International Journal of Computers & Technology
Volume 4 No. 1, Jan-Feb, 2013 ISSN 2277-3061

New Approach for Managing Keys in Cloud & Use Cases for Cloud Computing

Sarvesh Kumar, Anupam Shukla[1], Ankit Sharma, Kalimullah Lone
(sarvi899, anupam.yoopi, ankitsharma.com, kalimullahlone)@gmail.com
Department of Computer Science and Engineering
Lovely Professional University, Punjab
[1]Lecturer, D G Tatkare Mahavidyalaya, Mumbai

Abstract: *Now a day's cloud computing is best innovative technology in the field of IT. In its broadest usage, the term cloud computing refers to the delivery of IT resources over the internet as opposed to hosting and operating these resources locally, such as a college or university network. These resources can include application and services as well as infrastructure and services over the network. Any organization can purchase these resources on as needed basis and avoid the capital expenditure cost of software and hardware. Security is major problem in cloud computing, thus key distribution is important thing for managing security in cloud computing. In this paper we derived a proposed algorithms for managing keys in the cloud and also discuss uses cases for cloud computing***.**

Key words: cloud computing, IaaS, SaaS ,Paas

Introduction: Cloud computing is just internet based computing. If we have an internet connection, then we can now access the features of cloud computing. If we have Gmail account, it means we are using cloud.

First we do not download Gmail account on my hard drive of my computer, only we see and leave it. Then point arises here that where our Gmail files is stored or Face book account where we can upload picture, videos and YouTube uploading video, where it is stored. It is stored on clouds. If we leave anything on web so we uses cloud computing.

We can see again Gmail files by internet technology. Some years ago, software installed on your computer or on your mobile, and then we can use this software on your computer on your mobile. But using of cloud computing, we can use these types of software without installation or without download from your computer or your mobile or your tablets. We can use it, we can change it from any machine like Tablet, computer or mobile E.g. Google Doc. All the world companies want to use the power and benefits of cloud computing. Amazon allows to his customers to put their list of favourite songs on his clouds.

Apple is making own cloud called I Cloud. We can also find use of free cloud computing services e.g. Google doc, icloud.We will not pay for using this cloud service. As the many software runs on webs, then we going in clouds depend upon internet. In this paper we will discuss about challenges and use cases of cloud computing and searchable solution for managing security in cloud computing.

Basic terminology of cloud computing: there are some basic terms related to cloud computing.

1. **Service level agreement:** it is a contract between consumer and provider that specifies consumer requirements and providers commitment.
2. **Federation:** it is the act of combining data across multiple systems that is done by either cloud provider or cloud broker.
3. **Broker:** a broker has no cloud resources but matches between consumers and providers resources.
4. **Multi-Tenancy**: it is the property of applications or data from different enterprises hosted on same physical hardware.
5. **Cloud brusting:** it is a techniques used by hybrid clouds to provide additional resources to private cloud as needed basis. If the private cloud has no need of resources then hybrid cloud is not used.
6. **Policy:** general term for operating a procedure ie. A security policy means that it must specify that all requests to a particular cloud services must be in encrypted mode.
7. **Virtual machine:** A file typically called an image that when executed looks like user like an actual machine.

Challenges:

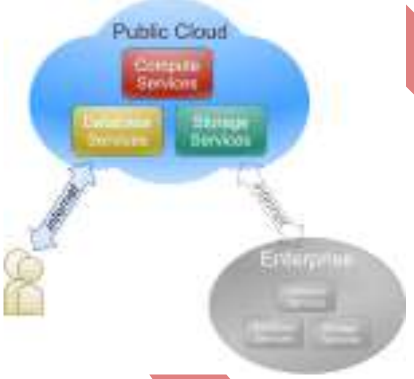
Cloud operators are expected to manipulate client data without necessarily being fully trusted. So there is need of designing cryptographic primitive protocols.

Problem formulation

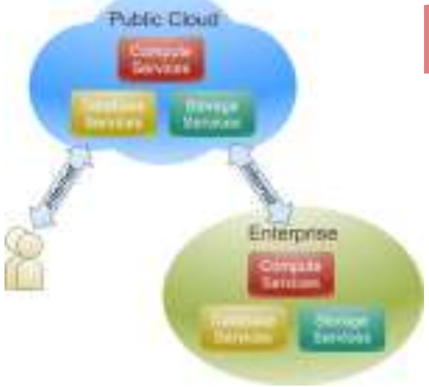
1. Problem of building a secure cloud storage device on top of a public cloud infrastructure where the service provider is not completely trusted by the customer.
2. at high level, several architectures that combine recent and non standard cryptographic primitives in order to achieve our goal.
3. Cloud security issues involves in protected clouds from outside threats are similar to those already facing large data centres except that responsibility is divided between the cloud user and cloud operator.

Use cases scenarios for cloud computing: there are some use cases approaches for cloud computing.

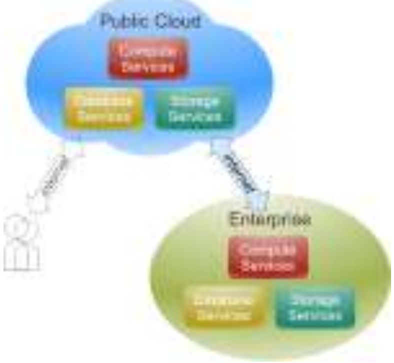
1. **End user to cloud:** Applications are running in the cloud and accessed by end users.



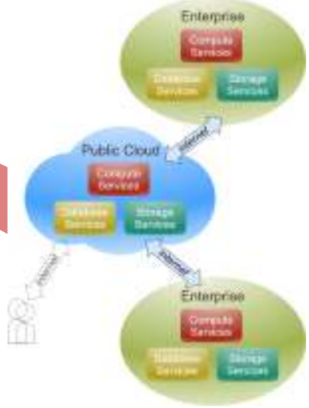
2. **Enterprise to cloud to end user:** Applications are running in the cloud and accessed by employees and customers.



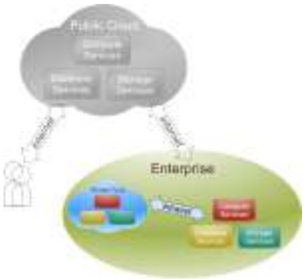
3. **Enterprise to cloud:** cloud applications are merged with internal capabilities.



4. **Enterprise to cloud to enterprise:** Applications running in the cloud and used by partner enterprises.



5. **Private cloud:** A cloud that is hosted by an organization inside their firewall.



Proposed approach:

A. Future cloud computing services will not only be encrypt documents to keep them safe in the cloud but also make it possible to search and retrieve this information without first decrypting it.
B.development of make the encrypted cloud more searchable.
C. cloud users could download software that would encrypt their data before it is sent into the cloud. In addition to software would issue encrypted strings called token, which can be used to check that documents are intact and crucially to search their contents without first having to decrypt them.

Implementation of cloud security:

Cloud security is major concern in cloud computing. Can we trust on cloud service provider? IS service provider is fully trusted for managing the keys and maintaining the data in cloud. Thus there are some points related it.

- Isolation among resources of different tenants like hypervisor,storage,network
- Interfaces for client controlled audits for long term process.
- Engage third party auditors.

Mechanism implemented by clients:

- Cryptographically protect the data
- Remote auditing

Proposed algorithms:

How we manage keys in the cloud for security purposes. This is defined by new proposed algorithms.

- ➢ Strong interface using unstructured objects called blobs.
- ➢ Each object is identified by unique key.
- ➢ Objects grouped into containers.
  Operations:
  Put (key, obj)
  Get (key, obj)-get(key)-obj
  List ()-{obj---}
  Remove key

Algorithm:

- ➢ Share secret key S among parties $P1$----Pn such that
  - Any $t<n/2$ parties have no info about S
  - Any group of $t+1$ parties can receive the secret S
- ➢ Trusted dealer picks random polynomial $a(x)$ that is $a(x)$ belongs to $F(x)$ degree t and $a(0)=s$
- Share for Pi is $Si = a(i)$
- Given set U of $(t+1)$ shares, recover secret
  $S=a(0)=$ Fj belongs to U dj aj
  Where dj-lagrange co-efficient w.r.t U

Conclusions:

Thus we can say cloud computing is one of the latest developments in the field of IT industry also known as on demand cloud computing. It is the application provided in the form of services over the internet. The implementation of algorithm will show that we can manage keys before putting data in the cloud. In this paper we also discussed about some use cases approach for cloud computing and some basic terminology that are used in cloud computing.

References:

[1] Hayes Brain, “Cloud Computing,” Communications and technology of the ACM, vol. 51, Iss. 7, July, 2008, pp. 9–11

[2] [Online: January, 2012] Searchcloudcomputing, World cloud Computing ?http://searchcloudcomputing.techtarget.com/definition/cloud-computing

[3] Boss Greg, Malladi Padma, Quan Dennis, Legregni Linda, Hall Harold, “Cloud Computing”, IBM Paper, October, 2007.

[4] R. Mikkilineni, V. Sarathy, “Cloud Computing and the Lessons from the Past”, Proceedings of 18th IEEE International Workshops on Enabling Technologies:Infrastructures for Collaborative Enterprises (WETICE’09), 2009, pp. 57-62.

[5] Sunbeam Islam, M. Mollah Baqer, Huq M. Imanul, M. Aman Ullah, “Cloud Computing for Future Generation of Computing Technology”, Proceedings of the 2nd IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems, Bangkok, Thailand, May, 2012, pp. 1-6.

[6] R. H. Katz, “Tech Titans Building Boom,” IEEE Spectrum, Vol. 46, Iss. 2, 2009, pp. 40–54.

[7] M. Pokharel, Hyun Yoon, Sou Park, “Cloud Computing in System Architecture”, Proceedings of IEEE International Symposium on Computer Network and Multimedia Technology, 2009, pp. 1-5.

[8] [Online: January, 2012] Cloud Computing Platform: AbiCloud; http://www.abiquo.com/news-and-events/announcesformalrelease.php

[9] [Online: January, 2012] Cloud Computing Platform: Eucalyptus; http://www.eucalyptus.com/

[10] [Online: January, 2012] Cloud Computing Platform: Nimbus; http://www.nimbusproject.org/

[11] [Online: January, 2012] Cloud Computing Platform: OpenNebula;http://opennebula.org/

[12] Junjie Peng, Xuejun Zhang, Zhou Lei, Bofeng Zhang, Wu Zhang, Qing Li, “Comparison of Several Cloud Computing Platforms”, Proceedings of 2nd IEEE International Symposium on Information Science and Engineering, 2009, pp. 23-27