An Comparison with Property Based Resource Attestation to Secure Cloud Environment

Mr. Ravindra K. Gupta[1], Mr. Rajat Pali[2], Dr. Shailendra Singh[3],
Mr. Gajendra Singh[4], Mr. Ashutosh k. Dubey[5]

ravindra_p84@rediffmail.com[1]
M.Tech Scholar, CSE, SSSIST, Sehore[2]
rajat14pali@gmail.com
Professor (CSE), NITTTR, Bhopal[3]
ssingh@nitttrbpl.ac.in
HOD(CSE/IT),Sssist,Sehore[4]
AP, CSE, TITR, Bhopal, India[5]
ashutoshdubey123@gmail.com

ABSTRACT

In this paper we propose a new cloud computing environment where we approach a trusted cloud environment which is controlled by both the client and the cloud environment. Our approach is mainly divided into two parts. First part is controlled by the normal user which gets permission by the cloud environment for performing operation and for loading data. Second part shows a secure trusted computing for the cloud, if the admin of the cloud want to see the data then it take permission from the client environment. This provides a way to hide the data and normal user can protect their data from the cloud provider. This provides a two way security which helps both the cloud and the normal user. For the above concept we propose a java based algorithm. In this paper we also provide a comparative study between our novel and the traditional approach. It also proof that our method shows good result in comparison to the previous one.

KEYWORDS

Cloud environment, Two Way security, Sharing, Java

1. INTRODUCTION

Cloud computing is a paradigm of computing that aims at providing dynamically scalable computing resources over the Internet as a service. Users do not need to bother about the management of technology infrastructure. They simply use the resources on a pay-per-use basis, commissioning and decommissioning as many instances of computing resources as needed.

Cloud Architectures solve such difficulties. Applications built on Cloud Architectures run in-the-cloud where the physical location of the infrastructure is determined by the provider. They take advantage of simple APIs of Internet-accessible services that scale on demand, that are industrial-strength, where the complex reliability and scalability logic of the underlying services remains implemented and hidden inside-the-cloud. The usage of resources in Cloud Architectures is as needed, sometimes ephemeral or seasonal, thereby providing the highest utilization and optimum bang for the buck.

David C. Wyld, et al. (Eds): CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 319–330, 2012.

DOI : 10.5121/csit.2012.2232

The applications are upgraded very easily through internet. The user no needs to do it manually using the upgraded version software. The motive of Cloud Computing is serving On Demand means when the need arises; it's very easy to get extra resource instantly. Any small amount of resource can be used from the cloud.

The advantages of cloud computing over traditional computing include: agility, lower entry cost, device independency, location independency, and scalability [**1**].In order to solve the problem of data integrity checking, many schemes are proposed under different systems and security models [2], [3], [4], [5], [6]. In all these works, great efforts are made to design solutions that meet various requirements: high scheme efficiency, stateless verification, unbounded use of queries and retrievability of data, etc. Considering the role of the verifier in the model, all the schemes presented before fall into two categories: private auditability and public auditability. Although schemes with private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private information.

We provide here an overview of cloud computing. The rest of this paper is arranged as follows: Section 2 describes the security consideration; Section 3 describes about recent scenario; Section 4 shows the proposed approach; Section 5 shows the result analysis. Section 6 describes Conclusion.

2. Security Consideration

With the PaaS (Platform as a Service) model the vendor offers a complete development environment in which application developers can then create and deploy their code. This approach means that instead of building a server environment to run an application and installing a development environment to create applications on that server, the customer can simply connect to a PaaS cloud provider and by using a PaaS complianct development tool, start creating applications that can be deployed worldwide without any delay. The vendor will typically provide code building blocks so that the customer can build applications rapidly and the development environment can either be web-based or by using a development environment on the local computer.

Distributed applications can be challenging to adapt to a cloud environment. For example, consider the situation where you have a n-tier, on-premises, distributed line-of-business application and you want to migrate this application to the cloud. For security reasons, you decide to keep the data tier in a Private Cloud environment but to migrate the business and presentation tiers to the Public Cloud.

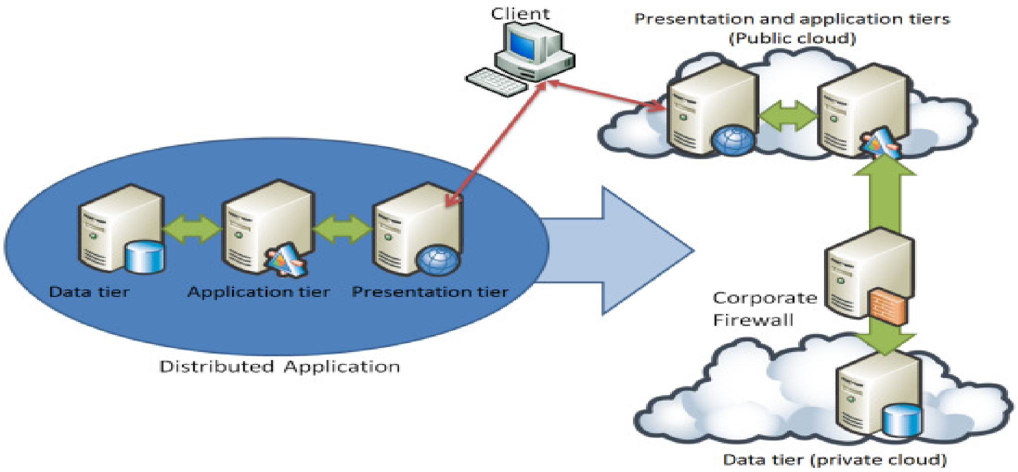

Figure 1: N-Tier Cloud Application

Some of the challenges that you may face from this type of migration include:

- Security, particularly authentication, cryptography, access control and firewall ports
- Replacing synchronous operations with asynchronous ones
- Performance management
- Exception management and error reporting

A well-architected distributed application should be able to make the transition from an on-premises environment to a cloud-based configuration relatively painlessly. However, poor architecture and design can result in performance degradation and poor security can result in compromise of some or all components of the application.

Performance degradation can come from design errors such as excessive querying of parameters or heavy use of object properties. In a high-speed, low-latency LAN environment, these factors have minimal effect; in cloud-based environments, such issues can cause the application to perform very slowly.

3. RECENT SCENARIO

In 2010, Wei-Tek Tsai et al. [7] provide an overview survey of current cloud computing architectures, discusses issues that current cloud computing implementations have and proposes a Service-Oriented Cloud Computing Architecture (SOCCA) so that clouds can interoperate with each other. Furthermore, the SOCCA also proposes high level designs to better support multi-tenancy feature of cloud computing.

In 2010, Zhidong Shen et al. [8] proposed a new prototype system, in which cloud computing system is combined with Trusted Platform Support Service (TSS) and TSS is based on Trusted Platform Module (TPM). In this design, better effect can be obtained in authentication, role based access and data protection in cloud computing environment.

In 2010, Zhidong Shen et al. [9] proposed a method to build a trusted computing environment for cloud computing system by integrating the trusted computing platform into cloud computing system. They propose a model system in which cloud computing system is combined with trusted computing platform with trusted platform module. In this model, some important security services, including authentication, confidentiality and integrity, are provided in cloud computing system.

In 2011, Pritesh Jain et al. [10] survey several aspects of cloud computing security concerns. They concern on the major challenges that faces the cloud computing is how to secure and protect the data and processes the data of the user. To provide secure and reliable services in cloud computing environment is an important issue. One of the security issues is how to reduce the impact of denial-of-service (DoS) attack or distributed denial-of-service (DDoS) in this environment.

In 2011, Siyuan Xin et al. [11] proposed about the property-based remote attestation mechanism in Trusted Computing is imported into clouding computing, and a property-based remote attestation method oriented to cloud computing is designed based on the characteristics of cloud computing. In this method, through the attestation proxy, the remote attestation of the computing platform's security property is realized without disclosing the platform's configuration, and users can validate the security property of the actual computing platform in the virtual cloud computing environment.

4. PROPOSED APPROACH

In our proposed approach we consider the security in the cloud side and also the data of the user is safe. For this we proposed an architecture which is java based. By using this architecture we can provide security to the cloud environment and to the user. Any normal can register their detail in this environment and according to the detail Admin of the cloud provide an userid and password. For the session in the cloud and for data sharing we again request to the admin cloud , if admin provide the session and sharing key then the normal user can perform the operation. User's data is also safe in this environment, if admin want to see the data of the normal user , then they can request the normal user to provide a password , so that admin can see the data of the normal user. Normal user may decline for the above condition also. Admin of the cloud can also block the user if a cloud provider wants to do so.

We present a secure architecture in which we can enter in two ways, first by computing and second by admin task. Through the admin task environment we can enter by entering the appropriate admin password. Admin can create the user, check the time, block or unblock user, check for space and also compute task.

Admin create a user with their userid, pwd and username. Then the normal user can enter in the computing environment by entering the proper user id and password. We now provide the steps for the problem domain of section four.

Secure API and Interfaces:

Analyze the security model of cloud provider interfaces and ensure strong authentication and access controls and all are implemented in concert with encrypted transmission. We can apply this type of security by authentication control for the users of the cloud; they can enter by applying their user id and password which is monitor by the cloud environment. They can demand the cloud environment according to their choice and need.

Now we discuss our algorithm.

Assumption:
Dnc- demand new cloud
Ec- Exiting Cloud
Dsk- Database Session Key

Algorithm

```
1. Select admin\normal user
If(admin)
{
Goto step 3;
}

Else
{
Goto step2;
}

2. [Check the Authentication for normal user]
Enter the userid and password.
If(uid==userid && pwd==password)
{
Enter in the cloud environment
If(dnc)
{
Enter the space
Enter the environment
Enter the cloud type
Enter the name of the cloud
}

Else If(ec)
{
Select cloud1,cloud2….cloudn[Environment]
Add(data)
Delete(data)
Share(data)
}

Else If(dsk)
{
Request(admin)
}

3. Admin (pwd)
{
Request(database);
CreateUser();
Time();
Permission();
Password();
Skey();
Check();
}

Add(data)
{
```

```
FileWriter fstream = new FileWriter("out.txt",true);
BufferedWriter out = new BufferedWriter(fstream);
out.write("string");
}

Delete(data)
{
File f1 = new File(file);
and delete the file using delete function f1.delete();
}

Share(data)
{
File folder = new File("C:\\userfolder");
File[] files = folder.listFiles();
for (int i = 0; i < files.length; i++) {
list.add(i, files[i].toString());
}

Request (database)
{
NUser (permission)

}

CreateUser()
{
[Enter Your UID]
If(Success)
{
Print("Registration Successful");
Print(your password is=);
}
else
[enter Missing Parameters]
}

Time()
{
time = System.currentTimeMillis();
}

Permission()
{
If(block)
Permission is blocked
else if(unblock)
Regain Permission
}

Password()
{
```

```
[This is used for creating password for data sharing]

getKey();
}

Skey()
{
[This is used for a single session]
getKey();
}

Check()
{
File file = new File("C:");
System.out.println("C:");
System.out.println("Total:" + file.getTotalSpace());
System.out.println("Free: " + file.getFreeSpace());
System.out.println("Usable:" + file.getUsableSpace());
}

getKey()
{
Random random = new Random();
        String s1=new String("abcdefghijklmnopqrstvuwxyz");
String s2=new String("ABCDEFGHIJKLMNOPQRSTVUWXYZ");
                String s3=new String("0123456789");
        int r1 = random.nextInt(26);
        String key=new String();
        key=String.valueOf(s1.charAt(r1));
        r1 = random.nextInt(26);
        key=key+String.valueOf(s2.charAt(r1));
        r1 = random.nextInt(10);
        key=key+String.valueOf(s3.charAt(r1));
        r1 = random.nextInt(26);
        key=key+String.valueOf(s2.charAt(r1));
        r1 = random.nextInt(26);
        key=key+String.valueOf(s1.charAt(r1));
        r1 = random.nextInt(10);
        key=key+String.valueOf(s3.charAt(r1));
        System.out.println(key);
        return(key);
}

NUser (permission)
{
[Admin can read the data of the user after getting the security key from the normal user]
getKey ();
}
```

5. RESULT ANALYSIS

According to the survey by Global Industry Analysts & Gartner's, cloud computing is one of the fastest growing markets, the market size is forecast to touch $222.5 billion by 2015.

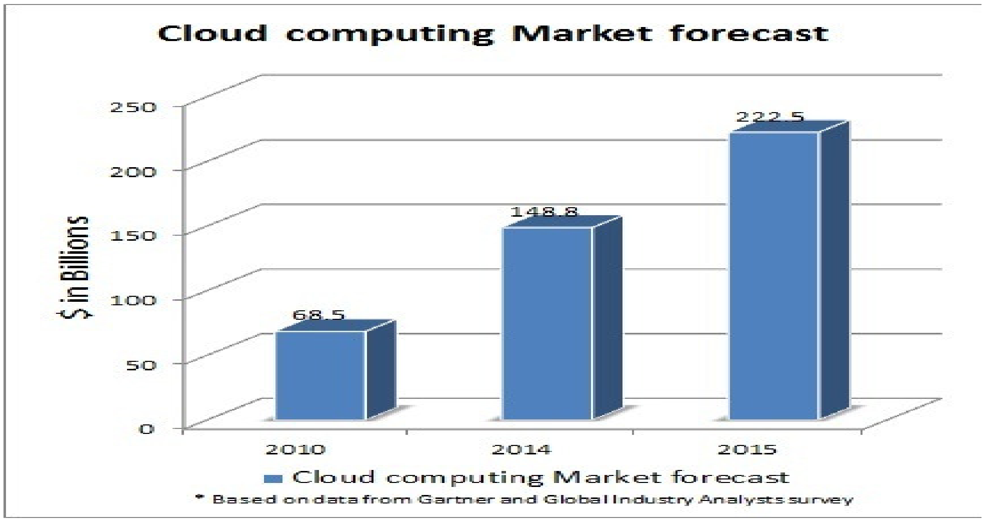

Figure 2: Cloud Computing Market Forecast

Now that we have set the context about how Cloud computing is going to be way of life, let's discuss about what are the issues that may hold back or slow down the progress, what are the issues that are causing worry lines and making the consumers think.

One of the biggest concerns that the consumers around the world have is of security. We present a graph [Figure 3] that is taken from IDC Enterprise panel. In this graph we present the challenges issue of the cloud on demand model. If we analyze then we think about the major concern which is security.

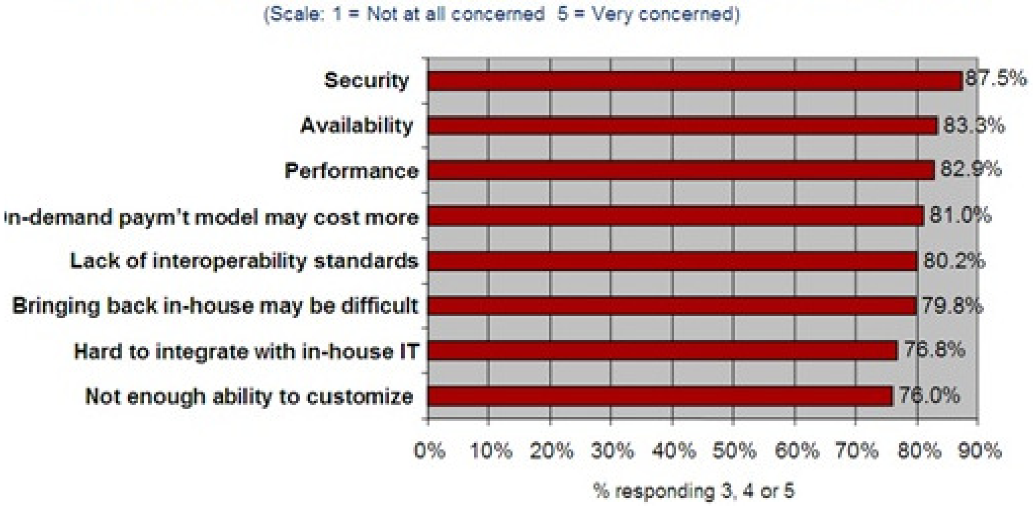

Figure 3: Source IDC Enterprise Panel

When our data, business process, applications are deployed to Cloud, how secure are our data, business process & applications going to be. This is one of the top most questions by the customers. What are security solutions that are provided by cloud service provider, what are the security solutions that can be built into products, Business applications, and Enterprise applications by different IT vendors?

We were really pleased to see such a positive reaction from local businesses about the buzz of cloud computing. As IT professionals, we are always on the lookout for innovative processes that can help other businesses in our area. We have a strong vision for the future of cloud computing especially as as industry research has shown that it is being adopted five times faster than traditional IT. We want to be able to bring SMEs in Coventry forward in terms of this technological revolution.

- 100% of feedback respondents at the workshop had faith in the security of a cloud system following our presentation.
- The following chart shows the respondents opinion on cloud's main benefits:

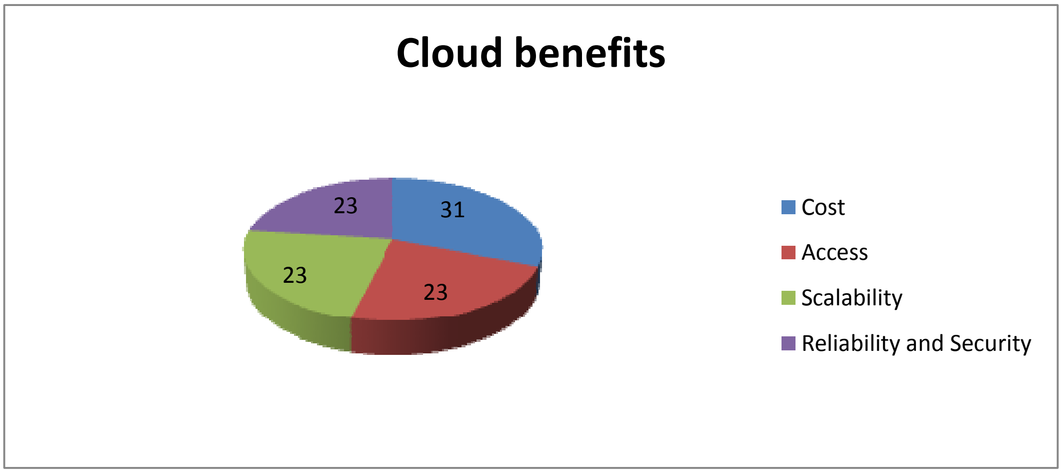

Figure 4: Cloud Benefits

In our approach we show the cloud security which is in four phase's session Key, Sharing key, Block user and User Data Key. By which the security is increases.

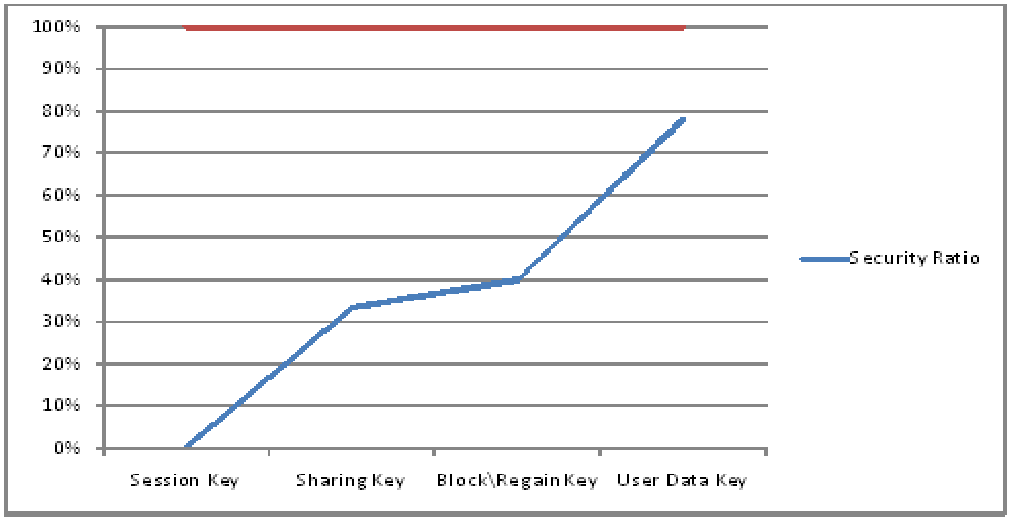

Figure 5: Cloud Security in Four phases

In terms of Operation in our application the security is increases according to the operation. When the operation is less, security is also less. But if the operation is increases security are also increases.

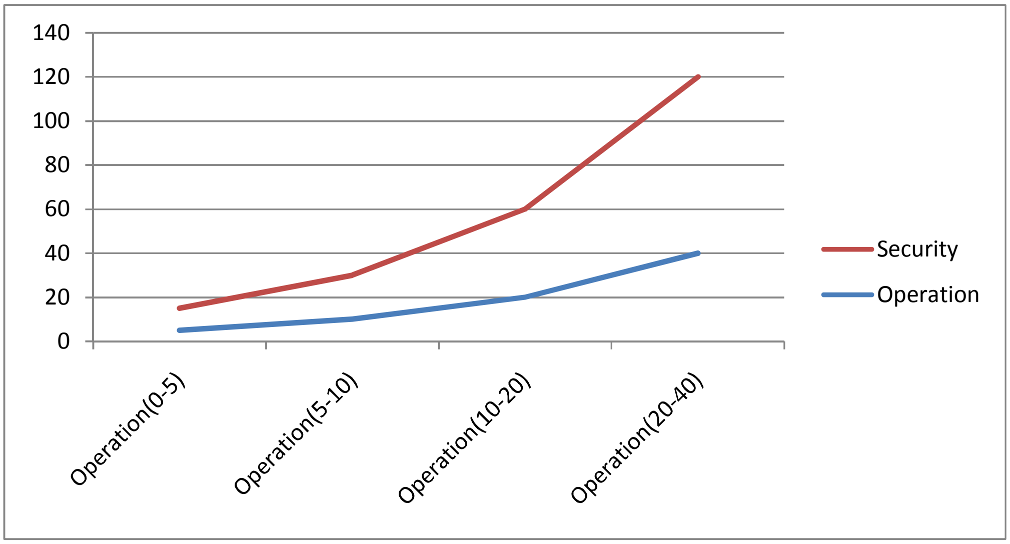

Figure 6: Operation in Cloud security

Area distribution graph is shown in figure 7.

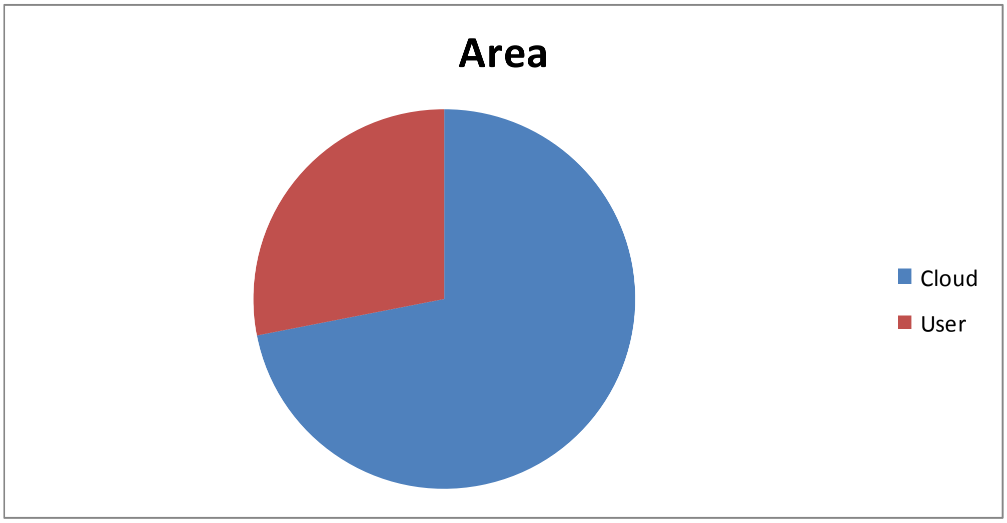

Figure 7: Area Distribution

In terms of security comparison in the old and our new approach we are in higher position, because of the user data security and the session key security which is not available as per my knowledge in the today's cloud environment.

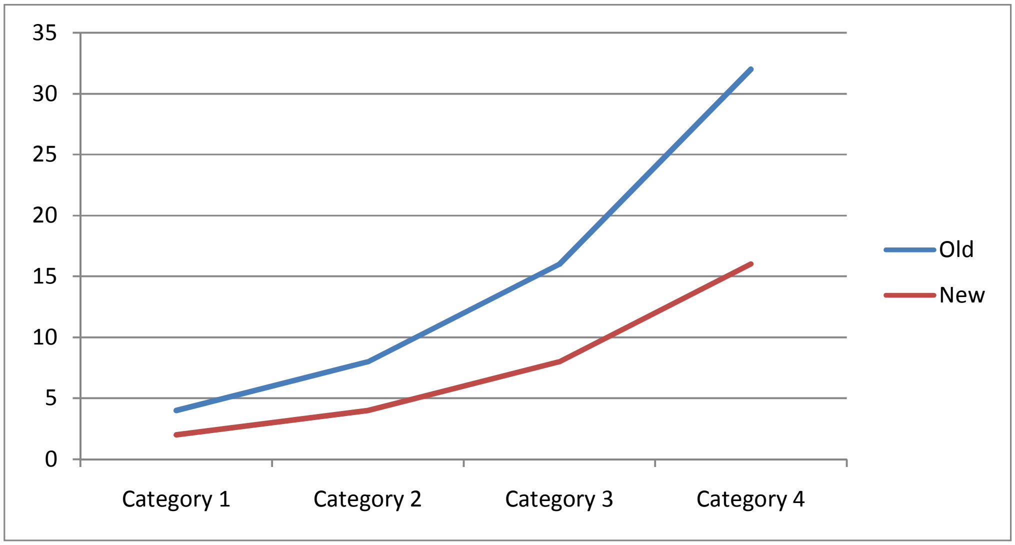

Figure 8: Old vs. New (In terms of Security)

6. CONCLUSION

In this paper we proposed a novel approach to provide sharing in the cloud environment with two way secure user cloud security. We present a secure architecture in which we can enter in two ways, first by computing and second by admin task. Through the admin task environment we can enter by entering the appropriate admin password. Admin can create the user, check the time, block or unblock user, check for space and also compute task. We also present a comparative study in different scale so that we prove that our method is good in comparison to the previous security concerns.

REFERENCES

[1] Wikipedia - Cloud Computing. [Online]. http://en.wikipedia.org/wiki/Cloud_computing

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 598-609, 2007.

[3] A. Juels and B.S. Kaliski Jr., “Pors: Proofs of Retrievability for Large Files,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 584-597, 2007.

[4] H. Shacham and B. Waters, “Compact Proofs of Retrievability,” Proc. 14th Int’l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT ’08), pp. 90-107, 2008.

[5] K.D. Bowers, A. Juels, and A. Oprea, “Proofs of Retrievability: Theory and Implementation,” Report 2008/175, Cryptology ePrint Archive, 2008.

[6] M. Naor and G.N. Rothblum, “The Complexity of Online Memory Checking,” Proc. 46th Ann. IEEE Symp. Foundations of Computer Science (FOCS ’05), pp. 573-584, 2005.

[7] Wei-Tek Tsai, Xin Sun, Janaka Balasooriya , “Service-Oriented Cloud Computing Architecture” , 2010 Seventh International Conference on Information Technology.

[8] Zhidong Shen, Li Li , Fei Yan, Xiaoping Wu , “Cloud Computing System Based on Trusted Computing Platform”, 2010 International Conference on Intelligent Computation Technology and Automation.

[9] Zhidong Shen , Qiang Tong , “The Security of Cloud Computing System enabled by Trusted Computing Technology” , 2010 2nd International Conference on Signal Processing Systems (ICSPS).

[10] Mr. Pritesh Jain, Prof. Vaishali Chourey, Prof. Dheeraj Rane,” An Analysis of Cloud Model-Based Security for Computing Secure Cloud Bursting and Aggregation in Real Environment”, International Journal of advanced Computer Research(IJACR) Volume 1, September 2011.

[11] Siyuan Xin, Yong Zhao, Yu Li,“ Property-Based Remote Attestation Oriented to Cloud Computing” , 2011 Seventh International Conference on Computational Intelligence and Security.