ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

# Guarding Approach for Storing Secrete Data Over Cloud

[I]Akhil Kumar Tripathi, [II]S. Aravinth Kumar, [III]Avinash Kumar
[I,III]M.Tech, Dept. of SCSE, Galgotias University, Greater Noida, India
[II]Asst. Professor, Dept. of SCSE, Galgotias University, Greater Noida, India

**Abstract**
*The emerging of cloud is increasing the use of web- connected devices which is resulting in huge numbers of threats due to many mischievous attackers and hackers. So we need to make the cloud more secure. The major security challenge with cloud is that the owner of the data may not have control of where the data is placed. This may lead to the violation of government law for data storage in a particular country or continent. Also there is a need to store data over cloud in encrypted form to safeguard ourselves from any dishonesty that might be shown by the Cloud Service provider. I want to suggest ways to overcome the problem of data storage location over the Cloud.*

**Keywords**
*Government Policies, Virtualization, Padlock.*

## I. Introduction

There is a great need for securing secret data on cloud storage servers. The need comes with the privacy of cloud user who intends to keep their personal data secure even from the cloud service provider. The storage of data over remote server is the term which comes when the client needs to use its resource at minimal level. This critical nature of remote storage enforces need for making cloud more secure. The major security challenge with clouds is that the owner of the data may not have control of where the data is placed [2]. This led to implementation of two things that is resource allocation and scheduling. There is a need to encrypt the data before sending over the cloud to get less affected by any untrusted activity that might come from cloud service provider.

### A. Security Issues for Clouds [2]

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that Interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing results in several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds. We have extended the technologies and concepts we have developed for secure grid to a secure cloud. We have defined a layered framework for assured cloud computing consisting of the secure virtual machine layer, secure cloud storage layer, secure cloud data layer, and the secure virtual network monitor layer (Figure 1). Cross cutting services are provided by the policy layer, the cloud monitoring layer, the reliability layer and the risk analysis layer.

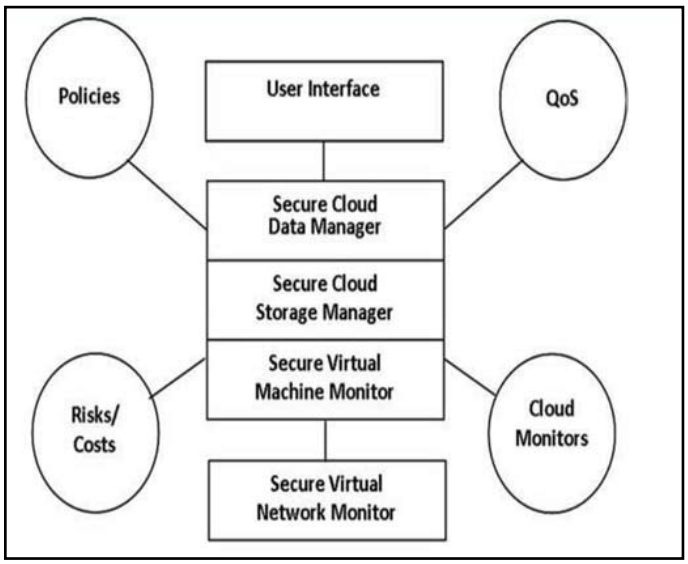

Fig. 1: Layered framework for assured cloud

1) Secure Virtual Machine (VM) Monitor: We are combining both hardware and software solutions in virtual machines to handle problems such as key logger examining XEN developed at the University of Cambridge and exploring security to meet the needs of our applications (e.g., secure distributed storage and data management).

2) Secure Cloud Storage Management: we are developing a storage infrastructure which integrates resources from multiple providers to form a massive virtual storage system. When a storage node hosts the data from multiple domains, a VM will be created for each domain to isolate the information and created and allocated to storage nodes, we are investigating corresponding data processing. Since data may be dynamically secure VM management services including VM pool management, VM diversification management, and VM access control management. Hadoop and MapReduce are the technologies being used.

3) Secure Cloud Data Management: We have developed secure query processing algorithms for RDF (Resource Description Framework) and SQL (HIVE) data in clouds with an XACML-based (eXtensible Access Control Markup Language) policy manager utilizing the Hadoop/MapReduce Framework.

4) Secure Cloud Network Management: Our goal is to implement a Secure Virtual Network Monitor (VNM) that will create end-to-end virtual links with the requested bandwidth, as well as monitor the computing resources.

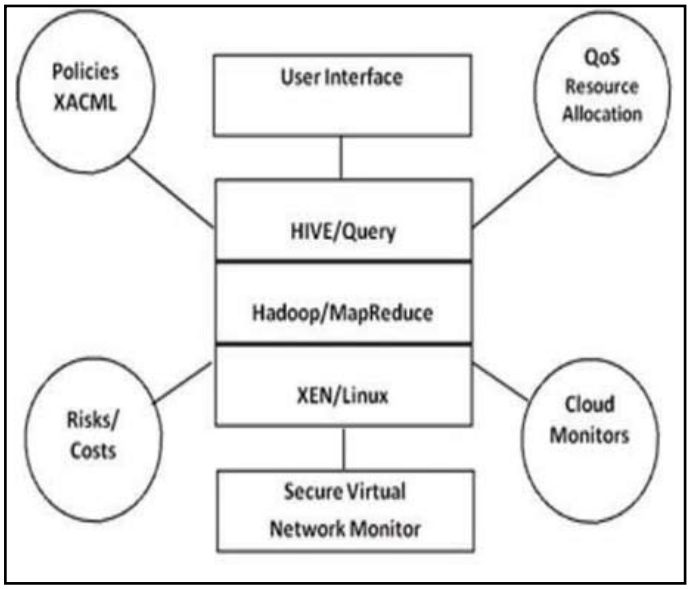


Fig: Layered framework for assured cloud

## II. Discussion

Problem Statement: The storage of the data online like cloud comes with two possible demerits. The one is the violation of the law and the other one is the possible attack because of keeping data to another threat prone data.

Solutions: There could be two possible solutions, the one is to know where the data is being kept and other one is to go for encryption of data on the Client-side rather than the Server- side.

### A. Methodologies proposed:

1) For large Corporate based Cloud User: The large sectors or companies like Facebook have huge amount of capital and efficient technologies to go for cryptography by their own. They can encrypt their data before sending it to its Cloud Service provider like Hadoop. So, even if the Cloud company makes the replica of the original data and try to use it illegally, it won't succeed as they do not know the technique that were used by the User to encrypt the data.

2) The small scale companies: We do not have such huge amount of capital and also it is possible that every small scale companies do not have efficient technologies for up- to-date cryptography mechanism. This led security threat to them. They can go for standardized protocols and government protected protocols .These small companies should go with only those Cloud Service providers which follows either of below three mentioned techniques or features:

### 2.1) https protocols

The Cloud Service provider should allow to send data only through https (hyper text transfer protocols security). Like https for Twitter uses verified Symantec class 3 EV SSL CA- G3. It encrypts through 128-bit and TLS 1.2 and it is being encrypted and authenticated using AES_128_GCM and ECDHE_RSA as exchange mechanism.


Fig: https

### 2.2) Padlock

This is another system which shows high level security over the web. You have noticed a padlock icon at the bottom of certain web pages. Padlock indicates that the page uses the SSL protocol (a data transfer security standard that encrypts data and authenticates the server and the integrity of the message) or the TLS protocol. This indicates that all information is secured. To be sure that these pages are indeed protected by SSL, we can also check the site's URL, which must begin https://, this's' indicating that this security system is in force. We can also click the padlock in the browser bar to view the identity of the Web site owner and also check that it comes from a valid Certificate Authority. This digital certificate is a document that an organization provides from its Web site to confirm their identity, and to enable a secure connection [].

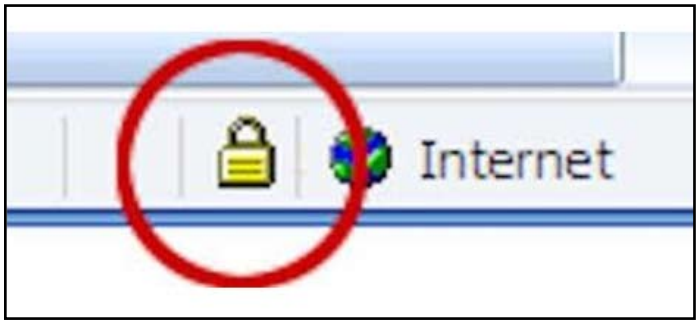


Fig: Padlock

### 2.3) Government Policy [8]:

Different countries have different policies for keeping data or uploading data over the online storage system. It might be possible that some data which are allowed to be kept over Cloud storage system is permissible in one country but not in other, like YouTube is banned in some countries but not in every country. In cloud we do not know the location of the data centers. If our data on cloud is kept over a country's Cloud Server then it might conflict its laws, so we need to know the location and it is only possible if we include the governing bodies to keep watch of data over the cloud storage. So the small companies seeking for Cloud service should look for this option. The government should enforce the concept of distributed database system to watch the law violation for keeping data online.

#### 2.3.1) Example: Government policy in the USA

1) Interdependency with Cyber Security initiatives:

- The Department of Homeland Security Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) project, which is providing an architecture for

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

dynamic system monitoring and reporting;
- The Security Content Automation Protocol (SCAP) initiative at NIST, which provides specifications for expressing security configurations and events, event management, and incident handling;
- The National Science Foundation Future Internet Architectures initiative which is developing Internet architectures to provide advanced security and reliability in the context of emerging Internet usage patterns; and
- The Federal Information Security Management Act (FISMA). In accordance with the Act, Federal Information Processing Standards (FIPS) 200 and NIST Special Publication 800-53 (periodically updated) provide baseline security controls and guidance for federal information systems.

2) Interdependency with Organizational Policy

Highlighted in the cyber law it is necessary to have technical solutions which allow differing policies to coexist side by side in a global environment irrespective of geographical location and sovereignty. The ability to bridge policy differences is essential for maintaining service while policies evolve. The main function of cyber law is to precisely watch the service- level agreement including commonality of pricing unit definition ,customers prospective contract term, liability ownerships, audit rights, exit provisions, and business continuity.

3) Interdependency with Other National Priority Initiatives

The Cloud Computing model is clearly an enabler of national priority initiatives such as Health IT and Smart Grid, and is enabled by programs such as National Strategy for Trusted Identities in Cyberspace (NSTIC). NSTIC will enhance security and privacy for cloud services. NSTIC defines a means to create a secure, trusted Identity Ecosystem that is capable of establishing a user-centric privacy protection for any Cloud Ecosystem. The NSTIC Strategy 18 calls for the development of interoperable technology standards and policies—the "Identity Ecosystem"— where individuals, organizations, and underlying infrastructure — such as routers and servers—can be authoritatively authenticated.

The above mentioned criteria are being depicted by below diagram.

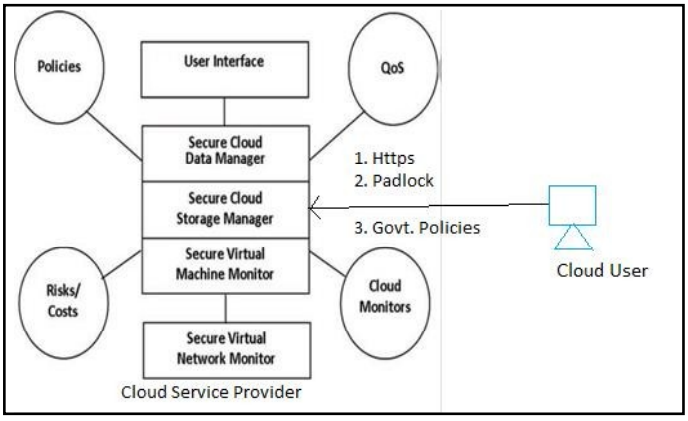


Fig: Proposed Model for Data Storage

## III. Conclusion

The methods and ways proposed are optimal with the level of security needed over the cloud. But the security is always incremental in the level to achieve confidentiality and reliability. The further modification could be done on the policy part of the government. The policy should be made basically more precisely for data storage over the cloud.

## References

[1] *Guidelines for Indian Government Websites, An Integral part of Central Secretariat of Office Procedure.*

[2] *Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham ―Security Issues for Cloud Computing ,‖ International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010*

[3] *McNabb, A., Monson, C., & Seppi, K. (2007). MRPSO: MapReduce particle swarm optimization. In Proceedings of the 9th annual conference on genetic and evolutionary computation (GECCO 2007) (p.177). New York: ACM Press.*

[4] *Miao Zhou,‖ Data Security and Integrity in Cloud Computing,‖ University of Wollongong Research Online.*

[5] *Mladen A. Vouk,‖ Cloud Computing – Issues, Research and Implementations,‖ Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246 doi:10.2498/ cit.1001391*

[6] *John W. Rittinghouse, J. Ransome, ―Cloud Computing Implementation, Management, and Security, CRC Press*

[7] *] Sunita Sharma, Amit Chugh, ―Survey Paper on Cloud Storage Security ‖, International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 2, April 2013*

[8] *US GovernmentCloud Computing TechnologyRoadmap Volume I Release 1.0 (Draft)*