Need of Multi-Cloud Environment and Related Issues: A Survey

Sudheer Shetty
Associate Professor, Department of CSE, Sahyadri College of Engineering & Management, Mangaluru,
Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India
sudheershetty06@gmail.com

A P Manu
Professor, Department of CSE, PES Institute of Technology & Management, Shivamogga,
Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India
apmanu@gmail.com

Pavan Kumar V
Associate Professor, Department of IT, MLR Institute of Technology, Hyderabad,
Autonomous under Jawaharlal Nehru Technological University, Hyderabad, Telangana, India
sadgurupavan@gmail.com

Chanchal Antony
Assistant Professor, Department of CSE, A. J. Institute of Engineering & Technology, Mangaluru,
Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India
antonychanchal@gmail.com

Abstract - The cloud computing provides virtualized resources to the users on the basis of demand. The user need not setup an expensive computing environment in his premises, but obtains the services from the cloud service providers which are cost-effective in nature. Organizations and users have begun moving their files, software and services to cloud storage due to the availability of many services and scalability features. But, this transformation from local computing to remote computing brought many issues and challenges for both consumer and provider. The purpose of this paper is to provide a glimpse of cloud computing and the various issues faced by it. To overcome the various problems of cloud computing, multi-cloud collaboration is suggested in this paper. Further, few challenges related to security of multi-clouds such as trust, policy and privacy are discussed. The paper helps the reader understand the problems of cloud computing, how multi-clouds could resolve some of these issues and inspire multi-cloud platform building by looking into the security aspects of it.

Keywords – Cloud Computing, Data Centers, Virtual Machines, Multi-Cloud, Interoperability.

I. INTRODUCTION

Cloud computing is a distributed computing model developed in the year 2008 where computing is treated as a utility. Here, the customers can chose the resources like software, platforms, memory, CPUs, bandwidth, hardware load, security policies on the basis of pay-as-you-go manner similar to traditional public utility services such as water, electricity etc. This new technology enables the user to get the complete IT infrastructure in a completely virtualized manner from a remote place based on the demand. As a result, the industries started moving their computing resources from premises based data centers to public cloud computing environments.

The National Institute of Standards and Technology (NIST) defines cloud computing as a “model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [1]. This cloud model is composed of five essential characteristics, three service models and four deployment models. The essential characteristics are on-demand self service, broad network access, resource pooling, rapid elasticity and measured service as defined by NIST. Cloud provides three service deployment models which are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) to its users. Finally, NIST community defines a cloud deployment model which includes private, public, hybrid and community clouds. Cloud computing architecture is shown in Figure 1, which describes the three service models with examples.

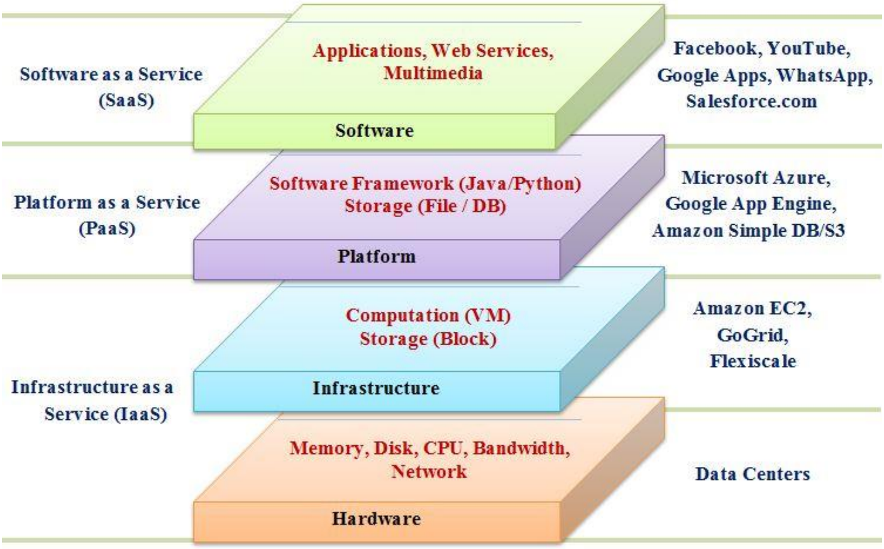
Software as a Service (SaaS)
Applications, Web Services, Multimedia
Software
Facebook, YouTube, Google Apps, WhatsApp, Salesforce.com
Platform as a Service (PaaS)
Software Framework (Java/Python) Storage (File / DB)
Platform
Microsoft Azure, Google App Engine, Amazon Simple DB/S3
Infrastructure as a Service (IaaS)
Computation (VM) Storage (Block)
Infrastructure
Amazon EC2, GoGrid, Flexiscale
Memory, Disk, CPU, Bandwidth, Network
Hardware
Data Centers

Figure 1. Cloud Computing Architecture

The cloud computing addresses many solutions to the users in a protected way. But, cloud computing technology involves several security issues. Therefore, the user needs to be aware of this while using the services of cloud. Many organizations adopt this emerging technology and day by day it has found its growth. But, at the same time, several security issues started building and organizations need to identify secure infrastructure to store their data. NIST identified that security, portability and interoperability are the major obstacles for the adoption of cloud computing. Since, security plays a major role among these; many organizations hesitate to transfer their sensitive data into cloud.

Though the standard, single cloud computing provides virtualized resources in a pay-as-you-go fashion over the Internet [2] and is an economical model for renting technical resources, it introduces some issues like

1. Service unavailability which leaves thousands of customers relying on it alone without access to critical resources.
2. It makes it difficult to incorporate sufficient responsiveness and usability for globally dispersed customers.

These prime factors influence the usage of multiple clouds to achieve better QoS, reliability and flexibility. Multi-cloud systems have more than one Cloud Service Providers (CSPs). Here, the clients utilize the services of more than one cloud for different applications in their businesses. They can store their valuable data on a private cloud, share documents on a public cloud and use another cloud to analyze data, for example. Such systems concurrently utilize a range of cloud networks and facilities.

Multi-cloud architecture is shown in Figure 2. Whenever, a client requests for a service, it is parsed by the client side interface and passed on to CSP side interface after processing by the middleware. The service request will be granted by one of the clouds based on the availability, underlying algorithms and request criteria. Selection of proper cloud on the basis of service request requires sophisticated technologies.

The rest of the paper is organized as follows. Related work and summary of literature is given in section II. Issues in cloud computing are presented in section III. Need and Issues of multi-cloud collaboration are explained in section IV. Concluding remarks are given in section IV.

II. RELATED WORK

A cloud always needs good internet connection flexible access and it is the responsibility of the CSPs to see that the user uses the existing bandwidth to get connectivity. The customer should be able to store and retrieve their valuable data as and when need it in the cloud. If its requirement is not met, the availability of data will be poor and its purpose will not be served. The CSP will be responsible for this and the customer's company will be adversely affected.

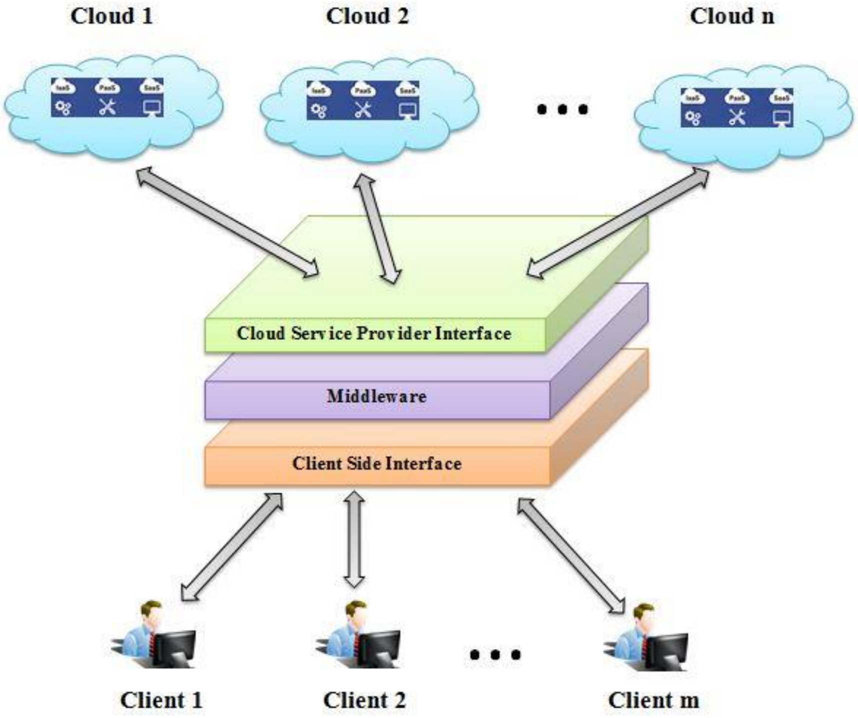

Figure 2. Multi-cloud Architecture

The problem can be resolved by tailoring multiple cloud service provider services. Whenever a specific service is broken, the service provider which provides multiple services will give the user the same access. Fox et al. [3] focused on this customer-friendly high availability service. Several obstacles with opportunities were listed here too. Service availability, data lock-in, data confidentiality & auditability, data transfer bottlenecks, performance unpredictability, scaling problems, software licensing, etc., are some of the challenges that require researcher's attention.

Ferrer et al. [4] highlighted the taxonomy of computing multiple clouds, but suggest multiple clouds aren't well known. They agree on two types of multiple cloud models: Federated cloud and Multi-cloud. This classification is made based on clients' interactions with clouds. There is an agreement in the federated cloud for sharing resources between different cloud providers where there is no such agreement in multi-cloud.

Petcu Dana [5] explored a number of reasons for need of multi-cloud services and resources. According to this, different kinds of actors are interested in different scenarios. Some common scenarios deal with demand peaks, reducing prices, responding to provider change of deals, ensuring disaster-related backups, using various specialty services, etc.

Buyya, Ranjan and Calheiros [6] noted that flexible provision of services under variable workload and network conditions can be accomplished through cloud interoperation. One would assume that with the idea of limitless resources and provisioning, the public cloud is enough to satisfy the customer requirements. But, this argument may not suit large-scale operators where they need good service quality to meet their needs. The authors emphasized the importance of interoperated clouds.

Rochwerger et al. [7] explained that most cloud providers provide their own proprietary frameworks, processes, and solutions for accessing tools and services. This heterogeneity can impose vendor lock-in problems where the customer is restricted to using the service provided by the existing cloud provider and cannot switch elsewhere. This particular problem can be solved with federated clouds that help to handle the load during peak time by sharing resources and supplying additional nodes or servers as required. In the contemporary cloud, interoperability requires greater attention. Some solutions have been mentioned for the resource contention problem in federated clouds and other distributed computing systems. Cloud infrastructure provider collaboration is not an easy job since they have separate administrative domains. The author discussed resource pooling ideas from various cloud providers and the development of the federated cloud.

The research by Le et al. [8] explored the possibility of lowering the cost and energy usage of multi-cloud data centers. A scenario of placing and migrating loads around geographically scattered data centers would cut costs due to time-based variations in electricity prices. Besides this, the required cooling can vary based on data center locations, and energy can be saved. Interoperation between such clouds would generally help in saving costs and power.

Toosi et al. [9] noted that the interoperability with multi-cloud can be achieved using service brokering or standard interfaces. Using the brokering mechanisms, the customers can switch to various cloud providers as and when they require. The service broker assists in exchanging messages between various interfaces in the multi-cloud. The analysis also discusses several mechanisms that contribute to the inter-cloud system standardization. However, it is difficult to adopt this standardization in practice, since cloud providers have distinct administrative approaches.

Singhal et al. [10] explained that collaboration across multi-cloud applications introduces new security concerns which may affect federated cloud overall performance. Some of the concerns include increased attack due to system complexity, loss of control over data and resources, data privacy issues, etc. Collaboration-related security issues are trust establishment with multi-cloud providers, addressing policy heterogeneity, privacy and data identity, etc.

Contention over resources is also an issue in federated cloud environments. Several solutions for resource contention in federated environments and other interconnected distributed computing systems have been detailed in [7], [11] and [12].

Mihailescu and Teo [13] explained the market-based methods for resource allocation in federated computing systems. The federated members of the cloud propose this dynamic pricing allocation scheme whenever user requests are successful. This in effect has a significant impact on consumer satisfaction and an improvement in the amount of available capital relative to the fixed pricing.

Goiri, Guitart and Torres [14] proposed a federated cloud model that assists in features such as when to outsource resources to federated members, when to admit requests from other members and how much contribution to the federation, etc.

In the inter-cloud scenario, Virtual Machine (VM) mobility is one of the cloud application specifications. The mobility of VMs should not infringe the independence of the respective clouds in terms of autonomy, privacy, and protection. Inter-cloud VM migration involves memory and state transfer between members of cloud providers, according to [15]. This requires a careful mechanism as it disrupts the privacy of independent cloud providers.

Users or applications that store data or resources in the cloud sometimes require access to services from other cloud service providers. Flexible transfer of resources or data from one CSP to another should take place, depending on the choice of the user. Users should have full control over their data so that trust can be established and a fully interconnected cloud environment can be created. Issues related to this are explained in [16].

It is difficult for users to transfer their data and resources to other vendors unless there is a standardized format acceptable to all vendors. Considerable costs and technical efforts must be made to move data if the cloud provider uses its own proprietary format. To avoid data lock-in, there should be a publicly documented data and resource storage standard. The lack of technology and standards currently hinders data portability and is explained by Petcu et al. [17].

There are a number of issues related to Service Level Agreements (SLA) in the federated cloud environment. There will be conflicting policies and objectives of the different members, which are very different from the overall objective of the federation. For example, if the federation provides a highly reliable service and none of the members is interested in offering that service, saying it is costly, and then there will be no consensus. Contrail [18] is a project that proposed a federated, integrated cloud architecture. As members of the federated cloud have their own SLA management system, Contrail tries to set up, coordinate and enforce the federation-level SLA.

The summary of literature is shown in Table - 1.

III. Issues in Cloud Computing

Cloud computing is always useful to businesses as it avoids the need for planned provisioning and ability to scale as per the needs. Although, there are several benefits in using cloud computing technology, there are some issues and challenges which need to be addressed too. Some of the basic issues in Cloud computing technology are

3.1 Security

This is a primary concern in every software system. There are several categories of security issues like safety issues, data confidentiality, cloud server monitoring, malicious attacks etc. The problems pertaining to data storage can be separated into components like data integrity, data confidentiality, data availability and data privacy. Maintaining data integrity involves ensuring that the data present cannot be deleted, updated or inserted without authorization. Data confidentiality deals with protecting important data from insider threats and external breaches. One more dimension of security is data availability which is a degree to which data can be recovered. Sharing the information privately and selectively amongst the users is data privacy.

3.2 Legal Issues

Data storage and access regulations are different for different geographical locations. Since, cloud servers are maintained at different parts of the world, a good standard for service selection need to be formulated. Although, there are service level agreements maintained between service providers and consumers, there is no guaranteed standard concerning legal issues. So, if consumer is not able to access his data from the cloud due to the local law of that place, conflict may start which affects his business. Therefore, a careful planning and coordination is essential while establishing these systems.

3.3 Data Management

For large organizations that rely on data storage, this is also a critical issue. What happens if the cloud system is unable to recover from a catastrophic failure? This is a complete or unexpected failure of machine or computer network where recovery is difficult to happen. If the important data stored in cloud providers is unable to recover, then the organizations will lose huge amount of their business. So, management and retrieval of critical data requires sophisticated architecture.

3.4 Interoperability

One more important aspect of cloud computing is interoperability where the different cloud providers work together to serve the needs of the customer. This is a challenging issue as these providers belong to different administrative domains. Of course, this is essential for flexible access of services and also to avoid vendor lock-in whereby users completely dependent on a single CSP. There is no proper standardization available where customers' data can easily be migrated between CSPs.

3.5 High Latency

This is a lag from when the transfer of data begins following an instruction for its transfer. As the data is stored in cloud, it always has some latency to get transferred to the clients' machine. Customers always expect an immediate response for their need of service. Some mechanisms for speedy data transfer are required with sophisticated networking technologies and protocols.

Table - 1: The Summary of Literature

Literature	Contribution	Future Perspective
Fox et al. [3]	• **Several obstacles in cloud computing like service availability, data lock-in, data confidentiality & auditability, data transfer bottlenecks, performance unpredictability, scaling problems, software licensing, etc. are listed and explained.**	• **Use multiple cloud providers for the continuity of business.** • **Deploy good encryption technologies, improve VM support, flash memory etc.**
Ferrer et al. [4]	• **Highlighted the fundamental challenges for wide adoption of cloud computing** • **Taxonomy of multi-cloud architecture is explained**	• **Develop a novel technology or toolkit for cloud service provisioning.**
Petcu Dana [5]	• **Explained the reasons for the need of services and resources from multi-cloud system.** • **Discussed Vendor lock-in issue of migrating from one cloud to another.**	• **Identify the technological barriers to enable the multi-cloud.** • **Devise suitable methods to resolve interoperability conflicts in Vendor lock-in problem.**
Buyya, Ranjan and Calheiros [6]	• **Emphasized importance of interoperated clouds.** • **Provisioning capabilities of few cloud platforms are summarized.**	• **Use Cloud brokers and Cloud coordinators for coordinating the members of interoperated clouds and users.** • **Develop comprehensive model driven approach for provisioning and delivering of services.**
Rochwerger et al. [7]	• **Highlighted that most cloud providers use their own proprietary frameworks for provisioning resources and services.** • **Explained some resource pooling ideas in developing federated cloud.**	• **Facilitate an open, service-based online economy in which resources and services are transparently provisioned and managed with high-quality of service.**
Le et al. [8]	• **Studied possibility of lowering energy consumption in cloud providers who operate at geographically distributed data centers.** • **Developed a model of data center cooling and simulated.**	• **Develop a similar model which helps in data center cooling in interoperated cloud environment.**
Toosi et al. [9]	• **Surveyed different aspects which enable interoperability among cloud providers along with technologies and mechanisms.** • **Focused on standardization initiatives in cloud interoperability.**	• **Develop federated and hybrid cloud environments having standard interfaces for service provisioning.** • **Facilitate novel methods of pricing and formation of inter-cloud market places.**
Singhal et al. [10]	• **Collaboration with multiple clouds introduces security concerns like increased attack, loss of control over data and data privacy issues etc.** • **Proxies can facilitate collaboration without the requirement of prior agreement between cloud service providers**	• **Refine proxy deployment scenarios and develop infrastructural and operational components of a multi-cloud system.** • **Implement an experimental platform using open source tools and libraries to evaluate the system functionalities of cloud service providers.**
Salehi, Javadi and Buyya [11]	• **Resource provisioning using queuing model in federated grid environment.** • **Introduced preemption-aware workload allocation policy for the users.**	• **Strategies to further reduce the number of VM preemptions by considering the co-allocation of the external requests on different clusters.**
Toosi et al. [12]	• **Proposed policies to increase profit of IaaS provider when it is a member of federated cloud.** • **Idle resources can be sold to other members of the federation when there is need.**	• **Devise policies for dynamic pricing of resources to offer idling capacity of the data center.** • **Strategies to shut down unused hosts of data centers to save energy consumption.**
Mihailescu and Teo [13]	• **Developed a dynamic resource pricing strategy on federated clouds.**	• **Refine dynamic pricing scheme using scalability as a factor.**
Goiri, Guitart and Torres [14]	• **Explained methods on saving capital and operational costs on federated clouds.**	• **Network bandwidth, storage and SLA's can also be considered for VM pricing.**
Nagin et al. [15]	• **Presented an inter-cloud VM mobility enablement technology.**	• **Refine further to include entire virtual applications.**
Fitzpatrick and Lueck [16]	• **Giving user the complete control over his data establishes trust on service providers.**	• **Authenticate before exporting sensitive data.** • **Develop mechanisms to deal with large data sets.**
Petcu et al. [17]	• **Focused on portability across clouds** • **Proposed a layered set of APIs that offers degree of freedom from programming languages and styles.**	• **Enhance technology and standards for flexible data portability.**
Carlini et al. [18]	• **Support horizontal integration of different cloud providers by distributing applications among them using negotiated SLA's.**	• **Devise methods to match overall objectives of the federation with the policies of individual members.**

3.6 Vendor Lock-in

This specific issue has been addressed by various authors where the client becomes dependent on a specific cloud provider. When a client loses trust over the existing CSP, he definitely wants to switch over to other CSPs. But, this will not happen easily as client is completely tied to that CSP. Vendor lock-in is a typical problem which happens due to lack of standardization with respect to operating platforms, Application Programming Interfaces (API) and Service Level Agreements (SLAs) [19]. Therefore, the client cannot easily shift his resources to another CSP for a better opportunity. The problem will be serious if a business hires a CSP and that provider goes bankrupt and the business is going to lose all the data stored in that CSP. Technologies on vendor-independent activities need to be envisaged to deal with this issue of cloud computing.

IV. NEED AND ISSUES OF MULTI-CLOUD COLLABORATION

Based on the Survey, several issues in cloud computing have been listed out. Multi-cloud collaboration may help in minimizing the effect of some of the issues. Of course, this collaboration also imposes new operations challenges and concerns. Operational overhead increases due to the management of multiple platforms with different sets of APIs and features. Delivery of services at multiple places with different interfaces and controls makes the system more expensive.

One of the issues which need much attention is security of multi-clouds and is explained below. Several security issues like isolation management, data exposure and confidentiality, VM security, trust, specific security concerns due to collaboration are discussed by many researchers and industry experts. In particular, issues pertaining to trust, policy and privacy are major concerns in multi-cloud environments and are discussed below.

4.1 Establishing Trust in Secure Service Selection

Trust is an important factor existing in any IT system for the secure exchange of information between entities involved [20]. In case of cloud computing, the client relinquishes control over data and services to the service provider. So, client loses complete control over it and has to trust the service provider. This imposes new set of issues which otherwise would not exist in the internal organization. The risks include insider security threats and reduced data ownership rights due to less knowledge of the security features of the service cloud provider. The client always needs to trust the CSP in cloud-based services with the help of SLAs.

The risk of trust establishment increases further in case of multi-cloud environment as the number of CSPs increases. In some multi-cloud environments, a proxy is involved as an intermediary for establishing connection and providing services. The operations of CSP and client are delegated to this proxy and it does the work on behalf of these entities. Now, one more additional level of security issue comes into picture as both CSP and client need to trust the proxy layer. The proxy’s availability, security, reliability etc., need to be known at both the ends. The proxies impose own set of problems, be it own-premise of client or at CSP. The client side proxy is controlled by the client where as CSP side proxy is owned by the CSP. So, issues occurring by the addition of a new component to the existing architecture need to be compromised by identifying new technologies and ideas. So, researchers need to evaluate the existing architecture and develop a comprehensive protocol so that users can trust the CSPs of multi-cloud architecture. For, establishing the secure connection to multi-cloud, OTP based multilevel authentication scheme can be used as suggested in [21].

4.2 Policy Inconsistency and Conflicts

Since CSPs have their own set of policies and administrative domains of operation, the collaboration into multi-cloud not an easy one to do. This inconsistency leads to conflicts and imposes new security breaches. Even if the policies are well-defined at individual CSPs, the integration among them is a challenge in moving towards a unique goal. The service request from the client leads to intense interactions between the CSPs with different domains. The set up of multi-cloud requires careful analysis of the differences between policy versions in individual CSPs. Policy integration must be carried out to bring agreement on access and issue rights. This is a careful process and requires a systematic approach to avoid conflicts.

The multiple participating parties must agree upon the common access policies to reflect security requirements in the complex and dynamic multi-cloud environments. The multi-cloud environment needs to adapt some dynamic algorithms to reflect change of policies among the CSPs. In case of proxy-based environment, the proxy needs to verify that policies are consistent throughout and in case of conflict; it must ensure that the security is not violated. The composition of policies from multiple CSPs results in a large collection of policies and proxy must put lot of efforts in bringing down the inconsistency among the CSPs. Otherwise, adverse effect may happen in the performance and security issues. Since, multiple requests arrive at the same time; suitable load balancing techniques in multi-cloud also need to be identified as explained in [22] and [23].

4.3 Client Data Privacy and Identity

Cloud data privacy is an important aspect where in the sensitive data of the client should not be shared among the people who are not authorized to use. When the data is stored in multi-cloud, there should be a mechanism to deal with the privacy and identity of data. In order to protect anonymity, clients need to mask their identity attributes from CSPs when the volume of data is highly sensitive. Suitable data encoding techniques should be used to prevent unauthorized access during transfer and storage of data in clouds. This degree of privacy and encoding techniques will be much costlier if data is stored in multiple clouds.

The data privacy methods used should be applicable to any number of CSPs irrespective of the amount of data to be handled. Some compression methods can be used to handle large amount of data so that data transfer and storage issues will be reduced. The multi-cloud scenario always requires new data privacy solutions as more number of CSPs is involved.

V. CONCLUSION

Cloud computing is an emerging technology having lot of applications from the industry point of view. Many of the industries are shifting their IT infrastructure to cloud environment. It has the benefit of quick deployment, access anytime and anywhere, large storage, cost efficiency etc. This is a technology which is widely accepted by all in a short span of time. However, there are some security and privacy concerns to adopt the cloud computing. The amount of these concerns increase in case of multi-cloud environment as the system complexity is high.

In this paper, a survey of issues related to cloud computing and multi-cloud collaboration is discussed. The table presented the future perspective of the cloud computing. The primary issues and challenges in building cloud computing environment are focused. Subsequently, to overcome these issues, need of multi-cloud collaboration is suggested. Finally, the important security issues of multi-cloud environment such as trust, policy and privacy are discussed.

REFERENCES

[1] Mell, Peter, and Tim Grance. "The NIST definition of Cloud Computing." (2011).

[2] Buyya, Rajkumar, Chee Shin Yeo, Srikumar Venugopal, James Broberg, and Ivona Brandic. "Cloud Computing and Emerging IT Platforms: Vision, hype and Reality for Delivering Computing as the 5th Utility." *Future Generation Computer Systems* 25, no. 6 (2009): 599-616.

[3] Fox, Armando, Rean Griffith, Anthony Joseph, Randy Katz, Andrew Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, and Ion Stoica. "Above the Clouds: A Berkeley View of Cloud Computing." *Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS* 28, no. 13 (2009): 2009.

[4] Ferrer, Ana Juan, Francisco HernáNdez, Johan Tordsson, Erik Elmroth, Ahmed Ali-Eldin, Csilla Zsigri, RaüL Sirvent et al. "OPTIMIS: A Holistic Approach to Cloud Service Provisioning." *Future Generation Computer Systems* 28, no. 1 (2012): 66-77.

[5] Petcu, Dana. "Multi-Cloud: Expectations and Current Approaches." In *Proceedings of the 2013 International Workshop on Multi-cloud Applications and Federated Clouds*, pp. 1-6. 2013.

[6] Buyya, Rajkumar, Rajiv Ranjan, and Rodrigo N. Calheiros. "Intercloud: Utility-oriented Federation of Cloud Computing Environments for Scaling of Application Services." In *International Conference on Algorithms and Architectures for Parallel Processing*, pp. 13-31. Springer, Berlin, Heidelberg, 2010.

[7] Rochwerger, Benny, David Breitgand, Eliezer Levy, Alex Galis, Kenneth Nagin, Ignacio Martín Llorente, Rubén Montero et al. "The Reservoir Model and Architecture for Open Federated Cloud Computing." *IBM Journal of Research and Development* 53, no. 4 (2009): 4-1.

[8] Le, Kien, Ricardo Bianchini, Jingru Zhang, Yogesh Jaluria, Jiandong Meng, and Thu D. Nguyen. "Reducing Electricity Cost through Virtual Machine Placement in High Performance Computing Clouds." In *Proceedings of 2011 International Conference for High Performance Computing, Networking, Storage and Analysis*, pp. 1-12. 2011.

[9] Toosi, Adel Nadjaran, Rodrigo N. Calheiros, and Rajkumar Buyya. "Interconnected Cloud Computing Environments: Challenges, Taxonomy, and Survey." *ACM Computing Surveys (CSUR)* 47, no. 1 (2014): 1-47.

[10] Singhal, Mukesh, Santosh Chandrasekhar, Tingjian Ge, Ravi Sandhu, Ram Krishnan, Gail-Joon Ahn, and Elisa Bertino. "Collaboration in Multicloud Computing Environments: Framework and Security Issues." *Computer* 46, no. 2 (2013): 76-84.

[11] Salehi, Mohsen Amini, Bahman Javadi, and Rajkumar Buyya. "QoS and Preemption Aware Scheduling in Federated and Virtualized Grid Computing Environments." *Journal of Parallel and Distributed Computing* 72, no. 2 (2012): 231-245.

[12] Toosi, Adel Nadjaran, Rodrigo N. Calheiros, Ruppa K. Thulasiram, and Rajkumar Buyya. "Resource Provisioning Policies to Increase IaaS Provider's Profit in a Federated Cloud Environment." In *2011 IEEE International Conference on High Performance Computing and Communications*, pp. 279-287. IEEE, 2011.

[13] Mihailescu, Marian, and Yong Meng Teo. "Strategy-proof Dynamic Resource Pricing of Multiple Resource Types on Federated Clouds." In *International Conference on Algorithms and Architectures for Parallel Processing*, pp. 337-350. Springer, Berlin, Heidelberg, 2010.

[14] Goiri, Íñigo, Jordi Guitart, and Jordi Torres. "Economic Model of a Cloud Provider Operating in a Federated Cloud." *Information Systems Frontiers* 14, no. 4 (2012): 827-843.

[15] Nagin, Kenneth, David Hadas, Zvi Dubitzky, Alex Glikson, Irit Loy, Benny Rochwerger, and Liran Schour. "Inter-cloud Mobility of Virtual Machines." In *Proceedings of the 4th Annual International Conference on Systems and Storage*, pp. 1-12. 2011.

[16] Fitzpatrick, Brian W., and J. J. Lueck. "The Case against Data Lock-in." *Communications of the ACM* 53, no. 11 (2010): 42-46.

[17] Petcu, Dana, Georgiana Macariu, Silviu Panica, and Ciprian Crăciun. "Portable Cloud Applications—from Theory to Practice." *Future Generation Computer Systems* 29, no. 6 (2013): 1417-1430.

[18] Carlini, Emanuele, Massimo Coppola, Patrizio Dazzi, Laura Ricci, and Giacomo Righetti. "Cloud Federations in Contrail." In *European Conference on Parallel Processing*, pp. 159-168. Springer, Berlin, Heidelberg, 2011.

[19] Hong, Jiangshui, Thomas Dreibholz, Joseph Adam Schenkel, and Jiaxi Alessia Hu. "An Overview of Multi-cloud Computing." In *Workshops of the International Conference on Advanced Information Networking and Applications*, pp. 1055-1068. Springer, Cham, 2019.

[20] Singh, Ashish, and Kakali Chatterjee. "Cloud Security Issues and Challenges: A Survey." *Journal of Network and Computer Applications* 79 (2017): 88-115.

[21] Thorwat, Ms Priya D., and Mr Sudheer Shetty. "Implementation of Multilevel Authentication Scheme for Multicloud Environment." *International Journal of Computer Applications* 975 (2014): 8887.

[22] Shetty, Sweekriti M., and Sudheer Shetty. "Analysis of Load Balancing in Cloud Data Centers." *Journal of Ambient Intelligence and Humanized Computing* (2019): 1-9.

[23] Sweekriti, Shetty. "S.: Distributed and Dynamic Load Balancing in Cloud Data Center." *Int. J. Comput. Sci. Mobile Comput. IJCSMC4* 5 (2015).