness and competence are said to be estimated with the interactions with the users with the cloud service providers and the recent interaction of the providers. The confidence level is established by considering the recent interaction and interaction intensity of the providers with the users. Later the trust network has to be formed, that contains the indirect interaction can also be formed by the users and providers. Then the trust has to be estimated from the social network like Twitter, from that the direct communication and feedback of the users to the providers can be determined. The framework estimates trust worthiness in terms of context specific, dynamic trust and reputation feedbacks. It also computes competence of a service provider in terms of transparency of SLAs. Both these entities are combined to model interaction risk, which gives an estimate of risk level involved in an interaction we implemented a multi-cloud environment where users can store data in multiple clouds. The advantages of this kind of environment include high service availability, low security risks and the insider theft is eliminated to a greater extent.

In the future it is important for the adoption of public cloud systems, consumers and citizens are reassured that the privacy and security is not compromised. It will be necessary to address concerns expressed the problems of privacy and security in this chapter to provide trustworthy and innovative cloud computing services available and support that are useful for a number of different situations.

References

[1] Y. Chen, V. Paxson, and R. H. Katz, "What's new about cloud computing security," EECS Dept., Univ. California, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2010-5, Jan. 20, 2010

[2] R. Mahowald, C. Sullivan, and A. Konary, "Market analysis perspective: Worldwide saas and cloud services, 2012–new models for delivering software (2012)."

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.

[4] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of the-art and research challenges," Journal of internet services and applications, vol. 1, no. 1, pp. 7–18, 2010.

[5] Z. Chen, Y. Zhu, Y. Di, and S. Feng, "Optimized self-adaptive fault tolerance strategy in simulation system based on virtualization technology." IAENG International Journal of Computer Science, vol. 42, no. 4, pp. 305–312, 2015

[6] X. Zhong, G. Yang, L. Li, and L. Zhong, "Clustering and correlation based collaborative filtering algorithm for cloud platform." IAENG International Journal of Computer Science, vol. 43, no. 1, pp. 108– 114, 2016

[7] C. Pettey and B. Tudor, "Gartner says worldwide cloud services market to surpass $109 billion in 2012," Gartner Inc., Stamford, Press release, 2012.

[8] "The future of cloud adoption," See http://cloudtimes.org/2012/07/14/the-future-of-cloud-adoption, 2012

[9] Cloud based file transfer of We transfer has cloud computing storage .

[10] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "NIST cloud computing reference architecture," NIST Special Publication, vol. 500, p. 292, 2011.

[11] D. Manchala, "Trust metrics, models and protocols for electronic commerce transactions," in Proc. 18th Int. Conf. Distrib. Comput. Syst., 1998, pp. 312–321.

[12] A. Jøsang and S. L. Presti, "Analysing the relationship between risk IJSER International Journal Of Scientific & Engineering Research, Volume 7, Issue 7, July-2016 1301 ISSN 2229-5518 IJSER

[13] L. Freeman, "Centrality on social networks," Social Netw., vol. 1, pp. 215–239, 1979.

[14] N. Ghosh, S. K. Ghosh, S. K. Das. SelCSP: A Framework to Facilitate Selection of Cloud Service Providers, In IEEE Trans. Cloud Computing, vol. 3, no. 1, pp. 66–79, Jan.-March. 2015.

[15] M.A. AlZain and E. Pardede, "Using Multi Sharesfor Ensuring Privacy in Database-as-a-service", 44th Hawaii Intl. Conf. on System Sciences(HICSS), 2011, pp. 1-9.

[16] A.J. Feldman, W.P. Zeller, M.J. Freedman andE.W. Felten, "SPORC: Group collaboration using untrusted cloud resources", OSDI, October 2010, pp. 1-14.

