Using proxies to facilitate collaboration in Multi-Cloud Computing Environments

[1]Solmaz Vaghri, [2]Mohan KG

[1]M.Tech Student, [2]Professor Dept. CSE
Acharya Institute of Technology (Affiliated to VTU) Bangalore, India
Email: [1]Solmaz_vaghri@yahoo.com, [2]mohankg@acharya.ac.in

Abstract—As cloud computing becomes more predominant, the problem of scalability has become critical for cloud computing providers. For the client to be able to simultaneously use services from multiple clouds; individually interaction with each cloud service provider, gathering intermediate results, processing the collective data, and generating final results is necessary. Collaboration among multiple cloud-based services, like cloud mashups, opens up opportunities for Cloud service providers (CSP's) to offer more-sophisticated services that will benefit clients. Today, cloud mashups need pre-established agreements among providers. This approach to building new collaborative services does not support agility, flexibility, and openness. This paper present the survey of the proxy-based multi-cloud computing framework which provides on the-fly, dynamic collaborations and cloud-based resource sharing services, addressing, policy trust, and privacy issues without pre-established collaboration agreements or standardized interfaces.

Keywords- Cloud Computing, data privacy, Collaboration, cloud-based services, security of data.

I. INTRODUCTION

Cloud computing is a pay per utility model for enabling ubiquitous, on-demand network based access to a shared configurable pool of computing resources such as networks, servers, storage, applications, etc. It can be rapidly provisioned and released with minimal effort for managing or service provider interaction.

According to NIST cloud computing provides following essential futures [1]:

- On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Location independence means that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
- Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

The development of cyber societies and online transactions imposes continuously organizations expanding their IT infrastructure. Cloud computing services become their nominal solutions since they provide economic benefits; they reduce hardware and

software expenses while canceling out related maintenance and upgrade costs. They offer flexible and on demand access to appropriate level of computation, memory, and storage resources. The advantage is brought by their multitenant feature, which enables an IT asset to host multiple tenants [5].

As more organizations employ cloud computing, cloud service providers (CSPs) are motivated for developing new technologies in order to enhance the capabilities of clouds. Cloud mashups have a similar structure to distributed data mining applications merges different services from several clouds into a single service, possibly in client side data and service. This service composition allows CSPs offer new functionalities at lower development costs to clients. Examples of cloud mashups and technologies to support them include IBM's Mashup Center, Appirio Cloud Storage and Force.com for the Google App Engine [3].

Today, cloud mashups require pre-written agreements among provider and also use of custom-built, recovery tools that combine services through low-level, tightly controlled and constraining integration techniques. This approach to building new collaborative services does not support agility, flexibility, and openness. Realizing multi-cloud collaboration's full potential will require implicit, transparent, universal, and on-the-fly interaction involving different services spread across multiple clouds that lack pre-established agreements and proprietary collaboration tools [3].

The research community is beginning to develop architectures, technologies, and standards to support collaboration among multiple cloud systems [2]-[5].

However, these research proposals still remain constraining due to their provider-centric approach or limited scope. Provider-centric approaches require CSPs to adopt and implement the standardized interfaces, protocols, formats, and other specifications, as well as new architectural and infrastructure components to facilitate collaboration, such that without these provider-centric changes, current proposals do not provide facilities for client-centric, on-the-fly, and opportunistic combinations of heterogeneous cloud-based services. While cloud standardization will promote collaboration, there are several hurdles to its adoption [6], [7].

For cloud collaboration to be alive, it is needed to developed mechanisms allowing opportunistic collaboration among services without requiring standards and extensive changes to the cloud service delivery model [3].

This approach will allow incremental provisioning of collaborative services to clients, which will continue to improve as more cloud services become interoperable in the future. Security is probably the hardest and most important problem that needs to be solved on the way towards cloud collaboration. It is a cross-cutting concern influencing all other aspects of the collaboration .In depth security analysis for identifying new threats and concerns resulting from collaboration must be considered to maintaining privacy of data and identity during collaboration, establishing trust among different cloud providers and addressing policy heterogeneity among multiple clouds so that composite services will include effective monitoring of policy anomalies to minimize security breaches [3].

This survey is organized as follows: In Section II, we discuss about proxy based framework in the area of interconnected Cloud environments to clarify the positioning of this work. In Section III, we explore the possible proxy architecture model between Clouds. Then, we discussed security issues for multiple Cloud collaboration in Section IV. Finally, we conclude the study and provide a basis for future developments in this area.

II. PROXY BASED FRAMEWORK FOR CLOUD COLLABORATION

Collaboration framework for multi-cloud systems allows applications and clients to use services simultaneously and also route data among multiple clouds without adopting standards, specifications and pre-established agreements among cloud providers. The following restrictions in the current cloud computing model prevent direct collaboration among applications hosted by different clouds [3]:

- Pre-established business agreements. The current business model requires pre-established agreements between CSPs before collaboration can occur. These agreements are necessary for clouds to establish their willingness to collaborate and establish trust with one another. The lack of such agreements prohibits multi-cloud collaborative efforts due to incompatible intentions, business rules, and policies. Moreover, collaborations resulting from pre-established agreements typically exhibit tight integration between the participants and cannot be extended to provide universal and dynamic collaboration

- Service delivery model. Clouds use a service delivery model that provides service access to legitimate subscribing clients and denies all other requests because of security and privacy concerns. This prevents direct interaction between services from different clouds.

Also, CSPs typically package their service offerings with other resources and services. This results in a tight dependency of a service on the hosting CSP. Such a service delivery model limits a client's ability to

customize a service and use it in combination with service offerings from different CSPs.

- Heterogeneity and tight coupling. Clouds implement proprietary interfaces for service access, configuration, and management as well as for interaction with other cloud components. Each service layer of a cloud tightly integrates with lower service layers or is highly dependent on the value-added proprietary solutions that the cloud offers. This heterogeneity and tight coupling prohibit interoperation between services from different clouds.

To overcome this restriction a network of proxies can be used. A proxy is an edge-node-hosted software instance that a client or a CSP can delegate to carry out operations on its behalf [3].

The proxy network consists of a large number of logically connected edge nodes that may assume a rich set of data roles to boost the performance and reliability of distributed data-intensive applications, including [14]:

- Cloud service interaction: A proxy may act as a client to a cloud service. This role allows a proxy with better network connectivity to access one or more cloud services. For example, a proxy may have very high bandwidth to/from a cloud service relative to the end-user.

- Computing: A proxy may carry out computations on data via a set of data operators. This role allows a proxy to filter, compress, merge, mine, and transform data.

We envision a set of well-defined data operators C_1, C_2, ...,C_k where Ci: $D_{in} \rightarrow D_{out}$, that is, Ci maps an input data into an output data.

- Caching: A proxy may efficiently store and serve data to other nearby proxies that may consume the data later on. Proxies can also cache intermediate results from a cloud interaction that may be reused again.

- Routing: A proxy may route data to another proxy as part of an application workflow. This role allows a proxy to efficiently send data to another proxy for additional processing, caching, cloud service interactions, etc. This role is particularly important if the application is interacting with multiple clouds which are all widely distributed, and there may be no single proxy that can efficiently orchestrate all of these interactions. The real power of proxies lies in the combination of these roles.

Depending on the situation, the system can employ a network of proxies as a collection of virtual software instances logically connected via a virtual network or a set of physical nodes connected via an underlying network infrastructure.

The basic idea is to enable proxies that act on behalf of a subscribing client or a cloud to provide a diverse set of functionalities: cloud service interaction on behalf of a client, data processing using a rich set of operations, caching of intermediate results, and routing, among others. With these additional functionalities, proxies can act as mediators for collaboration among services on different clouds [3].

As an example, if a client or CSP wants to simultaneously use a collection of services that multiple clouds provide. First, the requesting entity selects proxies for acting on its behalf as delegator and to interact with cloud applications. A client or a CSP might use multiple proxies to interact with many CSPs. It can select proxies based on several factors, for example, delays between clouds and proxies or workload conditions at various proxies. Once it chooses proxies, the client or CSP delegates the necessary service-specific privileges to the proxies to carry out the service request using the necessary security precautions [3].

These proxies can further delegate to other proxies if necessary and initiate the service request. In some instances, clients or CSPs can assign special roles to one or more proxies in the network to coordinate the operations in a service request among the multiple delegate proxies [3].

Following delegation, the requesting entity need not further interact with the proxy network until the proxies complete the service request. During execution of a service request, proxies would interact with cloud-based applications, playing the role of the service subscriber(s). By independently requesting services from the clouds, and by routing data between each other in a manner transparent to cloud applications, proxies can ease collaboration without requiring prior agreements between the CSPs. Proxies can also perform operations to help solve incompatibilities among services to allow data exchange between them [3].

III. PROXYARCHITECTURE MODEL

Cloud computing depend on sharing of network connected resource clusters such as server farms, data warehouses, and so on that host geographically distributed virtual machines and storage components that ensure scalability, reliability, and high availability . Cloud resources are not only shared by multiple users but dynamically can be re-allocated per demand.

A multi-cloud system model that employs proxies for collaboration consists a set of cloud services logically connected by a proxy network, and has three principle entities: (1) cloud services (2) proxy network, and (3) client‘s application initiator . Such systems can use

several possible strategies for placing proxies in the proxy network.

A. Cloud -hosted proxy

As Figure 1 shows, each CSP can host proxies within its cloud infrastructure, administer all proxies within its domain, and handle service requests from clients that wish to use those proxies for collaboration. The proxy instances might need to be CSP specific. For example, in Figure 1, both C1 and C2 might mutually and dynamically provision sharing and collaboration logic as proxy virtual instances within their respective administrative domains [3].

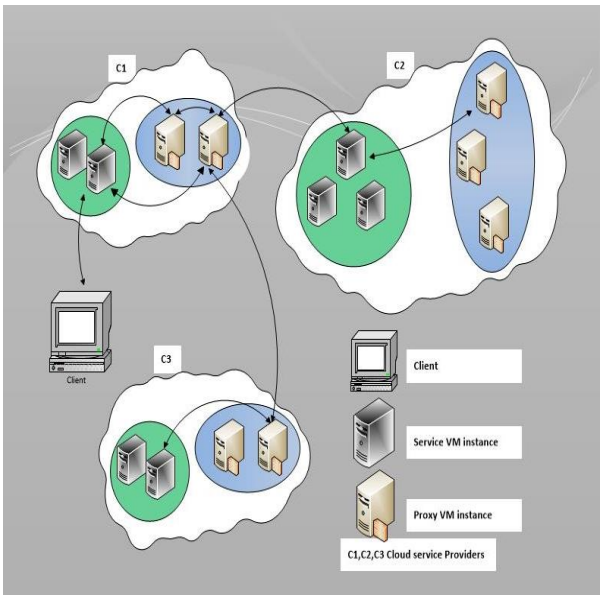

Figure1.In this case client sends a request to C1, which dynamically detects the need to use services from other clouds C2 and C3. The proxies will be employed by C1 to administer these interactions.

B. Proxy as a service

This case involves using proxies as an autonomous cloud that provides collaborative services to cloud service providers as well as clients ;as shown in figure 2 [3]. A group of CSPs that are ready to collaborate can administer this proxy-as-a-service cloud, or a proxy service provider (PSP), can provide administration. Clients directly interact with proxy cloud service and employ them for inter-cloud collaboration.

C. Peer-to-peer proxy

Proxies can also interact in a peer-to-peer network managed by either a PSP or a group of CSPs that wish to collaborate. Another possibility is for proxies to have no collective management: each proxy in the peer-to-peer network is an independent entity that manages itself [3].In this case, the proxy itself must handle requests to use its services.

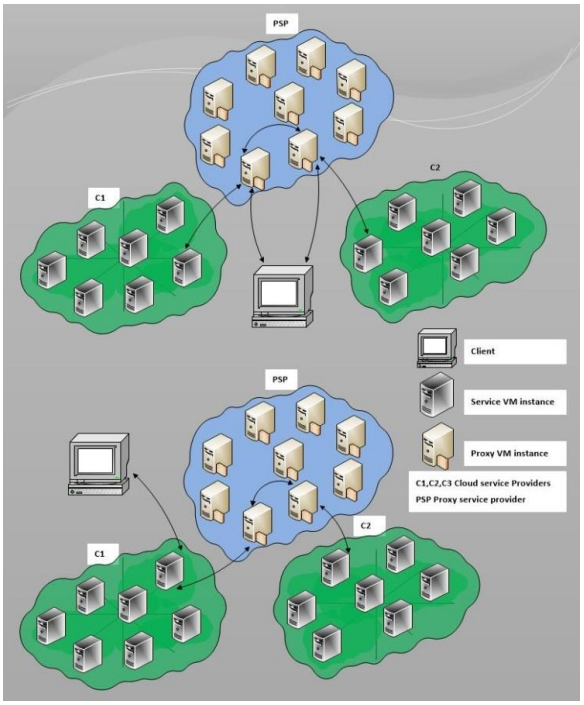

Figure2. Proxy as a service, CSPs set up proxies as an autonomous cloud system and offers it as a service to client. (a) A client uses two proxies to collaborate with CSPs C_1 and C_2. (b) Alternatively, a client starts request services with C1, which then detects the need for a service from C_2.

D. On-premise proxy

In the scenario shown in Figure3, a client can host proxies within its organization's infrastructure (or on premises) and manage all proxies within its administrative domain [3].

A client that wishes to use proxies for collaboration will employ its on-premises proxies, whereas CSPs that wish to collaborate with other CSPs must employ proxies that are within the domain of the service-requesting client.

E. Hybrid proxy infrastructure

A hybrid infrastructure can include on-premises, CSP- and PSP-maintained, and peer to- peer proxies. Selecting proxies for collaboration will depend on the type of service being requested and the entity that initiates collaboration, among other factors [3].For example, clients that must initiate a service request with two CSPs can employ on-premises proxies for collaboration. On the other hand, a cloud-based application that discovers it needs a service from another CSP to fulfill a client's request can employ a CSP-maintained proxy. The proposed architectures illustrate the various options that are available for deploying proxies to support collaboration [3].

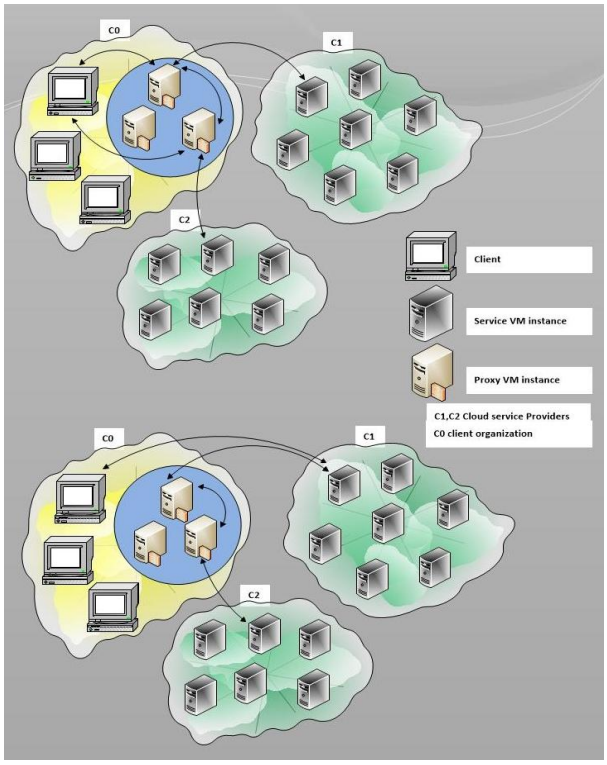

Figure3. On- premises proxy. Proxies are deployed within the infrastructure of client's organization. (a) A client employs two proxies to collaborate with CPS's C_1 and C_2 (b) A client starts requesting services with cloud C_1, which then detects the need for a service from C_2.

Developing these architectures serves as the first step in building a proxy-based, collaborative, multi-cloud computing environment. A complete solution will entail several additional tasks.

For example, an important task is a comprehensive study and evaluation of the proposed proxy-based architectures. Such an evaluation must cover architecture's possible variations under diverse practical use cases and scenarios for multi-cloud collaboration. Based on this study, researchers can refine the proposed architectures, develop new variations to support different scenarios and use cases, and, if possible, merge the architectures into a universal proxy-based architecture for multi-cloud collaboration.

Another important task is developing a full suite of protocols and mechanisms that proxies must implement to support all the functionalities necessary for acting as mediators among services from multiple clouds. For example, supporting collaboration scenarios migrate a client-subscribed virtual machine from one cloud to another requires techniques for translation between various virtual machine packages and distribution formats [3].

IV. SECURITY ISSUES IN MULTICLOUD COLLABORATION

Generally, trust typically refers to a situation where one party is willing to trust on the actions of another party; Control over the actions left by the former to the latter. Ultimately, there is an uncertainty if the trusted party will behave or deliver as promised.

The cloud computing is still in its beginning steps, so current status is associated with numerous challenges like security, performance, availability, integrity, cost etc. Out of these, security issue has the most important role in obstructing cloud computing. Putting data, running application at someone else's hard disk using someone else's CPU seems daunting to many. Researchers have highlighted several major security issues in cloud computing, including isolation management, data exposure and, virtual OS security, trust and compliance, and mission assurance, confidentiality, integrity and availability [8]-[16].

Using Proxies for collaboration require trust where the need for trust arises because a client leaves direct control of its assets' security and privacy to a CSP. These risks include insider security threats, weakening of data ownership rights, transitive trust issues with third-party providers in composite cloud services, and diminished oversight of system security [8]. So a client should give a high level of trust to a CSP based on its ability to implement effective controls and processes to secure assets. Thus, a client must be able to accept the higher levels of risk in using cloud-based services.By using proxy trust boundary increase because clients and CSP must accept proxy's security and establish trust with proxies [3].

For establishing a trust relationship, CSP must trust the proxy to legitimately act on behalf of the client or another CSP. Proxy networks are a potential platform for developing proxy-based security architectures and solutions for multi-cloud systems. At a minimum, the proxy network must implement security and privacy mechanisms that mirror, extend, or complement similar mechanisms offered by clouds to maintain asset protection outside the domain of clouds and client organizations [8].

In addition, clients, clouds, and proxies must implement mechanisms that ensure secure delegation, which entails the following [3]:

- On-the-fly agreements. Delegating to a proxy must establish, on the fly, an explicit agreement between the delegator and proxy that lets the proxy act on the delegator's behalf. Techniques for delegation to a proxy must include mechanisms that restrict the proxy's behavior, including data and resource

access, to comply with delegator-specified constraints[3].

- Expected behavior. After delegation, a proxy must not deviate from the expected behavior. It must act only on behalf of the delegator (a client or a CSP). After the proxy fulfills the service request, it can no longer act on the delegator's behalf. The proxy cannot modify the intended service request or misuse client assets, and it must not transitively delegate its capabilities to other proxies without the delegator's explicit consent[3].

When proxies enable dynamic collaboration between multiple CSPs, heterogeneous security policies can be the source of policy conflicts that result in security breaches. Even though existing policy evaluation mechanisms can verify individual domain policies, security violations can easily occur during integration [12].

Proxies must analyze relationships between policies to detect and resolve policy anomalies using mechanisms that easily adapt to handle composite policies evaluated as a whole. Possible policy anomalies include policy inconsistencies and inefficiencies.

Once proxies identify conflicts, they must use conflict resolution strategies to resolve them. However, current conflict resolution mechanisms have limitations. Multi-cloud environments require adaptively applying different algorithms to resolve different conflicts.

For keeping Identity attributes and data privacy in shared computing environments like clouds, protecting the privacy of client assets is critical.[8] The privacy issues pertaining to both data and identity. Privacy protection methods (other than encryption) fall broadly into two categories [15].

- Data perturbation (also known as input perturbation), which adds some form of noise to the data itself, and

- Output perturbation, which adds noise to the otherwise accurate query answers.

Earlier research studied data privacy in outsourcing data aggregation services [16]. Regardless of the methods used to maintain data privacy, the resulting solution must scale to use for large amounts of data and many CSPs.

V. CONCLUSION

In this paper we have introduced the concept of a proxy network to accelerate dynamic collaboration spanning multiple specialized clouds. The proposed framework employs proxies to act as mediators between applications in multiple clouds that must share data; it has ability to overcome several restrictions in the current cloud computing model that can restrict dynamic collaboration among applications within different cloud systems.

Future works oversight for the proposed framework includes refining the proxy deployment scenarios and development of infrastructural and operational components of a multi-cloud system. This must be accompanied by implementation of an experimental platform using open source tools and libraries that work in combination with real-world cloud services to evaluate the system's functionality and limitations, and make further refinements and also exploring techniques that can identify suitable proxies automatically based on application needs.

REFERENCES

[1] P. Mell and T. Grance, The NIST Definition of Cloud Computing, special publication 800-145, Nat'l Inst. Standards and Technology, 2011, p. iii + 3.

[2] D. Bernstein and D. Vij, "Intercloud Security Considerations," Proc. 2nd Int'l Conf. Cloud Computing (CloudCom 10), IEEE Press, 2010, pp. 537-544.

[3] M. Singhal and S. Chandrasekhar, T. Ge, R.Sandh and R. Krishnan, G. Ahn E. Bertino, "Collaboration in Multicloud Computing Environments: Framework and Security Issues" Published by IEEE Computer Society , Feb. 2013

[4] R. Buyya et al., "Market-Oriented Cloud Computing: Vision, Hype, and Reality of Delivering Computing as the 5th Utility," Proc. 9th IEEE/ACM Int'l Symp. Cluster Computing and the Grid (CCGRID 09), IEEE CS, 2009, pp. 599-616.

[5] B. Rochwerger et al., "Reservoir—When One Cloud Is Not Enough," Computer, Mar. 2011, pp. 44-51.

[6] M.P. Papazoglou and W. van den Heuvel, "Blueprinting the Cloud," IEEE Internet Computing, Nov./Dec 2011, pp. 74-79.

[7] S. Ortiz Jr., "The Problem with Cloud Computing Standardization," Computer, July 2011, pp. 13-16.

[8] P. Mell and T. Grance, "Perspectives on Cloud Computing and Standards, NIST Information Technology Laboratory," Nat'l Inst. Standards and Technology, 2008;

http://csrc.nist.gov/groups/SMA/ispab/documents /minutes/2008 12/cloudcomputing- standards_ ISPAB Dec2008_P-Mell.pdf.

[9] W. Jansen and T. Grance," Guidelines on Security and Privacy in Public Cloud Computing", special publication 800-144, Nat'l Inst. Standards and Technology, 2011, p. x + 70.

[10] Gundeep S, Prashant K, Krishen K, seema Kh "cloud security: Analysis and risk management of VM images" Proceeding of the IEEE International Conference on Information and Automation Shenyang, China, June 2012

[11] C.M. Ellison et al., SPKI Certificate Theory, IETF RFC 2693, Sept. 1999; www.ietf.org/rfc/rfc2693.txt.

[12] E. Hammer-Lahav, ed., The OAuth 1.0 Protocol, IETF RFC 5849, Apr. 2010; http://tools.ietf.org/html/rfc5849.

[13] Y. Zhang and J.B.D. Joshi, "Access Control and Trust Management for Emerging Multidomain Environments," Ann.Emerging Research in Information Assurance, Security and Privacy Services, Emerald Group Publishing, 2009, pp. 421-452.

[14] Jon Weissman "Using proxies to accelerate cloud applications" Proceeding HotCloud'09 Proceedings of the 2009 conference on Hot topics in cloud computing ,Article No. 20

[15] J. Weissman and S. Ramakrishan, "Using Proxies to Accelerate Cloud Application", Proceeding HotCloud'09 Proceedings of the 2009 conference on Hot topics in cloud computing, No. 20, USENIX Association Berkeley, CA, USA ©2009

[16] N.R. Adam and J.C. Wortmann, "Security-Control Methods for Statistical Databases: A Comparative S16. L. Xiong, S. Chitti, and L. Liu, "Preserving Data Privacy in Outsourcing Data Aggregation Services," ACM Trans. Internet Technology, Aug. 2007, p. 17

◈◈◈