# Security and Privacy for Group Data Sharing in the Multi-cloud Node Environment

**Sandeep Srinivas Dwaram, Manisha Yeruva**

***Abstract*— Time and Trend has its own significance to build the technology smarter, better and easier to the end user. To the Better stretch of the Information Technology, the Innovation and renovation has changed computing approach to the next level. In this paper, we try to give the glimpse of the contextual virtual cloud storage in the public data distribution. These days cloud storage become common, but having the constraint towards the technical advancement is the Security. If we consider behavioral aspect of the cloud storage, we will come across much aspect. Hence, In this one we have overcome the public protection in terms of the privacy towards the authorization of public audit, which we call it as the best to the trend of the acknowledgement based identification with the cryptographic model where ever the node to the parallel cloud distributed elastic stretchable environment with the high end cloud data center marinating the graphics of the flow triggering the security in the public Domain. In this we have implemented the node based Architectural model with acknowledgement encrypted based on the level of the data to these data moved in the network with the classification of the node based data in the preview model of the datacenter to monitor the traffic of the data and the shortest path Mechanism.**

***Index Terms*—Searchable encryption, data sharing, cloud storage, data privacy**

## I. INTRODUCTION

Technology and its advancement lead us to research for the next level of the advancement. In the context of the Cloud computing which we can tell as the technological advancement plays the vital role in the industry of Information Technology. In the modern age of the cloud computing generation, the idea of cloud

Computing is almost as old as the computer itself. Its principle is to have the user's computer, Smartphone, tablet or any internet-connected device acting as a front-end displaying an application, as the resources connected in remote servers. Regarding data confidentiality, all three providers claim that they provide and support encryption. Many cloud providers allow their customers to encrypt data before sending it to the cloud. For instance, Amazon S3 makes it optional to users to encrypt data for additional security, but not recommended in the case of third party or external auditors depending on the model of service they are offering. The first model is the Infrastructure as a service (IaaS), which is the most basic model. The IaaS model consists in providing Virtual Machines to the clients whom will have to install operating systems as well as their applications on top of the vendors providers like Amazon EC2, Google Compute Engine .Today's data centers are already containing thousands of servers, and this number is very likely to increase during the forthcoming years. Furthermore, the customers can request the creation or the removal node to meet their needs.


**Fig.1.1. Tiered structure of the cloud**

Therefore, the networks are highly elastic and can reach an immense number of traffic. Because of that,

***Sandeep Srinivas Dwaram,** (M.Tech) Computer Science &Technology,ANU,Rajahmundry, INDIA, 533103.*
***Manisha Yeruva**, (B.Tech) Computer Science & Engineering, GIERCollegeofEngineering, ,Rajahmundry INDIA, 533103*



ISSN: 2278 – 7798 

networks architecture has to be scalable in order to ensure a good performance whatever number of VIRTUAL is running in the network.

## II. RELATED WORK

In the IaaS model, the customers to dynamically scale up and down to as many machines as needed inside the cloud in a “pay-as-use" manner. The clients can dynamically provision resources to meet the current demand by adjusting their leasing of resources from the cloud provider. Customers can also then use more efficient hardware without being preoccupied by its maintenance, cooling and storage. In each model, the cloud providers can use multi-tenancy, where virtual machines from multiple customers can share the same sets of physical servers and the network, in order to reduce the waste of resources. However, economies of scale are so important that their users benefit from both aspects like efficient and cheaper solution.

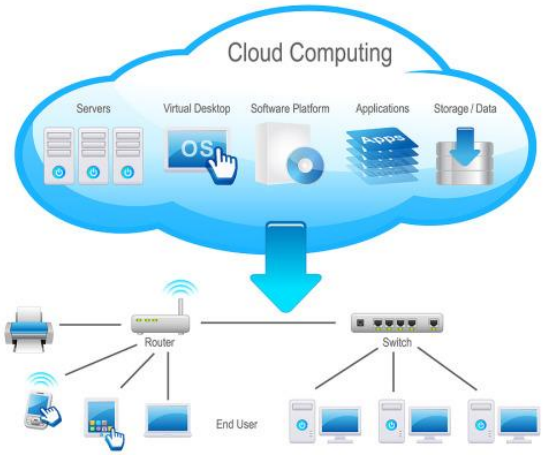


**Fig.2.1. Illustration of the Centralized cloud node**

Due to the of an ever growing number of people connected to the internet, the constant evolution of computer science along with the decreasing of hardware prices, the use of cloud computing instead of classic networks architecture has recently become a reality. In order to optimize the resources in the data centers or for maintenance reasons, cloud providers often have to migrate from the physical server to another. Migrations are used in order to pool the active and then reduce the number of turned on physical servers inside the data center, in order to reduce cost. Migrations also reveal themselves handy when there is a hardware problem on a physical server, for example. The running on this server is moved to other physical servers and the alleged deficient server can be turned off and replaced. The impact of node migration on the network is important. Since the virtualization is potentially moving from a physical server to another, the routes between them are also impacted, and the topology of the network is thus changing. Most importantly, the end points of the routes are changing. This causes the need to reconfigure the network with each migration.

## III. METHODOLOGY

In this paper, we have given emphasis on the Privacy and Security involved in the multi-cloud architecture. The big threat to cloud is the security which has not yet robust and need much more advancement to give the client that is the best solution especially in the industry domain of banking and financial services. The advancement of the technology and its usefulness makes us to research the best of the best service for the automation world more precisely the cloud computing security can be breached by several actors. In the cloud, there are the cloud provider and the tenants. Our project aims to secure the traffic of a tenant. In this situation, this traffic could first be threatened by other tenants. Indeed, malicious tenants could be willing to access data of other tenants or to gain access to their network by using techniques such as ARP cache poisoning or IP spoofing. Furthermore, a configuration of routing appliances could lead to a breach in confidentiality. The other threat comes from inside the tenant's network itself. This threat is the most important one in security today, as malicious software can enter the enterprise network downloaded by the employees browsing the internet. In the enterprise network, the traffic is secured by the traversal of virtual middle boxes along the path. Our project aims to create a framework enabling the traversal of virtual middle boxes despite the elastic nature of the cloud, meanwhile providing isolation of traffic in order to prevent the risk of an attack by another tenant. The switches between the source switch and the first ingress switch will all have the same type of rule. Based on the, the packet will be routed to a particular port.

This port has been calculated during the route calculation. At the ingress switch of a virtual middle box, the rule will consist in matching one attribute and applying two actions. The matching attribute is obviously the tag corresponding to the virtual middle boxes. The packet must then be sent to the virtual middle boxes, but before that, the tag must be popped, so the virtual middle boxes receive an unmodified packet. The progress switch of the virtual middle boxes will receive an untagged packet. The policy management in a secure enterprise network today can therefore be quite complex. For instance, it may require restricting a machine containing



ISSN: 2278 – 7798 

sensitive data to be accessed only by a small group of users, or preventing external traffic from directly reaching internal servers.

The actual realization may involve servers having complex communication patterns governed by network access control, such as the traversal of several virtual middle boxes before being reached. When enterprises decide to move to the cloud, they want to keep the same requirements regarding their policy management. It would be possible for the network manager of the enterprise to implement the virtual middle boxes and the routing policies on in the same way as before moving to the cloud. However, one of the goals of moving to the cloud is to escape the burden of network administration and configuration. Furthermore, the type of security policies in place in enterprises networks is often quite similar as it consists in the traversal of several virtual middle boxes.

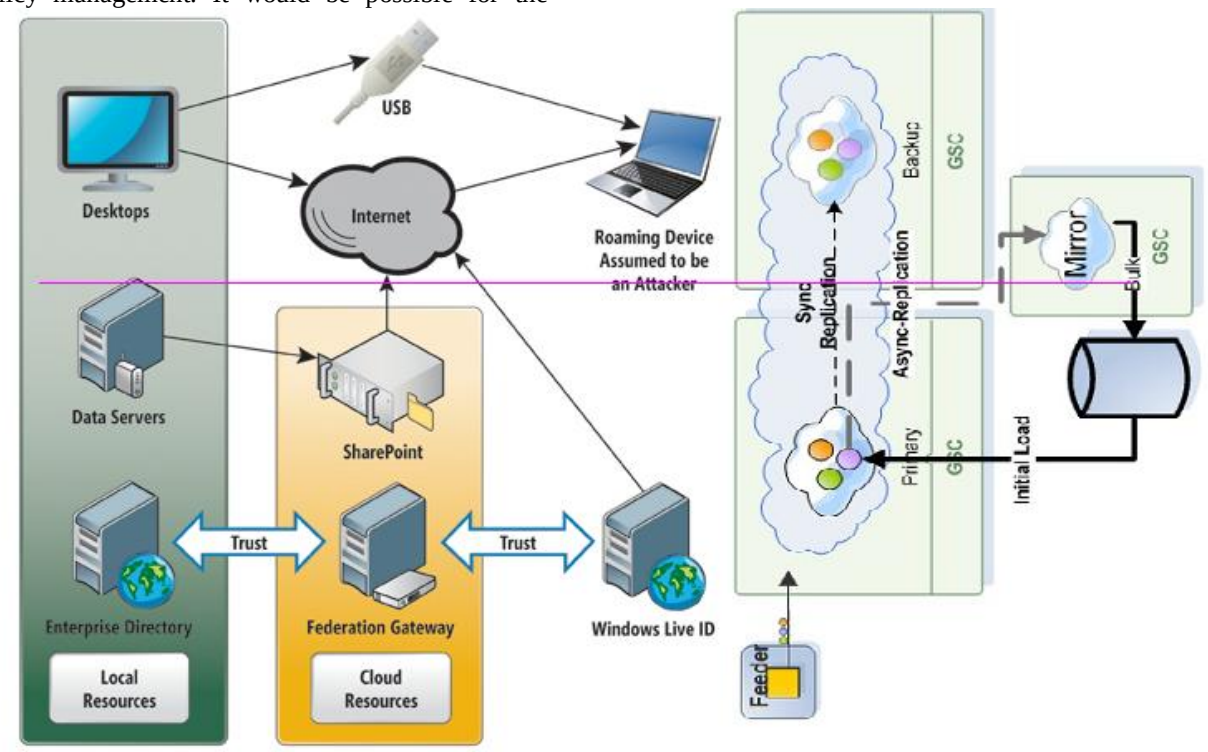


**Fig.3.1. Multi- Cloud Architecture design involves the Agility platform**



ISSN: 2278 – 7798 

A tenant could be attacked by the cloud provider or by other clients. The cloud provider could be attacked by tenants. Our project does not consider the situation where the provider is malicious. Indeed, we suppose that the cloud provider is honest. We further suppose that all network appliances are compliant and secure. Based on the source and destination field, as well as the port from which the packet arrived, the controller will have to push the down to the packet. A second rule consists in matching this tag and to route the packet to the adequate port. The rules set in the forthcoming switches are the same as previous, until we reach the last virtual middle boxes. From the progress switch of the last virtual middle boxes to the destination switch, there are two cases. First, the destination machine is located in the current zone, and the destination switch is connected to the destination machine. In that case, the routing in the last segment is done by matching the destination address. Network security is a key aspect in designing modern applications.

## IV. EVALUATION AND ANALYSIS

We can see that in both cases, the security policy has been reconfigured automatically after migration. The middle box sequences have been applied accordingly to the Application ID present in the packet, even though the instances traversed have changed. We chose to show both these cases of migration in order to demonstrate that *all or part* of the traversed middle box instances can be modified.Our model allows us to dynamically enforce security policies in a multi-tenant cloud network. In addition, the security policies stay coherent in spite of the node migration. So as to create a prototype of our network controller, we had to implement several modules in order to demonstrate the relevance of our policy enforcement mechanism. Particularly, a routing protocol has been implemented in order to figure out the route from the source to the destination, throughout the virtual middle boxes.

## V. CONCLUSION AND FUTURE WORK

Apart from the above mentioned domain other domains are fair and fine enough to us the technology. In this one we use the data partitioning and the security of the node and agent based cryptography, which will provide the tiered or layered security. In the context of the security; particularly, we considered the criteria of scalability and auto in a context where the network is shared by multiple tenants and the migration of nodes are increasing with the number of request. We first considered the different existing solutions in order to differentiate the traffic between the different tenants, as the isolation between tenants is the basis of a secure network. There are many solutions allowing traffic separation. However, the precision of these solutions varies greatly, as the isolation can be made from a complete separation of physical network and automatic centralized control of the network. We then analyzed the way security policies are defined and enforced. The security policies are defined in several ways. Some solutions focus on the isolation only or the routing rules and their consistency, whereas other architectures put more emphasis on the traversal of virtual middle boxes.

## 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] F. Gens, "IT Cloud Services User Survey, pt.2: Top Benefits & Challenges," blog, http://blogs.idc.com/ie/?p=210, 2008.

[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-VIRTUAL Side Channels and Their Use to Extract Private Keys," Proc. ACM Conf. Computer and Comm. Security (CCS '12), pp. 305-316, 2012.

[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] M. McIntosh and P. Austel, "XML Signature Element Wrapping Attacks and Countermeasures," Proc. Workshop Secure Web Services, pp. 20-27, 2005.

[11] J. Kincaid, "Google Privacy Blunder Shares Your Docs without Permission," TechCrunch, http://techcrunch.com/2009/03/07/huge-google-privacy-blunder-shares-your-docs-withoutpermission/, 2009.

[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.

[13] 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.

[14] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, "Blueprint for the Intercloud—Protocols and Formats for Cloud Computing Interoperability," Proc. Int'l Conf. Internet and Web Applications and Services, pp. 328-336, 2009.

[15] 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.

[16] R. Turpin and B.A. Coan, "Extending Binary Byzantine Agreement to Multivalued Byzantine Agreement," Information Processing Letters, vol. 18, no. 2, pp. 73-76, 1984.

[17] I. Koren and C.M.C. Krishna, Fault-Tolerant Systems. Morgan Kaufmann, 2007.



**Sandeep Srinivas Dwaram,**He had completed his B.Tech.degree in Information Technology at SRM university in the year 2011.He had worked with MNC companies like TCS and Mindcraft.He is currently Pursuing final year of M.Tech in Computer Science Technology at ANU, Rajahmundry .His research interests are Information Security, ComputerNetworks, Parallel& Distributed Systems and Cloud Computing.



**Manisha Yeruva,** she is currently pursuing final year of B.Tech in Computer Science and Engineering at GIER College of Engineering, Rajahmundry. Her research interests are Information Security and Computer Networks.