ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Enhanced Privacy in a Resource Sharing Cloud Environment by Utilizing Proxy-Based Multicloud Computing

Mohammed Waheeduddin Hussain
Professor
Department of CSE
Nawab Shah Alam Khan College of Engineering and Technology
Hyderabad, Telangana, India.

Mohammed Abbas Qureshi
M Tech Student
Department of CSE
Nawab Shah Alam Khan College of Engineering and Technology
Hyderabad, Telangana, India.

Abstract:
Cloud computing is computing in which large groups of remote servers are networked to allow centralized data storage and online access to computer services or resources. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. 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 preestablished 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 preestablished collaboration agreements or standardized interfaces.

Keywords: ***Privacy Preserving, Cloud Computin, Virtual Machine(VM), Proxy, Data Security, Trust***

Introduction:

Business can scale up or scale down companies operation and storage needs quickly to suit organizations situation, allowing flexibility as your needs change. Rather than purchasing and installing expensive upgrades yourself, your cloud computer service provider can handle this for you. Cloud computing security or, more simply, cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

Security issues associated with the cloud:

Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community). There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the on the cloud). The responsibility goes both ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures.

When an organization elects to store data or host applications on the public cloud, it loses its ability to

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

have physical access to the servers hosting its information. As a result, potentially business sensitive and confidential data is at risk from insider attacks. According to a recent Cloud Security Alliance Report, insider attacks are the third biggest threat in cloud computing. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity.

In order to conserve resources, cut costs, and maintain efficiency, Cloud Service Providers often store more than one customer's data on the same server. As a result there is a chance that one user's private data can by viewed by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation.

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist. For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole datacenter to go down or be reconfigured to an attacker's liking.

Some security and privacy issues that need to be considered are as follows

1) Authentication: Only authorized user can access data in the cloud

2) Correctness of data: This is the way through which user will get the confirmation that the data stored in the cloud is secure

3) Availability: The cloud data should be easily available and accessible without any burden. The user should access the cloud data as if he is accessing local data

4) No storage Overhead and easy maintenance: User doesn't have to worry about the storage requirement & maintenance of the data on a cloud

5) No data Leakage: The user data stored on a cloud can accessed by only authorize the user or owner. So all the contents are accessible by only authorize the user.

6) No Data Loss: Provider may hide data loss on a cloud for the user to maintain their reputation

Compliance & Audits in Cloud:

Numerous laws and regulations pertain to the storage and use of data. In the US these include privacy or data protection laws, Payment Card Industry - Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, the Federal Information Security Management Act of 2002 (FISMA), and Children's Online Privacy Protection Act of 1998, among others.

Similar laws may apply in different legal jurisdictions and may differ quite markedly from those enforced in the US. Cloud service users may often need to be aware of the legal and regulatory differences between the jurisdictions. For example data stored by a Cloud Service Provider may be located in, say, Singapore and mirrored in the US.

Many of these regulations mandate particular controls (such as strong access controls and audit trails) and require regular reporting. Cloud customers must ensure that their cloud providers adequately fulfil such requirements as appropriate, enabling them to comply with their obligations since, to a large extent, they remain accountable.

Business continuity and data recovery

Cloud providers have business continuity and data recovery plans in place to ensure that service can be maintained in case of a disaster or an emergency and that any data loss will be recovered. These plans may be shared with and reviewed by their customers, ideally dovetailing with the customers' own continuity

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

arrangements. Joint continuity exercises may be appropriate, simulating a major Internet or electricity supply failure for instance.

Logs and audit trails

In addition to producing logs and audit trails, cloud providers work with their customers to ensure that these logs and audit trails are properly secured, maintained for as long as the customer requires, and are accessible for the purposes of forensic investigation (e.g., eDiscovery).

Unique compliance requirements

In addition to the requirements to which customers are subject, the data centers used by cloud providers may also be subject to compliance requirements. Using a cloud service provider (CSP) can lead to additional security concerns around data jurisdiction since customer or tenant data may not remain on the same system, or in the same data center or even within the same provider's cloud.

Related Work:

Proxy Based Framework

A proposed proxy based multi-cloud computing system permits dynamic, on the-fly collaboration and resource sharing around cloud-based services, tending to trust, policy, and privacy issues without pre-established collaboration agreement or standardized interfaces. It incorporates the utilization of proxy in multi-cloud environment in different forms as follows:

1) Cloud-Hosted Proxy

In this situation the cloud service provider hosts proxies inside its framework and manage and deal with the proxy, also will handle the service request from the customer who needs to get to these proxies.

2) Proxy service

Here the proxy is been deployed as a self-sufficient cloud.

Numerous cloud service providers with collaboration can deal with this proxy or a third party proxy service provider can oversee it for the cloud service providers.

3) Point-to-Point proxy

Proxy can additionally be interfaced on point-to-point network which is overseen by the proxy service provider or cloud service provider those who have an agreement of collaboration.

4) On-premise proxy

The customer himself can host proxy inside infrastructural space and oversee it in regulatory area. The client who wishes to utilize proxies will need to deploy it on premise proxies and the service providers that wish to team up with other service provider will have to implement it inside the service requesting customer domain

Using Virtual Machine

Abhishek Mohta proposed Virtual machines which uses

RSA algorithm, for client data/file encryption and decryptions. It also uses SHA 512 algorithm which makes message digest and check the data integrity. The Digital signature is used as an identity measure for client or data owner. It solves the problem of integrity, unauthorized access, privacy and consistency.

Existing System:

Many existing cloud data services provide similar access control models, in which individual and organizational privacy, a key requirement for digital identity management, is unprotected. Also, with cloud computing initiatives, the scope of insider threats, a major source of data theft and privacy breaches, is no longer limited to the organizational perimeter. Multicloud environments exacerbate these issues because proxies can access data (which the environment might dynamically move or partition across different clouds) on behalf of clients. Revealing sensitive information in identity attributes to proxies that grant them authorization to access the data on behalf of clients is not an attractive solution. Thus, assuring the private and consistent management of information relevant to ABAC becomes more complex in multicloud systems.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Disadvantages:

Inefficiencies in composite policies include

• Redundancy—a policy is redundant if every access request that matches the policy also matches another policy with the same effect;

• Verbosity—similar to data element merging in data integration, policy composition can merge similar policies from different origins; resolving the policy verbosity during composition affects the policy size.

Proposed System:

Our proposed framework for generic cloud collaboration allows clients and cloud applications to simultaneously use services from and route data among multiple clouds. This framework supports universal and dynamic collaboration in a multicloud system. It lets clients simultaneously use services from multiple clouds without prior business agreements among cloud providers, and without adopting common standards and specifications. As more organizations adopt cloud computing, cloud service providers (CSPs) are developing new technologies to enhance the cloud's capabilities. Cloud mashups are a recent trend; mashups combine services from multiple clouds into a single service or application, possibly with on-premises (client-side) data and services. This service composition lets CSPs offer new functionalities to clients at lower development costs.

Advantages:

The specific security issues associated with collaboration among heterogeneous clouds include:

• establishing trust among different cloud providers to encourage collaboration;

• addressing policy heterogeneity among multiple clouds so that composite services will include effective monitoring of policy anomalies to minimize security breaches;

• maintaining privacy of data and identity during collaboration.

PROBLEM STATEMENT:

Policy inconsistencies can result in security and availability problems; they include the following:

• Contradiction. Two policies are contradictory if they have different effects on the same subjects, targets, and conditions. Contradictions are the most common form of policy conflicts.

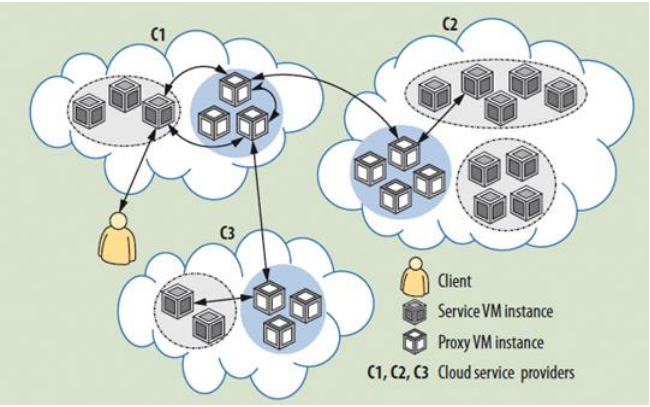
• Exception. A policy is an exception of another policy if they have different effects, but one policy is a subset of the other. The exception might not be a policy conflict, but access policy evaluation mechanisms commonly use exceptions to exclude a specific access request from general access permission.

• Correlation. Two policies are correlated if they have different effects but intersect each other. In this case, one policy permits the intersection, but the other does not. This is a partial policy conflict.

Scope:

Future research directions for the proposed framework include refining the proxy deployment scenarios and development of infrastructural and operational components of a multicloud 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.

Architecture:



Module Description:

Number of Modules

After careful analysis the system has been identified to have the following modules:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

1. Collaboration Framework For Multicloud System Module.
2. Client/Users Module.
3. Cloud Service Provider Module.
4. Proxy Service Provider Module

1. Collaboration Framework For Multicloud System Module:

Cloud collaboration allows clients and cloud applications to simultaneously use services from and route data among multiple clouds. This framework supports universal and dynamic collaboration in a multicloud system. It lets clients simultaneously use services from multiple clouds without prior business agreements among cloud providers, and without adopting common standards and specifications.

2. Client/Users Module:

Client sends a request to cloud C1, which dynamically discovers the need to use services from clouds C2 and C3. C1 employs proxies to manage these interactions. A client that wishes to simultaneously use services from multiple clouds must individually interact with each cloud service, gather intermediate results, process the collective data, and generate final results. Proxies can facilitate collaboration without requiring prior agreements between the cloud service providers. First, the requesting entity chooses proxies to act on its behalf and to interact with cloud applications. A client or a CSP might employ multiple proxies to interact with multiple CSPs. It can select proxies based on, for example, latencies between proxies and clouds or workload conditions at various proxies.

3. Cloud Service Provider Module:

Cloud service providers (CSPs) deploy proxies as an autonomous cloud system and offer it as a service to clients. A client employs two proxies to interact with CSPs C1 and C2. Alternatively, a client initiates a service request with C1, which then discovers the need for a service from C2. PSP: proxy service provider. Clients deploy proxies within the infrastructure of their organization. A client employs two proxies to interact with CSPs C1 and C2. A client initiates a service request with C1, which then discovers the need for a service from C2.

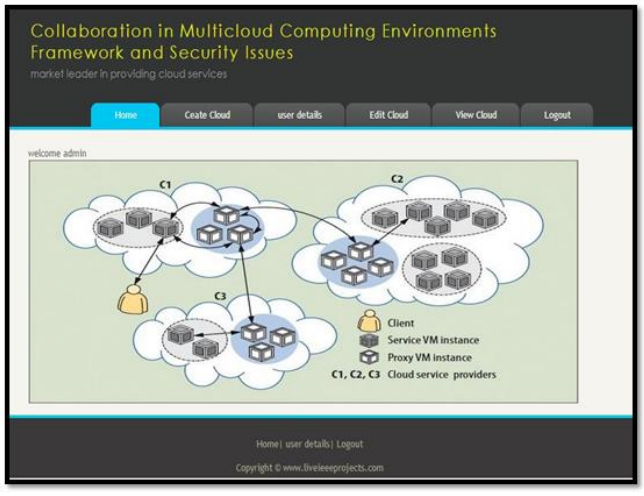
4. Proxy Service Provider Module:

It involves deploying proxies as an autonomous cloud that offers collaborative services to clients and CSPs. A group of CSPs that are willing to collaborate can manage this proxy-as-a-service cloud, or a third-party entity, a proxy service provider (PSP), can provide management. Clients directly subscribe to the proxy cloud service and employ them for intercloud collaboration. To protect data at rest and data in transit, proxies must provide a trusted computing platform that prevents malicious software from taking control and compromising sensitive client and cloud application data.

Screenshots:

Login:

Administrator: Home Page

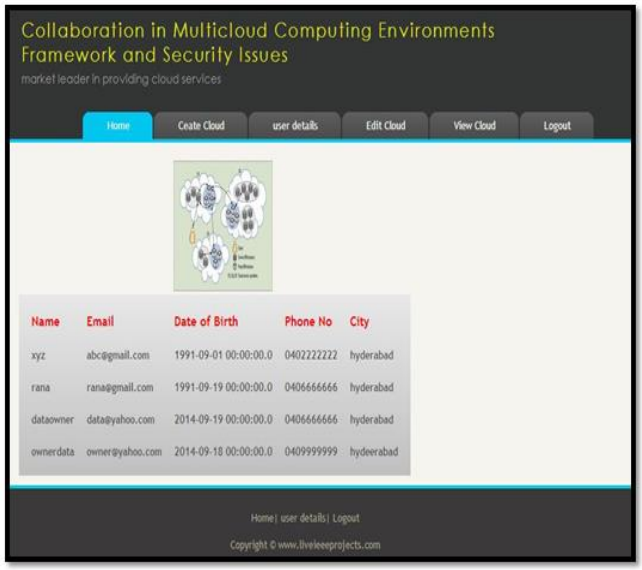


Administrator: Create Cloud

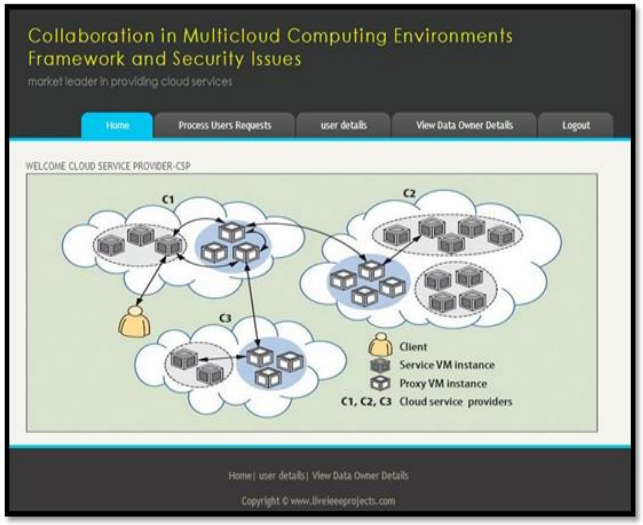
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Administrator: User Details

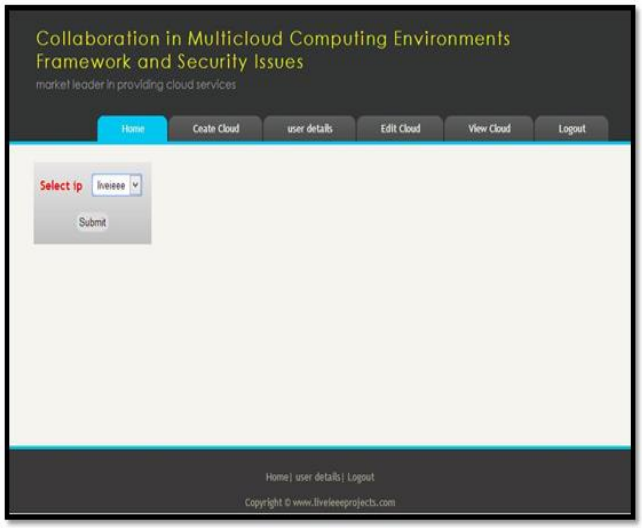
Cloud Service Provider (Csp): Home Page



Administrator: Edit Cloud



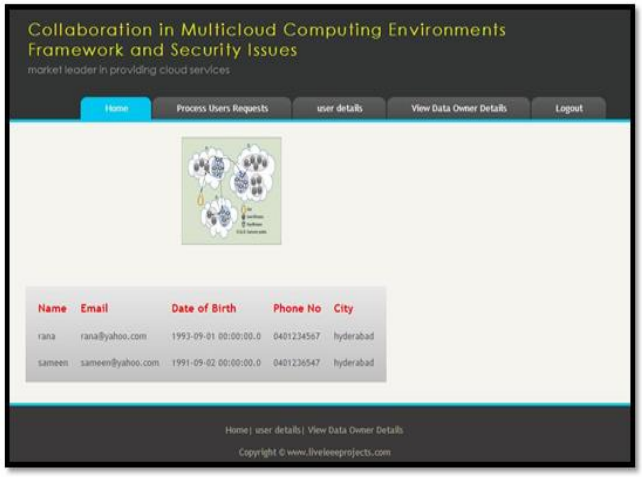
Cloud Service Provider (Csp): Process User Requests



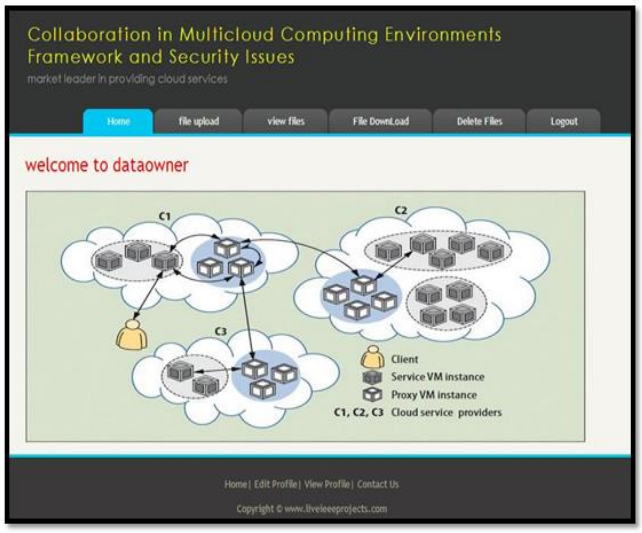
Administrator: View Cloud

Cloud Service Provider (Csp): User Details

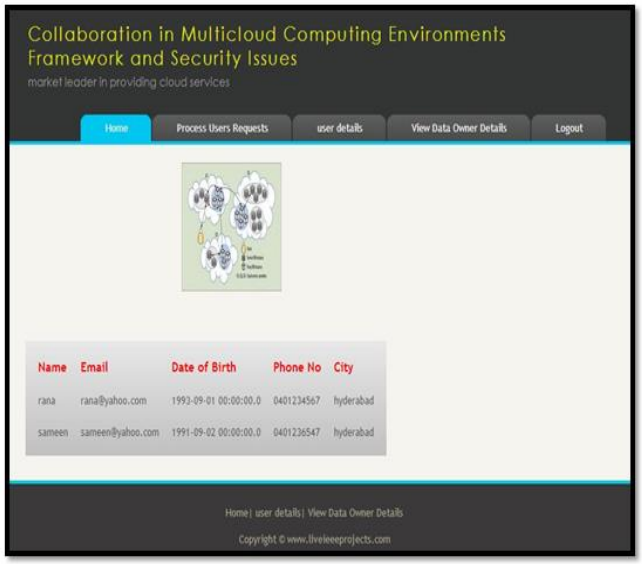
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



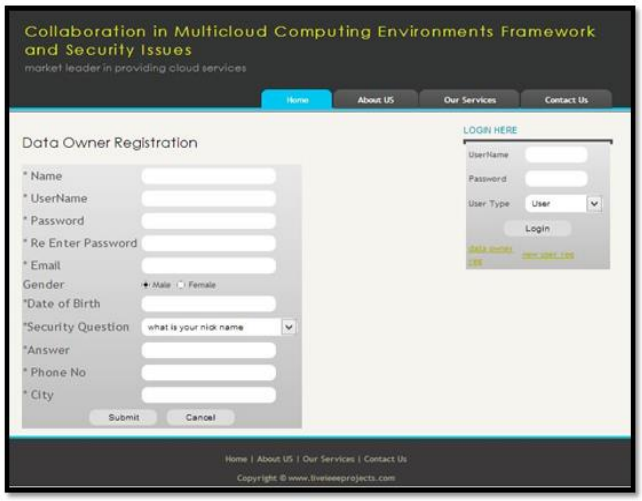
Cloud Service Provider (Csp): View Data Owner Details



Data Owner: File Upload

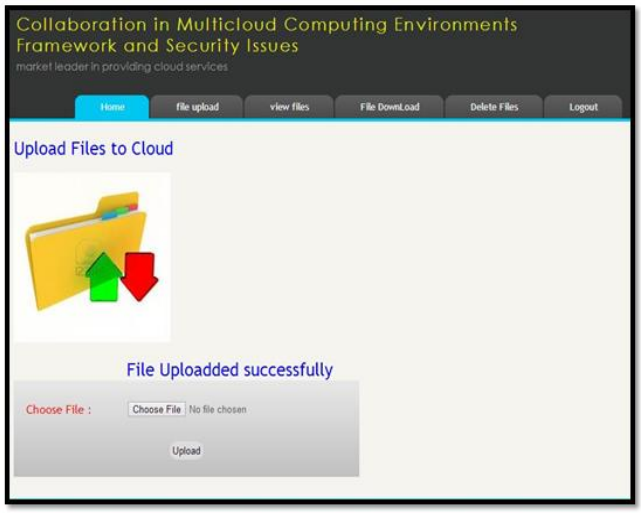


Data Owner: Registration



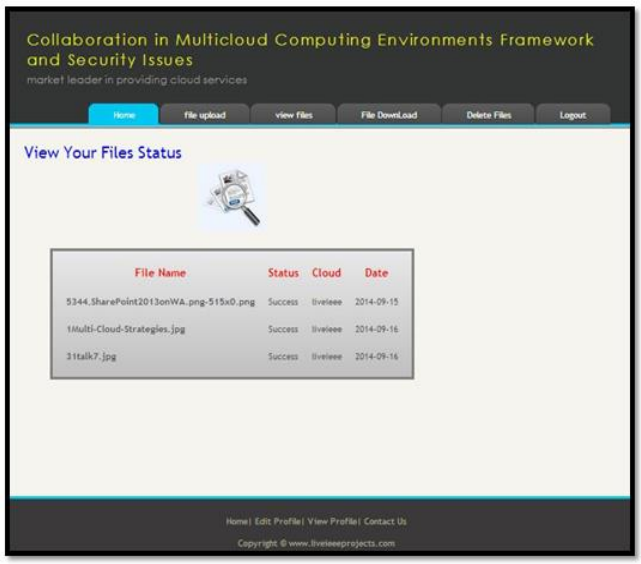
Data Owner: Home Page

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



Data Owner: View Files

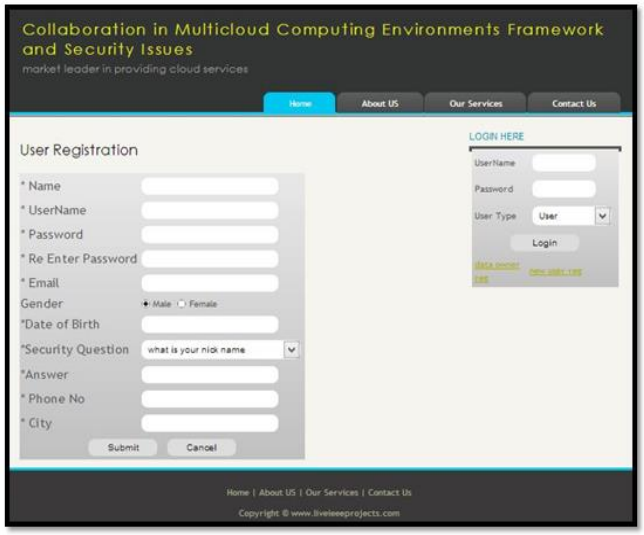
Data Owner: Delete File



Data Owner: File Request

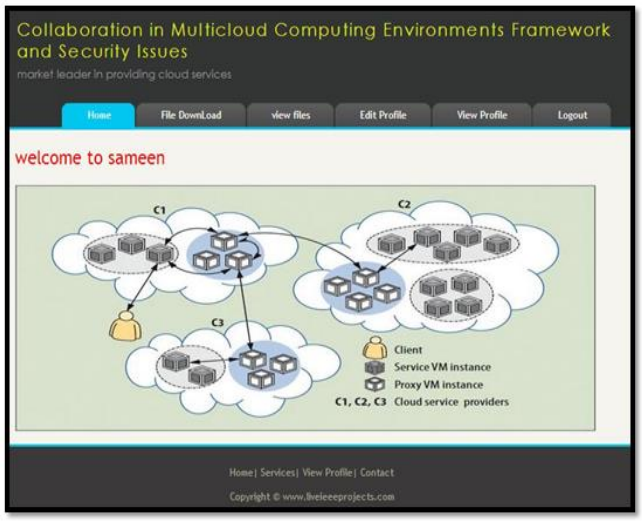
User: Registration

Data Owner: File Download

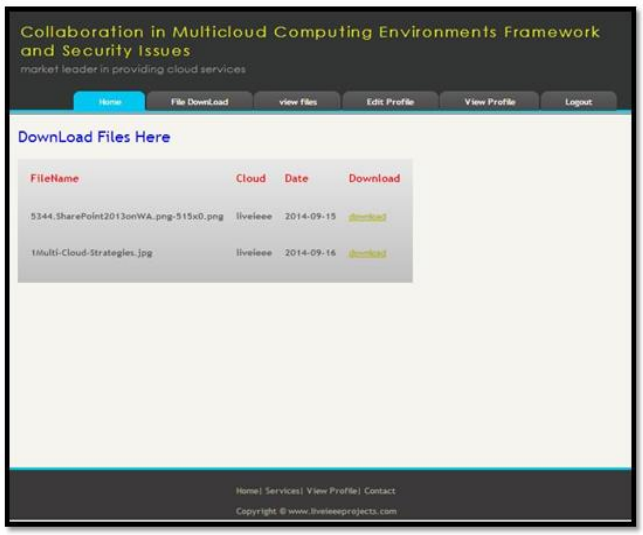


User: Home Page

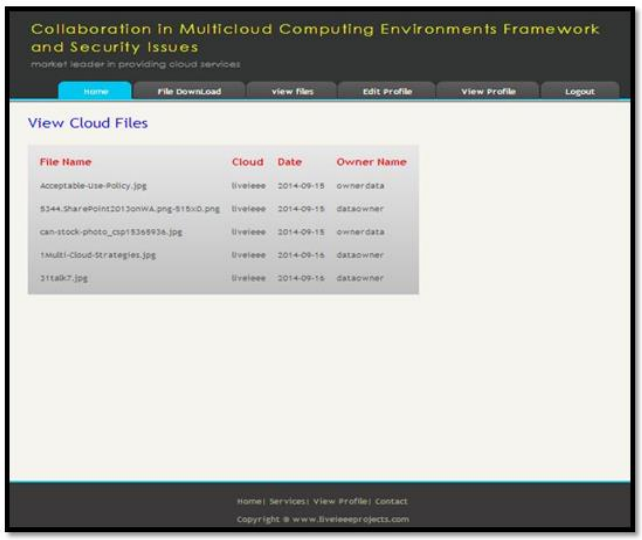
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



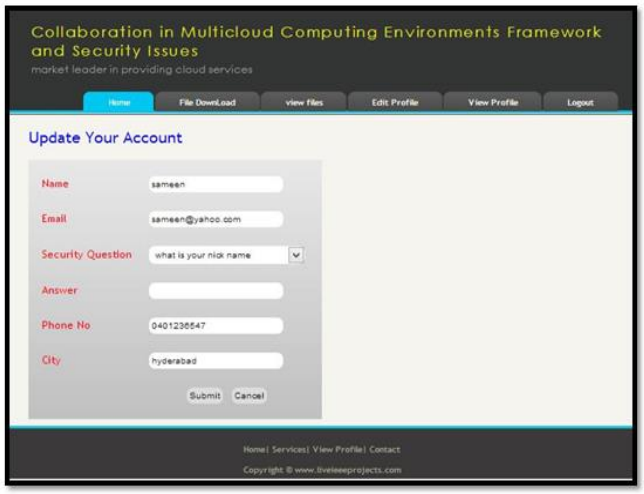
User: File Download



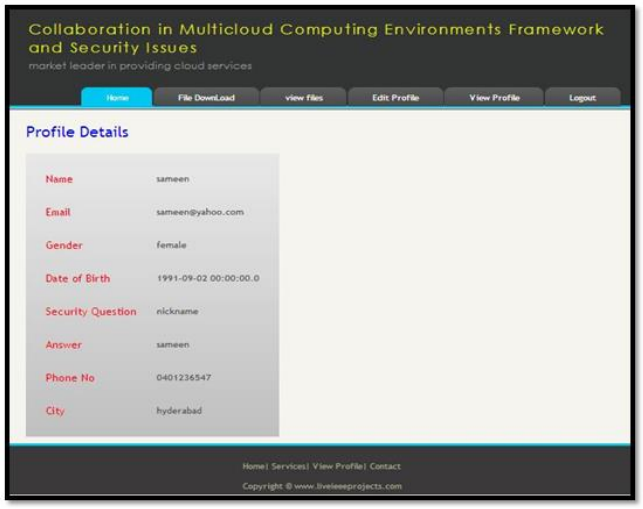
User: View File



User: Edit Profile



User: View Profile



Conclusion:

In this paper, we studied and implemented a secure multicloud computing which provides collaboration between clouds and gives the user opportunity to download the files from different cloud that are present. This also provides the security to the user's password and also to the files and data present in the cloud. The multi-cloud environment can end the vendor lock-in of the consumer which is a trait in the single cloud. The significant zone of concern in this field is the understanding between the cloud service providers for collaboration of their services in multi-cloud. The purchaser will get exceptionally profited with multi-cloud environment and acquire services dependent upon his inclination and prerequisite and not dependent upon his cloud service provider.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

References:

[1] 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"

[2] R. Thandeeswaran, S. Subhashini, N. Jeyanthi1, M. A. Saleem Durai, "Secured Multi-Cloud Virtual Infrastructure with Improved Performance", cybernetics and information technologies XII, (2), pp. 11-22, 2012

[3] Cong Wang, Student Member, Qian Wang, Student Member, Kui Ren, Senior Member, Ning Cao, and Wenjing Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE transactions on services computing, V, (2), 2012.

[4] Ayad Barsoum and Anwar Hasan, "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems", IEEE transactions on parallel and distributed systems.

[5] Fawaz Paraiso, Nicolas Haderer, Philippe Merle, Romain Rouvoy, Lionel Seinturier, "A Federated Multi-Cloud PaaS Infrastructure", 5th IEEE International Conference on Cloud Computing pp.392 – 399, 2012Published by IEEE Computer Society , Feb. 2013

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

[7] 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/cloud computing standards_ISPABDec2008_P-Mell.pdf.

[8] 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.

[9] S. Chandrasekhar et al., "Efficient Proxy Signatures Based on Trapdoor Hash Functions," IET Information Security, Dec. 2010, pp. 322-332.

[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