Conceptualizing Workflow in Dependable and Safe Cloud Computing

Dan Tang[1,2,a], Xiao-Hong Kuang[1,2,b] and Wang Chen[3,c]

[1]Hunan police academy, Changsha, China

[2] Key Laboratory of Network Crime Investigation ,Colleges of Hunan Province, Changsha, China

[3]The people's procuratorate of BeiLun district,Ningbo

[a] tacom@sohu.com [b] tacom@163.com [c] tt-aa@tom.com

Keywords—cloud computing; workflow; dependable cloud computing; safe cloud workflow

Abstract—adapting workflows to the cloud is a popular modern computing approach. The preference based on the cost benefits and ready availability of add-ons is however prone to security challenges. Considering that an increasing number of critical systems; for example, railway, airport and manufacturing workflows are adapting the model—there exists a need to examine whether cloud computing addresses dependability and security concerns. This research investigates the issues of redundancy, rapid isolation and removal of faults in cloud computing. Moreover, it proposes a generic framework that provides the necessary security checks capable of assuring a safe computing environment.

I. INTRODUCTION

Businesses choose cloud computing for their workflow needs because of the cost benefits on offer. [1] refers to the phenomenon as an offering of “everything as a service”. The cloud computing services (or also referred to as XaaS) commonly include aspects of:

- Software as a Service (SaaS);
- Platform as a Service (PaaS); and
- Infrastructure as a Service (IaaS).[1, 2]

The workflows adapted to cloud computing have to choose a trade-off between the costs associated with dependability and security and the overall costs of adopting the paradigm. In addressing dependability, cloud computing services provide for virtually unlimited processing networking and storage capabilities.[2] Hence, concerns of service availability, reliability and redundancy are incorporated in the paradigm’s setup. System designers and analysts get to choose which aspects of the workflow get transferred to cloud computing. However, such choices expose critical systems; for example—transport, security or manufacturing infrastructure; to cost-related considerations, which could impact the reliability of workflow segments which are erroneously assumed as non-critical; like, upload of documents.[3]

In addition to the nature of service an entity employs, there exist four major models for deployment. Caytiles and Lee [2] expose the (1) public; (2) private; (3) hybrid; and (4) community cloud computing deployment models. While public clouds offer services to undifferentiated customers, private clouds either serve one customer or are bespoke as pertains to one client’s demands. On the other hand, hybrid clouds are a combination of the features that public and private clouds offer. Community clouds, however, serve a differentiated industry, for example telecommunication firms. In terms of security concerns, private clouds offer a closely-monitored safety aspect that serves the unique demands of the client in question. The various trade-offs that the cloud computing services and deployment models propose are worthy of examination, which this research ultimately presents in a generic framework meant to address the core considerations of security and dependability.

II. Related Work

While examining the current trends and challenges in cloud computing, Bilal et al.[4] indicates that the reliance "on the Internet and cloud computing" has exposed the issues of dependability and safety associated with critical infrastructure and business workflows. Bilal et al. [4] terms the concerns as a measure of the quality of service (QoS) that clients of cloud computing services demand of their providers. On the other hand, service providers increasingly develop advanced scheduling and failsafe cloud computing platforms, which manage to host extensive and concurrent resource requests. However, Stein et al. [5] argues that the developments have not removed the concerns on whether cloud computing clients receive services whose QoS is comparable to the extent of damage risked by issues of dependability and security. Accordingly, this section will examine the works related to the issues of dependability and safety concerns of cloud computing systems.

A. *Dependability*

In the conventional model of achieving dependability, cloud computing providers use redundancy to achieve fault tolerance.[5] Although effective, the existing literature terms the approach "ad hoc in nature and requires a considerable investment on the part of the provider".[5] On the other hand, dependability is achieved through a model that relies on estimating the performance requirements of each client—then, in turn, allocating the necessary computing demands to manage in a 'resource pooling and scheduling' formula.[6]

Other studies contend that the largest dependability factor that cloud computing demand of their providers is uninterrupted uptimes.[4] Nevertheless, all the pertinent studies and reports argue that dependability is positively correlated to the competitiveness, or at least, the costs demands of the cloud computing clients.

TABLE I. SECURITY APPROACHES

Possible security mechanisms
Identifying and seeking out new threats
Enhancing the protection of virtual assets
Enhancing the protection of outsourced services
Enhancing the protection of user data—hence, enhancing confidentiality
Managing Big Data access

B. *Security*

Providers have established mechanisms of authenticating access requests from their clients. Moreover, the providers contend that "performing [regular] proofs and verification of the underlying systems"[4] enhances the security factor available to the clients. However, some security concerns also put precedence on confidentiality.[7] If, for example, a cloud computing client fulfills the verification requirements of the provider, but in the process leaves a trail of identifying data, which, when accessed by malicious code or devices; has the potential of endangering critical processes—then the security concern would still pose a significant basis for adapting workflow. As a means of improving the safety of the cloud computing model, existing studies have proposed adopting a policy of actively seeking out new threats, instead of relying on successful attacks to inform new security mechanisms [7]—see Table 1.

Although the existing works indicate the need to enhance dependability and security of cloud computing services, they report that providers have adopted technologies that have made these aims more feasible. Nonetheless, they also report that these concerns remain a priority for clients when deciding on the service provider, because current technologies do not provide for 100% failsafe services. The prevailing concerns, as a result, continue to form the basis of generic frameworks, which propose approaches that argue for cost tradeoffs in favor of dependability and security.[8]

III. Generic Framework

The cloud computing concerns of dependability and security are addressable at three major levels of the cloud framework. The workflow application (ε) manipulates the client's user data according to the user requirements. The workflow scheduler (ϕ) interfaces with the provider's cloud service to offer scheduled access to the storage, processing or networking capabilities offered by the cloud service (γ) (see Fig. 1). The client expects her data to access the scheduling service while taking into consideration the aspect of privacy and security [7]. As a result, the provider needs to provide a scheduling service that provides for verification, encryption, and ultimately, reliable uploads. Likewise, the provider's cloud architecture offers the advantages of distributed computing and networking. At this level, the cloud architecture is prone to resource contention challenges as pertains to how robust the system is capable of processing massive amounts of requests. Here, the provider should manage the clients' expectations of dependability by offering fault redundancy, removal and forecasting.

The proposed framework would therefore address the concerns of dependability and security in three major categories, (1) the workflow application; (2) scheduler/interface; and (3) cloud computing architecture.

- The workflow application: the client's user requirements and data inform the nature of workflow that this level will express. Since this level encapsulates the demands of users, for instance, a telecommunication company, a manufacturing firm or a power station; it is not possible to estimate the nature and frequency of data supplied to the cloud computing provider. However, at this level, the client should deploy a workflow model that mitigates security concerns, which are addressable through the organization's security policies. If, for example, the security policy demands that all users use passwords longer than a set number of characters, the provider would have difficulty managing the privacy of the data containing short passwords, which could be exposed by 'brute force' cracking.

- The scheduler/interface: at this level, the cloud computing service accepts the various requests from the clients. As a result, in includes a performance evaluator, which monitors the reliability indicators established through a performance benchmarking. When, for example, the task pool takes a longer time to respond to client requests for service access, the logging facilities could notify the provider, who in turn could increase the allocation of bandwidth or processing power assigned to the scheduler. Here, the client would notice instances of low dependability if the scheduler fails to attend to the requests severally. As a result, the service provider could address the concerns of dependability at this juncture by improving the performance metrics [8]. On the other hand, this level is also prone to security breaches if the lower level; that is, the workflow application; failed to observe the established security policies.

- The cloud computing architecture: this level contains the distributed services, which the client subscribes for. If improperly executed, the workflow application's request could suffer from low turnaround times and inefficient transfer to other remote services. The dependability concerns at this level could improve with more efficient hardware and advanced pooling and scheduling routines. Since this level also depends on a networked and virtualized model to realize distributed computing, the provider achieves dependability through redundancy. In terms of security, the provider enhances protection and privacy by authenticating all services which request access to any part of the processing activities. Moreover, data verification and validation procedures would provide for enhanced monitoring of the flow of data from a particular client to other related privileges.

Thus, service dependability and security starts from the manner the client exploits her workflow system. Poor observation of the organization's system-use policies would expose the cloud computing provider's interfacing application to vulnerable data, which is prone to attack before accessing the cloud architecture. It is difficult to isolate the stage at which an attack occurs in cases of data hijacking. The provider, therefore, has the responsibility to also install data validation and verification routines at the interface level to prevent access to the core cloud infrastructure by malicious agents. On the other hand, the provider's system implementation should include the

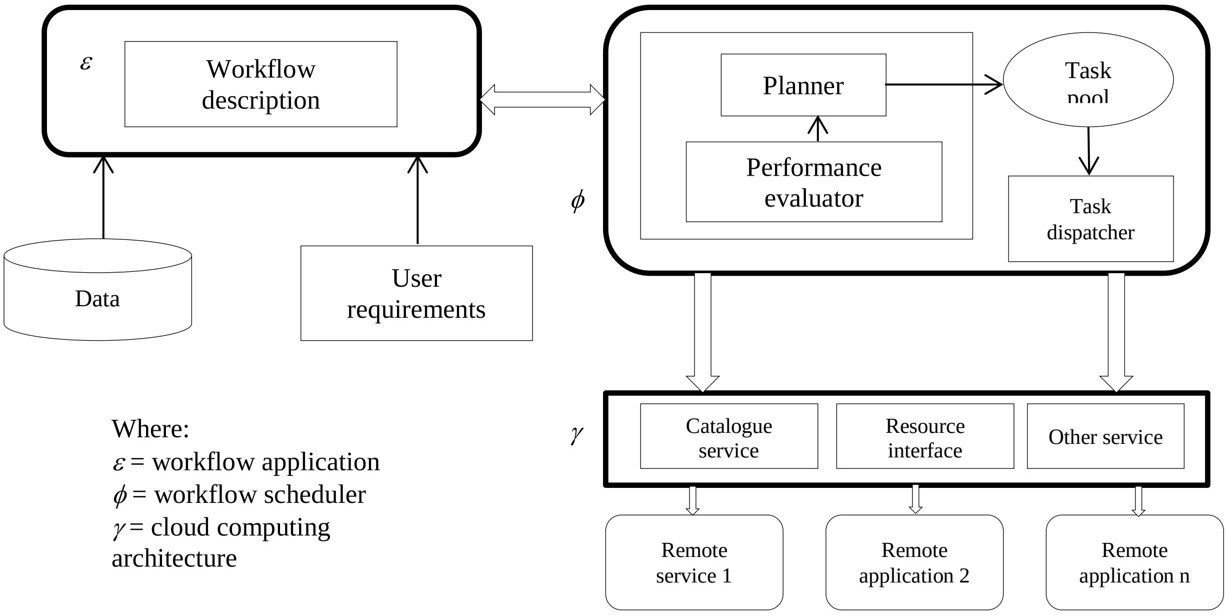

Fig. 1. Framework of a cloud computing paradigm

capability to forecast faults in order to mitigate wide-scale system overloads, which has an impact on the dependability of multiple services.

IV. Conclusion

This research has indicated that cloud computing is offered as a service by various providers. According to their workflow requirements, clients have a choice between SaaS, PaaS, and IaaS. Additionally, clients can choose whether to deploy their applications in public, private, community or hybrid clouds. Nevertheless, these choices display weakness in mitigating dependability and security concerns. Hence, the research examined existing work to establish the specific areas of the cloud computing paradigm, which display susceptibility to the established concerns. The consequent proposal argued that in as much as the providers have the responsibility of enhancing their services, workflow applications should observe the organizational data and security policies to reduce incidences of the computing architecture processing vulnerable data. On the other hand, the generic model proposed a review of performance metrics at its three levels of operation to improve dependability and data integrity.

References

[1] X. Liu, Y. Yang, D. Yuan, G. Zhang, W. Li and D. Cao, “A generic QoS framework for cloud workflow systems”, *2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing*, 2011.

[2] R. Caytiles and S. Lee, “Security considerations for public mobile cloud computing”, *International Journal of Advanced Science and Technology*, vol. 44, pp. 81-88, 2012.

[3] P. Kumar and S. Anand, “An approach to optimize workflow scheduling for cloud computing environment”, *Journal of Theoretical and Applied Information Technology*, vol. 57, no. 3, pp. 617-623, 2013.

[4] K. Bilal, S. Malik, S. Khan and A. Zomaya, “Trends and challenges in cloud datacenters”, *IEEE Cloud Computing*, vol. 1, no. 1, pp. 10-20, 2014.

[5] S. Stein, T. Payne and N. Jennings, “Robust execution of service workflows using redundancy and advance reservations”, *IEEE Trans. Serv. Comput.*, vol. 4, no. 2, pp. 125-139, 2011.

[6] C. Yan, H. Luo, Z. Hu, X. Li and Y. Zhang, “Deadline guarantee enhanced scheduling of scientific workflow applications in grid”, *JCP*, vol. 8, no. 4, 2013.

[7] Z. Tari, “Security and privacy in cloud computing”, *IEEE Cloud Computing*, vol. 1, no. 1, pp. 54-57, 2014.

[8] L. Mao, Y. Yang and H. Xu, “Design and optimization of cloud-oriented workflow system”, *Journal of Software*, vol. 8, no. 1, pp. 251-258, 2013.