BREAK / RETRIEVE AGENT FOR CLOUD ORIENTED APPLICATIONS

Suresh Kumar RG[1]
[1]*Department of Computer Science and Engineering*
Rajiv Gandhi College of Engineering and Technology, Pondicherry, India.

ABSTRACT

As studies quote, Cloud computing is an end user technology. Corruption takes a great hindrance to economy of any developing country. This paper is proposed to control the corruption in "Tender/Construction" alongside with confidential supervisor that guarantees the confidentiality of the files stored in the Hybrid cloud. Instead of paper based transaction of data, a sequential computerized system over the CaaS Layer of Cloud to document the data is incorporated. The existing scenario flows with paper work which as to be authorized manually, the take-down procedures are manual. These manual works must be monitored duly in order to avoid any type of procedural fault. In particular, when account information is transferred by manual process then defining to the protection mechanism must also be considered. This work mainly differs from counterpart in the way; the automation of tender management along with the release of payment from the government is carried out. These data stored in the cloud is made secure with break/retrieve encryption module. The work proposes a new architecture which leads to the formation of smart confidential supervisor and bug handler which controls the cloud storage and also secures confidential information as like tender quotations and the other contract details.

Keywords – ***CaaS, Cloud computing, Hybrid cloud, Clouds.***

I. INTRODUCTION

Everything has cloud linked to it by one means or the other. Let it be a technical magazine or a blog, all talk about fresh new emergent technology so called cloud computing. Definition of Cloud computing varies from professionals to professionals and from individual to individual. Everyone has their own way of defining cloud computing. Basic working motto of cloud computing is to provide cheap and efficient service to the mass. This reduces infrastructure cost, data management cost, etc. cloud providers offers also few hints of monitoring as a service. These are services faces a common problem of data integrity problem. In recent times, most of the enterprise application is deployed in cloud. Cloud is of three types, public cloud which is mostly maintained by third parties, private cloud which is used for Specific application and hybrid cloud which is a combination of both the above mentioned clouds. Recent times, lot of hacking stuff are coming into report. This is due to poor security measures of corporation. In addition to the fault of corporation, there is a third party often at fault, the users.

II. CLOUD COMPUTING

Cloud computing is an expression used to describe a variety of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. In science, cloud computing is a synonym for distributed computing over a network, and means the ability to run a program or application on many connected computers at the same time [1]. The phrase also more commonly refers to network-based services, which appear to be provided by real server hardware, and are in fact served up by virtual hardware, simulated by software running on one or more real machines. Such virtual servers do not physically exist and can therefore be moved around and scaled up (or down) on the fly without affecting the end user - arguably, rather like a cloud. The popularity of the term can be attributed to its use in marketing to sell hosted services in the sense of application service provisioning that run client server software on a remote location.

SERVICE MODELS

Once a cloud is established, how its cloud computing services are deployed in terms of business models can differ depending on requirements. The primary service models being deployed are commonly known as:

Software as a Service (SaaS) — Consumers purchase the ability to access and use an application or service that is hosted in the cloud. A benchmark example of this is Salesforce.com, as discussed previously, where necessary information for the interaction between the consumer and the service is hosted as part of the service in the cloud. Also, Microsoft is expanding its involvement in this area, and as part of the cloud computing option for Microsoft® Office 2010, its Office Web Apps are available to Office volume licensing customers and Office Web App subscriptions through its cloud-based Online Services.

Platform as a Service (PaaS) — Consumers purchase access to the platforms, enabling them to deploy their own software and applications in the cloud. The operating systems and network access are not managed by the consumer, and there might be constraints as to which applications can be deployed.

Infrastructure as a Service (IaaS) — Consumers control and manage the systems in terms of the operating systems, applications, storage, and network connectivity, but do not themselves control the cloud infrastructure. Also known are the various subsets of these models that may be related to a particular industry or market. Communications as a Service (CaaS) is one such subset model used to describe hosted IP telephony services. Along with the move to CaaS is a shift to more IP-centric communications and more SIP trucking deployments. With IP and SIP in place, it can be as easy to have the PBX in the cloud as it is to have it on the premise. In this context, CaaS could be seen as a subset of SaaS.

III. DEPLOYMENT MODELS

Deploying cloud computing can differ depending on requirements, and the following four deployment models have been identified, each with specific characteristics that support the needs of the services and users of the clouds in particular ways[2].

Private Cloud — The cloud infrastructure has been deployed, and is maintained and operated for a specific organization. The operation may be in-house or with a third party on the premises.

Community Cloud — The cloud infrastructure is shared among a number of organizations with similar interests and requirements. This may help limit the capital expenditure costs for its establishment as the costs are shared among the organizations. The operation may be in-house or with a third party on the premises.

Public Cloud — The cloud infrastructure is available to the public on a commercial basis by a cloud service provider. This enables a consumer to develop and deploy a service in the cloud with very little financial outlay compared to the capital expenditure requirements normally associated with other deployment options.

Hybrid Cloud — The cloud infrastructure consists of a number of clouds of any type, but the clouds have the ability through their interfaces to allow data and/or applications to be moved from one cloud to another. This can be a combination of private and public clouds that support the requirement to retain some data in an organization, and also the need to offer services in the cloud [2].

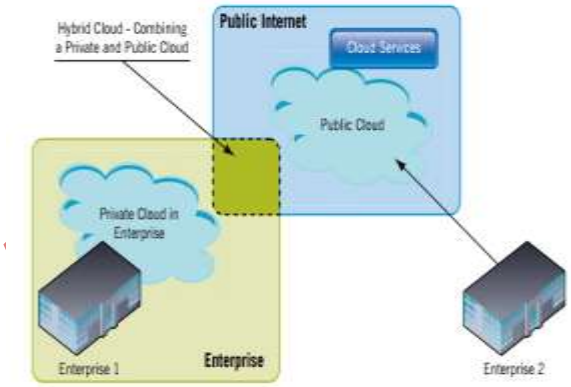

Fig 1.1 PRIVATE, PUBLIC AND HYBRID CLOUD DEPLOYMENT EXAMPLES

IV.BENEFITS

The following are some of the possible benefits for those who offer cloud computing-based services and applications:

Cost Savings — Companies can reduce their capital expenditures and use operational expenditures for increasing their computing capabilities. This is a lower barrier to entry and also requires fewer in-house IT resources to provide system support.

Scalability/Flexibility — Companies can start with a small deployment and grow to a large deployment fairly rapidly, and then scale back if necessary. Also, the flexibility of cloud computing allows companies to use extra resources at peak times, enabling them to satisfy consumer demands.

Reliability — Services using multiple redundant sites can support business continuity and disaster recovery.

Maintenance — Cloud service providers do the system maintenance, and access is through APIs that do not require application installations onto PCs, thus further reducing maintenance requirements.

Mobile Accessible — Mobile workers have increased productivity due to systems accessible in an infrastructure available from anywhere.

V. CHALLENGES

The following are some of the notable challenges associated with cloud computing, and although some of these may cause a slowdown when delivering more services in the cloud, most also can provide opportunities, if resolved with due care and attention in the planning stages [10].

Security and Privacy — Perhaps two of the more "hot button" issues surrounding cloud computing relate to storing and securing data, and monitoring the use of the cloud by the service providers. These issues are generally attributed to slowing the deployment of cloud services. These challenges can be addressed, for example, by storing the information internal to the organization, but allowing it to be used in the cloud. For this to occur, though, the security mechanisms between organization and the cloud need to be robust and a Hybrid cloud could support such a deployment.

Lack of Standards — Clouds have documented interfaces; however, no standards are associated with these, and thus it is unlikely that most clouds will be interoperable. The Open Grid Forum is developing an Open Cloud Computing Interface to resolve this issue and the Open Cloud Consortium is working on cloud computing standards and practices. The findings of these groups will need to mature, but it is not known whether they will address the needs of the people deploying the services and the specific interfaces these services need. However, keeping up to date on the latest standards as they evolve will allow them to be leveraged, if applicable [11].

Continuously Evolving — User requirements are continuously evolving, as are the requirements for interfaces, networking, and storage. This means that a "cloud," especially a public one, does not remain static and is also continuously evolving [11].

Compliance Concerns — The Sarbanes-Oxley Act (SOX) in the US and Data Protection directives in the EU are just two among many compliance issues affecting cloud computing, based on the type of data and application for which the cloud is being used. The EU has a legislative backing for data protection across all member states, but in the US data protection is different and can vary from state to state. As with security and privacy mentioned previously, these typically result in Hybrid cloud deployment with one cloud storing the data internal to the organization [11].

VI. HYBRID CLOUD ARCHITECTURE USING EUCALYPTUS

When we talk to various IT organizations about using AWS-compatible Eucalyptus to set up a private or hybrid cloud, the question we often get is, "How do I get started?" We recently published a series of Reference Architectures which are specific to common cloud use cases deployed in the field. The Dev/Test Reference Architecture is good hybrid cloud architecture for application development and QA purposes [3]. Service and

credibility gaps exist in many IT organizations between developers and their IT operations teams. Developers want to create and deploy new applications quickly. But provisioning the infrastructure and resources that developers need can take a lot of time - days or weeks in some cases. The culprits are usually a backlog of requests that require some form of manual review and approval or the lack of time or resources to perform the actual provisioning. These delays often lead to squandered market opportunities, not to mention lost productivity.

Eucalyptus provides AWS-compatible private and hybrid cloud architecture and open source software solution that provides developers, QA engineers, and IT operations teams with the same flexibility and agility that is usually associated with the public cloud, while still allowing IT operations teams to maintain control and costs. The Eucalyptus private cloud platform provides self-service resource provisioning so developers and QA engineers can gain access to the resources they need through streamlined workflow processes and get their work done quickly and efficiently. Developers don't need to submit an IT ticket and wait for days or weeks to get the resources they need. They can quickly self-service provision and configure the compute, storage, and networking resources they need on demand [3].

In addition, because Eucalyptus and AWS have pledged to maintain AWS API compatibility, hybrid clouds can be designed in order to develop and test applications on a Eucalyptus private cloud and then deploy them unchanged to production on the AWS public cloud. Eucalyptus currently maintains API compatibility with EC2, S3, EBS, ELB, Auto Scaling, Cloud Watch, and IAM, with additional functionality planned for future releases. Organizations can maintain the flexibility and agility they need to empower innovation while simultaneously maintaining control over resources and costs.

So where does the Reference Hybrid Cloud Architectures fit in? The Reference Architecture provides a configuration and deployment template for IT operations teams to assist in setting up a Eucalyptus private or hybrid cloud. The Reference Architecture provides the scope of resources necessary and the recommended deployment model for the specific use case, such as Dev/Test, Scalable Web Services, or Virtualization Management. This is important for two reasons: First, it prescribes a bill of materials and detailed notes on how to deploy the Eucalyptus cloud platform on it. Second, the Reference Architecture provides a "recipe" for the bill of materials needed to run the cloud.

In the case of a Dev/Test environment, Infrastructure as a Service (IaaS) provides the automation for provisioning and de-provisioning resources as application and workload demand ebbs and flows. The Reference Architecture provides design choices for the IaaS solution, including physical resources required and a deployment topology.
The Reference Architecture also outlines technologies commonly deployed with Eucalyptus to provide a complete IaaS solution – such as configuration management, monitoring, and workflow management [8].

VII. RELATED WORK

Even in this modern era were most of the works are automated in all the government departments, construction department is one place were all the process from producing an tender to calculating project budget and the amount of commodities needed are still carried out in paper and manually, as we all know chances of error increases whenever there is some form of manual work that too when it is done by human in groups [4].

Storage in cloud is an area of concern for confidential departments. The files over network can be sniffed by any malicious intruder. This makes many vendors and small companies hesitate to use cloud service. This forces the use of manual process. The most incurred problems by use of manual work and paper work is time consumption, error and misplacement of documents. Search of any particular detail becomes too time consuming and tedious. Many problems go unseen such as survey reports, etc. The existing scenario flows with paper work which as to be authorized manually, the take-down procedures are manual. These manual works must be monitored duly in order to avoid any type of procedural fault. Manual process also engages with uncovered money perseverance, and if any type of sight fault will lead to missing of paper work which sometimes tends to re-establishment of the entire scenario by the management person. In particular, when account information is transferred by manual process then defining to the protection mechanism must also be considered. The time concept plays a role in the manual process, which sometimes extremes if the person/management in-charge is unavailable of a period of time.

In addition the superior complexity is also to be considered in the manual definition of government oriented paper made work scenario. Even in case of any small error then the entire work flow must be re-defined from the scratch. Taking down old file will be also a tedious process for long time pending process by an applicant. The work generally, decreases by paper work since any type of error will lead to work fault. The un-signed must duly, verify the entire scenario every time in the progression.

In this paper right from the release of tender, publishing in website and the release of tender are handled automatically by the cloud. The process of not allowing any manual work other than quoting tender amount guarantees error free process. Every government employee is provided with ID. Wholesale shops and also retail shops from where things can be purchased must be government recognized as of ration shops. The stock of these shops is directly maintained in the cloud. A periodic checking of stock in these shops will reduce corruption in one way. Whenever potential employee comes for buying an item, initially the ID is entered and password is entered.
Then list of items purchased is noted online and no cash is got from the employee. The cash is directly settled to the retail shops by the government. At the same time, the cost of item purchased will be deducted from the amount that is needed to be settled to the potential tender holder. Now this flow can be said to avoid corruption to far extend as there is no commission involved anywhere and also low quality products can't be purchased as stock of retail shops are maintained online. There is less chance of buying extra goods and selling to other non-government recognized shops. Black marketing of tons of cement or other goods is almost impossible leading to control in corruption.

VIII. PROPOSED SYSTEM

Break/Retrieve mechanism can be incorporated along with the above said process to safeguard the files and data stored in cloud. The confidential file mainly stored will be tender quotation file, employee profile and status of any ongoing projects. This can be efficiently stored and retrieved in COBRA mechanism, Bug handler can be used to trigger an event in case of any error spotted stock management of wholesale shops, Stock management of retail shops, Tender management, ID generation of all government employees, Break/Retrieve mechanism, Bug Handler ,Encryption and Decryption [5].

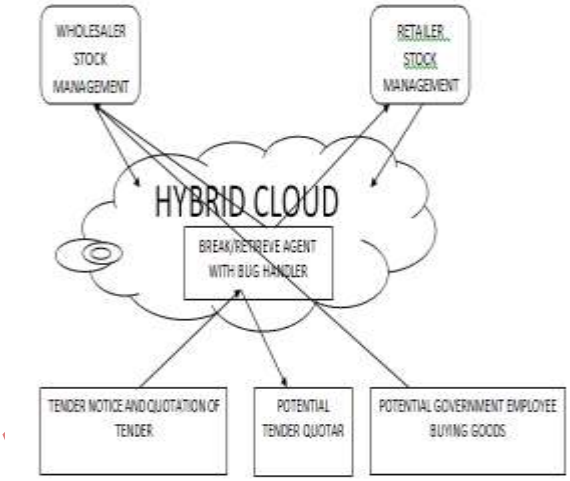

Figure 1.2 Architecture of Proposed Solution

BREAK/RETRIEVE MECHANISM

The files such as tender quotations and employee profile will be stored in the cloud. These files will be encrypted and will be broken into pieces and will be stored in random location in same cloud server. These pieces can be sniffed but cannot be read or manipulated. Whenever a legitimate request to access the file comes, retrieve agent collects all file fragments and decrypts them and send to the requester. The file size will be calculated.

If file size > k(minimum size)

Then (file size / k) parts of file will be broken.

And while reunion, k parts must reunite for

Successful transaction.

If reunited parts <k.

Then bug handler asks for retransmission.

BUG HANDLER

Bug handler does the job of notifying any error occurring during retrieval. If any part of file doesn't assemble, then error handler does the job of reunification.

ENCRYPTION

Encryption algorithm used is RSA [6] over DES [7] algorithm to double protect the data. The encrypted file only will be sent for break/retrieval process. The encrypting key will be unique for different files.

DECRYPTION

After retrieval of all parts of file, the decryption is started. The decryption is done and the file is sent to legitimate user in readable original format.

IX. CONCLUSION

In our work we are providing security and eventually providing peace of mind to the users. Here we incorporate various security features thereby providing protection against url rewriting, sql injection, ip spoofing and sniffing. Usage of cloud space is generally a backup when we run out of disk space and make use of applications which we don't possess and hence security is of prime importance which we have effectively for cloud space providers and users and we allot all the required features and classify them to make sure that the users and the cloud space providers get the most of what is available.

REFERENCES

[1] Aiiad Albeshri, William Caelli," Mutual Protection in a Cloud Computing Environment" in 12th IEEE International Conference on High Performance Computing and Communications 2010.

[2] Balachandra Reddy Kandukuri, Ramakrishnaaturi V, Dr.Atanu Rakshit," Cloud Security Issues" in IEEE International Conference on Services Computing 2009.

[3] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham," Security Issues for Cloud Computing" in International Journal of Information Security and Privacy, April-June 2010.

[4] Lombardi, R. Di Pietro, "Secure Virtualization for cloud computing". Journal of Network and Computer Applications, Elsevier, June 2010.

[5] Riley, X. Jiang, D. Xu, "Guest-transparent prevention of kernel rootkits with vmm- based memory shadowing". In RAID '08: Proceedings of the 11th international symposium on recent advances in intrusion

detection, Springer-Verlag, Berlin, Heidelberg, 2008.

[6] Samoud Ali, Cherif Adnen," RSA ALGORITHM IMPLEMENTATION FOR CIPHERING MEDICAL IMAGING", Signal processing Laboratory - Science Faculty of Tunis, 1060 Tunis.

[7] Sombir Singh, Sunil K. Maakar, Dr.Sudesh Kumar "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques", International Journal of Advanced Research in Computer Science And Software Engineering Volume 3, Issue 6, June 2013.

[8] https://www.eucalyptus.com/eucalyptus-cloud/iaas/architecture.

[9] R. Balasubramanian, M., Aramudhan "Security Issues: Public vs Private vs Hybrid Cloud Computing" International Journal of Computer Applications, Volume 55 - Number 13, 2012.

[10] R. Kalaichelvi Chandrahasan, S Shanmuga Priya and Dr. L. Arockiam, "Research Challenges and Security Issues in Cloud Computing" International Journal of Computational Intelligence and Information Security, March 2012 Vol. 3, No. 3.

[11] Rajesh Piplode, Umesh Kumar Singh "An Overview and Study of Security Issues & Challenges in Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012.