ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Service and Data Security for Multi Cloud Environment

Rajkumar B[1], Balamurugan K[2]

M.Tech, Dept of IT, K.S.R. College of Engineering, Tamilnadu, India[1]

Associate Professor, Dept of IT, K.S.R. College of Engineering, Tamilnadu, India[2]

ABSTRACT: Software, storage data and infrastructure are shared under the cloud environment. Cloud computing provides many benefits in terms of low cost and accessibility of data. Cloud provider manages data values from the data owners. Risks of service availability failure and the possibility of malicious insiders problems are raised in the single cloud. A public cloud is offered by third-party service providers and involves resources outside the user's premises. The cloud system is installed on the user's premise under the private cloud model. Multi clouds or inter clouds are used to provide the reliable data delivery. Multi-cloud environment control several clouds and avoids dependency on any one individual cloud.

Multi-cloud resource sharing scheme uses data and application partitioning mechanism. Four types of architectures are used to distributing resources to multiple cloud providers. They are Replication of applications, Partition of application System, Partition of application logic into fragments, Partition of application data into fragments. Replication of applications allows receiving multiple results from one operation performed in distinct clouds. Partition of application System into tiers allows separating the logic from the data. Partition of application logic into fragments allows distributing the application logic to distinct clouds. Partition of application data into fragments allows distributing fine-grained fragments of the data to distinct clouds. Data security and attack handling operation are managed by centralized or distributed manner in the cloud.

Service and data management architectures are combined to provide a complete solution for security requirements. Multiparty communication based security system is used to improve the security over different clouds. Integrity is provided for data and service components sharing environment. An integrated intrusion detection system is proposed to handle malicious attacks.

I. INTRODUCTION

A number of enabling technologies contribute to Cloud computing several state-of-the-art techniques. Virtualization technologies partition hardware and thus provide flexible and scalable computing platforms. Virtual machine techniques, such as VMware and Xen, offer virtualized IT-infrastructures on demand. Virtual network advances, such as VPN, support users with a customized network environment to access Cloud resources. Virtualization techniques are the bases of the Cloud computing since they render flexible and scalable hardware services.

Computing Clouds offer a complete set of service templates on demand, which could be composed by services inside the computing Cloud. Computing Clouds therefore should be able to automatically orchestrate services from different sources and of different types to form a service flow or a workflow transparently and dynamically for users. Computing Cloud services are normally exposed as Web services, which follow the industry standards such as WSDL, SOAP and UDDI. The services organization and orchestration inside Clouds could be managed in a Service Oriented Architecture (SOA). A set of Cloud services furthermore could be used in a SOA application environment, thus making them available on various distributed platforms and could be further accessed across the Internet.

Web 2.0 is an emerging technology describing the innovative trends of using World Wide Web technology and Web design that aims to enhance creativity, information sharing, collaboration and functionality of the Web. The essential idea behind Web 2.0 is to improve the interconnectivity and interactivity of Web applications. The new paradigm to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

develop and access Web applications enables users access the Web more easily and efficiently. Cloud computing services in nature are Web applications which render desirable computing services on demand. It is thus a natural technical evolution that the Cloud computing adopts the Web 2.0 technique.

A network storage system, which is backed by distributed storage providers, offers storage capacity for users to lease. The data storage could be migrated, merged, and managed transparently to end users for whatever data formats. Examples are Google File System and Amazon S3. A Mashup is a Web application that combines data from more than one source into a single integrated storage tool. The SmugMug is an example of Mashup, which is a digital photo sharing Web site, allowing the upload of an unlimited number of photos for all account types, providing a published API which allows programmers to create new functionality, and supporting XML-based RSS and Atom feeds. A distributed data system which provides data sources accessed in a semantic way. Users could locate data sources in a large distributed environment by the logical name instead of physical locations. Virtual Data System (VDS) is good reference.

Users drive into the computing Cloud with data and applications. Some Cloud programming models should be proposed for users to adapt to the Cloud infrastructure. For the simplicity and easy access of Cloud services, the Cloud programming model, however, should not be too complex or too innovative for end users. The MapReduce is a programming model and an associated implementation for processing and generating large data sets across the Google worldwide infrastructures. The MapReduce model firstly involves applying a "map" operation to some data records – a set of key/value pairs, and then processes a "reduce" operation to all the values that shared the same key. The Map-Reduce-Merge method evolves the MapReduce paradigm by adding a "merge" operation. Hadoop is a framework for running applications on large clusters built of commodity hardware. It implements the MapReduce paradigm and provides a distributed file system -− the Hadoop Distributed File System. The MapReduce and the Hadoop are adopted by recently created international Cloud computing project of Yahoo!, Intel and HP.

II. RELATED WORKS

Cloud computing creates a large number of security issues and challenges. A list of security threats to cloud computing is presented in [5]. These issues range from the required trust in the cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems. The main problem that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as business-critical data and processes. When considering using a cloud service, the user must be aware of the fact that all data given to the cloud provider leave the own control and protection sphere. Even more, if deploying data-processing applications to the cloud (via IaaS or PaaS), a cloud provider gains full control on these processes. Hence, a strong trust relationship between the cloud provider and the cloud user is considered a general prerequisite in cloud computing.

Depending on the political context this trust may touch legal obligations. For instance, Italian legislation requires that government data of Italian citizens, if collected by official agencies, have to remain within Italy. Thus, using a cloud provider from outside of Italy for realizing an e-government service provided to Italian citizens would immediately violate this obligation. Hence, the cloud users must trust the cloud provider hosting their data within the borders of the country and never copying them to an off-country location nor providing access to the data to entities from abroad.

An attacker that has access to the cloud storage component is able to take snapshots or alter data in the storage. This might be done once, multiple times, or continuously. An attacker that also has access to the processing logic of the cloud can also modify the functions and their input and output data. Even though in the majority of cases it may be legitimate to assume a cloud provider to be honest and handling the customers' affairs in a respectful and responsible manner, there still remains a risk of malicious employees of the cloud provider, successful attacks and compromisation by third parties, or of actions ordered by a subpoena.

In [6], an overview of security flaws and attacks on cloud infrastructures is given. Some examples and more recent advances are briefly discussed in the following. Ristenpart et al. [7], [8] presented some attack techniques for the virtualization of the Amazon EC2 IaaS service. In their approach, the attacker allocates new virtual machines until one runs

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

on the same physical machine as the victim's machine. Then, the attacker can perform cross-VM side channel attacks to learn or modify the victim's data. The authors present strategies to reach the desired victim machine with a high probability, and show how to exploit this position for extracting confidential data, e.g., a cryptographic key, from the victim's VM. Finally, they propose the usage of blinding techniques to fend cross-VM side-channel attacks.

In [9], a flaw in the management interface of Amazon's EC2 was found. The SOAP-based interface uses XML Signature as defined in WS-Security for integrity protection and authenticity verification. Gruschka and Iacono [9] discovered that the EC2 implementation for signature verification is vulnerable to the Signature Wrapping Attack. In this attack, the attacker—who eavesdropped a legitimate request message—can add a second arbitrary operation to the message while keeping the original signature. Due to the flaw in the EC2 framework, the modification of the message is not detected and the injected operation is executed on behalf of the legitimate user and billed to the victim's account.

A major incident in a SaaS cloud happened in 2009 with Google Docs. Google Docs allows users to edit documents online and share these documents with other users. However, this system had the following flaw: Once a document was shared with anyone, it was accessible for everyone the document owner has ever shared documents with before. For this technical glitch, not even any criminal intent was required to get unauthorized access to confidential data. Recent attacks have demonstrated that cloud systems of major cloud providers may contain severe security flaws in different types of clouds (see [12], [10]).

As can be seen from this review of the related work on cloud system attacks, the cloud computing paradigm contains an implicit threat of working in a compromised cloud system. If an attacker is able to infiltrate the cloud system itself, all data and all processes of all users operating on that cloud system may become subject to malicious actions in an avalanche manner. Hence, the cloud computing paradigm requires an in-depth reconsideration on what security requirements might be affected by such an exploitation incident. For the common case of a single cloud provider hosting and processing all of its user's data, an intrusion would immediately affect all security requirements: Accessibility, integrity, and confidentiality of data and processes may become violated, and further malicious actions may be performed on behalf of the cloud user's identity.

These cloud security issues and challenges triggered a lot of research activities, resulting in a quantity of proposals targeting the various cloud security threats. Alongside with these security issues, the cloud paradigm comes with a new set of unique features that open the path toward novel security approaches, techniques, and architectures. One promising concept makes use of multiple distinct clouds simultaneously.

III. MULTI CLOUD SECURITY MODEL

Cloud computing offers dynamically scalable resources provisioned as a service over the Internet. The third party, on-demand, self-service, pay-per-use, and seamlessly scalable computing resources and services offered by the cloud paradigm promise to reduce capital as well as operational expenditures for hardware and software.

Clouds can be categorized taking the physical location from the viewpoint of the user into account [1]. A public cloud is offered by third-party service providers and involves resources outside the user's premises. In case the cloud system is installed on the user's premise—usually in the own data center—this setup is called private cloud. A hybrid approach is denoted as hybrid cloud. This paper will concentrate on public clouds, because these services demand for the highest security requirements but also—as this paper will start arguing—include high potential for security prospects.

In public clouds, all of the three common cloud service layers (IaaS, Paas, SaaS) share the commonality that the end-users' digital assets are taken from an intra organizational to an inter organizational context. This creates a number of issues, among which security aspects are regarded as the most critical factors when considering cloud computing adoption. Legislation and compliance frameworks raise further challenges on the outsourcing of data, applications, and processes. The high privacy standards in the European Union, e.g., and their legal variations between the continent's countries give rise to specific technical and organizational challenges [3].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

One idea on reducing the risk for data and applications in a public cloud is the simultaneous usage of multiple clouds. Several approaches employing this paradigm have been proposed recently. They differ in partitioning and distribution patterns, technologies, cryptographic methods, and targeted scenarios as well as security levels. This paper is an extension of [4] and contains a survey on this different security by multicloud adoption approaches. It provides four distinct models in form of abstracted multicloud architectures. These developed multicloud architectures allow to categorize the available schemes and to analyze them according to their security benefits. An assessment of the different methods with regards to legal aspects and compliance implications is given in particular.

IV. ISSUES ON MULTI CLOUD SECURITY

Multi-cloud resource sharing scheme uses data and application partitioning mechanism. Four types of architectures are used to distributing resources to multiple cloud providers. They are Replication of applications, Partition of application System, Partition of application logic into fragments, Partition of application data into fragments. Replication of applications allows receiving multiple results from one operation performed in distinct clouds. Partition of application System into tiers allows separating the logic from the data. Partition of application logic into fragments allows distributing the application logic to distinct clouds. Partition of application data into fragments allows distributing fine-grained fragments of the data to distinct clouds. Data security and attack handling operation are managed by centralized or distributed manner in the cloud. The following drawbacks are identified from the existing system.

- Stand alone security systems
- Malicious attacks are not handled
- Encrypted data processing is not supported
- Data integrity is not provided

V. SECURITY PROSPECTS BY MULTICLOUD ARCHITECTURES

The basic underlying idea is to use multiple distinct clouds at the same time to mitigate the risks of malicious data manipulation, disclosure, and process tampering. By integrating distinct clouds, the trust assumption can be lowered to an assumption of non collaborating cloud service providers. Further, this setting makes it much harder for an external attacker to retrieve or tamper hosted data or applications of a specific cloud user. The idea of making use of multiple clouds has been proposed by Bernstein and Celesti [2]. However, this previous work did not focus on security. Since then, other approaches considering the security effects have been proposed. These approaches are operating on different cloud service levels, are partly combined with cryptographic methods, and targeting different usage scenarios.

In this paper, we introduce a model of different architectural patterns for distributing resources to multiple cloud providers. This model is used to discuss the security benefits and also to classify existing approaches. In our model, we distinguish the following four architectural patterns:

- Replication of applications allows to receive multiple results from one operation performed in distinct clouds and to compare them within the own premise. This enables the user to get evidence on the integrity of the result.
- Partition of application System into tiers allows separating the logic from the data. This gives additional protection against data leakage due to flaws in the application logic.
- Partition of application logic into fragments allows distributing the application logic to distinct clouds. This has two benefits. First, no cloud provider learns the complete application logic. Second, no cloud provider learns the overall calculated result of the application. Thus, this leads to data and application confidentiality.
- Partition of application data into fragments allows distributing fine-grained fragments of the data to distinct clouds. None of the involved cloud providers gains access to all the data, which safeguards the data's confidentiality.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Each of the introduced architectural patterns provides individual security merits, which map to different application scenarios and their security needs. Obviously, the patterns can be combined resulting in combined security merits, but also in higher deployment and runtime effort. The following sections present the four patterns in more detail and investigate their merits and flaws with respect to the stated security requirements under the assumption of one or more compromised cloud systems.

5.1. Replication of Application

How does a cloud customer know whether his data were processed correctly within the cloud? There is no technical way to guarantee that an operation performed in a cloud system was not tampered with or that the cloud system was not compromised by an attacker. The only kind of guarantee is based on the level of trust between the cloud customer and the cloud provider and on the contractual regulations made between them such as SLAs, applicable laws, and regulations of the involved jurisdictional domains. But even if the relation and agreements are perfectly respected by all participants, there still remains a residual risk of getting compromised by third parties.

5.2. Partition of Application System Into Tiers

The architectural pattern described in the cloud user to get some evidence on the integrity of the computations performed on a third-party's resources or services. The architecture introduced in this section targets the risk of undesired data leakage. It answers the question on how a cloud user can be sure that the data access is implemented and enforced effectively and that errors in the application logic do not affect the user's data?

To limit the risk of undesired data leakage due to application logic flaws, the separation of the application system's tiers and their delegation to distinct clouds is proposed. In case of an application failure, the data are not immediately at risk since it is physically separated and protected by an independent access control scheme. Moreover, the cloud user has the choice to select a particular—probably specially trusted—cloud provider for data storage services and a different cloud provider for applications.

5.3. Partition of Application Logic Into Fragments

This architecture variant targets the confidentiality of data and processing logic. It gives an answer to the following question: How can a cloud user avoid fully revealing the data or processing logic to the cloud provider? The data should not only be protected while in the persistent storage, but in particular when it is processed. The idea of this architecture is that the application logic needs to be partitioned into fine-grained parts and these parts are distributed to distinct clouds. This approach can be instantiated in different ways depending on how the partitioning is performed. The clouds participating in the fragmented applications can be symmetric or asymmetric in terms of computing power and trust. Two concepts are common. The first involves a trusted private cloud that takes a small critical share of the computation, and a untrusted public cloud that takes most of the computational load. The second distributes the computation among several untrusted public clouds, with the assumption that these clouds will not collude to break the security.

5.4. Partition of Application Data Into Fragments

This multicloud architecture specifies that the application data is partitioned and distributed to distinct clouds. The most common forms of data storage are files and databases. Files typically contain unstructured data and do not allow for easily splitting or exchanging parts of the data. This kind of data can only be partitioned using cryptographic methods. Databases contain data in structured form organized in columns and rows. Here, data partitioning can be performed by distributing different parts of the database to different cloud providers. Finally, files can also contain structured data. Here,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

the data can be splitted using similar approaches like for databases. XML data, for example, can be partitioned on XML element level. However, such operations are very costly. Thus, this data are commonly rather treated using cryptographic data splitting.

VI. SERVICE AND DATA SECURITY FOR MULTI CLOUDS

Secure Multiparty Computation (SMC) and Secret Sharing (SS) algorithm are used to improve the cloud security. Secure data exchange is handled using the Secure Multiparty Computation protocol. The Secret Sharing Algorithm is used to share key values between the users and providers. Data integrity and service integrity verification is performed using the signature models. Intrusion detection scheme is integrated with the multi-cloud environment for malicious attack handling.

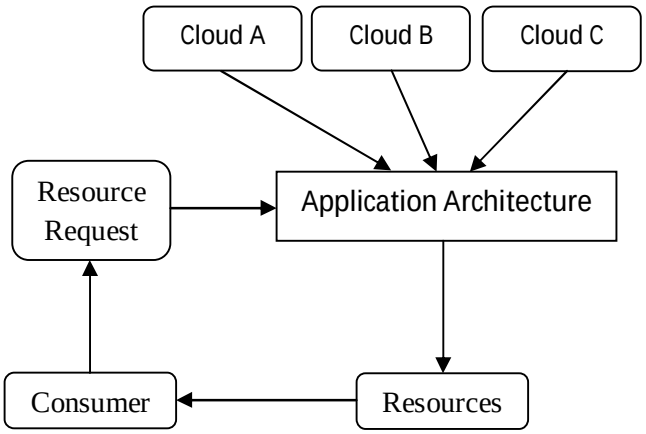

Fig. No. 6.1 Service and Data Security for Multi Clouds

Service and data management architectures are combined to provide a complete solution for security requirements. Multiparty communication based security system is used to improve the security over different clouds. Integrity is provided for data and service components sharing environment. An integrated intrusion detection system is proposed to handle malicious attacks. The multi cloud security model is used to protect service and data providers. Different cloud resource sharing architectures are integrated in the system. Intrusion detection is performed to control malicious attackers. The system is divided into five major modules. They are resource provider, consumer, scheduling process, security process and intrusion detection process. Resource provider provides the hardware and data resources. Consumers are used to access the cloud resources. Scheduling schemes are used for the resource allocation process. Data and services are protected in the security process. Malicious attacks are handled in the intrusion detection process.

6.1. Resource Provider

Resource provider provides the computational resources to the consumers. Resource monitoring is performed to fetch current resource levels. Provider manages the application replication process. Data sources are also provided by the resource provider.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

6.2. Consumer

The consumer is the resource users. Consumer submits the resource requests. Task requests are submitted resource level and time period information. Resources are allocated from multiple cloud environments.

6.3. Scheduling Process

The scheduling process is used to assign resources to the tasks. Application replication and fragmentation methods are used in the scheduling process. Applications are fragmented with reference to the logic and modules. Data fragmentation is used for the data distribution process.

6.4. Security Process

The data and services are protected with security schemes. Data values are secured with secret sharing algorithm. Multi party computations are used to protect sensitive data values. Data integrity verification is provided in the security process.

6.5. Intrusion Detection Process

Intrusion detection is performed to detect malicious requests. Request sources and intervals are analyzed in the intrusion detection process. Anonymous requests are detected in the intrusion detection process. Data and service providers are secured from intruders.

VII. CONCLUSION

Multi-cloud systems are used to share resources among different cloud environment. The resource sharing process is handled with partitioned data and service model. Secure Multiparty Computation (SMC) and Secret Sharing (SS) algorithm are used to improve the cloud security. Intrusion detection scheme is integrated with the multi-cloud environment for malicious attack handling. The system supports data and application model. Integrated security solution schemes are used to protect data and services. Attack resistant resource sharing system controls the service based attacks. Risk free resource management mechanism assures service availability in all situations.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing, Version 15," Nat'l Inst. of Standards and Technology, Information Technology Laboratory, vol. 53, p. 50, http://csrc.nist.gov/groups/SNS/cloud-computing/, 2010.
[2] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "How to Enhance Cloud Architectures to Enable Cross-Federation," Proc. IEEE Third Int'l Conf. Cloud Computing (CLOUD), pp. 337-345, 2010.
[3] Gartner, "Gartner Says Cloud Adoption in Europe Will Trail U.S. by at Least Two Years," http://www.gartner.com/it/page.jsp?id=2032215, May 2012.
[4] J.-M. Bohli, M. Jensen, N. Gruschka, J. Schwenk, and L.L.L. Iacono, "Security Prospects through Cloud Computing by Adopting Multiple Clouds," Proc. IEEE Fourth Int'l Conf. Cloud Computing (CLOUD), 2011.
[5] D. Hubbard and M. Sutton, "Top Threats to Cloud Computing V1.0," Cloud Security Alliance, http://www.cloudsecurityalliance.org/topthreats, 2010.
[6] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "On Technical Security Issues in Cloud Computing," Proc. IEEE Int'l Conf. Cloud Computing (CLOUD-II), 2009.
[7] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 199-212, 2009.
[8] Y. Zhang, A. Juels, M.K.M. Reiter, and T. Ristenpart, "Cross-VM Side Channels and Their Use to Extract Private Keys," Proc. ACM Conf. Computer and Comm. Security (CCS '12), pp. 305-316, 2012.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[9] N. Gruschka and L. Lo Iacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited," Proc. IEEE Int'l Conf. Web Services (ICWS '09), 2009.
[10] S. Bugiel, S. Nu¨ rnberger, T. Po¨ppelmann, A.-R. Sadeghi, and T. Schneider, "AmazonIA: When Elasticity Snaps Back," Proc. 18th ACM Conf. Computer and Comm. Security (CCS '11), pp. 389-400, 2011.
[11] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono, and Ninja Marnau, "Security and Privacy-Enhancing Multicloud Architectures", IEEE Transactions on Dependable and Secure Computing, Vol. 10, No. 4, July/August 2013.
[12] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "All Your Clouds Are Belong to Us: Security Analysis of Cloud Management Interfaces," Proc. Third ACM Workshop Cloud Computing Security Workshop (CCSW '11), pp. 3-14, 2011.